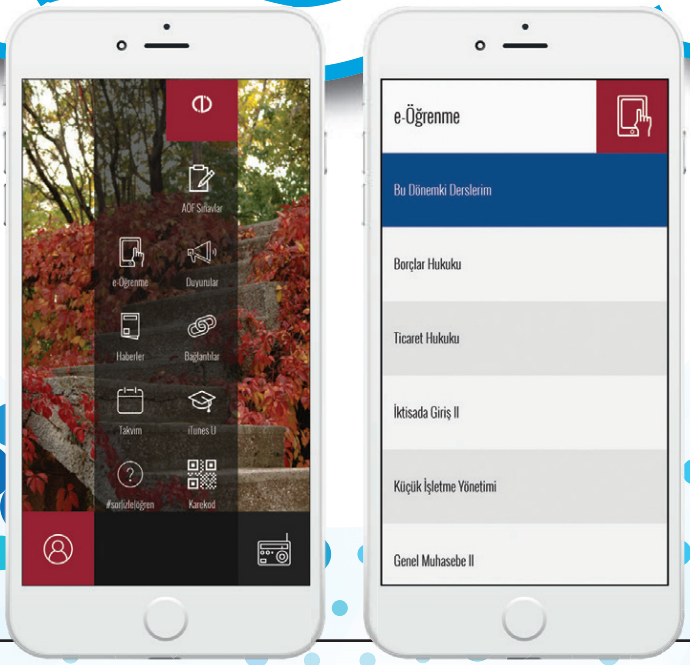
ANADOLU ÜNİVERSİTESİ

ANADOLU mobil



- AÖF sınavları
- sınav giriş belgesi
- sınav sonuçları
- itunes u
- duyurular
- sor/izle/öğren
- ders kitabı
- sesli kitap
- deneme sınavları
- konu anlatım videoları
- TRT okul videoları
- e-seminer dersleri
- takvim

444 10 26
0850 200 46 10-19 (10hat)
www.anadolu.edu.tr

/anadoluuniversitesi /Anadolu_Univ instagram.com/anadoluuniv

ekampus.anadolu.edu.tr

ANADOLU ÜNİVERSİTESİ

T.C. ANADOLU ÜNİVERSİTESİ YAYINI NO: 3446
AÇIKÖĞRETİM FAKÜLTESİ YAYINI NO: 2294

AĞ YÖNETİMİ VE BİLGİ GÜVENLİĞİ

Yazarlar
Öğr.Gör. Emre KAÇMAZ (Ünite 1, 2)
Yrd.Doç.Dr. Bülent TUĞRUL (Ünite 3, 4, 5, 6)
Yrd.Doç.Dr. Emin GERMEN (Ünite 7)
Yrd.Doç.Dr. İsmail SAN (Ünite 8)

Editör
Yrd.Doç.Dr. Alper BİLGE

UZAKTAN ÖĞRETİM TASARIM BİRİMİ

Genel Koordinatör
Prof.Dr. Müjgan Yazıcı

Genel Koordinatör Yardımcısı
Doç.Dr. İrem Erdem Aydın

Öğretim Tasarımcısı
Öğr.Gör. Orkun Şen

Grafik Tasarım Yönetmenleri
Prof. Tevfik Fikret Uçar
Yrd.Doç. Nilgün Salur
Öğr.Gör. Cemalettin Yıldız

Dil ve Yazım Danışmanı
Okt. Sebahat Yaşar

Ölçme Değerlendirme Sorumlusu
Öğr.Gör. E. Emre Özkeskin

Kitap Yazım Basım ve Dağıtım Koordinatörü
Uzm. Nermin Özgür

Kapak Düzeni
Doç.Dr. Halit Turgay Ünalan

Grafikerler
Ayşegül Dibek
Gülşah Karabulut
Hilal Küçükdağaşan
Ufuk Önce

Dizgi
Açıköğretim Fakültesi Dizgi Ekibi

Ağ Yönetimi ve Bilgi Güvenliği

ISBN
978-975-06-2065-2

1. Baskı

Bu kitap ANADOLU ÜNİVERSİTESİ Basımevinde 15.000 adet basılmıştır.
ESKİŞEHİR, Aralık 2016

İçindekiler

Önsöz

Sevgili öğrenciler,

Bilgisayar ağları kavramı, uzak mesafelerdeki iletişim cihazlarını birbirine bağlayarak veri aktarımını mümkün kılmakla birlikte bilgi ve sistem kaynaklarının da paylaşılmasını sağlayarak, günümüz iletişim sistemlerinin en temel bileşenlerinden birini oluşturmaktadır. Bilindiği gibi en büyük bilgisayar ağı, İnternet'tir. İletişim kabiliyetlerinin artması ve İnternet teknolojisiyle birlikte günümüzde bilgi, tarihte hiç olmadığı kadar kullanılabilir ve erişilebilir durumdadır. Bu kitapta, bilgisayarlar arası ağların nasıl kurulduğu hakkında detaylı bilgiye sahip olacaksınız. Bu denli önemli bir kavram olan bilgisayar ağlarının nasıl ortaya çıktığı, hangi aşamalardan geçerek geliştiği ve ne tür hizmetler sunduğu hakkında fikir sahibi olacaksınız.

Ağların yaygınlaşmasıyla erişilebilirliği artan ve kolaylıkla paylaşılabilen bilginin güvenliği, bilgisayar ağları kapsamında detaylı olarak incelenmesi gereken bir konudur. Ağ teknolojilerinin gelişmesiyle, ağ üzerinde taşınan bilginin gizliliği, bütünlüğü ve kullanılabilirliği ile ilgilenen kendi başına bir bilim dalı bulunmaktadır. Kriptoloji adı verilen bu bilim dalı bilginin izinsiz erişimini, kullanımını, yayılımını, değiştirilmesini, bozulmasını ve yok edilmesini engellemek üzere çalışır. Bu kitap ile temel kriptografik yöntemler kullanarak bilgi şifreleme ve şifre çözme işlemlerinin matematiksel yöntemler kullanılarak nasıl gerçekleştirildiği hakkında geniş bilgiye sahip olacaksınız. Ayrıca Bilgi Güvenliği kavramı ile bu alandaki uluslararası standartlar konusunda farkındalık kazanacaksınız.

Ağ kavramı ve yönetimi ile bilgi güvenliği konularının ayrıntılı biçimde harmanlandığı bu kitabın sizler için bir başvuru kaynağı olması hedeflenmiştir. Bilişim sistemleri temelleri açısından oldukça önemli olan bu konuların tek bir kaynak ile sunulduğu bu kitabın hazırlanmasında emeği geçen, başta yazarlar olmak üzere tüm çalışma arkadaşlarıma teşekkürü bir borç bilirim.

Başta değerli Yönetim Bilişim Sistemleri öğrencileri olmak üzere bu kitaptan faydalanacak herkese sağlık, mutluluk ve başarılar dilerim.

Editör
Yrd.Doç.Dr. Alper BİLGE

1

Amaçlarımız

Bu üniteyi tamamladıktan sonra;

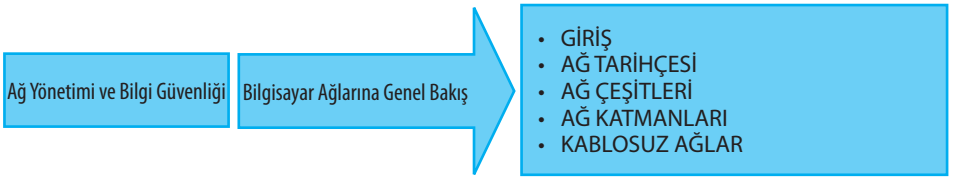
- Ağ kavramını tanımlayabilecek,
- Ağ tarihçesi ve gelişimini açıklayabilecek,
- Ağ çeşitlerini açıklayabilecek,
- Ağ katmanlarını tanımlayabilecek,
- Kablosuz ağları açıklayabilecek

bilgi ve becerilere sahip olacaksınız.

Anahtar Kavramlar

- Bilgisayar Ağları
- Ağ Tarihçesi
- Ağ Çeşitleri
- Ağ Topolojileri
- Ağ Katmanları
- Uygulama Katmanı
- Taşıma Katmanı
- Ağ Katmanı
- Veri Bağ Katmanı
- Fiziksel Katman
- Kablosuz Ağlar

İçindekiler



Bilgisayar Ağlarına Genel Bakış

GİRİŞ

En az iki istemcinin birbirine bağlanması ile oluşturulan bilgisayar ağları, temelde iki ana amaca ulaşmak üzere gerçeklenir. Bu amaçlardan ilki, istemciler arasında bilgi paylaşımı yapabilmektir. Başka bir deyişle, bir istemcide depolanan bilginin diğer bir istemciye, herhangi bir fiziksel kayıt ortamı (Floppy disk, CD, DVD, taşınabilir sabit sürücü, flash bellek vb.) kullanılmaksızın aktarımını sağlamaktır. İkinci amaç ise istemcilere bağlı donanımların ağa bağlı olan diğer istemcilerle ortak kullanımını sağlamaktır. Eğer ağ yapısı oluşturulmamış olsa bir bilgisayara bağlı bulunan yazıcının diğer bilgisayarlar tarafından da kullanılabilmesi için öncelikle verinin yukarıda sayılan fiziksel kayıt ortamlarından biriyle yazıcının bağlı bulunduğu bilgisayara taşınması gerekir; daha sonra da o yazıcının bağlı bulunduğu bilgisayar aracılığıyla yazdırma işlemi gerçekleştirilmek zorunda kalınırdı. Ağ yapısının kurulmasıyla ağa bağlı olan istemcilerin arasında yazıcı donanımı ortak olarak kullanılabileceği gibi, yazdırılacak veri de yine ağ üzerinden aktarılabilir. İşte temelde bu iki amacı gerçekleştirmek üzere tasarlanan ve belirli bir bölgedeki bilgisayarları birbirine bağlayarak onları istemciler haline getiren yapılara bilgisayar ağları denir. Bilgisayarların yaygınlaşması ile ağ kavramı önem kazanmıştır. Özellikle 1980'li yıllarda Ethernet bağlantı teknolojisinin gelişmesi ile ağ ortamı kullanımı ev ve ofis gibi mekânlarda hızla yaygınlaşmıştır. İlk olarak küçük bir alan içerisinde bulunan en az iki istemci bağlantısı ile oluşturulan bilgisayar ağı kavramı, günümüzün vazgeçilmez teknolojilerinden olan İnternet ağının da temelini atmıştır.

AĞ TARİHÇESİ

Bilgisayar ağlarının oluşumu ve tarihçesi incelendiğinde, bugün bildiğimiz şekliyle tasarlanan ilk ağ oluşumu, ABD Savunma Bakanlığı bünyesinde geliştirilen paket dağıtım ağı ARPANET (Advanced Research Projects Agency Network – Gelişmiş Araştırma Projeleri Dairesi Ağı)'tir. ARPANET, yeni adıyla DARPA (The Defense Advanced Research Projects Agency – İleri Savunma Araştırma Projeleri Dairesi), soğuk savaş sırasında, askeri ve stratejik öneme sahip olan bilgilerin birçok istemci arasında paylaşılabilmesini sağlamak amacıyla geliştirilmiştir. Daha önce, tıpkı telefon görüşmeleri gibi, iki istemcinin belirli bir süre boyunca yalnızca birbirleriyle haberleşebilmelerine olanak tanıyan, ancak ilgili süre boyunca başka bir istemciyle haberleşmesini engelleyen devre anahtarlama yöntemi kullanılıyordu. ARPANET, veri iletişiminde günümüzde de kullanılan paket anahtarlama yönteminin ilk örneği olması dolayısıyla, bugün kullanılmakta olan İnternet ağının da öncülü ve atasıdır. ARPANET üzerinden ilk paket anahtarlama tabanlı ağ bağlantısı Los Angeles, ABD'de bulunan UCLA Üniversitesi'nden (University of California, Los Angeles), San Francisco, ABD'de bulunan Stanford Üniversitesi'ne gerçekleştirilmiştir. 1969

yılına gelindiğinde günümüz İnternet ağının da temeli atılmıştır. Başlangıçta yalnızca dört üniversiteyi birbirine bağlayan ağ, zaman içerisinde farklı kurumların katılımı ile genişlemiştir. Ray Tomlinson tarafından geliştirilen elektronik posta uygulamaları da 1972 yılında ARPANET'e dâhil edilmiştir ve "@ (at)" işaretinin kullanıcı adlarını ve alan adreslerini birleştirmek üzere ilk kullanımı da aynı yıllarda olmuştur. Zaman içerisinde geliştirilen Telnet protokolü ile uzak istemcilere bağlantı ve FTP (File Transfer Protocol-Dosya Transfer Protokolü) ile de dosya transferi, ağ ortamında gerçeklenebilir hale gelmiştir.

Protokoller, bilgisayarlar arası haberleşmede mesaj biçimi, sırası, gönderim ve alım esnasında yapılması gerekenleri tanımlamaktadır.

1970'li yıllarda belirlenen **protokoller** ile TCP/IP mimarisi de ortaya çıkmıştır. TCP/IP mimarisini daha iyi anlamak için önce protokol kavramı ele alınmalıdır. Protokol, bilgisayar ağları kullanılarak yapılacak olan veri transferi için düzeni sağlayacak kurallar dizesini ifade etmektedir. Gerçek hayata dair bir örnek vermek, kavramın anlaşılmasını kolaylaştıracaktır. Bir ders esnasındaki sınıf örneğini ele alalım: Ders anlatılırken sessiz olmak ve dinlemek, sorulacak bir soru ya da söylenecek bir söz olduğunda el kaldırarak söz istemek, derse zamanında gelmek ve ders bitmeden sınıfı terk etmemek, sınıfta ders işlenirken dışarıdan dâhil olmak için kapıyı çalarak izin istemek vb. gibi kurallar dizini, ders protokolünü oluşturur. Bu protokol, sınıf düzenini ve dersin sağlıklı bir biçimde işlenebilmesini sağlamak adına yapılmaktadır. İşte, bilgisayar ağları tarafından kullanılan protokoller de hatasız veri aktarımını sağlamak amacıyla bu tür kurallar barındırmaktadır. Bu amaçla oluşturulan katmanlı yapı ve katmanlar üzerinde oluşturulan çeşitli protokoller, ünitenin ve kitabın ilerleyen kısımlarında detaylı olarak incelenecektir.

1972 yılında XEROX firması tarafından geliştirilmeye başlanan Ethernet protokolü ve bu protokolü uygulayan bütünleşik devre kartları, 1975 yılında piyasaya sürülmüştür. Bu kartın ilk sürümü, 1 km. uzunluğunda kablo ile 100'den fazla bilgisayarı birbirine yaklaşık 3 Mbps (saniyede 3 megabit) hızında bağlamayı amaçlamıştır. Daha sonra 10 Mbps ve giderek artan hızlarda ağ bağlantısı desteklenmiştir.

Müstakil bir kablo aracılıyla ağ bağlantısı her ne kadar hızlı iletişimi desteklese de maliyeti yüksek bir teknolojidir. Bu nedenle, daha önceden kurulmuş ortak bir ağ altyapısına katılarak ağ bağlantısı kurma çalışmaları da hız kazanmıştır. 1986 yılında Amerika Birleşik Devletleri Ulusal Bilim Vakfı, ülke çapında 56 Kbps hızında ortak bir ağ altyapısı üzerinden İnternet ağı kullanımına başlamıştır. Ülkemizde de uzun süre benzeri bir omurga ağ altyapısı ile 56 Kbps hızında veri akışı sağlanmaktaydı. Günümüz hızlarıyla karşılaştırıldığında oldukça yavaş olduğu gözlenen ağ bağlantı hızı, veri taşımada telefon hatları altyapısının kullanılmasından kaynaklanıyordu. Bilindiği üzere telefon şebekeleri (PSTN – Public Switched Telephone Network – Genel Aktarmalı Telefon Şebekesi) analog veri olan ses sinyallerini taşımaya yönelik olarak tasarlanmıştır. Bilgisayarların çalışma mantığı düşünüldüğünde, elektrik ve elektronik devreleri kullanan makineler, sayısal '1'ler ve '0'lar ile çalışmaktadır. En basit anlatımı ile devrenin belirli bir anda elektrik yüklü olma durumu '1', yüksüz olma durumu ise '0' ile gösterilebilir. Bu '1' ve '0'lardan her birine BİT (BİnaryigiT – İkili Sayı) adı verilmektedir. İki istemci arasında gerçekleştirilen basit ağ yapısında bile, '1'ler ve '0'lardan oluşan sayısal verinin, sadece analog ses verisini iletme kapasitesine sahip bir yapı üzerinden taşınması gerekmektedir. Bu nedenle sayısal veri telefon şebekesi üzerinde, ses sinyallerine dönüştürülerek aktarılmaktadır. Çevirmeli bağdaştırıcı olarak da adlandırılan 56 Kbps hızındaki modem cihazları ile gönderici bilgisayarda sayısal veri ses sinyallerine dönüştürülmüş, alıcı bilgisayarda ise tersine bir işlem yapılarak yine modem cihazı yardımıyla ses sinyalleri, sayısal verilere dönüştürülmüştür. Bu sayede, telefon şebekesi üzerinden iki bilgisayar arasında veri transferi gerçekleştirilmiştir. Geçmişte ülkemizde de kullanılan bu teknolojinin hız yetersizliğinin yanı sıra bir diğer zararı da bağlantı esnasında telefon görüşmesi yapılamaması ve maliyetinin yüksek olmasıdır. Ayrıca bağlantı esnasında telefon, dışarıdan gelen aramalara karşı meşgul sinyali vermektedir. Günümüzde

kullanılan ADSL (Asymmetric Digital Subscriber Line-Asimetrik Sayısal Abone Hattı) teknolojisi ile Frekansı Bölerek Çoklama (FDM - Frequency Division Multiplexing) yapılarak, telefon bağlantısı için kullanılan bakır kablo üzerinde ses ve veri aktarımı farklı frekanslar üzerinden gerçekleştirilmektedir. Böylece hem bağlantı hızı artmış hem de bağlantı esnasında telefon hattının meşgul olması durumu sona ermiştir.

Bu gelişmelerle birlikte, 1989 yılında WWW (World Wide Web – Dünya Çapında Ağ) kavramı ortaya atılmıştır. WWW, hiper metinlere dayanan bir protokoldür. Bu hiper metinlerin her birine web sayfası denilmektedir. Günümüzde yaygın biçimde kullanılan WWW kavramı, özellikle son yıllarda ağ ortamının yayılması ile daha da önem kazanmıştır. Daha önce de bahsedildiği gibi, dünyanın en büyük bilgisayar ağı İnternet'tir. Özellikle son yıllarda ağ bağlantı hızlarının artması, kablosuz bağlantının birçok alanda hayatımıza dâhil olmasıyla internet ortamına bağlı olmayan bilgisayar neredeyse kalmamıştır. Mobil cihazlardaki gelişim ve akıllı cihazların kullanımı da internet teknolojisinin yayılmasında ve genişlemesinde önemli rol oynamıştır.

AĞ ÇEŞİTLERİ

Tarihçesi kısaca anlatılan bilgisayar ağları, anlaşıldığı üzere zaman içerisinde hızla gelişmiştir. İlk bilgisayar ağının sadece iki bilgisayarı birbirine bağladığı düşünüldüğünde, günümüzde kullanılan ve dünya üzerindeki neredeyse tüm bilgisayarların bağlı bulunduğu **internet** ağı teknolojisi inanılmaz boyutlardadır. Ağlar, oluşumunu sağlayan birbirine bağlı bulunan bilgisayarların sayılarına yani büyüklüklerine, bu bilgisayarların yerleşim şekillerine yani topolojilerine ve birbirlerine ve ağ kaynağına bağlantı şekillerine göre çeşitlilik göstermektedir. İlk önce büyüklüklerine göre ağ çeşitleri incelenecektir. Daha sonra, sırasıyla topolojilerine ve bağlantı ortamlarına göre ağ çeşitlerinden bahsedilecektir.

İnternet, dünyanın en büyük geniş alan ağıdır.

Büyüklüklerine Göre Ağlar

Ağ ortamına dâhil olan bilgisayar sayısı, ağın büyüklüğünü belirler. Büyüklüklerine göre ağlar, aşağıda açıklanan yedi farklı kategoride incelenebilir:

PAN (Personal Area Network – Kişisel Alan Ağları): Son yıllarda özellikle akıllı cihazların yaygınlaşmasıyla hayatımıza giren bir ağ çeşididir. Kişiye yakın cihazların (akıllı telefon, tablet, kişisel dijital asistan vb.) oluşturduğu ağları temsil etmektedir. Genellikle veri aktarımı USB, Firewire gibi veri yolları ile sağlanır. Kablosuz ağ teknolojisini kullanan çeşitlerinde ise bağlantı, IrDA ve Bluetooth gibi ağ teknolojileri ile sağlanmaktadır.

LAN (Local Area Network – Yerel Alan Ağı): Ağ kavramının iki bilgisayarın birbirine bağlanması ile oluşturulduğunu yeniden hatırlatacak olursak, yerel alan ağları, oluşturulan ilk ağ çeşididir. Günümüzde birbirine çok yakın coğrafi konumda bulunan bilgisayarlar tarafından oluşturulan bilgisayar ağı çeşididir. Ev, okul, laboratuvar, iş binaları vb. sınırlı alanları kapsamaktadır. Geniş bir coğrafi mekânı kapsamadığı için hız olarak da en verimli çeşittir. Kablolu ve kablosuz ağ ortamlarını kullanabilmektedir.

MAN (Metropolitan Area Network – Şehirsel Alan Ağı): Bir şehir ya da bir yerleşkede oluşturulan alan ağıdır. Genellikle Yerel Alan Ağlarının birkaçının birbirine bağlanması ile oluşturulur. Yerel Alan Ağlarını birbirine bağlamak için fiber optik gibi kablolu ya da Wimax gibi kablosuz ortamlar kullanılır. Ağlar arasında geçişi düzenlemek için yönlendirici (router) adı verilen cihazlardan faydalanılır.

WAN (Wide Area Network – Geniş Alan Ağı): Yerel Alan Ağlarının ya da Şehirsel Alan Ağlarının birleşmesiyle oluşturulan en geniş alan ağıdır. Dünyadaki en geniş alan ağının adı İnternet'tir. İnternet tüm dünyada bulunan bilgisayarların ve bilgisayar mantığına sahip çalışan cihazların bağlanmasıyla oluşmaktadır. Dünya üzerinde verilerin doğru alıcılara ulaştırılması işlemi yönlendiricilerin sorumluluğundadır.

VPN (Virtual Private Network – Sanal Özel Ağ): Sanal olarak uzaktaki bir cihazın ağın içerisine dâhil olmasını sağlayan özel bir ağ türüdür. Uzak makine, Sanal Özel Ağ sayesinde fiziksel olarak uzaktaki bir ağa dâhilmiş gibi davranmakta ve o ağ ile veri alış verişinde bulunmaktadır. Örnek vermek gerekirse, ticari paket program kullanan bir firmanın uzaktaki deposunun bilgisayarı, Sanal Özel Ağ sayesinde firma merkezinde kurulu bulunan ağa ve sunucu makineye bağlanmakta, irsaliye, fatura işlemlerini gerçekleştirmekte, stok kayıtlarını ve cari hesapları güncellemektedir.

Bahsedilen ağlar, büyüklüklerine göre çeşitlendirilmiş ağlardır. Bu çeşitlerden farklı olarak üniversite yerleşkelerini birbirine bağlamayı sağlayan CAN (Campus Area Network – Kampüs Alan Ağı) ve depolama işlemlerini kolaylaştırmak amacıyla depolama sunucularına bağlantıyı sağlayan SAN (Storage Area Network – Depolama Alan Ağı) gibi ağ çeşitleri de bulunmaktadır.

SIRA SİZDE 1

Bahsedilenler dışında, büyüklüklerine göre başka ağ çeşitleri olup olmadığını araştırınız.

İNTERNET

Farklı ağ çeşitleri için https://goo.gl/RJNb2X internet adresinden bilgi alabilirsiniz.

Topolojilerine Göre Ağlar

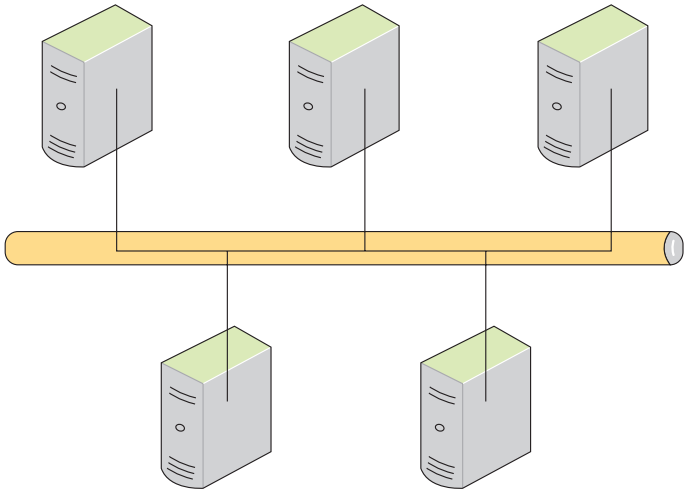
Ağ çeşitlerinden bahsedilirken incelenmesi gereken ikinci kavram, ağ topolojisidir. Ağ topolojisi, bilgisayar ve aracı cihazların yardımıyla oluşturulan bilgi ağında, yine bilgisayar ve yardımcı cihazların yerleşimi ve birbirleriyle olan bağlantılarının yapısı anlamına gelir. İlerleyen kısımlarda kısaca bahsedileceği üzere, yerleşim şekillerine göre Ortak Yol (BUS), Halka (Ring), Örgü (Mesh), Ağaç (Tree) ve Yıldız (Star) gibi çeşitli ağ topolojileri bulunmaktadır.

Ortak Yol (BUS) Topolojisi: Resim 1.1'de görüldüğü gibi kurulumu ve genişletilmesi en basit topoloji türüdür. Tek bir kablo üzerinde ve genellikle BNC adaptöre sahip Ethernet kartlarının birbirine bağlanması ile oluşturulan ağ türüdür. Bir merkez birimine ihtiyaç duymadan ağın kurulumu sağlanır. Tek bir kablo üzerinde işlem yapılacağından hız düşüktür. Ağa bağlı tüm bilgisayarlar aynı kabloyu ortak kullandığı için kaynaktaki toplam veri taşıma kapasitesi bilgisayar sayısına bölünecektir. Çalışması için kablonun sonlandırılması gereklidir. Günümüzde çok da popüler olmayan bu topoloji türü, sınırlı sayıda bilgisayar ve sınırlı mesafeler için kullanılmaktadır.

Resim 1.1

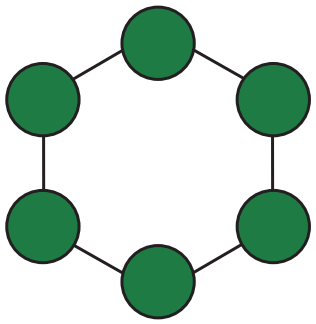
Ortak Yol (BUS) Topolojisi.

Kaynak: *https://goo.gl/dX88E4*



Halka (Ring) Topolojisi: Resim 1.2'de şematik halde görülen halka topolojisi bir anlamda ortak yol topolojisinin iki ucunun bir araya getirilmesi ile oluşturulan bir topoloji türüdür. İlk olarak IBM firması tarafından geliştirilmiştir. Her bir bilgisayar kendine ait zamanda veri iletimi yapar ve böylece karışıklık önlenmiş olur. Daha geniş ağlarda Andıçlı Halka (Token Ring) kullanılabilmektedir. Bu tür topolojide elinde andıcı bulunduran bilgisayar veri gönderme işlemini yapar. Andıç, genellikle saat yönünün tersine olmak üzere belirli zaman aralıkları ile tüm bilgisayarları gezer. Hatalı bir iş istasyonunun sistemde bulunması tüm sistemin aksamasına sebep olabilir.

Resim 1.2



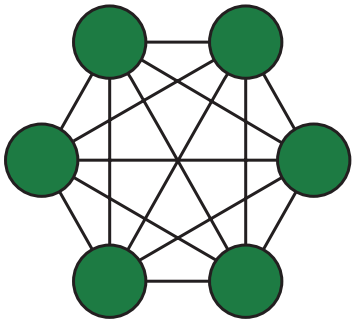
Halka (Ring) Topolojisi.

Kaynak: *https://goo.gl/SypcT0*

Örgü (Mesh) Topolojisi: Bu topolojide her bir düğüm, bir diğerinin yerini alabilmektedir. Verilerin düğümden düğüme yayılarak ya da yönlendirme ile çalıştığı topoloji türüdür. Resim 1.3'te tamamen bağlı bir örgü topolojisi görülmektedir. Örgü şeklinde yapılan bağlantılar sayesinde hatalı düğümler veri akışında soruna yol açmamaktadır. Örgü topolojisinin bir benzer kullanım şekli de MANET (Mobile Ad Hoc Network – Mobil Özel Amaçlı Ağlar)'tir. MANET ağlarda düğümler birbirine örgü şeklinde bağlanmış olsa da hareketlilikten dolayı farklı sorunlara çözümler bulunması da gerekmektedir. Resim 1.4'te görüldüğü gibi bu hareketlilik tamamen bağlı örgü topolojisi yerine kısmen bağlantılı örgü topolojisi ile sağlanmaktadır.

Resim 1.3

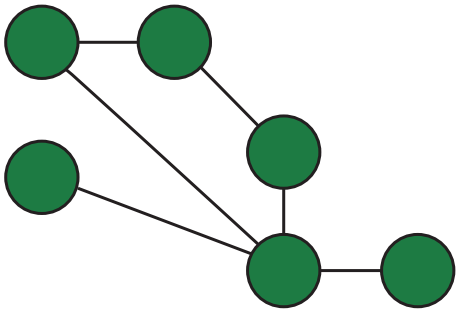
Tamamen Bağlı Örgü (Mesh) Topolojisi.



Kaynak: *https://goo.gl/jk8b3j*

Resim 1.4

Kısmen Bağlı Örgü (Mesh) Topolojisi.

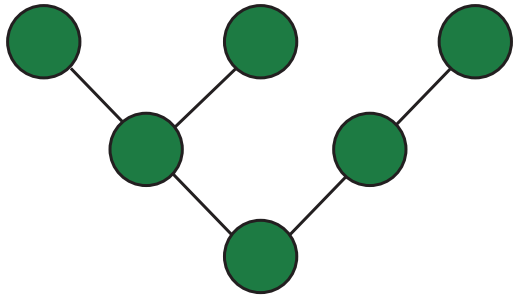


Kaynak: *https://goo.gl/jk8b3j*

Ağaç Topoloji: Ağaç topolojisinde bir merkez düğümü, alt seviyede bir veya daha fazla düğüm ile bağlıdır. Ağaç yapısı simetriktir. Bir ağın ağaç topolojisinde olması için en az üç seviye bulunmalıdır. Ağaç topolojisinin şematik gösterimi Resim 1.5'te verildiği gibidir.

Yıldız (Star) topolojisi: Özellikle günümüz yerel alan ağlarında en fazla karşımıza çıkan topoloji olan yıldız topolojisi, bir merkez dağıtıcı cihaz ve ona direkt bağlı

Resim 1.5



Üç Seviyeli Bir Ağaç Topolojisi.

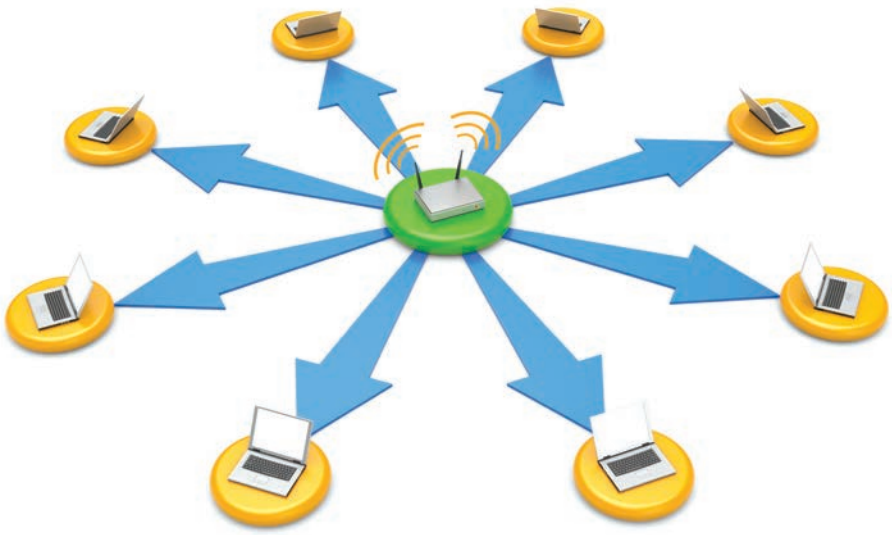
Kaynak: *https://goo.gl/DXgLdL*

düğümlerden oluşmaktadır. Yıldız topolojisinde merkez dağıtıcı cihaz olarak genellikle bir Anahtarlama Cihazı (Switch) kullanılmaktadır. Kablosuz kullanım durumunda ise dağıtıcı cihaz yerini Erişim Noktası (Access Point) cihazına bırakmaktadır. Dağıtıcı cihazdan her bir düğüme, yani bilgisayara, ayrı ayrı kablolama gerektirdiği için maliyeti daha yüksektir. Ancak her bir bilgisayara ayrı kablo gitmesi hızı arttırmakta ve anahtar cihaza bağlı farklı bilgisayar çiftlerinin birbirlerini rahatsız etmeden aynı anda veri iletişimi yapmalarına olanak sağlamaktadır. Kablosuz iletişimde de yıldız topolojisinden faydalanılmaktadır. Resim 1.6'da anahtar cihaz ile bağlanmış farklı düğüm cihazları görülmektedir.

Resim 1.6

Yıldız (Star) Topolojisi.

Kaynak: *115454768*



DİKKAT

Bir ağ altyapısı tasarlarken dikkat edilmesi gereken ilk konu, büyüklüğüne göre ağ yapısı oluştururken, ağ topolojisine karar vermektir.

Bağlantı Ortamlarına Göre Ağlar

Büyüklüklerine göre ve cihazların birbirine göre yerleşim yerleri dikkate alınarak belirlenen ağ çeşitlerinden yukarıda bahsedilmiştir. Ağ çeşitlerinin sonuncusu, ağı oluşturan düğümlerin birbirleri ile olan haberleşme ortamlarına göre ağları çeşitlendirmektir. Birçok farklı bağlantı ortamı bulunmasına karşın, bu bölümde en sık kullanılan teknolojiler olan ATM, FDDI, Token Ring (Andıçlı Halka) ve Ethernet bağlantı ortamlarından bahsedilecektir.

ATM (Asynchronous Transfer Mode – Eşzamansız Aktarım Modu): Verilerin sabit büyüklükte hücreler halinde aktarılmasını sağlayan bir veri aktarım modelidir. Hücreler halinde veri aktarımı paket anahtarlama tekniğine uygundur. Fakat aynı zamanda bu modelde sanal devreler oluşturularak devre anahtarlama modelinden de faydalanılır. ATM ile küçük paketler, donanım desteği ile 10 Gbps gibi yüksek hızlarda alıcı düğümlere iletilir.

FDDI (Fiber Distributed Data Interface – Fiber Dağıtılmış Veri Arayüzü): Fiber optik kablolar ile kullanılmak üzere geliştirilmiş yüksek hızlı bir bilgisayar ağı çeşididir. Ethernetin yeterli hıza ulaşamadığı geçmiş zamanlarda yüksek hızlı veri aktarımı için kullanılmıştır. Ethernet teknolojisindeki hızlanma sayesinde popülerliğini yitirmiştir.

Token Ring (Andıçlı Halka): Andıç adı verilen ve 3 bayttan oluşan bir veri paketinin düğümleri dolaşmasını esas alan bağlantı ortamıdır. Tahmin edilebileceği gibi halka topolojisi ile birlikte kullanılır. Andıca sahip düğüm veri gönderme hakkına sahiptir. Andıç, halkanın tümünü dolaşarak tüm düğümlerin sırasıyla veri göndermesi sağlanmaktadır.

Ethernet: Günümüzde en yaygın kullanılan bağlantı ortamıdır. Genellikle yerel alan ağlarında kullanılmaktadır. İlk olarak XEROX firması tarafından geliştirilen Ethernet, zaman içerisinde standartlaşarak günümüze kadar gelmiştir. Temeli, bir kablo vasıtasıyla bilgisayarların birbirine bağlanması ve veri alış verişine imkân sağlanması mantığına dayanmaktadır. Farklı hızlarda ve kablo türlerinde kullanım desteği de yaygınlaşmasında önemli rol oynamıştır. Ünitenin bundan sonraki kısmında anlatılacak olan katman yapıları, Ethernet teknolojisine dayanarak anlatılmıştır.

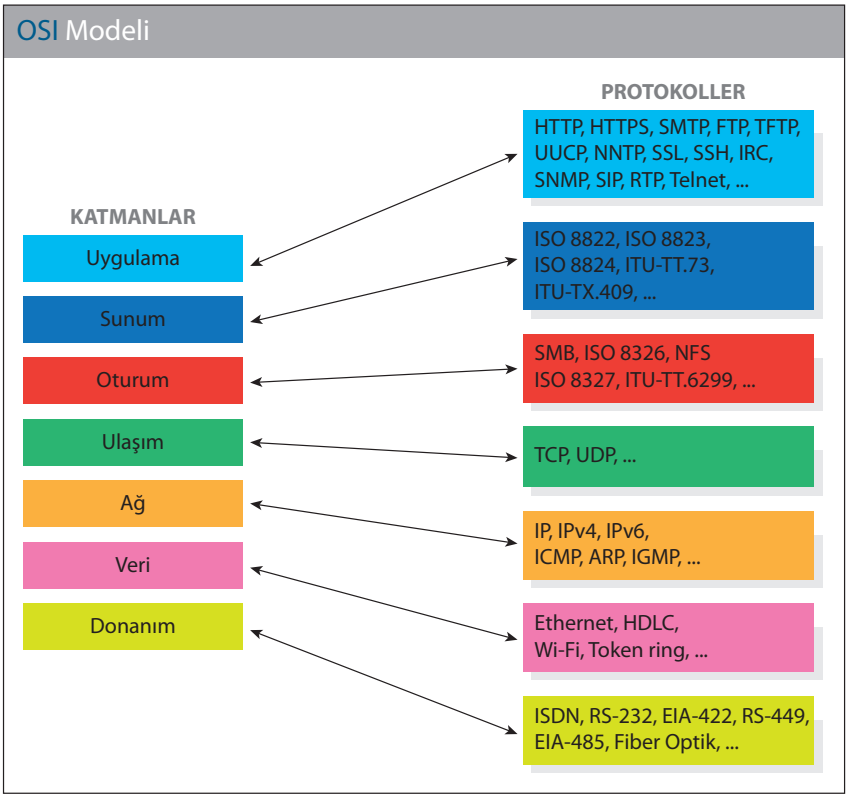
Ethernet teknolojisinin en yüksek hızı konusunda araştırma yapınız.

SIRA SİZDE 2

AĞ KATMANLARI

Bilgi ağlarının haberleşmesi esnasında düzenin sağlanması ve korunması için protokol adı verilen kurallar dizesinden faydalanıldığından önceki bölümde bahsedilmiştir. Bir bilgisayardaki uygulama tarafından yaratılan sayısal '1'ler ve '0'lardan oluşan veri, gönderici bilgisayardan alıcı bilgisayara giderken farklı katmanlarda protokollere göre işlenmektedir. Bu katmanlar ve protokoller sırasıyla ele alınacaktır.

Her ne kadar günümüz haberleşmesinde TCP/IP modeli kullanılıyor olsa da katmanlı ağ mantığını ilk standartlaştıran, OSI (Open System Interconnection – Açık Sistemler Bağlantısı) modelidir. OSI modeline göre ağ yapısı yedi farklı katmandan oluşmaktadır. Her birinin kendine ait görevleri olan bu yedi katman, Uygulama Katmanı (Application Layer), Sunum Katmanı (Presentation Layer), Oturum Katmanı (Session Layer), Taşıma (Ulaşım) Katmanı (Transmission Layer), Ağ Katmanı (Network Layer), Veri Bağlantısı Katmanı (Data Link Layer) ve Fiziksel (Donanım) Katman (Physical Layer) olarak adlandırılmaktadır. OSI katmanları ve her katmana bağlı bulunan protokoller Resim 1.7'de görüntülenmektedir.



Resim 1.7

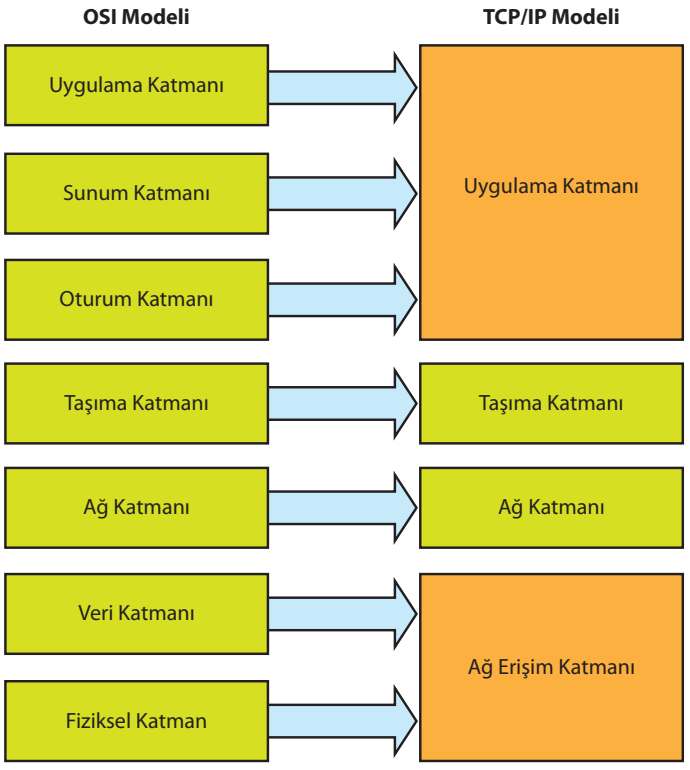
OSI Modeli ve Bağlı Protokoller.

Kaynak: *https://goo.gl/QG7QCK*

OSI modeli standartları tanımlayan referans model olarak kullanılmaktadır. OSI modeli referans alınarak geliştirilen TCP/IP modeli ise günümüz ağ bağlantılarında en yaygın kullanılan model haline gelmiştir. OSI modelindeki bazı katmanların görevlerinin paylaştırılarak ya da birleştirilerek azaltılması esasına dayanmaktadır. OSI modelinde bulunan yedi katman yerine, işlemleri aynı şekilde yerine getiren dört katman, TCP/IP modelinin katmanlarıdır. OSI Modelindeki Uygulama, Sunum ve Oturum katmanları birleştirilerek Uygulama Katmanı adı altında toplanmıştır. Ulaşım ve Ağ katmanları değişmemiştir. Son katman, OSI modelindeki veri ve donanım katmanlarının birleştirilmesi ile oluşturulmuştur. OSI ile TCP/IP modellerinin katmansal karşılaştırılması Resim 1.8'de görülmektedir.

Resim 1.8

OSI ve TCP/IP Modelleri Katman Karşılaştırması.



TCP/IP modelinde en alt katman olan Ağ Erişim Katmanı bazı durumlarda Fiziksel Katman ve Veri Bağlantısı Katmanı olarak ikiye ayrılmakta ve model beş katmana sahip olmaktadır. Ağa bağlı bir cihaz üzerinde bulunan bir uygulama tarafından karşı cihaza gönderilecek olan veriler sıra ile uygulama, taşıma, ağ ve ağ erişim katmanlarını ziyaret ederek, protokoller yardımıyla, gönderim için gerekli biçimi almaktadır. Alıcı cihaz veriyi ağ erişim katmanı tarafından almaktadır. Gönderici bilgisayarın tersine alınan veri sıra ile ağ, taşıma ve uygulama katmanlarına gönderilmektedir. Son olarak alıcı cihaz tarafından uygulama katmanında çözümlenen veri, uygulamaya teslim edilmektedir. Bu sayede ağ iletişimi gerçekleşmektedir. Kitabın tümünde esas alınan TCP/IP modelinin katmanları ve veriyi biçimlendiren protokoller ayrı ayrı incelenecektir.

Uygulama Katmanı

Uygulama katmanı, protokoller modelinin en üstünde yer alarak, uygulamaların ağ ortamını kullanabilmesini sağlamaktadır. Farklı uygulamalar için farklı ağ protokolleri bu katmanda yer almaktadır. Özellikle bilgisayarlar üzerinde kullanılan uygulamaların sayısı ve

çeşitliliği göz önüne alındığında, en fazla protokol içeren katman, uygulama katmanıdır. Web tarayıcılar, e-posta istemcileri, veritabanı uygulamaları vb. uygulamalar, bu katman sayesinde verilerini diğer bilgisayar ya da sunucu makinelere göndermektedir. Uygulama katmanı tarafından gönderilmek üzere hazırlanan veriler, bir alt katman olan taşıma katmanına verilmektedir. Birçok uygulama katmanı protokolü olmasına rağmen belli başlı sık kullanılan protokoller aşağıda kısaca açıklanmaktadır.

HTTP (Hyper Text Transfer Protocol - Hiper Metin Transfer Protokolü): WWW (World Wide Web) yani dünya çağında ağ üzerinde kullanılmak üzere geliştirilmiş bir protokoldür. Bilgisayarda kurulu bulunan bir web tarayıcı ile herhangi bir internet sayfası açılmak istendiğinde devreye girer. Web sunucu bilgisayara bir istek göndermeyi ve istek sonucunda gelen cevap verisini görüntülemeyi sağlamaktadır. Taşıma katmanı protokolü olarak TCP (Transmission Control Protocol – İletim Kontrol Protokolü) kullanılmaktadır. Günümüzde internet sitelerinin sayıca artması ve e-ticaret, bankacılık işlemleri vb. bilgi güvenliği gerektiren işlemlerin sıkça karşımıza çıkması dolayısıyla protokol güvenliği de ele alınmak durumunda kalmıştır. HTTP, sonuna güvenli kelimesinin İngilizce karşılığı "secure" kelimesinin baş harfini almıştır. HTTPS bu sebeplerle tasarlanmış, güvenli hiper metin aktarım iletişim kuralı olarak karşımıza çıkmaktadır.

SMTP (Simple Mail Transfer Protocol – Basit Posta Gönderim Protokolü): E-posta gönderiminde kullanılmak üzere tasarlanmış bir protokoldür. Bu protokol, istemci tarafından gönderilmek istenen bir e-postanın sunucu bilgisayara iletiminden sorumludur. Sunucu bilgisayardan gelen e-postaları almak için ise POP ya da IMAP protokolleri kullanılmaktadır.

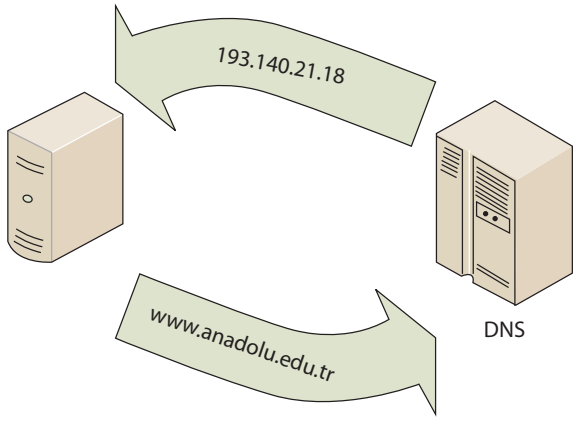
POP3 (Post Office Protocol – Posta Ofisi Protokolü): Sunucu bilgisayara gelmiş olan e-postayı istemci bilgisayara almak için kullanılan bir protokoldür. Kısacası gelen e-postaları bilgisayarımıza indirmek için kullanılmaktadır. Bu protokole benzer bir protokol de IMAP (Internet Message Access Protocol – İnternet İleti Erişim Protokolü)'tir. POP, birkaç farklı sürüme sahiptir. Günümüzde kullanılan sürüm numarası 3'tür. Bu sebeple protokol POP3 olarak adlandırılmaktadır.

FTP (File Transfer Protocol – Dosya Transfer Protokolü): Ağ üzerinde dosya transferi için kullanılan protokoldür. Birçok ağ sunucusu, üzerinde depolanan dosyaya erişim için kullanıcı adı ve şifre talep etmektedir. Kullanıcı adı ve şifre talebi başarılı olarak girilince dosya indirmeye olanak sağlamaktadır. Bazı durumlarda ise "anonim" kullanıcı olarak bağlanarak dosyayı indirmek mümkün olmaktadır. TCP taşıma katmanı protokolünü kullanan FTP, dosyanın güvenli ve eksiksiz bir şekilde istemci tarafından edinilmesini sağlamaktadır.

DNS (Domain Name System – Alan Adı Sistemi): Kullanıcı farkında olmasa da, uygulama katmanı tarafından en çok kullanılan protokollerden birisi olarak karşımıza çıkmaktadır. Alan adı bilinen bir sunucu bilgisayarın, ağ üzerinde tanımlanmasını sağlayan IP adresinin bulunmasını sağlayan protokol, İnternet sitelerine her bağlantı yapıldığında kullanılmaktadır. Örneğin web tarayıcısı ile www.anadolu.edu.tr adresi ziyaret edilmek istensin. Tarayıcı, yukarıda bahsedilen protokolü kullanarak Anadolu Üniversitesi web sunucusuna bir istek göndermektedir. Global internet üzerinde yer alan her cihaz, kendine ait bir IP adresi ile temsil edilmektedir. Bu sebeple tarayıcı, isteği web sunucunun IP adresine yapmalıdır. Yazılan alan adına ait IP adresini bulmak için DNS protokolünden faydalanılmaktadır. Bu sayede doğru sunucuya istek yapılmakta, cevap neticesinde de web sayfası tarayıcıda görüntülenmektedir. Resim 1.9 bir alan adı-IP adresi çözümlemesi örneği göstermektedir.

Resim 1.9

DNS Çalışma Örneği.



Taşıma Katmanı

UDP, hız ve basitlik temeline dayanan, popüler bir taşıma katmanı protokolüdür.

Uygulama tarafından gönderilerek uygulama katmanı tarafından gerekli protokollere göre düzenlenen veri, taşıma katmanına geçirilmektedir. Bu katman, bir anlamda verinin kendisinin düzenlenmesi ile veriye bakılmaksızın gönderme işlemini gerçekleştiren üst ve alt katmanlar arasında köprü vazifesi görmektedir. Bu katmanda en sık kullanılan iki protokol, **TCP** (Transmission Control Protocol – İletim Kontrol Protokolü) ve **UDP** (User Datagram Protokol – Kullanıcı Veri Bloğu Protokolü)'dir. Bu katmanda yer alan çoğu protokol de TCP ve UDP'nin farklı özelliklerini alarak oluşturulmuştur.

UDP: En basit taşıma katmanı protokolüdür. Verilerin en kolay şekilde gönderilmesi esas alınarak tasarlanmıştır. Verileri, öncesinde herhangi bir bağlantı oluşturmaksızın göndermektedir. Verilerin gönderimi esnasında güvenilirlik ve sıralama aranmamaktadır. Bu protokolde paket teslim garantisi yoktur. 8 Bayt'lık başlık büyüklüğü, protokolün hafifliği konusunda avantaj sağlamaktadır. UDP basit bir protokol olmasına karşın, iletim süresinin kısalığı, yani hızı sayesinde uygulamacılar tarafından tercih sebebi olmaktadır. Özellikle geniş alanlarda ses ve görüntü aktarımı gerektiren gerçek zamanlı uygulamalarda sıklıkla kullanılmaktadır. UDP aynı zamanda tek alıcıya ve çoklu alıcılara mesaj göndermek üzere tasarlanmıştır.

TCP: En gelişmiş taşıma katmanı protokolü olan TCP, verilerin alıcı bilgisayara eksiksiz, sıralı ve güvenilir bir şekilde ulaşmasını garanti etmektedir. Veri gönderiminden önce üç yollu el sıkışma adı verilen bağlantı sağlama metodu kullanılmaktadır. Bu metoda göre:

1. Gönderici bilgisayar, alıcı bilgisayara TCP Senkronizasyon mesajı gönderir.
2. Alıcı bilgisayar bu isteği aldığına dair bir TCP Senkronizasyon+Onay (Acknowledgement) mesajı ile cevap verir.
3. Gönderici bilgisayar bu mesaja TCP Onay mesajı ile cevap verir.
4. Alıcı bilgisayar, "Bağlantı Kurulmuştur" mesajını almaktadır.

Bu şekilde gönderici ile alıcı bilgisayar arasında bağlantı sağlanmış olmaktadır. Bağlantı sağlandıktan sonra gönderici bilgisayar, alıcı bilgisayara veri paketlerini göndermeye başlamaktadır. TCP gönderim esnasında da güvenilirliği sağlayan bir protokoldür. Her gönderilen mesajın, onaylandı mesajının, gönderen bilgisayara gelmesi sağlanmaktadır. Bu sayede onaylama mesajı alınamayan paketler kayıp kabul edilerek tekrar gönderilmektedir. TCP için paket sıralaması da önemlidir. Paketlerin gönderici bilgisayardan, alıcı bilgisayara sıralı bir şekilde gitmesini sağlamakla yükümlüdür.

TCP için önemli unsurlardan bir tanesi de alıcı bilgisayarın tampon belleğini (buffer) aşacak kadar hızlı ve çok paket gönderimi yapmamasıdır. Alıcı bilgisayarın belleğinin küçüklüğü ya da uygulamanın yavaşlığı bu tür bir soruna sebep olabilmektedir. Bu durumda alıcı bilgisayar, kaydedecek yeri olmadığı için, gelen paketleri kabul edememekte ve paketlerin yer açıldıktan sonra tekrar gönderilmesi gerekmektedir. Veri ağı yollarının verimsiz kullanımı olarak düşünülebilecek bu olaya sebep olmamak için TCP, alıcı bilgisayarın belleğinde veri paketi alımı için ayrılan boş yeri kontrol etmektedir. Bu bilgi sayesinde gönderimini düzenlemektedir. Bu metot Akış Kontrolü (Flow Control) olarak adlandırılmaktadır.

Veri gönderimi esnasında hattın yoğun olması, paketlerin ya da onaylama mesajlarının kaybolmasına sebep olmaktadır. Kaybolan paket ya da pakete ait onaylama mesajı, o paketin tekrar gönderilmesini gerektirmektedir. TCP kendi içerisinde çalışan belli metotlarla hattın durumunu da gözlemlemekte, hattın kapasitesini aşacak kadar fazla paket gönderimine engel olmaktadır. Çeşitli metotları içeren bu sistem, Tıkanıklık Kontrolü (Congestion Control) olarak adlandırılmaktadır.

Tüm bunların sağlanması için TCP, 20 ila 60 Bayt arasında değişen bir başlık büyüklüğüne sahiptir. Birçok hata oluşma senaryosu düşünülerek tasarlanan TCP protokolü ile paket gönderimi kesinlik kazanmaktadır. Tüm paket gönderimi tamamlandıktan sonra gönderici bilgisayar ile alıcı bilgisayar arasında ilk başta yapılan üç yollu el sıkışmaya benzer bir yöntemle bağlantı sonlandırılmaktadır. TCP protokolü bir bağlantıda tek bir alıcıya mesaj gönderebilmektedir. Çoklu gönderim için ayrı ayrı bağlantılar açılması gerekmektedir.

Tablo 1.1'de TCP ve UDP protokollerinin karşılaştırması incelenebilir.

Özellik Adı	TCP	UDP
Başlık Büyüklüğü	20-60 Bayt	8 Bayt
3 Yollu El Sıkışma	Var	Yok
Güvenilirlik	Var	Yok
Sıralı Gönderim	Var	Yok
Tek Alıcıya Gönderim	Var	Var
Çok Alıcıya Gönderim	Yok	Var
Akış Kontrolü	Var	Yok
Tıkanıklık Kontrolü	Var	Yok

Tablo 1.1
TCP ve UDP'nin Özelliklerinin Karşılaştırması

Farklı taşıma katman protokollerine internet ortamında https://goo.gl/unuvfU linkinden ulaşabilirsiniz.

İNTERNET

Ağ Katmanı

Modelin üçüncü katmanı olan Ağ Katmanı, temelde başka bir ağa gönderilmek istenen verinin alıcıya ulaşmasından sorumludur. En önemli özelliği IP adreslerinin bu katmanda tanımlanmasıdır. IP adresleri, ağa bağlı her bir cihaz için birbirinden farklı olan sayılardır. Küresel İnternet söz konusu olduğunda ise durum değişmemektedir. Dünya üzerinde internet ortamına bağlı tüm cihazların IP adreslerinin birbirinden farklı olması gereklidir. Bir anlamda, bu sayıları telefon numaraları ya da ev adresleri gibi düşünmek anlaşılmasını kolaylaştıracaktır. Telefon numaraları ya da adresler tüm dünya üzerinde tekildir, bir başka örnekleri daha yoktur. Dünya üzerinde herhangi bir telefondan ilgili bir numaraya arama yapıldığında, yalnızca o telefon çalacaktır. Ya da bir mektup üzerine yazılan bir adres, şüpheye yer bırakmayacak şekilde tek bir konuma işaret eder. İşte İnternet bağlantısı esnasında da aynı prensip geçerlidir. Tüm web sunucular, FTP sunucular, e-posta

sunucuları için birbirinden farklı IP adresleri bulunmaktadır. İnternet bağlantısı bulunan herhangi bir cihazdan yapılmak istenen bağlantıda, sunucu IP adresine bağlantı yapılması gerekmektedir. Örnek olarak, bir web sitesinin alan adı yazıldığında, ona karşılık gelen IP adresinin bulunması gerektiğinden DNS protokolünde bahsedilmişti. Tüm internet, IP adresleri üzerine tasarlanmıştır. İnternet'te gerekli yönlendirmeyi yapan ve verilerin doğru alıcılara ulaşmasından sorumlu yönlendirici (Router) cihazlar da IP adreslerine göre yönlendirme ve teslim etme işlemlerini gerçekleştirmektedirler. Bu katmanda kullanılan bazı protokoller aşağıdaki şekilde sıralanabilir.

IPv4 adresleri 32 bit, IPv6 adresleri 128 bit ve MAC Adresleri 48 bit olarak yapılandırılır.

IPv4: Günümüzde kullanılan IP adreslerinin sürüm numarası 4'tür. Bu sebeple IPv4 şeklinde de ifade edilir. 8'er bitlik dört blok halinde gösterilen IP adresleri toplamda 32 bitlik bir sayıya karşılık gelmektedir. İlk tasarlandığı zamanlarda A, B, C, D sınıfı olmak üzere dört sınıftan oluşan IPv4, daha sonraları bu kullanımın, zaten kısıtlı olan IP adres bloklarını verimli kullanmaması sebebiyle, sınıfsız olarak kullanılmaya devam edilmiştir. Sınıfsız kullanımda, Alt Ağ Maskesi (Subnet Mask) adı verilen 32 bitlik bir blok yardımıyla ağ adresleri saptanabilmektedir. Bu sayede, aranılan IP adresine sahip cihazın hangi ağa dâhil olduğu bulunabilmektedir. Buna rağmen, dünya üzerinde hızla artan sayıda internete bağlanan cihaz olmasından dolayı IPv4 adres alanı yetmemektedir. Bu adres kısıtlılığını giderebilmek için NAT (Network Address Translation – Ağ Adresi Dönüştürme) sisteminden faydalanılmaktadır. Sistem, bir yönlendirici arkasında bulunan ev, firma, kampüs vb. yerel alan ağlarına, kendi içlerinde tekil olmak kaydıyla, sanal IP adresleri vermeyi sağlamaktadır. Yönlendiricinin dış dünyaya çıkış kapısında bulunan IP adresi, küresel internetle uyumlu olmaktadır. IPv4 adres alanının yetersizliğinden dolayı altıncı sürüm adresleme çalışmaları yapılmaktadır.

IPv6: Sürüm numarası 6 olarak belirlenen yeni nesil IP adresleri, 128 bitten oluşan ve 16'lık tabanda 8 parçadan oluşan bir biçimde gösterilmektedir. Her ne kadar yeni nesil işletim sistemlerinde IPv6 kullanımına uygun olanaklar sağlansa da, IPv4'ü tamamen bırakarak IPv6 kullanımına geçmek, yönlendirici cihazların da desteklemesi gereken bir olgudur. IPv6 kullanımına yönelik pilot uygulamalar hız kazanmıştır. Fakat henüz tamamen kullanımı sağlanamamaktadır.

ARP (Address Resolution Protocol – Adres Çözümleme Protokolü): ARP'ı anlatmadan önce, veri bağlantısı katmanında bulunan farklı bir adresleme mantığından bahsetmek uygun olacaktır. Ağa bağlı cihazlar, kendisi ile aynı ağı paylaşan cihazlarla haberleşmek için IP adreslerine ihtiyaç duymamaktadırlar. Aynı ağdaki cihazların haberleşirken birbirlerinden ayrılmalarını, her birinin ağ arayüz kartının ROM belleğine yazılı bulunan MAC (Media Access Control – Ortam Erişim Kontrolü) adresleri sağlamaktadır. MAC Adresleri, fabrika çıkışında arayüz kartına verilir ve bir daha değişmemektedir. 48 bitten oluşan MAC adresleri de IP adresleri gibi her bir cihaz için farklı değerlere sahiptir. Farklı ağlara veri gönderimi esnasında, alıcı cihazın IP adresine yönlendirme yapıldığından bahsedilmişti. Yönlendirici cihaz, alıcı cihaz ile aynı ağa geldiğinde, yani veri teslim edilmeden bir basamak önce, alıcı bilgisayarın MAC Adresini de bilmeye ihtiyaç duymaktadır. Aynı ağda olan bir arayüze veriyi, Veri Bağlantı Katmanı sayesinde ulaştırmaktadır. İşte bu durumda, IP adresi bilinen bir cihazın MAC adresini öğrenme gereksiniminde ARP devreye girer. IP adresi bilinen cihaza bir sorgu paketi gönderilerek MAC adresi öğrenilmekte ve bu sayede veri iletişimi tamamlanmaktadır.

Bunların dışında ağ katmanının önemli özelliklerinden bir tanesi de paketlerin veri yolları tarafından taşınabilecek büyüklüklere getirilmesi işlemidir. Her veri yolunun bir seferde taşıyabileceği veri paketi büyüklüğü belirlidir. Bu değere Maksimum İletim Birimi (MTU - Maximum Transfer Unit) adı verilmektedir. Uygulama ve taşıma katmanlarını geçerek ağ katmanına gelen paket, eğer veri yolunun maksimum iletim biriminden bü-

yükse, ağ katmanı bu paketi tek seferde taşınabilecek en büyük paketler halinde parçalama işlemini gerçekleştirmektedir. Alıcı cihaz tarafından alınan paketler, bu sefer alıcı cihazın ağ katmanı tarafından birleştirilerek, yeniden tek bir paket haline getirilmektedir.

İnternet ortamına bağlı bir bilgisayarda IP adresini belirleyiniz.

SIRA SİZDE 3

Veri Bağlantı Katmanı

Ağ ortamının donanımsal kısmından alınan verilerin ilk uğradığı katman olan Veri Bağlantı Katmanı, ikinci katman olarak da adlandırılmaktadır. Fiziksel Katman ile Ağ Katmanlarının arasında yer almaktadır. Veri bağlantı katmanı, farklı fiziksel katman teknolojileri ve farklı ağ katman teknolojileri arasında çalışmak üzere tasarlanmıştır.

Ağ katmanından gelen veri paketlerine, öncelikle gönderen ve alıcıya ait MAC adres bilgileri eklenmektedir. Yukarıda bahsedildiği gibi MAC adresleri, aynı ağa bağlı cihazlar arasında haberleşme esnasında, cihazların birbirinden ayrılmasını sağlamak üzere, ağ arayüz kartında bulunan 48 bitlik sayılardır. Her bir arayüzün MAC adresi birbirinden farklıdır.

Devamında katman, paket sonuna Hata Yakalama Düzeltme Kodunu (EDC – Error Detection Correction Code) eklemektedir. Bu kod farklı algoritmalarla hesaplanabilmektedir. Bunlardan bir kaçı;

Sağlama Toplamı (Checksum): 16 bitlik sayılar halinde bölümlenen verinin sonuna "1"'lerin toplamının yazılmasını esas alan metottur. Çok basit ve az işlem gerektiren ancak güvenilir olmayan bir metot olduğu için sıklıkla kullanılmamaktadır.

Eşlik Denetimi (Parity Checking): Tek bit ve çift yönlü olmak üzere iki farklı kullanımı mevcuttur. Tek bit eşlik denetiminde 7 bitlik verinin sonuna "1"'lerin toplamının tek ya da çift sayı olması için bir eşlik biti konulmaktadır. Toplam sayının tek sayı mı çift sayı mı olacağına önceden karar verilmektedir. **Çift yönlü eşlik denetiminde** ise alıcıya, eşlik bitinin dışında bir de verinin sonunda eşlik baytı gönderilmektedir. Çift yönlü eşlik denetimi, tek bitlik hataların alıcı tarafından düzeltilmesi şansını da vermektedir.

Hata yakalama ve düzeltme algoritmaları içerisinde sadece **çift yönlü eşlik denetimi** hata düzeltme işlemi yapmaktadır. Bu düzeltme işlemi ise sadece tek bit hata olduğunda kullanılabilmektedir.

Çevrimsel Artıklık Kodlaması (CRC – Cyclic Redundancy Check): Günümüz internetinde kullanılan hata yakalama algoritması CRC'nin bir çeşidi olan CRC-32'dir. Verinin 32. dereceden bir polinoma XOR işlemi ile bölünmesi ve kalanın verinin sonuna eklenerek gönderilmesini esas alan algoritmadır. Alıcı bilgisayar, alınan veriyi yine aynı polinoma bölmekte ve kalan hanesini kontrol etmektedir. Eğer kalan 0 ise veri hatasızdır. Kalan hanesinin 0'dan farklı olması durumunda verinin alıcıya gelirken bozulduğu sonucuna ulaşılmaktadır.

Veri bağlantı katmanının görevlerinden bir tanesi de verinin baş ve son kısımlarını belirlemektir. Bu işleme çerçeveleme (Framing) adı verilmektedir. Çerçeveleme, özel bazı karakterler kullanılarak yapılabildiği gibi kablo ile bağlanılan ağlarda, özel voltaj değerleri kullanılarak da sağlanmaktadır.

Veri bağlantı katmanının, özellikle aynı ağa bağlı ikiden fazla bilgisayar olması durumunda önemli görevlerinden bir tanesi de MAC protokolünü işleme sokmaktır. MAC protokolü, veri hattını kimin kullanacağıyla ilgili karar vermeyi sağlamaktadır. Aynı ağa bağlı iki cihazın, aynı anda veri göndermeleri çarpışma (Collision) olarak adlandırılmaktadır ve bu durum gerçekleştiğinde her iki veri de kullanılamaz duruma gelmektedir. İşte bu sebeple, veri gönderiminden önce hattı dinlemek, eğer hat dolu ise beklemek, hat boş ise veri gönderimine başlamak MAC protokollerinin işlevleriyle sağlanır. Veri gönderimi esnasında da hat dinlenmeye devam edilmekte ve çarpışma durumunda veri gönderimi kesilerek belirli bir zaman sonra aynı veri tekrar gönderilmektedir.

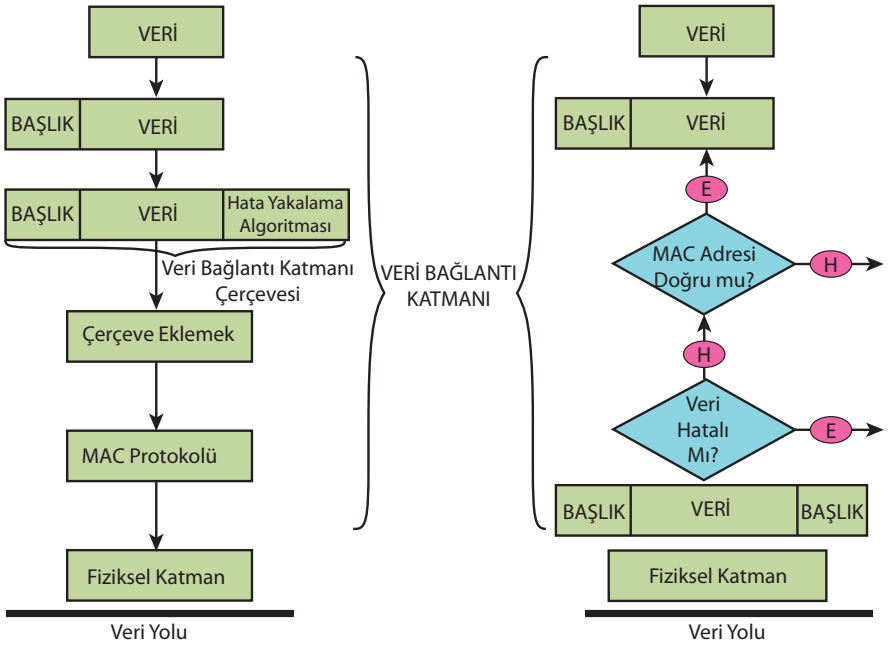
Kablolu ağlarda yukarıda anlatılan algoritma çalışırken kablosuz ağlarda hattı dinlemek, birbirinden uzak yerleşen cihazlar için mümkün olmamaktadır. Bu durumda MAC protokolü, hattı kullanmadan önce alıcı cihazdan izin almak (Request To Send – Gönderme İsteği) ve gönderim tamamlandığında bilgi vermek (Clear To Send – Gönderme Tamamlandı) şeklinde çalışmaktadır.

Taşıma katmanı, Ağ Katmanı ve Veri Bağlantı Katmanları, verinin yukarıda hangi protokolden geldiğini belirlemek için bir anahtar kullanmaktadırlar. Bu anahtar sayesinde alıcı bilgisayar, ilgili katmana gelindiğinde, verinin doğru protokole ulaşmasını sağlamaktadır. Örneğin taşıma katmanını ele alacak olursak yukarıda bulunan uygulama katmanından gelen veri HTTP ile işleme tabi tutulmuştur. Veri alt katmanlarda da gerekli işlemlerden geçirildikten sonra alıcıya gönderilmekte ve teslim alınarak taşıma katmanına kadar çıkmaktadır. Alıcı cihaz taşıma katmanı, uygulama katman protokolü olarak HTTP yerine FTP'yi kullanırsa sonuç hatalı olacak ve gönderilen veri uygulama tarafından kullanılamayacaktır. Üst katmandan teslim alınan ya da teslim edilecek protokolün belirlenmesi işlemi, gönderici için çoklama (Multiplexing), alıcı için ise çoklamayı çözme (Demultiplexing) olarak adlandırılmaktadır.

Veri bağlantı katmanında gerçekleştirilen işlemler Resim 1.10'da şematize edilmiştir.

Resim 1.10

Veri Bağlantı Katmanı Çalışma Yapısı.

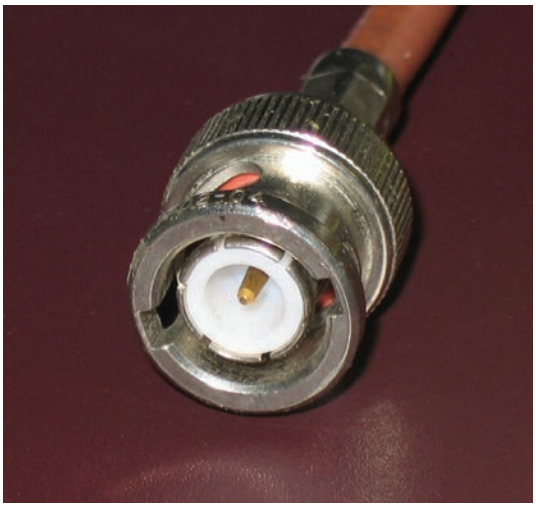


Fiziksel Katman

Veri yollarını da oluşturan donanım katmanı, fiziksel katman olarak adlandırılmaktadır. Kablolu ve kablosuz olmak üzere iki farklı bağlantı ortamından bahsetmek mümkündür. Bu bölümde kablolu bağlantı ortamları anlatılmaktadır. İzleyen bölümde ise kablosuz bağlantı ortamlarından bahsedilecektir. Bazı durumlarda sayısal verilerin veri yoluna kodlanması işlemini de fiziksel katman üstlenmektedir. Sayısal verilerin sayısal ve analog hatlara kodlanması için farklı algoritmalar kullanılmaktadır. Analog hatlara kodlama, kablolu ağlarda verinin farklı voltaj seviyeleri ile gönderilmesini esas almaktadır. Kablosuz ağlarda ise taşıma ortamı hava olduğundan radyo, ışık ya da ses dalgalarına çevirme şeklinde kodlama gerçekleştirilir.

Kablolu veri iletişim ağları için üç farklı kablo türünden bahsetmek mümkündür.

Eşmerkezli Kablo (Coaxial Cable): Anten kablosu olarak da adlandırılan kablodur. BNC adaptör ve konnektör ile birbirine bağlantı yapılan ağların veri transferi için kullanılmaktadır. Resim 1.11'de BNC Konnektör görülmektedir. Nispeten eski bir teknolojidir.



Resim 1.11

BNC Konnektör.

Kaynak: *https://goo.gl/E0Z9RG*

UTP Kablo (Unshielded Twisted Pair – Korumasız Bükümlü Çift): Günümüz internet altyapısının yerel alan ağlarında kullanımı sıklıkla görülen kablo türüdür. Sağladıkları bant genişliğine göre Cat1, Cat2, Cat3, Cat4, Cat5, Cat5e, Cat6, Cat6a gibi çeşitleri bulunmaktadır. Cat1 kablo telefon iletişimi için kullanılmaktadır. Cat2 kablo ile 4 Mbps hızdan başlayarak, Cat6a kabloda 10 Gbps hızına kadar veri akışı elde edilmektedir. İçerisinde Turuncu, Turuncu Beyaz, Yeşil, Yeşil Beyaz, Mavi, Mavi Beyaz, Kahverengi, Kahverengi Beyaz olmak üzere dört adet çift, bükümlü şekilde bulunmaktadır. Bükümlü olması, çevresel elektrik akımlarından etkilenmemesini sağlamaktadır. RJ45 adı verilen konnektörler yardımıyla Ethernet kartlarına bağlantı yapılmaktadır. Resim 1.12'de RJ45 konnektör kullanılarak bağlantısı yapılmış UTP kablo örneği görülmektedir. Sekiz adet kablodan birinci ve ikinci uçlar veri göndermek, üçüncü ve altıncı uçlar ise veri almak için kullanılmaktadır. Diğer uçlar yedek olarak bulunmaktadır. Fiber optik kablolardan daha ucuz olduğu için daha yaygın kullanımı görülmektedir. Yaklaşık olarak 100 metre menzile sahip bu kablolar ile daha uzak mesafe bağlantılar gerçekleştirmek için araya tekrarlayıcı cihazlar koyulmak zorundadır.

Resim 1.12

RJ45 Konnektör Bağlı Kablolar.

Kaynak: *102752444*

Fiber Optik Kablo: En hızlı ve en uzak mesafe veri iletimine imkân sağlayan kablo türüdür. Fiber optik kabloda gönderici taraf, kablonun çeşidine göre, led ışık kaynağı ya da lazer ışık kaynağı olabilmektedir. Alıcı taraf bir fotodiyottur. Işığın algılanması "1", ışık olmaması ise "0" kodlaması esasına göre çalışmaktadır. Plastik bir ceketin içerisinde ışığın geçebilmesine olanak sağlayan plastik ya da cam fiberlerden oluşmuş bir yapıya sahiptir. Maliyetinin yüksek ve işçiliğinin zor olmasına rağmen, yüksek hız ve uzun mesafe imkânı nedeniyle uzak mesafe bağlantılarda sıklıkla kullanılmaktadır.

KABLOSUZ AĞLAR

Mobil cihazların yaygınlaşması ve özellikle akıllı telefonların artması ile birlikte kablolu ağlara bir alternatif olarak kablosuz ağların kullanımı artmıştır. Kablo bağımlılığından kurtulma avantajının yanı sıra, her geçen gün artan veri transfer hızı ile kablosuz ağlar, son kullanıcı tarafında kablolu ağlara göre daha çok tercih edilen ağlara dönüşmektedir. Veri transferi için radyo frekansı dalgalarının kullanılması dışında kablosuz ağların protokolleri, kablolu ağlardan çok farklı değildir.

Kablosuz ağları iki farklı açıdan incelemek mümkündür. Bunlardan birincisi, ADSL teknolojisinin yaygınlaşmasıyla günlük hayatta sıklıkla karşılaşılan Wi-Fi (Wireless Fidelity – Kablosuz Bağlantı Alanı) kablosuz ağ teknolojisidir. İnternet servis sağlayıcısı aracılığıyla sağlanan internet ağ bağlantısı, kablosuz olarak son kullanıcılara, belirli bir mesafe sınırı dâhilinde iletilebilir. Wi-Fi ağları, IEEE 802.11a/b/g/n/ac standartlarına göre çeşitli yayın frekanslarında bağlantı hızları sunar. Bu tür kablosuz ağlar için herhangi bir lisans gerekmemektedir. 802.11 sadece 2 Mbps bağlantı hızı sunarken, 802.11a (5 GHz frekansında) 54 Mbps, 802.11b (2,4 GHz frekansında) 11 Mbps, 802.11g (2,4 GHz frekansında) 54 Mbps hıza sahiptir. 802.11n ise 300 Mbps hıza kadar ulaşmıştır.

Wi-Fi ağların kullanımında en büyük sorun, ağa yetkisiz kişilerin dâhil olmasıdır. Bunu önlemek için ağ kaynağına çeşitli şifreleme algoritmalarıyla erişim kontrolü uygulanabilmektedir. WEP (Wired Equivalent Privacy – Kabloya Eşdeğer Mahremiyet) olarak bilinen şifreleme yöntemi kolayca kırılabilmektedir ve ağa sızmaların gerçekleştiği, zaman içerisinde çokça gözlemlenmiştir. Bu algoritma yerine WPA (Wi-Fi Protected Access - Wi-Fi Korumalı Erişim) ve WPA2 teknolojileri devreye sokulmuştur. WPA ve WPA2'nin daha güvenilir bir şifreleme imkânı sunduğu gerçektir. Son yıllarda ortaya konan bir erişim kısıtlama metodu olan WPS (Wi-Fi Protected Setup – Wi-Fi Korumalı Kurulum) ise iki cihazın birbiri ile anlaşması esasına dayanan bir erişim kontrolü sunmaktadır.

Kablosuz kullanımın ikinci bir çeşidi ise GSM operatörleri tarafından sağlanan internet hizmetidir. Bu hizmete bağlanmak için öncelikle GSM operatörü ile anlaşma yapılması gerekmektedir. Birinci nesilden (1G) başlayarak beşinci nesile (5G) kadar uzanan teknoloji giderek hızlanmakta ve daha fazla veri iletimine olanak sağlamaktadır. Birinci nesil telefon şebekesi, analog veriyi hücresel ağ kullanarak iletime olanak sağlamaktadır. İkinci nesil (2G) şebeke sistemi, yine hücresel ağ kullanmasına rağmen, veri aktarımı sayısal hale gelmiştir. Bu sayede kısa mesaj, hücre bilgisi gibi ek bilgiler mobil telefonlar tarafından alınmıştır. İkinci nesil sistemlerden sonra geliştirilen GPRS (General Package Radio Service – Genel Paket Radyo Servisi) ile telefon şebekesi üzerinden paket anahtarlamalı veri iletimi sağlanmıştır. EDGE (Enhanced Data Rates for GSM Evolution – GSM Evrimi için Genişletilmiş Veri Aktarım Oranları) teknolojisi ile hızlanan veri iletişimi, üçüncü nesil (3G) teknolojisinde kablosuz telefon görüşmeleri, kablosuz veri aktarımı ve görüntülü konuşma gibi özelliklerin hepsine bir arada sahip olma imkânı sağlamıştır. Dördüncü nesil (4G) mobil şebeke kullanımı başlamış olmasına rağmen 5. Nesil (5G) şebekeleri ile ilgili çalışmalar sürmektedir. Dördüncü nesil, mobil telefonlarda 100 Mbps, bilgisayarlarda ise 1 Gbps hızı hedeflemektedir.

SIRA SİZDE 4 **Cep telefonunuzun hagi nesil iletişimi desteklediğini araştırınız.**

Özet

AMAÇ 1 *Ağ kavramını tanımlamak*

En az iki bilgisayarın birbirine bağlanması ile oluşturulan ağ, iki amaca yönelik geliştirilmiştir. Bunlardan birincisi farklı bilgisayarlar arasında veri paylaşımıdır. İkinci amaç ise kaynakların ortak kullanımına yöneliktir. Ağ yetenekleri sayesinde yazıcılar, depolama üniteleri, işlemci gücü gibi kaynakların farklı makineler tarafından ortak kullanılması sağlanmaktadır.

AMAÇ 2 *Ağ tarihçesi ve gelişimini açıklamak*

Dünya çapında ortaya konan ilk ağ ARPANET (Advanced Research Projects Agency Network - Amerikan Gelişmiş Savunma Araştırmaları Dairesi Ağı)'tir. Daha sonra DARPA (Defence Advanced Research Projects Agency, ABD Savunma Bakanlığı İleri Araştırma Projeleri Ajansı) adını alan ağ, soğuk savaş sırasında geliştirilmiş, dünyanın ilk çalışan paket anahtarlama ağı olmasının yanı sıra, İnternetin de atasıdır. 1972 yılında XEROX firması tarafından geliştirilen Ethernet teknolojisi ve yine aynı yıllarda ortaya konan TCP/IP protokoller modeli internetin bilgi ağlarının gelişiminde önemli rol oynamıştır.

AMAÇ 3 *Ağ çeşitlerini açıklamak*

Bilgi ağlarını büyüklüklerine göre, topoloji yani cihazların bağlantı konumlarına göre ve cihazların bağlantı ortamlarına göre üç farklı kategoride çeşitlendirmek mümkündür. Büyüklüklerine göre ağlar Kişisel Alan Ağları, Yerel Alan Ağları, Şehirsel Alan Ağları, Geniş Alan Ağları, Sanal Özel Ağlar ve Kampüs Alan Ağları gibi sınıflara ayrılmaktadır. Topolojilerine göre ağlar ise ortak yol, halka, örgü, ağaç ve yıldız topolojileri olarak sıralanır. Bağlantı şekillerine göre ağ çeşitlerinde en önemli ağ bağlantı türü Ethernet'tir. Bunun dışında ATM, FDDI ve Andıçlı Halka gibi teknolojiler de mevcuttur.

AMAÇ 4 *Ağ katmanlarını tanımlamak*

Bir bilgi ağı, kendine ait kurallar çerçevesinde haberleşmeyi sağlamak üzere tasarlanmıştır. Bu kuralların tamamı protokol adı altında standartlaştırılmıştır. Bir verinin gönderici cihazdan alıcı cihaza gidişine kadar kullanması gereken protokoller, TCP/IP modeline göre dört katmanda toplanmıştır. Bu katmanlar Uygulama Katmanı, Taşıma Katmanı, Ağ Katmanı ve Ağ Erişim Katmanıdır. Her bir katmanın farklı bir görevi vardır ve birbiri üzerine inşa edilen protokoller ile çalışmaktadır.

AMAÇ 5 *Kablosuz ağları açıklamak*

İki farklı kablosuz ağdan bahsetmek mümkündür. Bunlardan ilki olan Wi-Fi, genellikle daha kısa mesafeli iletişim için evlerde, ofislerde kullanılan ağ türüdür. İkindi tür ise GSM operatörleri tarafından daha uzak menzillerde veri haberleşmesine imkân sağlayan ağ türüdür. Günümüzde üçüncü nesil ve dördüncü nesil iletişim ağları kullanılmaktadır.

Kendimizi Sınayalım

1. Aşağıdakilerden hangisi ağ kurulumu amaçlarından biridir?

a. Bilgisayarların daha hızlı çalışması
b. Bilgisayar kaynaklarının ortak kullanımı
c. Bilgisayarların daha sessiz çalışması
d. Bilgisayarların daha az enerji sarfiyatı
e. Monitör boyutlarının genişlemesi

2. İlk bilgi paylaşım ağının adı aşağıdakilerden hangisidir?

a. ARPANET
b. DARPA
c. UCLA
d. ABD
e. Stanford

3. Aşağıdakilerden hangisi büyüklüklerine göre ağ çeşitlerinden biridir?

a. Halka
b. FDDI
c. ATM
d. Kişisel Alan Ağı
e. Yıldız

4. Aşağıdakilerden hangisi bir ağ topolojisi **değildir?**

a. Yıldız
b. Örgü
c. Andıçlı Halka
d. Halka
e. Ağaç

5. Aşağıdakilerden hangisi bağlantı ortamlarına göre ağ çeşidi **değildir?**

a. Ethernet
b. FDDI
c. ATM
d. Andıçlı Halka
e. Yıldız

6. Web tarayıcılar tarafından hiper metin transferi için kullanılan protokol aşağıdakilerden hangisidir?

a. SNMP
b. SMTP
c. UDP
d. HTTP
e. FTP

7. Aşağıdakilerden hangisi dosya aktarım protokolü (FTP) tarafından kullanılan taşıma katmanı protokolüdür?

a. FTP
b. UDP
c. SIP
d. HTTPS
e. TCP

8. Kullanıcı Veri Bloğu Protokolü (UDP) ile ilgili aşağıdakilerden hangisi **yanlıştır?**

a. Bağlantı gerektirmez.
b. Taşma kontrolü kullanmaz.
c. Akış kontrolü kullanır.
d. Tek alıcıya gönderimi destekler.
e. Çoklu alıcılara gönderimi destekler.

9. Aşağıdakilerden hangisi Veri Bağlantı Katmanının görevlerinden biridir?

a. MAC protokolünü çalıştırmak
b. Yönlendirici algoritmalarını yönetmek
c. Sıralı veri aktarımı gerçekleştirmek
d. IP Adresini atamak
e. İnternet tarayıcının güvenliğini arttırmak

10. Wi-Fi için kullanılacak en güvenli kablosuz şifreleme anahtar algoritması aşağıdakilerden hangisidir?

a. WEP
b. TCP
c. WPA
d. FTP
e. HTTPS

Kendimizi Sınayalım Yanıt Anahtarı

1. b	Yanıtınız yanlış ise "Giriş" konusunu yeniden gözden geçiriniz.
2. a	Yanıtınız yanlış ise "Ağ Tarihçesi" konusunu yeniden gözden geçiriniz.
3. d	Yanıtınız yanlış ise "Büyüklüklerine Göre Ağlar" konusunu yeniden gözden geçiriniz.
4. c	Yanıtınız yanlış ise "Topolojilerine Göre Ağlar" konusunu yeniden gözden geçiriniz.
5. e	Yanıtınız yanlış ise "Bağlantı Ortamlarına Göre Ağlar" konusunu yeniden gözden geçiriniz.
6. d	Yanıtınız yanlış ise "Uygulama Katmanı" konusunu yeniden gözden geçiriniz.
7. e	Yanıtınız yanlış ise "Uygulama Katmanı" konusunu yeniden gözden geçiriniz.
8. c	Yanıtınız yanlış ise "Taşıma Katmanı" konusunu yeniden gözden geçiriniz.
9. a	Yanıtınız yanlış ise "Veri Bağlantı Katmanı" konusunu yeniden gözden geçiriniz.
10. c	Yanıtınız yanlış ise "Kablosuz Ağlar" konusunu yeniden gözden geçiriniz.

Sıra Sizde Yanıt Anahtarı

Sıra Sizde 1

Bahsedilenler dışında giyilebilir cihazlar tarafından oluşturulan BAN (Body Area Network – Vücut Alan Ağı), akıllı cihazların haberleşmesinde kullanılan NFC (Near Field Communication – Yakın Alan İletişimi), yakın alandaki kablosuz cihazlarda kullanılan NAN (Near-Me Area Network – Yanımdaki Alan Ağı), bulut bilişim için kullanılan IAN (Internet Area Network – İnternet Alan Ağı) gibi çeşitler de mevcuttur.

Sıra Sizde 2

2009 yılı itibariyle 40 Gbps Ethernet ve 100 Gbps Ethernet hızları kullanımı mümkün olup standartlarıyla ilgili çalışmalar devam etmektedir.

Sıra Sizde 3

IP adresi belirlemek için Ağ özelliklerine girmeli ve IPv4 yazan kısımdaki adresi bulmalısınız. Bilgisayarınızın o anda kullanmakta olduğu IP adresi bu alanda görüntülenir.

Sıra Sizde 4

Cep telefonunuzun kullanma kılavuzu ya da üretici web sitesinden bu bilgiye erişebilirsiniz. Ayrıca GSM operatörünüz de size bu konuda destek verebilir.

Yararlanılan ve Başvurulabilecek Kaynaklar

ARPANET, Wikipedia, https://goo.gl/orQvZU
Bilgisayar ağı, Wikipedia, https://goo.gl/VPIhfj

AĞ YÖNETİMİ VE BİLGİ GÜVENLİĞİ

2

Amaçlarımız

Bu üniteyi tamamladıktan sonra;

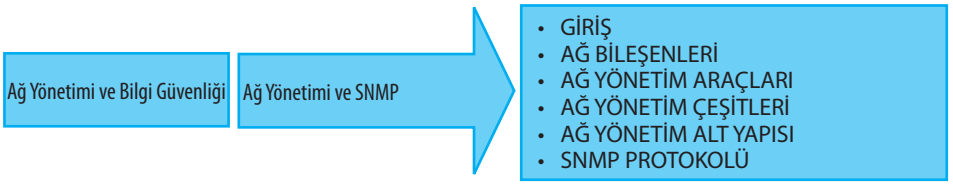
- Ağ yönetiminin gerekliliğini açıklayabilecek,
- Ağı oluşturan bileşenleri ifade edebilecek,
- Ağ yönetim araçlarını tanımlayabilecek,
- Ağ yönetim çeşitlerini tanımlayabilecek,
- Ağ yönetim alt yapısını açıklayabilecek,
- SNMP protokolü işlemlerini tanımlayabilecek

bilgi ve becerilere sahip olacaksınız.

Anahtar Kavramlar

- Ağ Yönetimi
- Ağ Bileşenleri
- Ağ Donanımları
- Anahtar
- Yönlendirici
- Yönlendirme Algoritmaları
- Ağ Arızaları
- Ağ Alt Yapısı
- SNMP Protokolü
- Taşıma Haritaları

İçindekiler



Ağ Yönetimi ve SNMP

GİRİŞ

Ağ kavramı ilk ünitede, en az iki bilgisayarın birleşmesi ile oluşan veri taşıma hattı şeklinde tanımlanmaktadır. Yalnızca iki bilgisayar ile başlayan ağ kavramı, zaman içerisinde diğer cihazların da katılımıyla büyüyerek, sonunda İnternet olarak adlandırdığımız ve tüm dünyayı kapsayan geniş alan ağına dönüşmüştür. Sadece bilgisayarlar değil, ağ ortamından ve İnternet teknolojisinden faydalanmak isteyen birçok farklı cihaz da ağa dâhil olmuştur. Tüm dünyayı coğrafi alan olarak kabul eden İnternet; veri alış verişini sağlamak için Göbek (Hub), Anahtar (Switch),Yönlendirici (Router) vb. cihazların da yardımına ihtiyaç duymaktadır. Ağ yönetimi, bir anlamda ağın sağlıklı çalışmasını sağlamak demektir. Bu kavramın gerçek hayatta da ağ sistemi dışında örneklerini görmekteyiz. Örnek olarak bir Hidroelektrik Santralini ele alalım. Santralde, kurulumundan sonra her ne kadar sistem çalışmayı sürdürse de bir merkez tarafından santralin durumu gerçek zamanlı olarak izlenmekte ve sağlıklı çalışması, eğer varsa hatanın bulunması ve ivedi olarak giderilmesi, gerektiğinde değişikliklerin yapılması için farklı cihaz ve bölgelerden gelen raporları değerlendiren merkez çalışanları görevlendirilmektedir. Örneğimizi nükleer bir santral olarak genişletecek olursak farklı cihaz ve bölgelerden gelen verilerin görüntülendiği bu merkezin önemi daha iyi anlaşılmaktadır. Özellikle soğutma sistemlerinde meydana gelen arıza, tehlikeli sonuçlara yol açacaktır. Bu sebeple sıcaklık değişiminin önemli olduğu noktalardaki alıcılar sayesinde merkezde bulunan göstergelerden, bu değişken her an gözlenmektedir. Sıcaklığın artması durumunda merkez personeli uyarılar ile bilgilendirilmekte, çözüm için gerekli işlemleri yapmaktadır. Aynı şekilde bir uçağın uçuş kabinini de ele alabiliriz. Uçağın durumuyla ilgili her türlü veri göstergelere yansımaktadır. Görevli pilotlar ise bu göstergeler ve cihazlar yardımıyla verilerin kabul edilir sınırlar içerisinde kalmasını sağlamaktadır.

Günümüzde ağ ortamına ne kadar fazla ihtiyaç duyulduğu, yaygın İnternet kullanımı dolayısıyla ortadadır. Aynen yukarıda bahsedilen örnekler gibi, ağın da izlenmesi, eğer varsa sorunların tespiti ve giderilmesi için gerekli işlemlerin yapılması, ağ yönetimi sayesinde mümkün olmaktadır. İnternet teknolojisinin atası olarak kabul edilen ARPANET'in 27 Ekim 1980 yılında yaşadığı sorun ve bu sorun sebebiyle yaklaşık olarak dört saat devre dışı kalması, ağ sisteminde meydana gelen ilk çökme olarak anılmaktadır. O yıllar için bu sorun, kullanıcı sayısının azlığı ve ağın kapasitesinin sınırlı olması dolayısıyla çok büyük zararlara yol açmadan atlatılmıştır. Fakat günümüzde değil saatler, dakikalar için bile böylesi bir sorunun meydana gelmesi, **büyük maddi kayıplarla** so-

İnternet ortamında meydana gelecek küresel bir kesinti, **büyük maddi kayıplara** yol açmaktadır.

nuçlanacaktır. Bu sebeple ağ yönetimi, ağ ortamında meydana gelecek hataları izlemek, hatayı oluşumundan önce belirlemek ve gidermek ile sorumludur. Ağ ortamında karşılaşılabilecek sorunlar, ağı oluşturan donanım ve/veya yazılımlarda meydana gelebilecek hatalardan oluşmaktadır. Ağ yönetimini sağlamak için, öncelikle ağı oluşturan bileşenleri tanımak ve hâkim olmak gerekmektedir. Bu bileşenlerin yapılarına göre hataları tespit etmek ve gidermek kolaylaşmaktadır.

AĞ BİLEŞENLERİ

Bir ağı oluşturan parçalar, basit ağlar için; bilgisayar, ağ kartı, kablolu ya da kablosuz iletişim ortamı, protokoller ve işletim sistemi olarak tanımlansa da aslında ağ dağıtımı için kullanılan cihazlar da ağ yönetiminde ön plana çıkmaktadır. Bu cihazlar Tekrarlayıcılar (Repeaters), Göbek Cihazlar (Hubs), Köprüler (Bridges), Anahtar Cihazlar (Switches) ve son ve en önemli olarak da Yönlendiricilerdir (Routers). Ağ yönetiminde, arızalı parçanın bulunması ve onarımı kadar, ağı izleyerek hızını ve doğru veri akışını tespit etmek de önemlidir. Bu sebeple dağıtıcı cihazlar, ağın geneli hakkında bilgi veren en önemli donanımlardır. Ünitenin bu kısmında ağ bileşenleri hakkında bilgi verilmektedir.

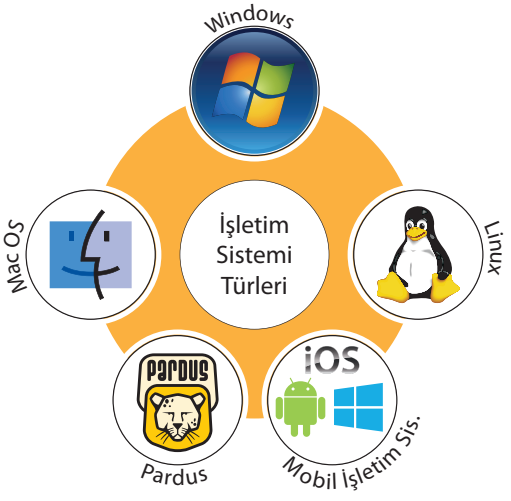
Bilgisayarlar

Ham veriyi alarak üzerinde işlemler yapan, bilgi olarak çıkış veren, gerektiği durumlarda ise bilgiyi depolayarak daha sonra kullanımına olanak sağlayan elektronik cihazlara bilgisayar adı verilmektedir. İkilik sayı sistemiyle çalışan bilgisayarlar, veriyi de ikilik sayı sisteminde almakta, işlemekte, çıktı olarak vermekte ve depolamaktadırlar. Bir bilgisayarın çalışması için donanımı kadar önemli bir bileşen de üzerinde koşmakta olan işletim sistemidir. İşletim sistemi, bilgisayarın donanımı ile kullanıcısı arasında arayüz oluşturmaktadır. Aynı zamanda donanımın hatasız ve verimli çalışmasını sağlayan da işletim sistemidir. İşletim sistemine sahip olmayan bir bilgisayar, elektronik bir yığından başka bir şey değildir. Donanımın doğru ve işlevsel biçimde çalışması için, üzerinde en az bir adet işletim sistemi bulunmak zorundadır. Yaygın olarak kullanılan işletim sistemleri Windows, Ubuntu Linux, Pardus, MacOS X gibi çeşitlendirilebilmektedir. Resim 2.1'de farklı İşletim Sistemleri türleri görülmektedir.

Resim 2.1

İşletim Sistemleri Türleri

Kaynak: *Temel Bilgi Teknolojileri Konu Anlatımı Sunu 2*

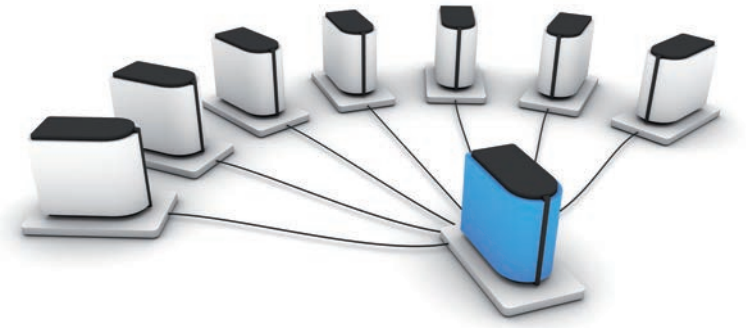


Bilgisayarların da kendi içlerinde çeşitleri bulunmaktadır.

Süper bilgisayarlar; en güçlü ve pahalı sınıfı oluşturmaktadırlar. Özel enstitüler, üniversiteler ya da araştırma kuruluşlarında bulunan süper bilgisayarlar, temelde iki amaca yönelik olarak çalışmaktadırlar. Bunlardan birincisi işlem gücü gerektiren durumlar (örneğin; gönderilecek bir uzay mekiği ile ilgili hesaplamaların yapılması gibi), ikincisi ise aynı anda çok kişiye hizmet verilmesini gerektiren durumlardır (örneğin; bir arama motoruna aynı anda yöneltilen birçok sorgunun kısa zamanda cevaplanması gibi).

Sunucu Bilgisayarlar; altında farklı bilgisayarları barındıran (web çıkışı, ticari program kullanılması ya da işletim sistemi desteği vermek vb.) cihazlardır. Kişisel bilgisayarlardan daha güçlü yapıdaki bu tür bilgisayarlar hiç kapanmadan sürekli çalışma esasına göre hizmet vermektedirler. Sunucu hizmeti verdikleri toplam bilgisayar sayısına göre kapasiteleri de farklılık göstermektedir.

Resim 2.2



Sunucu Bilgisayar Canlandırması

Kişisel bilgisayarlar; evlerde, okullarda kullanılan bilgisayar türüdür. Son kullanıcıların en sık karşılaştığı ve İnternet bağlantısı ile ağ ortamına en sık dâhil olduğu tür, bir ADSL modem ile bağlantıyı da en çok gerçekleştiren bilgisayar çeşididir.

Taşınabilir bilgisayarlar; son yıllarda günlük hayata giren ve neredeyse kişisel bilgisayarların yerini alma düzeyine gelen bilgisayar çeşididir. Diz üstü bilgisayarlar, tablet bilgisayarlar, akıllı cep telefonları, sayısal asistanlar bu sınıfta bulunmaktadır. Diz üstü bilgisayarların büyük bir çoğunluğu, kişisel bilgisayarlar ile aynı işletim sistemi çeşitlerini kullansa da, özellikle tablet bilgisayarlar ve akıllı telefonlar için taşınabilir cihazlara özel geliştirilen iOS, Android, Windows Mobile, Bada gibi farklı işletim sistemleri geliştirilmiştir.

Google firması tarafından mobil cihazlara yönelik geliştirilen işletim sistemi hangisidir? Araştırınız.

SIRA SİZDE 1

Ağ Kartı

Ethernet kartı olarak da bilinen teknoloji, kablolu ve kablosuz bağlantıya uyumlu olacak şekilde tasarlanmıştır. Günümüzde kullanılan kablolu ağ kartı, **UTP kablo** ucuna basılan RJ45 konnektör yardımıyla, üzerinde bağlı bulunduğu cihazın ağ ile bağlantısını sağlamaktadır. Kablosuz cihaz ise herhangi bir kablolu ortama ihtiyaç duymaksızın kablosuz ağ yayını yapan bir merkeze bağlanarak ağa dâhil olmaktadır. Bilgisayarlar için düşünülecek olursa Ethernet kartı anakart üzerinde bir genişletme yuvasına bağlı olabileceği gibi, anakart üzerinde yerleşik olarak da bulunabilmektedir. Özellikle taşınabilir bilgisayarlar üzerinde bulunan kablosuz ağ kartı, anakart üzerinde yerleşiktir.

Günümüz teknolojisinde ağ kartının **UTP kablo** üzerindeki hızı 1 Gbps ile 10 Gbps arasında değişmektedir.

Ağ kartının tekil özelliği, ilk ünitede açıklandığı gibi, fabrika çıkışında üzerinde bulunan yerleşik belleğe kodlanmış bulunan MAC adresidir. 48 bitten oluşan bu sayı, tüm ağ

kartları için farklı değer almakta ve yerel alan ağ haberleşmesi bu küresel tekil sayıya bağlı olarak gerçekleşmektedir. Örnek olarak, üzerinde iki adet kablolu bağlantıya uygun, bir adet de kablosuz bağlantıya uygun ağ kartı barındıran bir cihaz, her bir ağ kartı için ayrı ayrı olmak üzere birbirinden farklı üç adet MAC adresine sahip olacaktır.

Kablolu ve Kablosuz İletişim Ortamları

Birinci ünitede daha geniş anlatılan kablolu ve kablosuz iletişim ortamları, iki ağ kartının veri alışverişini sağlayan ortam olarak düşünülmektedir. En çok kullanılan kablolu ortamlar Eşeksenli Kablo (Coaxial Cable), Bükümlü Çift Kablo (UTP) ve Fiber Optik kablodur. Bükümlü Çift Kablo, ağ kartları ile en çok kullanılan kablo türüdür ve birçok çeşidi ile farklı hızları desteklemektedir. Kablosuz iletişimde de farklı hızları destekleyen ağ kartı çeşitleri bulunmaktadır. Aynı zamanda GSM tarafından kullanılan üçüncü nesil ve dördüncü nesil bağlantı ortamları da kablosuz ortama örnek teşkil etmektedir.

Protokoller

Her ağ bağlantısı, düzenli bir biçimde veri alışverişinde bulunmak için bazı kurallara ihtiyaç duymaktadır. Bu kurallar, protokoller olarak isimlendirilmiştir. TCP/IP modeline göre dört katman altında toplanan protokoller, uygulamanın alıcı bilgisayara ileteceği veriyi yaratmasıyla devreye girer ve sırası ile uygulama katmanı protokolleri, taşıma katmanı protokolleri, ağ katmanı protokolleri ve veri erişim katmanı protokollerinden gerekli olanlar tarafından işlenerek fiziksel ağa iletilir. Alıcı bilgisayar, ağ ortamından aldığı veriyi bu sefer tersten olmak üzere aynı katmanlardaki protokoller yardımıyla işleyerek uygulamaya teslim eder.

Tekrarlayıcılar (Repeaters) ve Göbek Cihazlar (Hubs)

Ağ ortamının, sadece bilgisayarlar ve onları birbirine bağlayan kablolu ya da kablosuz ortamlardan oluşmadığından bahsedilmiştir. Ağı bir araya getirmek için farklı dağıtıcı ve yönlendirici cihazlara da ihtiyaç duyulmaktadır. Tekrarlayıcılar bunlardan en basit olanıdır. İki arayüzü bulunan cihaz, bir taraftan aldığı veriyi, güçlendirerek diğer arayüzünden tekrar göndermektedir. Özellikle UTP kablo menzilinin 100 metre civarında olduğu düşünülürse daha uzun mesafelerde veri taşımak için tekrarlayıcılardan faydalanılmaktadır. Kablolu ağları UTP kablo ile oluştururken verinin kodlanması için farklı seviyelerde voltaja ihtiyaç duyulur. Tekrarlayıcı cihaz, bir arayüzünden aldığı zayıflamaya başlamış voltaj seviyesini (veriyi) güçlendirerek diğer çıkışından göndermektedir. Bu sayede verinin iletim menzili uzamaktadır. Kablosuz ortamda da aynı şekilde zayıflamaya başlayan ağ yayınını alıp kuvvetlendirerek tekrar veren ara cihazlar bulunmaktadır.

Tekrarlayıcı cihazın çok arayüze sahip olanına ise Göbek Cihaz (Hub) adı verilmektedir. Göbek cihaz, bir arayüzünden aldığı veriyi, diğer tüm arayüzlerine güçlendirerek göndermekte ve bu sayede aynı anda bağlantı yapan çok sayıda cihaza verinin ulaşması sağlanmaktadır.

Hem tekrarlayıcı hem de göbek cihaz TCP/IP modelinin fiziksel katmanında çalışan cihazlardır ve bağlantı katmanının görevlerini üstlenmezler. Bazı durumlarda özel bir takım tekrarlayıcı ya da göbek cihazlar, hat genişliği, çarpışma oranı vb. ağ istatistikleri için verilerin toplanmasına imkân sağlamaktadırlar.

Köprüler (Bridges) ve Anahtar Cihazlar (Switches)

Tekrarlayıcıların birinci katmanda çalışıyor olması güvenlik açıkları, seçimli göndermenin mümkün olamaması gibi bazı sorunları beraberinde getirmektedir. İkinci katman cihazlar olan köprüler sayesinde ağ bağlantıları, ağı iki farklı bölüme ayıracak şekilde düzenlenmektedir. İki arayüze sahip köprüler, paketlerin başlığında bulunan MAC adreslerine göre seçimli olarak veri iletimine imkân sağlamaktadır. Bu sayede iletimi gerekmeyen veriler diğer arayüze geçmemekte ve ağ kaynakları verimli biçimde kullanılmaktadır.

Köprülerin çok arayüzlü şekli olan anahtar cihazlar günümüzde oldukça yaygındır. Bir anlamda göbek cihazların akıllı sürümü olarak da nitelendirebileceğimiz **anahtar cihazlar** da ikinci katman olan bağlantı katmanında çalışmaktadır. İletilmek üzere gelen paketin MAC adresine göre seçimli iletme yapabilmesi sayesinde, diğer hatlara veri göndermeden, paketi yalnızca ilgili alıcının bulunduğu hatta yönlendirir. İletim esnasında, gönderimden önce ve gönderim esnasında dinleme yaparak gerekli ortam erişim kontrol protokollerini de yerine getirmektedir. Anahtar cihaz, topoloji olarak yıldız topolojisi kullanmaktadır. Anahtar cihazların bir özelliği de kendisine bağlı olan bilgisayar çiftlerinden aynı anda birkaçının, çarpışma olmadan veri iletimine olanak sağlamasıdır. Son yıllarda yönlendirici gibi çalışan anahtar cihazlar da kullanıma sunulmuştur.

Anahtar cihazların bir özelliği de farklı hızlardaki ağları birbiri ile haberleştirebilmektir.

Resim 2.3

Anahtar Cihaz

Yönlendiriciler (Routers)

TCP/IP modelinin üçüncü katmanında çalışan yönlendiricilerin asıl sorumluluğu, paket yönlendirmesi sayesinde küresel internete bağlı bilgisayarlar arasında paket değişimine olanak sağlamaktır. Tahmin edileceği üzere, binlerce ağ yolu ile cihazlar arası bağlantı sağlanmaktadır. Ağa bağlanan cihaz sayısının da artışı ile son yıllarda yönlendiriciler oldukça önemli hale gelmiştir. Kendisine gelen paketin IP adresine bakarak hangi arayüzden gönderileceğine karar vermek, yönlendiricinin görevidir. Paket gönderimi için doğru yolun seçimi adına yönlendiriciler, kendi içlerinde belirli algoritmalar yardımıyla oluşturulan tablolar barındırmaktadırlar. Bu tablolar, ağa bağlı cihazlar arasında paket gönderimi için en kısa, trafiği en az, maliyeti en düşük, kapasitesi en yüksek yolların seçimi ile oluşturulmaktadır. Küresel İnternet'i yaşayan bir canlı gibi düşünmek mantıklı olacaktır. Günün saatlerine göre ağ trafik yoğunluğu değişmekte, ağa yeni katılan

cihazlarla yeni ağ yolları eklenmekte ve bazı ağ yolları devreden çıkmaktadır. Yönlendiriciler, bu değişiklikleri göz önüne alarak tablolarını sürekli güncel tutmak zorundadırlar. Bu da yönlendiricilere ek bir yük getirmektedir. Yönlendirme tablosu adını verdiğimiz bu tablonun oluşturulması için farklı algoritmalar kullanılabilmektedir. Bu algoritmalar kendi içlerinde dağıtılmış (decentralized) ve küresel (global) algoritmalar olarak ikiye ayrılmaktadır. Yönlendiricilerin ağ yönetimi konusunda etkileri, diğer tüm cihazlardan fazladır. Yöneticiler, yönlendiricileri gerekli şekillerde programlayarak ağın topolojisine uygun davranmalarını, bağlı bulundukları alt ağları tanımalarını ve yönlendirme tablolarını oluşturmalarını sağlamaktadırlar.

SIRA SİZDE 2

En kısa yolu bulma algoritmalarından bir tanesi olan Dijkstra Algoritmasının ne çeşit bir yönlendirici algoritması olduğunu ve hangi mantıkla çalıştığını araştırınız.

AĞ YÖNETİM ARAÇLARI

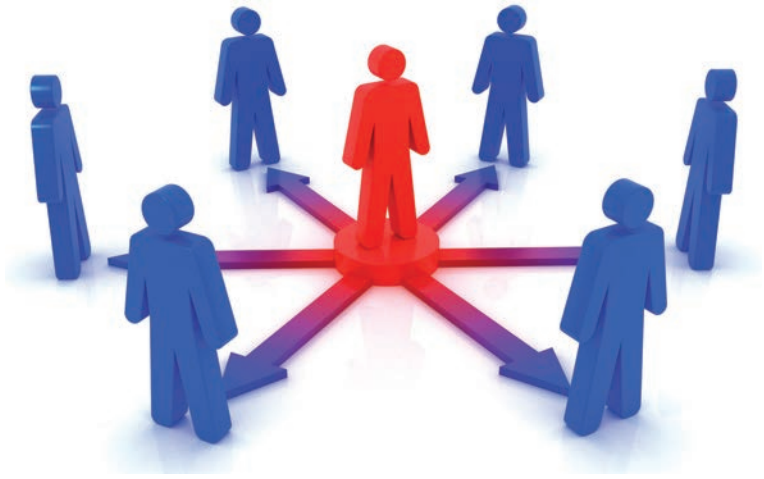
Ağ yönetiminde temel amaç, ağın büyüklüğü önemli olmaksızın, gerekli kontrolleri ve izlemeleri yaparak ağın sağlıklı çalışmasını sağlamaktır. Yukarıda bahsedilen ağ bileşenlerinden bir ya da birkaçının hatalı çalışması, tüm ağ içinde sorun yaratabilmektedir. Ağ yöneticileri bazı yöntemler ve araçlar ile ağı takip ederek verimli çalışmasını sağlamak için farklı araçlardan faydalanmaktadırlar. Bu araçlardan bazıları aşağıda açıklanmaktadır.

Bir ağ cihazında ya da yönlendiricide ağ kartının arızasını belirlemek: Ağ kartının arızalanması, eğer cihazda ise o cihazın ağ bağlantısının kesilmesi, eğer yönlendiricide ise o arayüze bağlı ağ için yönlendirme yapılamaması anlamını taşımaktadır. Sunucu bilgisayar ya da yönlendiricilerde meydana gelen bu problem ağın aksamasına, bazı hizmetlerin verilememesine sebep olmaktadır. Sorun oluşmadan önce çözüm bulabilmek adına ağ yöneticileri belirli yazılımlarla ağı izlemektedirler. Ağ kartına iletilen paketlerde sorunlar çıkmaya başlaması, ağ kartının arızalanacağının sinyali olarak yorumlanabilmektedir. Bu durumda ağ yöneticisi, kart tamamen işlevsiz kalmadan önce müdahale ederek ağ ortamının sorun yaşamasını önleyebilir.

Sistemi İzlemek: Ağ yöneticisi, sisteme bağlı cihazların aktivitelerini periyodik olarak izlemektedir. Yönetici bilgisi dışında devre dışı kalan bir cihaz ağ problemine sebep olmaktadır. Bu sebeple kullanıcının bilgisi dışında kapanan cihazlara karşı acil önlem almak, cihazın tekrar faaliyete girmesini sağlamak ya da arıza durumunda onarım ve yenisi ile değiştirmek gibi işlemler gerçekleştirilmelidir.

Kaynak Dağılımı için Ağ Trafiğini İzlemek: Kaynakları ortak kullanan ağlarda, kullanıcıların tamamı yeterli kaynağa sahip olmak istemektedirler. Hiçbir ek cihaz maliyeti olmadan yeterli kaynağa sahip olmak tüm kullanıcılar için gerekliliktir. Ağ yöneticisi, yerel alan ağlarının içerisinde ve yerel alan ağları arasında gerçekleşen trafiği izlemekte ve bu izleme aracılığıyla ağın verimliliğini de tespit etmektedir. Herhangi bir yerel alan ağında ya da ağlar arasında trafiğin aşırı artması, ağın kapasitesinin üzerine çıkması, tıkanıklığa (congestion) yol açmakta ve veri paketi kayıpları oluşmaktadır. Yönlendiricilerin, kendilerine ulaşan bir paketin IP adresine bakarak en doğru yoldan gönderilmesi işlemini gerçekleştirdiğinden yukarıda bahsedilmiştir. Bir yönlendiriciye işlemci gücünü aşan sayıda paket gelmesi durumunda, bu paketlerin bir kısmı yönlendirici belleğinde işlenmek üzere saklanmaktadır. Bellek dolduktan sonra gelen paketleri ise alamayacağı için veri paketleri kaybolmaktadır. Paketin kaybolması, aynı paketin göndericiden alıcıya tekrar gönderilmesini gerektirmekte ve bu da ağın verimliliğini doğrudan negatif olarak etkilemektedir. Trafiğin izlenmesi sırasında bazı yazılımlar sayesinde tıkanıklık seviyesi artan bölgeler ağ yöneticisine bildirilmektedir. Ağ yöneticisi gerekli önlemleri alarak kullanıcıların gerek duyduğu ağ verimliliğini sağlamaktadır.

Resim 2.4



Kaynakların Eşit Dağıtılmasından Ağ Yöneticisi Sorumludur

Yönlendirme tablolarındaki hızlı değişiklikleri belirlemek: Yönlendiricilerin, belirli algoritmalar yardımıyla veri paketlerinin izleyeceği en uygun yolları hesaplayarak, bu bilgileri yönlendirme tablolarında tuttuklarından ünitenin önceki bölümlerinde bahsedilmiştir. Aynı zaman da bu tabloların sürekli güncellendiği ve ağın aslında yaşayan bir sisteme benzetilebileceği de belirtilmiştir. Yönlendirme tablolarında olan hızlı değişimler, bir ağ ortamının devre dışı kalması sonucunda gerçekleşebilmektedir. Ağ yöneticisi, yönlendirme tablolarında olan değişiklikleri izleyerek, ağ ortamlarının değişiklikleri ve arızalı ortamların onarımı ile ilgili işlemleri yapmaktadır.

İstatistiklerin İzlenmesi: Veri paketlerinin ağ ortamında ilerleyişi sayesinde elde edilen istatistikler önemli değerlerdir. Bu istatistikler servislerin imkânları, hattın çıkış gücü, paket ulaşımındaki gecikme, varış bilgileri, paketin hasar görüp görmediği vb. değerlerdir. Bu verilere dayanarak ağ yöneticisi, ağ ve ağın performansı hakkında bilgiye sahip olmaktadır. Bu değerlerdeki değişimler, ağda problem olma olasılığını arttırmakta ve ağ yöneticisi gerekli durumlarda ağa müdahale edebilmektedir.

Ağa izinsiz girişleri tespit etmek: Ağ ortamında izinsiz girişler, hem ağa hem de ağa bağlı bulunan cihazlara saldırı niteliği taşımaktadır. İzinsiz girişlerin çoğunluğu, ağ sunucularına yapılan ağ saldırılarından oluştuğu için, ağa da zarar vermektedir. Ağ yöneticileri bu tür durumlarda gerekli önlemleri almaktadır. Ağa yapılan bir saldırı türü de ağ üzerindeki veri paketlerini yetkisiz olarak okumak ve içeriğindeki bilgileri elde etmek üzerinedir. Ağ yöneticisi, yetkisiz kişilerin veri paketlerini almasını da engellemek durumundadır. Ağ üzerinde gerçekleştirilen yetkisiz girişler ve saldırılar, izleyen ünitelerde detaylı olarak anlatılmaktadır.

AĞ YÖNETİM ÇEŞİTLERİ

Bir önceki konuda bahsedilen ağ yönetim araçlarından sonra, Uluslararası Standartlar Teşkilatı (**ISO**–International Organization for Standardization) tarafından oluşturulan ağ yönetim modelinden bahsetmek yerinde olacaktır. Bu model beş farklı kategoriye göre ağ yönetimini sınıflandırmaktadır. Ağ yöneticisi, sınıfına giren yönetim tipine göre gerekli ağ yönetim aracı ile ağ hakkında bilgi toplamaktadır. Problem çıkması durumunda yukarıda bahsedilen araca göre önlemini almakta ve ağın sağlıklı çalışmasını sağlamaktadır. Bu beş kategori Performans Yönetimi, Hata Yönetimi, Yapılandırma Yönetimi, Hesaplama Yönetimi ve Güvenlik Yönetimidir. Ünitenin devamında bu beş alan incelenmektedir:

ISO (International Organization for Standardization), Uluslararası Standartlar Teşkilâtı, Uluslararası Elektroteknik Komisyonu'nun çalışma sahasına giren elektrik ve elektronik mühendisliği konuları dışında, bütün teknik ve teknik dışı dallardaki standartların belirlenmesi çalışmalarını yürütmek amacıyla 1946'da Cenevre'de kurulan uluslararası teşkilâttır.

Performans Yönetimi: Performans yönetiminin asıl amacı, ağın verimliliğinin, çıkış gücü kavramlarının ele alınarak ölçülmesi, analiz edilmesi, raporlanması ve kontrol edilmesine dayanmaktadır. Bu ölçümlerde ağa bağlı bilgisayarların birinden diğerine veri akışı esas alındığı halde, zaman zaman ara cihazlar yani anahtar cihazlar ya da yönlendiricilerin performansı da önemli olmaktadır. Performans yönetiminde önemli protokollerden birisi olan Basit Ağ Yönetim Protokolü (SNMP–Simple Network Management Protocol) ilerleyen bölümlerde daha detaylı olarak incelenmektedir.

Hata Yönetimi: Hata yönetimi, ağın arızalarını kaydetmek ve raporlamak ve gerekli aksiyonları almak için geliştirilmiştir. Performans yönetimi ile belirli durumlarda karıştırılmasına rağmen, hata yönetimi anlık olarak hata durumlarında devreye giren, performans yönetimi ise daha uzun vadeli verilerle çalışan bir sistemdir. Basit Ağ Yönetim Protokolü hata yönetimine de yardımcı bir protokoldür.

Yapılandırma Yönetimi: Yapılandırma yönetimi sayesinde ağ yöneticisi, ağa bağlı bulunan cihazların durumları ve yapılandırmaları konusunda bilgi sahibi olmaktadır. Özellikle IP adresini esas alarak çalışan yönlendiriciler, ağa bağlanmadan önce belirli yapılandırmalara sahip olmalıdır. Bu yapılandırmalar sayesinde arayüzlerine bağlı bulunan alt ağ bilgisine, ağın diğer tarafında bulunan yönlendirici ya da yerel alan ağları bilgilerine sahip olmaktadır. Bağlantı sağlandıktan sonra da eğer gerekli ise yapılandırmalarda değişiklik yapılarak ağın sağlıklı çalışması sağlanmaktadır.

Hesaplama Yönetimi: Hesaplama yönetimi, ağ kaynaklarının, ağ cihazları tarafından nasıl kullanıldığı ile ilgilidir. Örneğin; ev kullanıcısı olarak internete bağlanmak üzere bir ADSL ağında kotalı internet hizmetinden faydalanıldığını düşünelim. İnternet hizmetinden faydalandıkça kotanın dolması, tamamen dolduktan sonra farklı ücretlendirme yapılması gibi konular hesaplama yönetiminin konu başlıkları arasında bulunmaktadır.

Resim 2.5

Temsili Ağ Yönetimi

Güvenlik Yönetimi: Güvenlik yönetimi, ağa bağlantı yapan kaynakların, ağın izin verdiği yazılımlarla bağlantı sağlaması anlamına gelmektedir. Dışarıdan yetkisiz girişler ve ağa ya da ağ cihazlarına zarar verecek şekilde geliştirilen yazılımların yasaklanması ya da pasif hale getirilmesi konusu, güvenlik yönetiminin alanıdır.

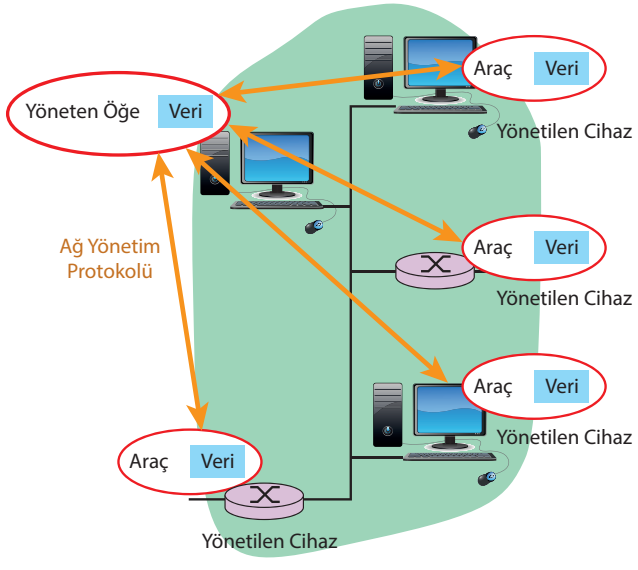
Ağ yönetimi şu ana kadar, sadece çalışan bir ağ ve onun üzerinde yapılan işlemler olarak tanımlanmıştır. Ağ yöneticileri çoğu zaman ağ kurulumundan önce, ağın tasarlanması aşamasında da yer almaktadırlar. Bir üniversite kampüsüne ağ kurulacağını varsayalım. Ağ yöneticileri öncelikle kullanılacak bilgisayar ve bilgisayar özelliği taşıyan cihaz sayısını bilmek isteyeceklerdir. Bu sayıya uygun olarak, gerekli kablolu ve kablosuz ağ ortamlarını

tasarlayacaklardır. Kablosuz ağda oluşabilecek etkilenmeler, hız azlığı gibi dezavantajlarla birlikte, kablolu ağda da maliyet faktörünü ön plana çıkarmaktadır. Cihazların tamamının ağdan faydalanmasını sağlamak için anahtar cihazlar ya da kablosuz vericilerden faydalanılacaktır. Kampüs eğer büyük bir alanda ise yönlendiricilerin yardımıyla ağ, alt ağlara bölünecek ve gerekli IP adres düzenlemeleri sağlanacaktır. Tüm bu işlemler tamamlandıktan sonra dışarıya çıkış yani İnternet bağlantısı için gerekli çalışmalar başlatılacak, gerekiyorsa İnternet Servis Sağlayıcı ile bir fiber optik bağlantısı yapılacaktır. Kampüs sistemi düşünüldüğüne göre güvenlik önemlidir. Dışarıdan ağa yapılacak saldırılara karşı bir Ateş Duvarı (Firewall) kullanımı gerekecektir. Web sayfası ve e-posta hizmetleri kampüs içerisinde bulunacaksa, bunlar için sunucular atanacak ve kurulumu gerçekleştirilecektir. Sayılan özellikler gibi birçok donanımsal ve yazılımsal destek konularında ağ yöneticisinden destek almak gerekmektedir. Ünitemizde ağ yönetimi, ağın kurulumundan itibaren değil, kurulu bir ağ üzerinde incelenmektedir. Bu sebeple ağın kurulumu için gerekli aşamalar yerine, çalışan sistemin izlenmesi, denetlenmesi, hatalarının bulunması ve gerekli düzeltme ve düzenlemelerin yapılmasına yönelik protokoller anlatılmaktadır.

AĞ YÖNETİM ALT YAPISI

Ağ yönetiminin basit anlamda ağı izlemek, yönetmek ve gerekli durumlarda müdahale etmek olduğu yukarıda anlatılmaktadır. Bu işlemlerin yapılabilmesi için öncelikle bu koşullara uygun alt yapının oluşturulması gerekmektedir. Ağ hakkında bilgi sahibi olmak, ağ istatistiklerini toplamak, ağı yapılandırmak ve ağ güvenliğini sağlayabilmek için ayrı ayrı protokollerden faydalanılmaktadır. Gerekli durumda ağa müdahale etmek ve gerekli değişiklikleri yapmak için doğru bir alt yapı ile ağa bağlanılması gerekmektedir.

Bir anlamda ağ yönetimi alt yapısı, bir işyerindeki ilişkiler ile örneklendirilebilir. Birçok alt birimden oluşan büyük bir ticari işletme düşünelim. Bu firmanın birçok alt birim çalışanı, alt birim yöneticisi, genel müdür yardımcıları ve genel müdür gibi çalışanları olduğunu varsayarsak herkesin gerekli verileri üst birimlere aktarması gerekmektedir. Üst yöneticiler, satış, gider, kasa gibi verileri her gün sonunda edinmek isterler. Aylık olarak genel müdür yardımcılarına hedeflerle ilgili veriler gönderilir. Genel müdür ve yardımcıları bir sorun oluşması durumunda acil olarak bilgilendirilir ve onlardan gelen direktifler doğrultusunda gerekli eylemler uygulanır. Ağ yönetimi alt yapısı da bu şekilde düşünülebilir. Üç ayrı parçadan oluşan alt yapı, yönetici öge, yönetilen cihaz ve yönetim protokolleri olarak sınıflandırılabilir.



Resim 2.6

Ağ Yönetim Alt Yapısı Örneği

Kaynak: *Computer Networking: A Top Down Approach, 4th edition. Jim Kurose, Keith Ross, Addison-Wesley, July 2007*

Ağ Yönetim Alt Yapısı Parçaları

Yönetici öge, ağ merkezinde bulunan ağ hakkında gerekli bilgileri sağlayan bir yazılımdır. Bu yazılım sayesinde ağın işlem gücü, analizleri, ağ yönetim bilgisine erişim sağlanmaktadır. Yönetici öge aynı zamanda ağ yöneticisi ile ağın haberleşmesini sağlamaktadır. Ağ yöneticisi, ağ ile ilgili ihtiyaç duyduğu verilerin tamamına bu yazılım ile sahip olmaktadır.

Yönetilen cihaz, ağa bağlı herhangi bir donanım ve bu cihazın üzerinde bulunan uygulamadan oluşmaktadır. Bu bir bilgisayar, bir programlanabilir anahtar cihaz, bir yönlendirici ya da bir modem olabilmektedir. Ağa bağlanması için kullanılan ağ kartı ara yüzü ile gerekli donanımsal ve yazılımsal değişiklikler yapılmaktadır. Tüm cihazların yapılandırması, **Yönetim Bilgi Üssünde** (MIB–Management Information Base) toplanmaktadır. Yönetim Bilgi Üssü, ret edilen IP adresleri, Ethernet paketlerindeki çarpışma hataları, DNS sunucu bilgisayar üzerindeki bilgilerin sürüm numaraları, yönlendirme yol haritaları gibi bilgilerin hepsinin tek bir yerde toplanması ile oluşturulmaktadır. Kısacası yönetilen cihazlarla ilgili tüm bilgiler bu üste toplanmaktadır. Bu bilgiler sayesinde ağ yöneticileri, ağ ve ağın işleyişi, performansı, verimliliği konularında bilgi sahibi olmakta ve gerekli değişiklikleri yapabilmektedir. Tüm yönetilen cihazlar aynı zamanda ağ yönetim aracı olarak da hizmet vermektedir.

Yönetim Bilgi Üssü, belirli bir cihazdan çok, üzerine kurulan yazılımlar sayesinde ağ yöneticisine gerekli bilgileri toplayan sanal bir depolama ünitesidir. Ağ yöneticisinin diz üstü bilgisayarı bile yazılım sayesinde Yönetim Bilgi Üssüne dönüştürülebilir. Bu cihaz, ağ yöneticisinin isteğine göre farklı lokasyonlarda işlevini gerçekleştirebilir.

Ağ alt yapısının son bileşeni, yönetim protokolleridir. Bu protokoller, yönetici öge ile yönetilen cihaz arasında bir köprü görevi görmektedir. Protokoller sayesinde yönetilen cihaz üzerindeki yönetim aracına ulaşılabilmekte ve gerekli düzenlemeler ve değişiklikler sağlanmaktadır. Şunu belirtmek gerekir ki ağ yönetim protokolleri kendi başlarına ağ yönetimi yapamazlar. Ağ yönetimi için ağ yöneticisi tarafından kullanılan bir yönetici ögeye ihtiyaç duyulmaktadır. Diğer taraftan cihazların yapılandırması ve cihazlar hakkında bilgi sağlamak için de yönetilen cihazlar üzerinde bulunan ağ yönetim araçlarından faydalanılmaktadır. Protokoller sadece yönetici öge ile yönetilen cihaz üzerindeki ağ yönetim aracının ortak bir dil kullanmasını sağlamaktadır.

SIRA SİZDE 3

Ağ yönetim alt yapısının üç bileşenini sayınız.

Standart İnternet Yönetim Yapısı

Ağ yönetiminde önerilen protokol, Basit Ağ Yönetim Protokolü (SNMP–Simple Network Management Protocol)'dür. Bir grup üniversite işbirliği ile oluşturulan Basit Ağ Geçidi İzleme Protokolü (SGMP–Simple Gateway Monitoring Protocol), SNMP'nin geliştirilmesinde öncü rol oynamıştır. Daha sonra SNMP, karşılaşılan güçlüklerle başa çıkmayı sağlayacak şekilde gelişmiştir. Ağ yönetim yapısını oluştururken şu sorulara cevap vermek önemlidir.

- İzlenecek olan nedir?
- Ağ yönetici tarafından kontrol edilecek veriler hangileridir?
- Raporlanacak ya da değişime tabi tutulacak özel form bilgisi nedir?
- Bu bilgi değişiminde kullanılacak protokoller hangileridir?

Standart internet yönetim yapısına göre ağ yönetim ögelerinin genel adı Yönetim Bilgi Üssüdür. Tüm yönetilen ögelerle ilgili bilgiler, bu üste toplanmaktadır. Bu üs aslında sanal bir depolama ünitesidir. Bir yazılım aracılığıyla herhangi bir bilgisayar, yönetim bilgi üssü olarak kullanılabilmektedir. Aynı şekilde, ağ yöneticisi ağa dâhil olduğu herhangi bir yerden de bu bilgilere ulaşabilmektedir. Bu sebeple yönetim bilgi üssü belirli bir lokasyona sahip olmak zorunda değildir.

Yönetim Bilgisinin Yapısı (SMI–Structure of Management Information) olarak da adlandırılan veri tanımlama dili, yönetim bilgisinin veri tiplerini, nesne modelini ve yazım

ve düzenlemedeki kuralları içermektedir. Yönetici öge ile yönetilen cihaz arasında gönderilen verinin biçimi, yönetim bilgisinin yapısı olarak da adlandırılabilmektedir.

Kurallar dizesi olarak adlandırılan protokoller olmadan veri iletişimi olanaksızdır. Gönderilen verinin alıcı tarafından anlaşılır halde karşı tarafa ulaşmasını sağlayan, protokollerdir. Bu sebeple yönetici öge ve yönetilen cihaz arasındaki veri trafiği de protokollere bağlı bir şekilde gerçekleşmektedir. Yukarıda da bahsedildiği gibi Basit Ağ Yönetim Protokolü bu konuda kuralları belirleyen protokoldür.

Son olarak, güvenlik ve yönetim yetkilerini de dikkate almak gerekmektedir. Ağ yöneticileri dışında farklı kişilerin ağ hakkında bilgi edinmesi ve gerektiğinde cihaz yapılandırmalarını değiştirmesi, ağa saldırı olarak nitelendirilir. Ağın belirli bir bölümünün ya da tamamının işlevsiz hale gelmesine sebep olacak bu tür bir olaya sebebiyet vermeden yetkilerin ve güvenlik ayarlarının yapılması gerekmektedir. Basit ağ yönetim protokolünün her çıkan üst sürümünde, bir öncekine göre yönetim yetkileri ve güvenlik konusunda gelişmeler olmaktadır.

Resim 2.7

Güvenlik, Ağ Yönetiminde Önemlidir

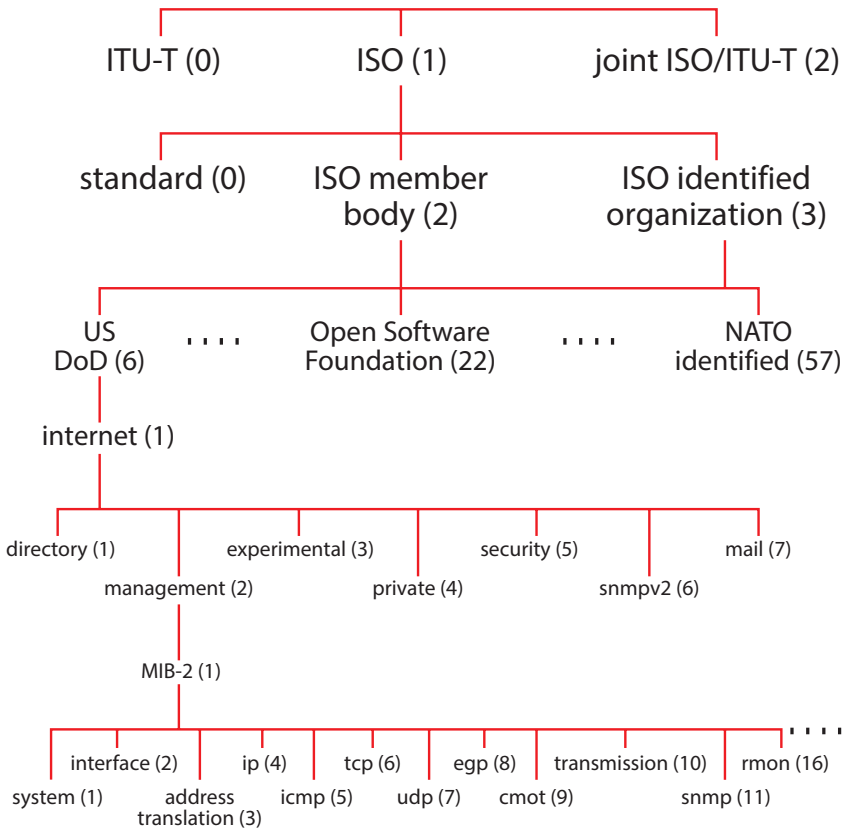
SNMP PROTOKOLÜ

Bilgi ağlarının genişlemesiyle yönetim ihtiyacı ortaya çıkmıştır. Ağa bağlanan bilgisayar sayısının artması ve farklı coğrafi bölgelere genişlemesi, anahtar cihaz ve yönlendirici kullanımını zorunlu kılmaktadır. Ağa bağlı bulunan son kullanıcı ve ara cihaz sayısının artması, ağın yönetim ve kontrolünü zorunlu hale getirmektedir. Bu sebeple oluşturulan SNMP protokolü de TCP/IP modelinin içerisinde yer almaktadır. Esas olarak TCP/IP modeli içerisinde bulunan katmanlar ve bu katmanlara bağlı çalışan protokoller, bir gönderici cihazdan başka bir alıcı cihaza verinin sorunsuz ulaşması için gerekli kurallar dizesi olarak görev yapmaktadırlar. Fakat bu protokollerin tamamı, iki farklı bilgisayar özelliğine sahip cihazın uygulamalarının haberleşmesi konusunda altyapı sağlamaktadır. SNMP de aynı şekilde gönderici bir cihazdan, alıcı cihaza veri aktarımı ile ilgili bir protokoldür. Fakat burada cihazlardan bir tanesi üzerinde özel yazılımlar çalışan bilgisayar özelliğine sahip bir cihaz iken, bir diğeri programlanabilir anahtar, modem ya da yönlendirici gibi ağ ara cihazı olabilmektedir. SNMP protokolü dâhilinde cihazların ısı değerleri, internet bağlantı hızları, yönlendirme tabloları, çalışma süreleri vb. verileri tutmayı sağlayan ağaç yapısı mevcut bulunmaktadır. Resim 2.7'de bu ağaç yapısı görülmektedir. SNMP aracılığıyla, ağ problemlerinin tanımlanması, çözümlerin zamanında uygulanması ve genişleme durumunda kolay karar verme yetisi kazanılmaktadır. Üç farklı sürümü bulunan SNMP'nin son sürümünde, özellikle güvenlik ile ilgili güncellemeler gerçekleştirilmiştir.

Resim 2.8

Nesne Tanımlama Ağacı

Kaynak: *Computer Networking: A Top Down Approach, 4th edition. Jim Kurose, Keith Ross, Addison-Wesley, July 2007*



SNMP protokolü kullanımı için gerekli **üç bileşen,** Araç Uygulama, Yönetici Uygulama ve Ağ Yönetim Sistemidir.

Yukarıda anlatıldığı gibi SNMP kullanımı için **üç farklı bileşen** bulunmaktadır. Bunlar;

- SNMP hizmetini cihaz üzerinde çalıştırarak gerekli bilgilerin alınmasını sağlayan Araç Uygulama,
- Araç uygulamadan gerekli bilgileri alarak ağ yöneticisinin izlemesine ve bilgilerin tümüne aynı anda ulaşmasını sağlayan, gerekli durumlarda ise ağ yöneticisinin değişiklik isteklerini araç uygulamalara ileten Yönetici Uygulama,
- Yönetici birimde çalışan ve ağa bağlı tüm cihazların izlenmesi ve yönetimini sağlayan Ağ Yönetim Sistemi'dir.

Tüm bilgiler Yönetim Bilgi Üssünde depolanmaktadır. Bu bilgilerin hiyerarşik bir yapıda tutulması için Resim 2.7'de gösterilen ağaç yapısından faydalanılmaktadır. Evrensel olarak belirlenmiş ağaç yapısının düzeni sayesinde, farklı uygulamalar kullanılsa da istenilen bilgiye kolayca ulaşılmaktadır. SNMP, istek gönderme ve cevap bekleme esasıyla çalışan basit bir protokoldür. Bilgi almak istediği konu ile ilgili cihazın üzerinde bulunan araca istekte bulunmakta, araç uygulama istenen bilginin cevabını yönetici uygulamaya göndermekte ve ağ yöneticisi bilgiyi uygulama üzerinden görüntülemektedir. SNMP ikinci sürümünde, büyük veri tablolarından oluşan verileri depolamak için gerekli düzenlemeler yapılmıştır. Bu sayede veriler tek tek değil, eğer gerekliyse tablo halinde alınmaktadır. SNMP, konum olarak uzakta bulunan sunucu, yönlendirici gibi cihazlara müdahale etmek için kolaylık sağlamaktadır. Ayrıca her geçen gün karmaşıklaşan İnternet ağlarında büyük cihazların tek bir merkezden yönetilmesine de olanak sağlamaktadır. Üzerinde SNMP uygulaması kurulu bir cihaz, istenilen istatistiki verileri göndermekle birlikte, aynı

zamanda arıza durumunda ağ yöneticisinin hızlı bir şekilde haberdar olmasını da sağlamaktadır. Her ne kadar son sürümünde güvenliğe yönelik iyileştirmeler yapılmış olsa da kişisel ağlarda kullanımı yaygınlaşmamıştır. SNMP protokolünün, üzerindeki güvenlik açıklarından dolayı güvenliği sağlanmamış ağlarda kullanımı risklidir.

Güvenlik açıklarından dolayı SNMPv1 ve SNMPv2'nin kişisel ağlarda kullanımı konusunda temkinli davranılmalıdır.

SNMPv1'in, araç uygulamadaki bir değere ulaşmak için ve tablodaki bir sonraki değeri okumak için kullanacağı komutları araştırınız.

Özet

AMAÇ 1 *Ağ yönetiminin gerekliliğini açıklamak*

Büyük bilgi ağlarının yönetime ihtiyacı bulunmaktadır. Ağ yöneticisinin ağı izlemesi, gerekli durumlarda müdahale etmesi ve arıza durumunda arızanın giderilmesi için gerekli işlemleri gerçekleştirmesi; bilgi ağının performansı, verimli çalışması ve kullanıcılara eşit kaynak dağılımı için gerekmektedir.

AMAÇ 2 *Ağı oluşturan bileşenleri ifade etmek*

Bilgi ağları oluşturulurken birçok farklı donanımdan faydalanılmaktadır. Bunlardan en önemlisi, üzerinde en az bir işletim sistemine sahip bilgisayarlardır. Bilgisayarların ağ ortamına dâhil olabilmeleri için kablolu ya da kablosuz ağ kartına ihtiyaçları bulunmaktadır. Ağ, veri iletimini gerçekleştirebilmek için tekrarlayıcı, göbek cihaz, köprü, anahtar cihaz, modem ve yönlendirici gibi ara cihazlara da ihtiyaç duymaktadır. Bu cihazlar sayesinde veriler, en uygun yolu izleyerek gönderen bilgisayardan, alıcı bilgisayara doğru yol almaktadırlar.

AMAÇ 3 *Ağ yönetim araçlarını tanımlamak*

Ağ yönetim araçları, ağın sağlıklı çalışması için gerekli belirlemeleri ve izlemeleri yapacak olan araçlardan oluşmaktadır. Bu araçların asıl amacı, ağda kesinti olmadan önce arıza çıkarabilecek kısımları tespit etmek ve önlem almaktır. Ağ yönetim araçları, bir ağ cihazında ya da yönlendiricide ağ kartının arızasını belirlemek, sistemi izlemek, kaynak dağılımı için ağ trafiğini izlemek, yönlendirme tablolarındaki hızlı değişiklikleri belirlemek, istatistiklerin izlenmesi ve ağa izinsiz girişleri tespit etmek olarak sınıflandırılabilir.

AMAÇ 4 *Ağ yönetim çeşitlerini tanımlamak*

Ağ yönetim çeşitleri, Uluslararası Standartlar Teşkilatı tarafından oluşturulan ağ yönetim modeline göre beş farklı kategoride ağ yönetimini sınıflandırılmaktadır. Bunlar Performans Yönetimi, Hata Yönetimi, Yapılandırma Yönetimi, Hesaplama Yönetimi ve Güvenlik Yönetimidir.

AMAÇ 5 *Ağ yönetim alt yapısını açıklamak*

Ağ yönetim alt yapısı, yönetici öge, yönetilen cihaz ve yönetim protokolleri alt bileşenlerinden oluşur. Standart İnternet Yönetim Yapısına göre verilerin tamamı Yönetim Bilgi Üssünde toplanmaktadır. Ağ cihazlarında çalışan araç uygulamalar yardımıyla toplanan veriler, ağ yöneticisi tarafından değerlendirilerek gerekli önlemler alınır ve işlemler yapılır.

AMAÇ 6 *SNMP protokolü işlemlerini tanımlamak*

Basit Ağ Yönetim Protokolü olan SNMP, araç uygulamalara istek göndermek ve gelen istekleri Yönetim Bilgi Üssündeki ağaç yapısında tutmak esasıyla çalışmaktadır. Üç farklı sürümü olan SNMP, günümüzde en yaygın kullanılan ağ yönetim protokolüdür.

Kendimizi Sınayalım

1. Bilgisayarlarda donanım ile kullanıcı arasında arayüz görevi üstlenen yazılım türü aşağıdakilerden hangisidir?

a. Uygulama Yazılımları
b. Yönetim Bilgi Üssü
c. İşletim Sistemleri
d. Araç Uygulaması
e. Yönetilen Cihaz

2. Aşağıdaki donanımlardan hangisi çok kapılı tekrarlayıcıdır?

a. Modem
b. Köprü
c. Anahtar Cihaz
d. Yönlendirici
e. Göbek Cihaz

3. MAC adreslerini, içerisinde bulunan bir tabloda saklayarak seçimli gönderim yapan çok kapılı cihaz aşağıdakilerden hangisidir?

a. Modem
b. Köprü
c. Anahtar Cihaz
d. Yönlendirici
e. Göbek Cihaz

4. Aşağıdakilerden hangisi ağ yönetimi için kullanılan araçlardan biri **değildir?**

a. İstatistiklerin İzlenmesi
b. Yönlendirme Tablolarının İzlenmesi
c. Sistem Isısının İzlenmesi
d. Yetkisiz Girişlerin İzlenmesi
e. Sistemin İzlenmesi

5. Aşağıdakilerden hangisi ağ yönetim çeşitlerini beş kategoride sınıflandıran kuruluşun kısaltmasıdır?

a. TCP/IP
b. ISO
c. ICANN
d. IEEE
e. OSI

6. Aşağıdakilerden hangisi bir ağ yönetim çeşidi **değildir?**

a. Performans Yönetimi
b. Hata Yönetimi
c. Yapılandırma Yönetimi
d. Güvenlik Yönetimi
e. IP Adresi Yönetimi

7. Ağ hakkında bilgi sağlayarak, gerektiğinde değişiklikleri bildirmeyi kolaylaştıran yazılım aşağıdakilerden hangisidir?

a. Yönetici Öğe
b. Yönetilen Cihaz
c. Yönetim Bilgi Üssü
d. Yönetim Protokolü
e. Araç Uygulaması

8. Aşağıdakilerden hangisi veri tanımlama dili, yönetim bilgisinin veri tipleri, nesne modeli ve yazım ve düzenlemedeki kuralları içermektedir?

a. Yönetici Öğe
b. Yönetim Bilgi Üssü
c. Yönetilen Öğe
d. Yönetim Bilgi Yapısı
e. SNMP

9. SNMP protokolünün geliştirilmesinde rol oynayan kontrol protokolü aşağıdakilerden hangisidir?

a. FTP
b. SMTP
c. SGMP
d. SIP
e. UDP

10. SNMP üzerinde güvenlik güncelleştirmeleri aşağıdaki sürümlerden hangisi ile kullanıma sunulmuştur?

a. SNMPv1
b. SNMPv2
c. SNMPv3
d. SNMPv4
e. SNMPv5

Kendimizi Sınayalım Yanıt Anahtarı

1. c	Yanıtınız yanlış ise "Ağ Bileşenleri" konusunu yeniden gözden geçiriniz.
2. e	Yanıtınız yanlış ise "Ağ Bileşenleri" konusunu yeniden gözden geçiriniz.
3. c	Yanıtınız yanlış ise "Ağ Bileşenleri" konusunu yeniden gözden geçiriniz.
4. c	Yanıtınız yanlış ise "Ağ Yönetim Araçları" konusunu yeniden gözden geçiriniz.
5. b	Yanıtınız yanlış ise "Ağ Yönetim Çeşitleri" konusunu yeniden gözden geçiriniz.
6. e	Yanıtınız yanlış ise "Ağ Yönetim Çeşitleri" konusunu yeniden gözden geçiriniz.
7. a	Yanıtınız yanlış ise "Ağ Yönetim Alt Yapısı" konusunu yeniden gözden geçiriniz.
8. d	Yanıtınız yanlış ise "Ağ Yönetim Alt Yapısı" konusunu yeniden gözden geçiriniz.
9. c	Yanıtınız yanlış ise "Ağ Yönetim Alt Yapısı" konusunu yeniden gözden geçiriniz.
10. c	Yanıtınız yanlış ise "SNMP Protokolü" konusunu yeniden gözden geçiriniz.

Sıra Sizde Yanıt Anahtarı

Sıra Sizde 1

Google firması tarafından geliştirilen mobil işletim sistemi, birçok akıllı telefon ve tablette kullanılmakta olan Android işletim sistemidir.

Sıra Sizde 2

Dijkstra Algoritması, küresel bir yönlendirme tablosu oluşturma algoritması olarak kullanılmaktadır. Tüm ağ hakkında bilgi sahibi olmak ve iki nokta arasındaki en az maliyetli yolu hesaplama işlemini, tüm ağ üzerinde gerçekleştirmek üzere kullanılmaktadır.

Sıra Sizde 3

Ağ yönetim alt yapısının üç bileşeni, yönetici öge, yönetilen cihaz ve yönetim protokolleridir.

Sıra Sizde 4

SNMPv1'in, araç uygulamadaki bir değere ulaşmak için istek göndermesini sağlayan komut "GET" komutudur. Tablodaki bir sonraki değeri okumak için kullanacağı komut ise "GET-NEXT" komutudur.

Yararlanılan ve Başvurulabilecek Kaynaklar

Computer Networking: A Top Down Approach, *4th* edition. Jim Kurose, Keith Ross Addison-Wesley, July 2007.

ISO standardı, Wikipedia, https://goo.gl/o5Eeqv

SNMP, Wikipedia, https://goo.gl/DCB6rF

3

Amaçlarımız

Bu üniteyi tamamladıktan sonra;

- Bilgi güvenliği kavramı ve ihtiyacını açıklayabilecek,
- Klasik şifreleme algoritmalarını açıklayabilecek,
- Dizi ve blok şifreleme arasındaki farkları sıralayabilecek,
- Rastgele sayılar arasındaki farkları açıklayabilecek,
- DES ve AES şifreleme yöntemlerinin çalışma prensiplerini tanımlayabilecek bilgi ve becerilere sahip olacaksınız.

Anahtar Kavramlar

- Simetrik Şifreleme
- Dizi Şifreleme
- Blok Şifreleme
- DES
- AES
- Blok Şifreleme Metotları

İçindekiler

Simetrik Şifreleme ve Mesaj Gizliliği

GİRİŞ

Bilginin güvenli bir şekilde iletilmesi ihtiyacı çok eski zamanlara dayanır. İlk gizli bilgi paylaşımı yöntemleri, savaş ortamında hükümdarın verdiği emirlerin, düşman kuvvetlerinin eline geçmeden askerlerini yönetmek amacıyla kullanılması için ortaya çıkmıştır (Trappe ve Washington, 2006). Zaman içinde bilişim teknolojilerinin gelişmesiyle, haberleşme, savunma, bankacılık gibi birçok alanda bilginin gizli olarak, değişime uğramadan iletilmesi ve sadece yetkili kişiler tarafından okunması ihtiyacı artan bir öneme sahip olmuştur.

Kriptoloji, kriptografi ve kriptoanaliz olmak üzere ikiye ayrılır (Paar ve Pelzl, 2010). Kriptografi güvenli veri paylaşımı için gerekli algoritmaları ve protokolleri ortaya koyar. Kriptoanaliz ise kriptografik algoritmaların, varsa açıklarını tespit ederek, onları kırmaya çalışır. Kriptoanaliz ile ilgilenen ve üzerinde araştırmalar yapan iki grup vardır. Birinci grup, algoritmalardaki açıkları ve eksiklikleri tespit ederek, kendilerine çıkar sağlamaya çalışan kişilerden oluşur. İkinci grupta yer alan kimseler ise genellikle bilim adamlarından oluşur ve algoritmaların varsa açıklarını tespit ederek, kimse zarar görmeden bu açıkların giderilmesini sağlarlar. Birinci grupta yer alan kimseler genelde kötü niyetli kişiler ya da saldırganlar olarak adlandırılır. Bunlar, şifreleme algoritmalarındaki açıkları tespit edip şifrelenmiş mesajları çözerek gizli veriye ulaşmayı amaçlarlar. İkinci grup insanlar iyi niyetlidirler ve güvenli iletişim ortamı sağlanması amacıyla araştırmalar yapmaktadırlar. Saldırganların şifreleme sistemlerine yaptıkları saldırılara karşı şifreleme sistemlerinin ilgili açıklarını ve eksikliklerini gidermeye çalışırlar. Geçmişten günümüze kötü niyetli kişiler şifreleme sistemlerine saldırırken, iyi niyetli kişiler de bu saldırılara karşı savunma mekanizmaları geliştirmektedir. Bu iki grubun faaliyetleri, Bilgi Güvenliği kavramını oluşturmuştur.

Kriptografi, kullanıcılar arasında güvenli bir iletişim oluşturmak için gerekli algoritmaları ve protokolleri tasarlayan ve geliştiren bilim dalıdır.

Bilgi değerli bir varlık olduğundan, güvenli bir şekilde saklanması ve gerektiğinde güvenli bir şekilde iletilmesi gerekmektedir. Bilginin güvenilir bir şekilde saklanması ve iletilmesi için farklı yöntemler kullanılabilir. Pratik uygulamalarda en çok kriptografik algoritmalar ve protokoller tercih edilir. Kriptografik algoritmalar ve protokoller dört temel alanda gruplandırılır. Bu gruplar;

- Simetrik şifreleme,
- Açık anahtar şifreleme,
- Veri bütünlüğü ve
- Kimlik doğrulama olarak sıralanabilir.

Yukarıdaki sınıflandırmaya ek olarak şifreleme algoritmaları, kullandıkları anahtar sayısına göre tek anahtar kullanan şifreleme algoritmaları (simetrik şifreleme algoritmaları), birbiri ile ilişkili iki anahtar kullanan şifreleme algoritmaları (açık anahtar şifreleme algoritmaları) ve anahtar kullanmayan algoritmalar (özet fonksiyonları) olarak üç ana başlıkta incelenebilir (Stallings, 2011). Simetrik şifrelemede tek anahtar kullanıldığından, bu şifreleme algoritmaları "tek anahtar şifreleme" ve "gizli anahtar şifreleme" algoritmaları olarak da bilinirler. Simetrik şifreleme algoritmalarına simetrik denmesinin nedeni, şifreleme ve çözme için tek ve aynı anahtarın kullanılmasıdır. Açık anahtar şifreleme algoritmalarında ise açık ve gizli olmak üzere iki anahtar kullanılır. Bunlardan biri şifreleme diğeri ise çözme işlemleri için kullanılır. Bu nedenle iki anahtarlı bu algoritmalar, asimetrik şifreleme algoritmaları olarak da adlandırılır. Özetleme algoritmaları ise veri bütünlüğünün kontrolü amacıyla kullanılmaktadır. 1976 yılına kadar yalnızca simetrik şifreleme algoritmaları kullanılmıştır. Zamanla simetrik şifreleme algoritmalarının zayıf ve eksik yönleri, açık anahtar şifreleme algoritmaları ile giderilmeye çalışılmıştır. Simetrik şifrelemede, güvenli iletişim sağlamak isteyen kullanıcıların paylaştığı tek bir anahtar olduğundan, algoritmaların güvenliği bu anahtarın yalnızca ilgili iki kullanıcı arasında bilinmesine dayanır. Eğer herhangi bir şekilde kullanıcılar arasındaki anahtar ifşa olursa, yaptıkları iletişim güvenilir olarak kabul edilmez.

Simetrik algoritmalarda, mesaj gizliliğini sağlayarak haberleşmek isteyen gönderici ve alıcı, aynı algoritmayı kullanır. Aynı anahtar hem şifreleme hem de şifre çözmek için kullanılır. Açık anahtar şifrelemede ise durum farklıdır. Kullanılan algoritma aynı olmasına rağmen şifreleme ve şifre çözmek için farklı anahtarlar kullanılır. Fakat bu anahtarlar matematiksel olarak birbiri ile bağlantılı anahtarlardır. Simetrik şifrelemede kullanılan tekil anahtar gizli tutulmalıdır. Bu anahtarı sadece gönderici ve alıcının bildiği varsayılır. Açık anahtar şifrelemede ise gizli anahtarın sadece anahtar sahibi tarafından bilinmesi gerekirken, açık anahtarın diğer kullanıcılar tarafından bilinmesinde hiçbir mahsur yoktur.

Simetrik şifreleme algoritmalarının beş temel öğesi vardır:

- **Açık metin:** Kullanıcının oluşturduğu ve güvenli şekilde paylaşmak istediği orijinal veridir ve şifreleme algoritmasının girdilerinden bir tanesidir. Açık metin, gizlenmek istenen her türlü içeriği ifade etmektedir. Açık metin bir e-posta mesajı olabileceği gibi, bir resim dosyası, bir kitap bölümü veya bir sayı dizisi de olabilir.
- **Şifreleme fonksiyonu:** Açık metnin yetkisi olmayan kişiler tarafından okunmaması için karıştırma işlemini yapma ile sorumludur. Simetrik algoritmalarda, şifreleme sırasında kullanılan iki ana fonksiyon karışıklık ve yayılma fonksiyonlarıdır. Şifreleme fonksiyonu çok sayıda birbirini takip eden karışıklık ve yayılma işlemlerinden meydana gelir.
- **Gizli anahtar:** Simetrik şifreleme algoritmalarının girdilerinden ikincisidir ve bu anahtarı yalnızca güvenli iletişim kurmak isteyen kullanıcıların bildiği kabul edilir. Simetrik şifreleme algoritmalarının güvenliği bu anahtarın gizliliğine dayandığından, gizli anahtarı yalnızca haberleşmekte olan iki kullanıcının bilmesi gerekmektedir. Bu anahtarın başkaları tarafından ele geçirilmesi, iletişimin gizliliğini ortadan kaldıracaktır.
- **Şifrelenmiş metin:** Şifreleme algoritmasının çıktısıdır. Şifrelenmiş metni elde eden kötü niyetli kişiler, kullanılan algoritmayı bilseler dahi açık metin hakkında bir çıkarımda bulunamazlar. Şifreleme algoritmalarının bütün adımları herkes tarafından bilinmektedir. Güvenliği sağlayan, gizli anahtarın haberleşen kullanıcılar dışında kimse tarafından bilinmemesi ve gizli tutulmasıdır.

- **Çözme fonksiyonu:** Çözme fonksiyonunun girdileri şifrelenmiş metin ve gizli anahtardır. Çıktı olarak ise açık metin elde edilir. Simetrik şifrelemede, şifreleme ve çözme işlemleri birbirinin tersidir. Bu nedenle açık (düz) metni şifrelemek için gerçekleştirilen tüm işlemlerin ters fonksiyonları, şifreli metni çözmek için sondan başa doğru uygulanır.

Bu temel bileşenler değişkenlerle ifade edilir. Açık veya düz metin *P*, şifrelenmiş metin *C*, gizli anahtar *K*, şifreleme fonksiyonu *E* ve çözme fonksiyonu *D* ile temsil edilir. Düz metin kümesi, olası bütün metinleri içermektedir. Buna benzer olarak, şifrelenmiş metin kümesi de açık metinlere karşı gelen şifrelenmiş metinlerden oluşur. Anahtar kümesi ise belli şartlara göre seçilebilecek sonlu sayıda anahtardan oluşmaktadır. Simetrik algoritmanın türüne göre anahtarların sağlaması gereken belli şartlar vardır. Bu şartlara göre anahtar seçimi yapıldığından, kullanılabilecek toplam anahtar sayısı sonlu sayıdadır. Şifreleme ve çözme fonksiyonlarının özelliği ise şöyle açıklanabilir. Herhangi bir düz metni şifreleme fonksiyonu ile şifreledikten sonra elde edilen şifrelenmiş metni, çözme fonksiyonu ile çözdüğümüzde orijinal açık metne ulaşmak gerekmektedir. Bu nedenle her fonksiyon şifreleme fonksiyonu olarak seçilemez.

Şifreleme fonksiyonları bire-bir ve örten fonksiyonlar olmalıdır. Neden?

SIRA SİZDE 1

Simetrik şifreleme algoritmaları, orijinal açık metnin şifrelenme yöntemine göre iki ana gruba ayrılabilir. Bu ölçüte göre simetrik algoritmalar, blok ve dizi şifreleme algoritmaları olarak sınıflandırılır. Blok şifrelemede, şifrelenecek metin bloklar şeklinde şifrelenir ve çözülür. Blok şifreleme algoritmaları, belirli uzunluktaki (blok) açık metni girdi olarak alır ve yine belirli uzunlukta şifrelenmiş metin çıktısı üretirler. Dizi şifreleme algoritmaları ise açık metinden bir bit alıp gizli anahtarı kullanarak bir bit şifrelenmiş metin üretirler.

DİZİ ŞİFRELEME

Dizi şifreleme bit tabanlı bir simetrik şifreleme yöntemidir. Bağımsız olarak, açık metinden sıradaki tek biti kayar anahtar yardımı ile işleme tabi tutar ve karşılığında bir bitlik şifrelenmiş metin üretir. Dizi şifreleme yöntemleri, eşzamanlı ve eşzamansız olmak üzere ikiye ayrılır. Eşzamanlı dizi şifrelemesinde kayan anahtar üretimi sadece kullanıcının gizli anahtarına bağlıdır. Eşzamansız dizi şifrelemede ise kayan anahtar üretimi hem kullanıcının gizli anahtarına hem de bir önceki adımda üretilmiş şifrelenmiş metine bağlıdır. Dizi şifreleme bir örnekle şöyle açıklanabilir. Şifrelenmek istenen açık metin "merhaba" olsun. Dizi şifrelemede önce açık metnin ilk karakteri olan "m" şifrelenir. Daha sonra ikinci karakter olan "e" şifrelenir. Bu şekilde açık metnin bütün karakterleri sıra ile teker teker şifrelenmiş metne dönüştürülür. Şifreli metin alıcı tarafından aynı sırayla çözülerek açık metinde yer alan harfler elde edilir.

Rastgele Sayılar

Rastgele sayılar kriptolojide büyük bir öneme sahiptir. Kriptolojik algoritmalarda kullanılacak rastgele sayıların iki önemli özelliği olmalıdır. Bu özellikler "rastgelelik" ve "tahmin edilemezlik" olarak adlandırılır. İstatistiksel olarak bir sayının rastgele olması için tekdüze dağılım göstermek ve bağımsız olmak üzere iki önemli özelliğe sahip olması gerekmektedir. Bilgisayar bilimlerinde üç farklı rastgele sayı vardır (Paar ve Pelzl, 2010).

- Gerçek rastgele sayılar,
- Sözde rastgele sayılar ve
- Kriptolojik olarak güvenli rastgele sayılar.

Gerçek Rastgele Sayılar

Para atışı işlemi sonucu gerçek rastgele sayı üretmek mümkündür. Para atışının 1.000 defa tekrar edilmesi durumunda büyük olasılıkla 500 defa tura ve 500 defa yazı gelmesi beklenir. İstatistiksel olarak bu sonuç, beklenen bir durumdur. Ama gerçekte sonuç bu şekilde çıkmayabilir. Yapılacak her para atışının tura mı yoksa yazı mı geleceği hiçbir şekilde bir önceki atıştaki sonuca bağlı değildir. Bir başka ifadeyle, para atışları birbirinden bağımsızdır. Para atışı işlemi, hem tekdüze dağılıma sahip olması hem de gelecek atışların önceki atışlara bağlı olmaması dolayısıyla rastgele sayılarda bulunması gereken iki özelliğe de sahiptir. Ancak tekrar üretilebilme özelliği yoktur. Yani 100 atış sonunda elde edilen sonucu tekrar elde etmek çok düşük bir olasılıkla mümkündür ve garanti edilemez. Gerçek rastgele sayılar bu özellikleriyle oturum anahtarı üretilmesinde kullanılmaktadır. Oturum anahtarı, her orijinal açık mesajın şifrelenmesi için birbirinden bağımsız olarak üretilen anahtar demektir. Aynı gizli anahtar bütün mesajları şifrelemek için kullanılırsa güvenlik problemi oluşabilir. Çünkü bu anahtar bir şekilde elde edilirse, bu anahtarla şifrelenen bütün mesajlara ulaşılmış olur. Ancak oturum anahtarı kullanılırsa, her mesaj için ayrı bir anahtar kullanılmış olur. Bu durumda, anahtarlardan biri ele geçirilmiş olsa bile sadece bir mesaja ulaşılmış olur. Diğer mesajlara hala ulaşılamaz ve güvenlik sağlanmış olur. Oturum anahtarları belli şartlara göre rastgele üretilir. Bu nedenle gerçek rastgele sayılarla bu anahtarları üretmek önemlidir.

Sözde Rastgele Sayılar

Birçok programlama dilinde var olan rastgele sayı üretici fonksiyonların (Örneğin; Java programlama dilinde Math.random()) ürettiği rastgele sayılar bu grupta yer alır. Bu fonksiyonlar belirli bir matematiksel fonksiyona bağlı olarak rastgele sayı üretirler. Dolayısıyla belirli sayıda üretilen rastgele sayı kullanılarak, ilgili matematiksel fonksiyona ait katsayılar hesaplanabilir. Sözde rastgele sayı fonksiyonları tekdüze dağılıma sahip olacak şekilde tasarlanmışlardır. Üretilen bir sayı dizisini, başlangıç parametreleri ve fonksiyon katsayılarının bilinmesi halinde tekrar üretmek mümkündür. Buna karşın, bir sonra üretilecek sayının tahmin edilmesi mümkün olduğu için kriptoloji algoritmalarında kullanım alanı sınırlıdır.

Kriptolojik Olarak Güvenli Rastgele Sayılar

Tekdüze dağılıma sahip, bir sonraki adımda üretilecek sayının tahmin edilemediği ve başlangıç parametrelerinin bilinmesi durumunda aynı sayı dizisinin tekrar üretilebildiği rastgele sayılar bu grupta yer alır. Kriptolojik olarak güvenli rastgele sayılar dizi şifreleme algoritmalarında büyük bir öneme sahiptir.

Tek Zamanlı Blok

Simetrik şifrelemede bir kullanımlık oturum anahtarları kullanmak önemlidir. Kullanılacak gizli anahtarın, şifrelenecek açık veya düz metnin uzunluğu kadar olması ve sadece bir kez kullanılması durumunda, şifrelenmiş metni ele geçiren saldırgan, hiçbir matematiksel yöntem ile ne orijinal açık metni ne de gizli anahtarı elde edebilir. Bu tür yöntemlere, teorik olarak kırılamaz sistemler adı verilir. x, y ve k değişkenlerinin 0 veya 1 değerine sahip olabileceği varsayılması durumunda şifreleme ve çözme fonksiyonları oldukça basittir.

Şifreleme fonksiyonu: $y_i = x_i + k_i \bmod 2$
Çözme fonksiyonu: $x_i = y_i + k_i \bmod 2$

Tek zamanlı blok veya bir kullanımlık oturum anahtarı ile şifrelemenin ve şifre çözmenin nasıl gerçekleştirildiğini sırasıyla Tablo 3.1 ve Tablo 3.2'deki gibi basit bir örnekle açıklayabiliriz.

Açık Metin	0	0	1	1	1	0	0	0
Anahtar Dizisi	1	1	1	0	0	1	1	0
Şifrelenmiş Metin	1	1	0	1	1	1	1	0

Tablo 3.1
Tek zamanlı blok ile şifreleme örneği

Şifrelenmiş Metin	1	1	0	1	1	1	1	0
Anahtar Dizisi	1	1	1	0	0	1	1	0
Açık Metin	0	0	1	1	1	0	0	0

Tablo 3.2
Tek zamanlı blok ile çözme örneği

Şifreleme ve çözme fonksiyonları bit tabanlı oldukları için aslında yapılan işlem, iki bitin XOR (eXclusive OR) fonksiyonuna tabi tutulması ile elde edilir. Tablo 3.1 ve Tablo 3.2'deki örnekte görüldüğü gibi XOR bit operasyonunda girdi olan iki bit aynı ise sonuç 0, farklı ise sonuç 1 değerini alır. Tablo 3.3'de görüldüğü gibi XOR operatörü ½ olasılıkla 0, ½ olasılıkla 1 değerini üretir. 0 veya 1 değerini üretme olasılıklarının eşit olması arzu edilen bir özelliktir.

x_i	k_i	y_i
0	0	0
0	1	1
1	0	1
1	1	0

Tablo 3.3
XOR doğruluk tablosu

Tek zamanlı blok, bütüncül güvenlik sağlayan bir şifreleme yöntemidir. Fakat uygulamada bazı zorluklar ortaya çıkmaktadır. Gizli anahtarın mesaj ile aynı uzunlukta olması ve tamamen gerçek rastgele sayılar kullanılarak elde edilmesi bu zorluklardan ikisidir. Ayrıca oluşturulacak gizli anahtarın güvenli bir yol ile iletişime geçilecek kullanıcıya ulaştırılması gerekmektedir. Son olarak, bu işlemin her bir şifreli mesaj için tekrar edilmesi gerekmektedir. Bütün bu zorluklar tek zamanlı blok yönteminin kullanımını sınırlandırmaktadır.

RC4

Tek zamanlı blok yönteminin uygulamasında karşılaşılan zorlukları ortadan kaldırmak için sonsuz kayan anahtar yerine, belirli uzunlukta anahtar kullanan birçok çözüm ortaya konmuştur. GSM şifrelemesinde kullanılan A5/1, A5/2 ve Wi-Fi güvenliğinde kullanılan RC4 gibi dizi şifreleme algoritmaları, bu tür şifreleme yöntemlerine örnektir (Stallings, 2011).

RC4, Ron Rivest tarafından 1987 yılında geliştirilmiştir (Katz ve Lindell, 2014). 40 ila 256 bit arasında değişken boyutta gizli anahtar kullanmaktadır. Algoritmanın temeli rastgele karıştırmaya (permutasyon) dayanmaktadır. Algoritma ilk olarak 256 bayt uzunluğundaki *S* dizisini ilk kullanım için hazırlar. Eğer gizli anahtar boyutu 256 bayt değilse, anahtarı tekrar ederek 256 baytlık *T* dizisini oluşturur. Anahtarı tutan *T* dizisi ve *S* dizisi kullanılarak *S* dizisi karıştırılır. Karıştırma işlemi sonunda *S* dizisinin içerisinde 0 ile 255 arasındaki sayılar karışık bir halde elde edilir. Kayan anahtar dizisini elde etmek için karıştırılmış *S* dizisi kullanılır.

K değişkeni ile 8 bitlik kayan anahtar tutulmaktadır. Şifreleme yapmak için açık metinden ilk karaktere karşılık gelen 8 bit alınır ve *K* değişkeni ile XOR'lanır. Böylece açık metindeki ilk karaktere karşılık gelen şifrelenmiş metin oluşturulur. Benzer şekilde açık metindeki ikinci karakteri şifrelemek için yeni K değişkeni elde edilir ve şifrelemeye açık

metindeki bütün karakterler bitinceye kadar devam edilir. Oluşan şifrelenmiş metin güvenli bir şekilde iletilir. Şifrelenmiş metni alan kullanıcı benzer adımları takip ederek aynı kayan anahtar dizisini oluşturmalıdır. Kayan anahtar dizisini elde ettikten sonra, ilk 8 biti kullanarak şifrelenmiş metindeki ilk karakter ile XOR'lar. Bu işlemi bütün karakterler için tekrar eder. İşlemin sonunda açık metni gizli bir şekilde elde eder. Kayan anahtar dizisini elde etmek için kullanılan kod, kullanıcının gizli anahtarı hakkında dışarıya bilgi vermektedir. Bu açığı kapatmak için RC4A ve RC4+ gibi alternatif çözümler önerilmiştir.

Yukarıda açıklanan şifreleme yönteminde XOR bit operatörü kullanılmıştır. XOR operatörüne ek olarak AND ve OR gibi diğer bit operatörleri de bulunmaktadır. Bit operatörleri içinde şifreleme ve şifre çözmek için kullanılan tek bit operatörü XOR operatörüdür. Diğer bit operatörleri bu amaçla kullanılmazlar. Hatırlanacağı gibi şifreleme ve çözme fonksiyonları öyle fonksiyonlar olarak seçilmelidir ki, herhangi bir açık metni şifreleme fonksiyonu ile şifreleyip şifreli metni elde ettikten sonra çözme fonksiyonu kullanılarak bu şifreli metin çözüldüğünde, orijinal açık metnin elde edilmesi gerekmektedir. Herhangi bir açık X metnini K gizli anahtarı ile XOR'layıp elde edilen şifreli metin Y olsun. Bir başka ifadeyle $Y = X$ (XOR) K olsun. Şifreli metin tekrar aynı gizli anahtar K ile XOR'lanırsa, orijinal metin olan X metni elde edilir. Yani $X = Y$ (XOR) K olur. Bu nedenle XOR bit operatörü şifreleme fonksiyonu olarak kullanmak için oldukça elverişli bir operatördür. Yukarıda anlatılan kavramı basit bir örnekle şöyle açıklayabiliriz. X açık metni 8 bitlik bir mesaj olsun. X = (11001010) olarak seçilsin. K gizli anahtarı ise K = (10010110) şeklinde seçilmiş olsun. Eğer X açık metni K gizli anahtarı kullanılarak şifreleme fonksiyonu olan XOR bit operatörü ile şifrelenirse elde edilecek şifreli metin $Y = X$ (XOR) K = 11001010 (XOR) 10010110 = 01011100 olur. Şifreli metni alıp tekrar aynı gizli anahtar ile XOR'larsak orijinal metne ulaşmamız gerekir. Yani $X = Y$ (XOR) K = 01011100 (XOR) 10010110 = 11001010 olarak elde edilmiş olur. Bu çözme işlemi sonucunda elde edilen mesaj orijinal açık metinle karşılaştırıldığında iki mesajın birbirine eşit olduğu görülür.

BLOK ŞİFRELEME

Blok şifreleme, iletilecek mesajı kullanılacak yönteme bağlı olarak eşit uzunlukta parçalara ayırarak şifrelenmiş metne dönüştürür.

Dizi şifrelemeden farklı olarak **blok şifrelemede** açık metinler bloklar halinde şifrelenir. Belli şartlara göre açık metin bloklara parçalanır. Her bir blok sırayla, simetrik algoritma kullanılarak şifrelenir. Elde edilen şifreli metinler yine aynı sırada çözülerek, açık metinler bloklar halinde elde edilir. Bu bloklar bir araya getirilerek orijinal metine ulaşılır. Dizi şifrelemede "merhaba" açık metni birer karakter şeklinde şifrelenirken, blok şifrelemede bu metin bütün olarak şifrelenebilir.

Klasik Şifreleme Algoritmaları

Günümüzde kullanılan modern şifreleme algoritmalarının yanında geçmiş zamanlarda kullanılmış ama şu an güvenilir kabul edilmeyen klasik şifreleme algoritmaları mevcuttur. Bu klasik algoritmalar, günümüz modern şifreleme algoritmalarına temel teşkil etmiştir. Geçmişten günümüze kullanılan şifreleme algoritmalarının açıkları ve eksiklikleri tespit edilerek yeni ve modern şifreleme algoritmaları geliştirilmiştir. Bu bölümde klasik şifreleme algoritmaları üzerinde kısaca durulacaktır.

Sezar Şifreleme Algoritması

Bilinen en eski ve en basit şifreleme yöntemidir. Alfabede her bir harfin belirli sayıda karakter ötelenmesi ile şifreleme tablosu elde edilir. İngiliz alfabesinde yer alan 26 harfe sıfırdan başlayarak sırayla bir pozisyon sayısı atanır. Alfabenin ilk harfi "a" 0 ile son harfi "z" ise 25 ile eşlenir.

Sezar şifreleme algoritması şu şekilde çalışır. Açık metinde yer alan her harfin pozisyon sayısı bulunur. Bu pozisyon sayılarının her biri 3 ile toplanır. Bu toplama işlemi sonucunda elde edilen sonuçların mod 26 işlemine göre sonuçları bulunur. Bulunan sayılar şifrelenmiş metinde yer alacak harflerin pozisyon sayılarıdır. Bu pozisyon sayılarına karşı gelen harfler belirlenerek şifreli metin elde edilir. Bu metin karşı tarafa gizli mesaj olarak gönderilir. Kısaca orijinal açık metin içinde yer alan her harf alfabede üç basamak sağda yer alan harf ile değiştirilmiştir. Bu şifreleme algoritmasında seçilen "3" rakamı gizli anahtardır. Bu anahtar her şifreleme için aynıdır. Sezar Şifreleme en eski ve en basit şifreleme olduğundan kırılması oldukça kolaydır.

Şifre çözme işlemi benzer şekilde yapılır. Şifreleme ve şifre çözme birbirinin tersi işlemlerdir. Alıcı, şifrelenmiş metni alınca önce her harfin pozisyon sayısını bulur. Bu sayılardan 3 çıkarır. Elde ettiği sonuçların mod 26'ya göre eşitliklerini bulur. Bu sayılar pozisyon sayıları olduğundan bunlara karşı gelen harfleri bularak açık metni elde etmiş olur.

Genel olarak açık metinler küçük harflerle şifreli metinler ise büyük harflerle yazılır. Açık metin içinde yer alan boşluklar ve noktalama işaretleri göz önüne alınmaz. Şifreli metinde yer alan harfler beşerli gruplar haline getirilir. Örneğin açık metin "Okul Ankara'da!" şeklinde olsun. Öncelikle noktalama işaretleri ve boşluklar göz ardı edilir. Açık metinde yer alan her harfin, alfabede üç basamak sağında yer alan harfler bulunarak bu harflerle yer değiştirilir ve şifreli metin elde edilir. Bu durumda açık metnin ilk harfi "O" olduğundan, bu harf üç sağında yer alan "R" ile yer değiştirilir. Benzer şekilde diğer harfler de yer değiştirilirse ve harfler beşerli gruplanırsa şifreli metin "RNXOD QNDUD GD" şeklinde elde edilir. Bu şifreli metin alıcıya gönderildiğinde, alıcı bu harflerin alfabede üç solunda yer alan harfleri bularak bunlarla yer değiştirir ve açık metne ulaşır.

İngiliz alfabesinde 26 harf olmasından dolayı Sezar yönteminde şifreleme ve çözme fonksiyonları aşağıdaki gibi olur:

Şifreleme fonksiyonu: $y = x + 3 \ \textbf{mod}\ 26$
Çözme fonksiyonu: $x = y - 3 \ \textbf{mod}\ 26$

Formüllerde x açık metne, y şifrelenmiş metne, 3 öteleme miktarı (gizli anahtar) ve mod ise modüler aritmetik işlemine karşılık gelmektedir. Sezar yönteminde öteleme miktarı sabittir. Sezar yöntemi genelleştirilirse toplama şifreleme yöntemi ortaya çıkar. Bu durumda şifreleme ve çözme fonksiyonları aşağıdaki gibi yazılır:

Şifreleme fonksiyonu: $y = x + k \ \textbf{mod}\ 26$
Çözme fonksiyonu: $x = y - k \ \textbf{mod}\ 26$

Toplama şifreleme yönteminde k gizli anahtarının alabileceği değerler 26'dan küçük doğal sayılardır. Bu durumda anahtarın alabileceği 26 farklı değer vardır. Ama anahtar değerinin 0 olması durumunda açık ve şifrelenmiş metin arasında bir fark oluşmaz. Bu nedenle anahtarın 0 olarak seçilmesinden kaçınılmalıdır. Anahtar uzayında 26 farklı değer olduğundan bu şifreleme yönteminde kullanılan anahtarı deneme yanılma ile bulmak için bu 26 farklı anahtar sırasıyla denenir. Başka bir ifadeyle, kaba kuvvet saldırısı kullanarak 26 farklı k değerinin denenmesi sonucu herhangi bir şifrelenmiş metine karşılık gelen açık metin kolayca elde edilir. En kötü durumda kötü niyetli kişi, gizli anahtarı bulmak için kaba kuvvet saldırısı kullanarak 26 deneme yapar. Ortalama olarak 26/2 = 13 denemede gizli anahtara ulaşabilir. En iyi durumda ise tek denemede anahtarı ele geçirebilir.

Sezar şifreleme algoritması ile "hello" mesajını şifreleyiniz.

SIRA SİZDE 2

Affine Şifreleme

Affine şifreleme yöntemi Sezar yönteminin geliştirilmesiyle elde edilmiştir. Şifreleme işlemi için açık metin belirlenen bir sayı ile çarpılır ve Sezar şifrelemesinde olduğu gibi öteleme miktarıyla toplanır. Şifreleme ve çözme fonksiyonları aşağıdaki gibidir:

Şifreleme fonksiyonu: $y = a * x + b$ **mod** 26
Çözme fonksiyonu: $x = a^{-1} (y - b)$ **mod** 26

İlk bakışta *a* ve *b* için 26 farklı değer kullanılabileceğini düşünürsek, anahtar uzayının toplam 26×26 = 676 farklı anahtardan oluşabileceği kabul edilebilir. Fakat çözme fonksiyonu için a değerinin mod 26 işleminde tersinin olması zorunludur. 26 asal bir sayı olmadığı için {0, 2, 4, 6, 8, 10, 12, 13, 14, 16, 18, 20, 22, 24} değerlerinden birinin *a* için seçilmesi durumunda tersini bulmak imkânsızdır. Dolayısıyla geriye kalan {1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25} sayılarından biri seçilmek zorundadır. Bu durumda Affine şifrelemesi için anahtar uzayı 12×26 = 312 farklı anahtardan oluşabilmektedir. Yukarıda bahsedilen hesaplama İngiliz alfabesi dikkate alınarak yapılmıştır. Türk alfabesi kullanılması durumunda 29 farklı harf olduğu için **mod** işlemlerinde 26 yerine 29 değeri kullanılmalıdır. 29 bir asal sayı olduğu için seçilebilecek *a* değeri 28 tane olmaktadır. Çünkü 29 asal sayı olduğundan, 29 ile aralarında asal olan 28 tane sayı vardır. Türk alfabesi kullanılması durumunda 29×28 = 812 farklı anahtar üretilebilir. İngiliz alfabesinde daha küçük bir anahtar uzayı varken, Türk alfabesinde kullanılan harf sayısının bir asal sayı olmasından dolayı anahtar uzayı çok daha geniştir.

SIRA SİZDE 3

23 harften oluşan bir alfabe ile çalışıldığını varsayalım. Buna göre Affine şifreleme kullanıldığında toplam kaç farklı anahtar kullanılabilir?

Monoalfabetik Şifreleme

Sezar yönteminde kullanılan 26 farklı anahtar yeterince güvenlik sağlayamaz. Monoalfabetik şifrelemede anahtar uzayını artırmak için alfabedeki her bir karakter başka bir karakter ile değiştirilerek şifreleme tablosu oluşturulur. Çözümleme ise bu işlemin tam tersi yapılarak elde edilir. Örnek bir şifreleme tablosu aşağıda verilmiştir.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
M	H	Z	U	X	I	C	P	O	Q	A	N	S	B	T	L	D	K	Y	R	E	J	G	W	F	V

Açık metnin "ankara" olması durumunda "MBAMKM" şifrelenmiş metni elde edilir. Çözme işlemi için ise tablodaki alt satırdaki karaktere karşı gelen üst satırdaki karakter kullanılır. Monoalfabetik yöntemi ile 26! = 403.291.461.126.606.000.000.000.000 farklı şifreleme tablosu oluşturulabilir. Kaba kuvvet saldırısı uygulanması durumunda doğru şifreleme tablosunu bulmak için uzun yıllar gerekmektedir.

Bilgisayar korsanları şifreleme algoritmalarının en zayıf noktalarını ararlar. Monoalfabetik şifreleme algoritması için uygulanan kaba kuvvet saldırısı ile korsan hiçbir sonuç elde edemez. Ancak bu kez de başka yöntemler kullanarak algoritmayı kırmaya çalışırlar. İngilizcede en sık kullanılan harf "e" dir. Dolayısıyla şifrelenmiş metinde en sık kullanılan karakteri tespit edip "e" karakteri ile yer değiştirilmesi durumunda bir takım çıkarımlar elde edilebilir. Buna ek olarak, dilin yapısıyla ilgili elde edeceği bilgiler yardımıyla, kaba kuvvet saldırısı ile kırılması imkânsız olan bir yöntemin çözülmesi mümkün hale gelebilmektedir.

Vigenere Şifreleme

Vigenere şifreleme algoritması, monoalfabetik yöntemleri çözmekte kullanılan sıklık analizi saldırılarına karşı olan zafiyeti, şifrelenmiş metinde kullanılan her harfin neredeyse eşit sıklıkta kullanılmasıyla ortadan kaldırmıştır. Vigenere algoritmasında bir parola vardır. Parolanın açık metinden kısa olması halinde parola açık metin uzunluğunca tekrar edilir. Paroladaki her harf açık metindeki "A" karakterine karşılık gelir ve diğer karakterler Sezar şifrelemesinde olduğu gibi ötelenir. Bu yöntemin getirdiği en önemli farklılık açık metindeki bir karakterin birçok farklı karakter kullanarak şifrelenmiş metin oluşturmasıdır. Tablo 3.4'de bir Vigenere şifreleme örneği sunulmaktadır.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J

Tablo 3.4
Parolanın "ESKI" ve açık metnin 7 karakter uzunluğunda olması durumunda elde edilen Vigenere tablosu

Açık metin	A	N	A	D	O	L	U
Parola	E	S	K	I	E	S	K
Şifrelenmiş metin	E	F	K	L	S	D	E

Modern Simetrik Şifreleme Yöntemleri

Klasik şifreleme yöntemleri hesaplama gücünün yüksek olmadığı haberleşme ortamları için tercih edilebilir yöntemlerdir. Bilindiği gibi günümüzde hesaplama gücü yüksek bilgisayarlar sayesinde klasik yöntemlerle şifrelenen metinler kolaylıkla kırılabilir. Bu nedenle karmaşık matematiksel işlemlere dayanan ve kırılması oldukça zor yeni yöntemler geliştirilmiştir. Bu bölümde günümüzde kullanılan simetrik şifreleme yöntemlerine değinilecektir.

Data Encryption Standard

Data Encryption Standard (**DES**–Veri Şifreleme Standardı) IBM tarafından geliştirilen, Amerikan Ulusal Güvenlik Ajansı tarafından algoritmanın bazı adımlarında değişiklik yapılarak kabul edilen ve 1977 – 2001 yılları arasında yaygın şekilde kullanılan bir blok şifreleme algoritmasıdır (Paar ve Pelzl, 2010). Bilgisayar teknolojisinin gelişmesiyle 2000'li yılların başında kaba kuvvet saldırılarına karşı zafiyeti olduğu için Advanced Encryption Standard (AES–Gelişmiş Şifreleme Standardı) algoritması DES'in yerini almıştır. Donanım üzerinde verimli ve hızlı bir şekilde şifreleme yapması amaçlanmıştır. Yazılımda çalışması arka planda kalmıştır. DES, 64-bit uzunluğunda bloklar kullanarak şifreleme yapar. 64 bitlik anahtar uzunluğu vardır ama 56 biti etkili şekilde kullanılır, geriye kalan 8 bit kontrol amaçlıdır. DES, 16 adet birbirinin aynısı işlemlerden oluşan turlardan meydana gelmektedir.

DES uzun yıllar boyunca güvenle kullanılmış ve üzerinde en çok araştırma yapılmış simetrik şifreleme algoritmalarından biridir.

Güçlü bir şifreleme algoritması iki temel operatör üzerine kurulmalıdır:

- **Karışıklık:** Bu operatör şifrelenmiş metin ile anahtar arasında ilişkinin anlaşılmasını zorlaştırır. DES ve AES gibi şifreleme algoritmalarında bu amaçla yer değiştirme işlemi sıklıkla kullanılmıştır.
- **Yayılma:** Açık metnin istatistiksel özelliklerini gizlemek için, açık metinde yapılacak en ufak değişikliğin genişleyerek şifrelenmiş metinde çok fazla değişikliğe sebep olmasıdır. DES ve AES algoritmalarında kullanılan permutasyon işlemleri yayılma etkisi oluştur.

Bu operatörler tek başlarına güvenli bir şifreleme algoritması oluşturmak için yeterli değildir. Birbirlerini takip edecek şekilde ve çok sayıda kullanılmalıdır. Bu amaçla DES algoritması birbirini takip eden 16 karışıklık ve yayılma operatöründen oluşmaktadır.

DES algoritması açık metinden 64 bitlik bir bloğu 48 bitlik tur anahtar ile birlikte işleme tabi tutarak 64 bitlik şifrelenmiş metin elde eder. DES Feistel şifreleme yöntemi üzerine kurulmuştur. Feistel şifreleme yönteminde 64 bitlik bloklar ikiye bölünerek sol 32 ve sağ 32 bitlik bloklar elde edilir. Sağ 32 bitlik blok tanımlanmış bir fonksiyona gönderilir. Bu fonksiyonun girdileri sağ 32 bitlik blok ve 48 bitlik tur anahtarıdır. Fonksiyondan çıkan sonuç sol 32 bit ile XOR'lanarak bir sonraki turun sağ 32 bitlik bölümüne kopyalanır. Sağ 32 bitlik blok aynı zamanda bir sonraki turun sol 32 bitlik bölümüne kopyalanır. Bu işlem 16 kez tekrarlanır ama her turda 56 bitlik gizli anahtardan elde edilen farklı 48 bitlik tur anahtarı kullanılır.

DES algoritmasının Feistel şifreleme yöntemi üzerine kurulmasından dolayı çözme fonksiyonu, şifreleme işlemlerinin aynısıdır. Tek fark, çözme işleminde tur anahtarının ters sırada kullanılmasıdır. Yani çözme işleminin birinci turunda on altıncı şifreleme tur anahtarı, ikinci turunda on beşinci tur anahtarı gibi ters sırayla kullanılması gerekir.

DES algoritmasında kullanılabilecek anahtar uzayının çok büyük maliyetler gerektirmeyen donanımlar kullanılarak kaba kuvvet saldırılarına açık olması ve tasarımında bulunan bir takım endişeler yeni bir şifreleme algoritmasının geliştirilmesini gerektiriyordu. Bu amaçla düzenlenen ve birkaç yıl süren yarışmanın sonunda, AES şifreleme algoritması DES'in yerini aldı.

3DES

DES algoritmasının yaygın olarak bilinmesi ve kullanılmasından dolayı kaba kuvvet saldırılarına karşı koyabilecek alternatif çözümler ortaya kondu. Bunlardan bir tanesi 3DES şifreleme yöntemidir. Adından da anlaşabileceği üzere DES algoritmasının üç defa peş peşe farklı gizli anahtarlar kullanmak suretiyle uygulanmasıdır.

Gizli anahtar seçimine bağlı olarak farklı uygulamaları mevcuttur. Birinci seçenek gizli anahtarların üçünün de farklı seçilmesi durumudur ve 3×56 = 168 bitlik anahtar uzunluğuna karşılık gelir. En güçlü güvenlik bu seçenekte sağlanır. İkinci seçenekte ise birinci ve üçüncü anahtarın aynı olduğu, ikinci anahtarın ise bunlardan farklı olduğu durumdur ve 2×56 = 112 bitlik uzunluğa karşılık gelen anahtar güvenliği elde edilir.

Advanced Encryption Standard

DES algoritmasında kullanılan anahtar uzunluğunun kaba kuvvet saldırılarına karşın yetersiz kalması ve hem yazılım hem de donanım ortamında verimli şekilde çalışacak modern bir şifreleme algoritmasına ihtiyaç duyulması nedeniyle, 1997 yılında Birleşmiş Milletler Ulusal Standartlar ve Teknoloji Enstitüsü bir yarışma çağrısı yaptı. Finale kalan beş algoritmadan iki Belçikalı bilim adamının geliştirdiği Rijndael birinci oldu ve gelişmiş şifreleme standardı **(AES)** olarak kabul edildi. AES algoritması SSH, IpSec, TLS ve Skype gibi güvenliğin önemli olduğu birçok protokolde kullanılmaktadır (Katz ve Lindell, 2014).

DES algoritmasında kullanılan anahtar uzunluğunun yetersiz kalmasıyla yeni bir algoritmaya gerek duyuldu. **AES** günümüzde en yaygın ve güvenilir şifreleme algoritması olarak kabul edilmektedir.

AES algoritması 128, 192, 256 bit olmak üzere üç farklı anahtar uzunluğu kullanarak 128 bitlik bloklar halinde şifreleme yapar. 128 bitlik blok 4×4 durum matrisinde saklanır ve bütün işlemler bu matris kullanılarak yapılır. 128 bit uzunluğundaki anahtar günümüzde yeterli güvenlik sağlarken, gizliliğin çok önemli olduğu durumlarda 192 veya 256 bitlik anahtar uzunluğu tercih edilebilir. AES, anahtar uzunluğuna bağlı olarak birbirinin benzeri turlardan oluşmaktadır.

Anahtar uzunluğu	Tur sayısı
128	10
192	12
256	14

Tablo 3.5
AES anahtar uzunluğu ve tur sayıları

AES şifreleme algoritmasının turları üç temel işlemden oluşmaktadır:

- **Anahtar ekleme katmanı:** Tur anahtarı ile durum matrisi XOR'lanır
- **Bayt yer değiştirme katmanı:** Durum matrisi S-Box adı verilen doğrusal olmayan bir tablo ile dönüştürülür.
- **Yayılma katmanı**
  - **Satır kaydırma katmanı (ShiftRows):** Durum matrisindeki satırlar dairesel olarak belirli sayıda kaydırılır.
  - **Sütun karıştırma katmanı (MixColumn):** Durum matrisinin sütunları karıştırılır.

AES şifreleme algoritmasının son turu hariç diğer bütün turlarda aynı işlemler uygulanır. Son turda sütun karıştırma katmanı (MixColumn) işlemi uygulanmaz. DES algoritmasına benzer şekilde kullanıcının gizli anahtarı kullanılarak her bir turda farklı olmak üzere tur anahtarları oluşturulur.

AES algoritmasında şifre çözme işlemi için, şifreleme işleminde uygulanan tüm işlemlerin tersi tanımlanmıştır. Çözme işleminde tur anahtarları DES'e benzer şekilde ters sırayla uygulanmalıdır. Yani çözme işleminde ilk turda kullanılacak anahtar, şifreleme işleminde en son turda kullanılan anahtar olmalıdır.

International Data Encryption Algorithm

DES, 3DES ve AES simetrik şifreleme algoritmalarına ek olarak kullanılan bir diğer simetrik şifreleme algoritması International Data Encryption Algorithm (IDEA–Uluslararası Veri Şifreleme Algoritması) olarak adlandırılır. IDEA algoritmasında açık metin boyu 64 bittir. Benzer şekilde şifrelenmiş metin boyu da 64 bittir. 64 bitlik metinleri şifrelediğinden dolayı IDEA da bir blok şifreleme algoritmasıdır. Kullanılan anahtar uzunluğu ise 128 bittir. 1991 yılında Xuejia Lai ve James L. Massey tarafından geliştirilmiştir. 64 bitlik açık metin 16 bitlik dört bloğa ayrılarak, 16 bitlik bloklar halinde şifrelenir. IDEA, çalışma şekli bakımından diğer simetrik algoritmalara benzemektedir. Özellikle DES ile birbirlerine çok benzerler.

IDEA kullanılarak yapılan şifrelemede toplam 17 iterasyon vardır. Öncelikle bu 17 iterasyon için seçilen 128 bitlik simetrik anahtardan iterasyon anahtarlarının nasıl elde edildiğini anlamak gerekir. 128 bitlik anahtardan toplam 52 iterasyon anahtarı üretilir. Bu anahtarların her biri 16 bit uzunluğundadır. Tekli iterasyonlarda dört iterasyon anahtarı kullanılır. Çiftli iterasyonlarda ise iki iterasyon anahtarı kullanılır. Toplam 17 iterasyon içinde dokuz tekli ve sekiz çiftli iterasyon vardır. Bu durumda $9\times4+8\times2 = 52$ iterasyon anahtarı kullanılır.

Şifreleme için kullanılan anahtarlar şifre çözmek için aynen kullanılmaz. Karşı taraf, şifre çözmek için elindeki aynı 128 bitlik anahtardan üreteceği 52 iterasyon anahtarının şifre çözme için karşılıklarını üretir. Tekli iterasyonlarda bit tabanlı toplama ve çarpma işlemleri yapıldığından şifreleme için kullanılan ilgili anahtarların toplama ve çarpmaya göre tersleri bulunarak şifre çözmek için kullanılır. Toplama ve çarpmaya ek olarak kullanılan diğer bir operasyon ise XOR operatörüdür.

Geçmişte IDEA birçok ülkede patentliydi. Patent süresinin 2011 yılı itibariyle bitmesiyle beraber ticari faaliyetler haricinde serbestçe kullanılmaktadır. IDEA algoritması güvenli elektronik posta şifreleme için geliştirilmiş olan PGP algoritması tarafından da kullanılmaktadır (Trappe ve Washington, 2006).

SIRA SİZDE 4

Yukarıda açıklanan DES, 3DES, AES ve IDEA gibi algoritmaların yanında diğer simetrik şifreleme algoritmalarını listeleyiniz.

Blok Şifreleme Metotları

Blok şifreleme algoritmaları açık metni bloklara parçalayarak şifrelenmiş metin elde eder. Blok uzunlukları kullanılan algoritmalara göre farklılık göstermektedir. Eğer son kalan parça blok uzunluğundan kısa ise uygun bir yöntem ile tamamlanır. Şifreleme yapmak için birçok mod tanımlanmıştır. Bu modlardan standartlarda kabul edilen ve yaygın olarak kullanılan beş tanesi aşağıda açıklamıştır (Stallings, 2011).

- **Elektronik Kod Kitabı (Electronic Code Book–ECB):** Açık metni, kullanılan algoritmaya göre uygun uzunluktaki bloklara böler. Her bir bloğu bağımsız şekilde gizli anahtar kullanarak şifrelenmiş metin elde eder. Aynı açık metin için her seferinde aynı şifrelenmiş metin elde edilir. Uzun ve belirli yapıda olan mesajlar için güvenlik açısından tavsiye edilmez. Bu yöntem, şifrelenmiş metinlerin yerlerini değiştirerek metnin içeriği ile oynanmasına da izin verir.
- **Şifre Blok Zincirleme (Cipher Block Chaining–CBC):** CBC mod hem üretilecek şifrelenmiş metnin kendisinden önceki bütün açık metinlere bağlı olmasını, hem de şifreleme yöntemini ilk turda rastgele sayılardan oluşturulan bir vektör kullanarak farklılaştırmayı amaçlamıştır. İlk tur hariç diğer bütün turlarda açık metin bloğu, bir önceki şifrelenmiş metin ile XOR'lanarak şifreleme algoritmasına girdi olarak gönderilir. İlk turda ise şifrelenmiş metin yerine rastgele oluşturulmuş bir blok kullanılır.
- **Çıktı Geribesleme Modu (Output Feedback Mode–OFM):** Bu mod dizi şifreleme algoritmalarında kullanılır. İlk olarak, rastgele üretilen başlangıç vektörü şifreleme algoritmasına girdi olarak gönderilir. Şifreleme algoritmasının çıktısı açık metin ile XOR'lanır ve ilk şifrelenmiş metin bloğu elde edilir. İlk turdan sonraki adımlarda başlangıç vektörü yerine bir önceki adımda elde edilen şifreleme algoritmasının çıktısı kullanılır. Bu mod CBC gibi aynı açık metin için faklı şifrelenmiş metinler üretir. CBC moda göre avantajı, açık metin yerine başlangıç vektörü kullanıldığı için önceden bütün turlar için gerekli verinin üretilebilir olması ve şifreleme algoritmasının daha hızlı çalışmasının sağlanmasıdır.
- **Sayaç Modu (Counter Mode–CM):** OFM moda benzerdir. Şifreleme algoritmasına başlangıç vektörünün sonuna ilk tur için 1 sayısı eklenerek gönderilir ve diğer turlarda bu sayı artırılır.
- **Şifre Geribesleme Modu (Cipher Feedback Mode–CFB):** İlk tur hariç diğer bütün turlarda üretilen şifrelenmiş metin, şifreleme algoritmasına girdi olarak gönderilir. Şifreleme algoritmasının çıktısı ile açık metin XOR'lanır. Başlangıç vektörü ilk tur için şifreleme algoritmasına girdi olarak gönderilir. Şifreleme algoritmasının çıktısı ile ilk açık metin bloğu XOR'lanır.

SİMETRİK ŞİFRELEME ALGORİTMALARININ PROBLEMLERİ

Simetrik şifreleme algoritmaları mesajların gizliliğini sağlamak amacıyla yaygın olarak kullanılmaktadır. İki kişi kendi aralarında gizliliklerini ifşa etmeden mesaj paylaşmak istediklerinde kullanacakları şifreleme algoritmaları, simetrik şifreleme algoritmaları olacaktır. Mesaj gizliliği için yaygın olarak kullanılan simetrik şifreleme algoritmalarının bir takım problemleri vardır.

Bu problemleri açıklamadan önce mesaj gizliliği için neden simetrik şifreleme algoritmalarının kullanıldığı üzerinde durmak gerekir. Kötü niyetli kişilerden korunacak olan mesaj, değişik uzunlukta herhangi bir mesaj olabilir. Bu mesaj "merhaba" gibi tek bir kelimeden oluşabileceği gibi yeni yazılan bir roman gibi bir kitap içeriği de olabilir. Bu nedenle mesaj boyutu çok büyük olduğunda şifreleme ve şifre çözmenin kısa zamanda gerçekleştirilmesi gerekebilir. Şifreleme algoritmalarının güvenli olmaları yanında performanslarının da (hızlı şifreleme ve çözme yeteneği) iyi olması beklenir. Açık anahtar şifreleme algoritmaları ile karşılaştırıldıklarında simetrik şifreleme algoritmaları daha hızlıdır. Simetrik şifreleme algoritmalarında mesaj gizliliği karıştırma ve yayılma gibi iki temel operasyonla sağlanır. Bu operasyonlar ise bit temelli operasyonlardır. Buna karşılık açık anahtar şifreleme algoritmaları matematiksel işlemlere dayanır. Bu nedenle simetrik şifreleme algoritmaları açık anahtar şifreleme algoritmalarından daha hızlıdır. Eğer mesaj gizliliği için açık anahtar şifreleme algoritmaları kullanılırsa, mesaj boyu büyüdükçe hız çok düşebilir. Mesaj gizliliği için bu algoritmalar yerine, hızlı olmalarından dolayı simetrik şifreleme algoritmaları tercih edilir.

Hızlı şifreleme algoritmaları olmaları, simetrik şifreleme algoritmalarının en önemli avantajıdır. Bu avantaj yanında simetrik şifreleme algoritmalarının dezavantajları da vardır. Birinci dezavantajları anahtar dağıtım problemi olarak adlandırılır. Simetrik şifreleme algoritmalarının şifreleme sürecini kısaca gözden geçirerek bu problemi açıklamaya çalışalım. Can ile Bora simetrik şifreleme kullanarak gizli mesajlaşmak istesinler. Güvenliği artırmak için her mesaj için bir oturum anahtarı üretilerek simetrik anahtar olarak kullanılır. Can bir mesaj yazmış olsun. Bu mesajı simetrik şifreleme ile şifrelemek için bir oturum anahtarı üretir. Daha sonra bu anahtar ile mesajı şifreler ve şifreli mesajı Bora'ya gönderir. Simetrik şifrelemede şifreleme ve şifre çözmek için aynı anahtar kullanılır. Bu nedenle Can'ın şifreleme için kullandığı oturum anahtarı şifre çözmek için gerekmektedir. Bora şifreli mesajı aldığında eğer elinde şifrelemede kullanılan bu oturum anahtarı yoksa şifreli mesajı çözerek açık mesaja ulaşamaz. Bunun için Can'ın üretip şifreleme için kullandığı bu anahtarı bir şekilde Bora'ya ulaştırması gerekmektedir. Benzer problem, Bora mesaj şifreleyip Can'a gönderdiği zaman da olur. Bu durumda Bora oturum anahtarı üretir ve bu anahtarın Can'a ulaştırılması gerekir. Bu probleme, simetrik şifreleme algoritmalarında anahtar dağıtımı problemi adı verilir. Bu problemin çözülmesi için değişik yöntemler kullanılmaktadır. Bu yöntemler kısaca şöyle açıklanabilir. Birincisi, Can ve Bora arasında daha önceden kullanılmış, bilinen bir anahtarla oturum anahtarı şifrelenerek birbirlerine gönderebilirler. İkincisi, Can ve Bora'nın bir araya gelerek anahtara karar vermeleri gerekmektedir. Bu tercih edilen bir yöntem değildir. Son yöntem ise en çok kullanılan ve en pratik yöntemdir. Oturum anahtarı, açık anahtar şifreleme algoritması kullanılarak şifrelenir ve karşı tarafa gönderilir. Daha sonraki bölümlerde açık anahtar şifreleme açıklanmıştır. Kısaca açıklamak gerekirse, yukarıdaki örneğe göre Can oturum anahtarını Bora'nın açık anahtarı ile şifreler ve Bora'ya gönderir. Bora bu açık anahtarına karşılık gelen, sadece kendisinin bildiği gizli anahtar ile gelen şifreyi çözer ve oturum anahtarına ulaşır. Daha sonra bu oturum anahtarını kullanıp gelen şifrelenmiş mesajı çözer ve açık mesaja ulaşır.

Simetrik şifreleme algoritmalarının ikinci problemi toplam anahtar sayısı problemi olarak adlandırılır. Birbirleri ile ikili gruplar halinde mesajları simetrik şifreleme algoritmaları kullanarak paylaşmak isteyen kişi sayısı çoğaldıkça kullanılacak toplam simetrik anahtar sayısı, kişi sayısıyla doğrusal olarak değil toplam kişi sayısının karesiyle orantılı olarak çoğalmaktadır. Simetrik şifrelemede birbiri ile mesajların gizliliğini koruyarak haberleşmek isteyen iki kişi, tek bir simetrik anahtar kullanarak mesajları gizli olarak iletebilir. Eğer grup üç kişi olursa, toplamda üç simetrik anahtara ihtiyaç vardır. Mesela Can, Duygu ve Bora simetrik şifreleme ile aralarında gizli mesajları iletmek istesinler. Can ve

Duygu mesaj değiştirmek için bir simetrik anahtara, Can ve Bora aralarında güvenli haberleşmek için başka bir simetrik anahtara ve son olarak Duygu ve Bora aralarında mesaj gizliliğini sağlamak için üçüncü bir simetrik anahtara ihtiyaç duyarlar. Bu durumda toplamda üç simetrik anahtara ihtiyaç vardır. Eğer dört kişilik bir grup simetrik şifreleme algoritmaları kullanarak mesaj gizliliğini yukarıdaki gibi sağlamak isterlerse, ihtiyaç duyulan toplam simetrik anahtar sayısı 6 olur. Toplam kişi sayısı beş olduğunda, toplam anahtar sayısı ise 10 olur. Bu durumu n kullanıcıdan oluşan bir grup için genelleştirirsek, ihtiyaç duyulan toplam simetrik anahtar sayısı $n\times(n\text{-}1)/2$ olur. Bu hesaplamadan görüldüğü gibi kullanıcı sayısı n olduğunda toplam anahtar sayısı n^2 ile orantılıdır. Sonraki bölümlerde anlatılacağı üzere bu n kullanıcı, mesaj gizliliği için açık anahtar şifreleme algoritmaları kullanmış olsa, ihtiyaç duyulan toplam anahtar sayısı $2n$ olur. Dolayısıyla anahtar sayısı kullanıcı sayısıyla doğru orantılı olarak değişmektedir.

Üçüncü problem, aynı simetrik anahtar bütün mesajları şifrelemek için kullanıldığında ortaya çıkan güvenlik problemidir. İki kişi, aralarında mesaj gizliliği için simetrik şifreleme kullandıkları zaman bütün mesajları daha önce güvenli paylaştıkları aynı gizli simetrik anahtarı kullanarak şifreleyebilirler. Aynı anahtar kullanılarak şifreli metinler çözülür. İki kişi uzun süre aynı simetrik anahtarı kullanarak şifreli mesajlaşabilir. Kötü niyetli kişi veya kişiler bu haberleşmeleri dinleyerek şifreli metinleri ele geçirebilir. Elde ettikleri şifreli metinleri ve diğer bilgileri kullanarak, bu iki kişinin şifreleme için kullandıkları simetrik anahtarı ele geçirebilirler. Bu anahtar elde edildikten sonra bu anahtar kullanılarak şifrelenen bütün gizli mesajlara ulaşabilirler. Bu problemin çözümü için kullanılan yöntem, daha önce açıklandığı gibi, oturum anahtarı kullanmaktır. Her gizli mesaj için ayrı bir oturum anahtarı kullanıldığında anahtarlardan biri ele geçirilse bile diğer mesajlara ulaşılamaz. Böylece her mesaj birbirinden bağımsız, farklı simetrik anahtarlarla şifrelendiğinden, mesaj güvenliği artırılmış olur. Oturum anahtarı seçmek konusunda kişilerin dikkat etmesi gereken diğer bir husus ise anahtar uzunluğudur. Anahtar uzunluğu, hem hızı hem de güvenliği etkilemektedir. Uzunluk arttıkça güvenlik artmaktadır. Güvenliğin tersi olarak anahtar uzunluğu arttıkça hız azalmaktadır. Ayrıca işlemler daha karışık hale gelmektedir. Bu nedenle anahtar uzunluğu, güvenlik ve hız kriterleri göz önüne alınarak, ne çok kısa ne de çok uzun seçilmelidir. En uygun anahtar uzunluğu seçilmelidir. Simetrik şifreleme algoritmalarında oturum anahtarı çok kısa seçildiğinde seçilebilecek anahtar sayısı az olmaktadır. Bu durumda kötü niyetli kişiler, oluşturulabilecek bütün anahtarları kaba kuvvet saldırısı yöntemi ile sırasıyla deneyerek seçilmiş anahtarı elde edebilirler. Eğer anahtar uzunluğu yeterince büyük seçilirse, anahtar kümesi içinde yer alacak seçilebilecek anahtar sayısı artmış olur. Anahtarları tek tek denemek daha uzun süreceğinden gerçek anahtarı elde etmek zorlaşır. Bu şekilde olası bütün anahtarları tek tek deneyerek gerçek anahtarı bulmaya çalışmak olarak tarif edilen saldırı şekline kaba kuvvet saldırısı adı verilir. Deneme yapılacak anahtar sayısı ne kadar çok olursa, kaba kuvvet saldırısı o kadar zor olur. Bu nedenle, bu tür saldırılara karşı güvenliği artırmak için oturum anahtarının uzunluğu yeterince büyük seçilmelidir.

SİMETRİK ŞİFRELEME ALGORİTMALARININ GÜVENLİĞİ

Herhangi bir simetrik şifreleme algoritmasının güvenliği için yerine getirilmesi gereken iki şart vardır. Bunlardan ilki ve en önemlisi, gizli mesajı gönderen ve bu mesajı alacak alıcının, güvenli bir şekilde şifreleme anahtarı olan oturum anahtarını birbirleri ile paylaşmaları ve bu anahtarı üçüncü kişilere ifşa etmeden güvenli bir şekilde saklamalarıdır. İkinci şart ise güçlü bir şifreleme fonksiyonunun olmasıdır. Kötü niyetli kişi şifreleme algoritmasını bildiğinde ve elinde bir veya daha fazla şifreli metin olduğunda, bu bilgileri kullanarak şifreli metni çözmesi ve anahtarı elde etmesi imkânsız olmalıdır.

Hem simetrik algoritmalar hem de diğer şifreleme algoritmalarında güvenlik tanımı yapılmalıdır. Herhangi bir şifreleme algoritmasının güvenli olması konusunda değişik tanımlamalar yapılsa bile, en yaygın kullanılan "Hesaplama Güvenlilik" tanımıdır. Simetrik şifreleme veya herhangi bir şifreleme algoritmasının hesaplama güvenli olması demek, iki şartın sağlanması anlamına gelir. Bu şartlardan ilki şöyle açıklanabilir. Gizli anahtarı elde etmek için yapılan harcamaların maliyeti, gizli bilgiye ulaşılması durumunda elde edilecek gelirden fazla olmalıdır. Günümüzde bilgi değerli bir varlıktır. Değeri zaman içinde değişebilir ve değeri genelde tahmin edilemez. Bu değerli bilgiden elde edilecek kazanç nedeniyle şifrelenmiş bilgiye erişmek hedeflenir. Ancak simetrik şifreleme ile korunan bu gizli bilgiye ulaşmak maliyetli bir iştir. Para, zaman, emek ve buna benzer değişik kaynaklar kullanarak şifreli metinler kırılmaya çalışılır. Bu amaçla yapılacak harcamalar gizli bilginin satılmasından elde edilecek kazanç miktarından çok olduğu zaman, şifreli metni elde etmenin herhangi bir anlamı olmaz. İkinci şart ise bilginin faydalı ömrü ile ilgilidir. Bilgi değerini koruduğu sürece değerlidir. Eğer bir bilgi değerini kaybetmişse, bunun ele geçirilmesi herhangi bir anlam ifade etmez. Bu nedenle simetrik şifreleme algoritmasını kırıp (gizli anahtarı ele geçirmek) gizli veriye ulaşmak için harcanan süre, elde edilecek gizli bilginin faydalı ömründen uzun olmalıdır. Bilgi değerini kaybettiğinde veya faydalı ömrü sona erdiğinde, bu gizli bilginin ele geçirilmesinin herhangi bir önemi yoktur. Bu iki şart sağlandığı zaman kullanılan şifreleme algoritmasının hesaplama güvenli olduğu söylenir.

Şifreleme algoritmalarının güvenliği kullanılan anahtar veya anahtarların ne kadar güvenli oldukları ile ilgilidir. Bu anahtarların ele geçirilmesi ne kadar zor ise, algoritmalar o kadar güvenlidir denebilir. Şifreleme ve şifre çözme fonksiyonları genelde herkese açıktır. Algoritmanın nasıl çalıştığı açık şekilde herkese sunulur. Şifreleme algoritmalarının güvenliğini artırmak için değişik yöntemler izlenebilir. Askeri uygulamalarda şifreleme algoritmaları gizlenerek, şifreleme algoritmalarının güvenliğinin artırılması hedeflenir. Algoritmanın kendisi, nasıl çalıştığı ve nasıl şifre çözüldüğü gibi hususlar kapalı kutu gibi üçüncü kişilerden saklanarak güvenlik artırılmak istenmektedir. Algoritma ile ilgili gizliliğin, güvenliği iyileştirdiği varsayılır. Askeri uygulamalardan farklı olarak, ticari şifreleme algoritmalarında ise şifreleme algoritmasının nasıl çalıştığı herkes ile paylaşılır. Bu şekilde yapılan açıklamalarla algoritmanın güvenliğinin artırılması hedeflenir. Güvenliğin neden arttığı şöyle açıklanabilir. Algoritma herkese açık olursa, kullanıcılar bu algoritmaların açıklarını bulmaya çalışırlar. Eğer açıklıklar tespit edilirse, algoritmayı tasarlayanlar bu açıklıkları gidermek için algoritmayı gözden geçirerek daha gelişmiş hale getirebilirler. Böylece tasarlanan algoritma daha güvenli hale gelmiş olur.

SİMETRİK ŞİFRELEME ALGORİTMALARIN UYGULAMA ALANLARI

Simetrik şifreleme algoritmaları değişik amaçlar için kullanılabilir. Bunlar içinde en önemli uygulama alanı, güvensiz bir ağ üzerinde verilerin güvenli bir şekilde iletilmesidir. Günümüzde kullanılan haberleşme kanalları ve ağları genelde güvenli değildir. Bu ağlar üzerinde ve özellikle İnternet vasıtasıyla yapılacak veri iletiminde ve her türlü haberleşmede verinin güvenli bir şekilde paylaşılması gerekmektedir. Bunun için simetrik şifreleme algoritmaları kullanılabilir. Diyelim ki, Can ve Bora mesajlarını ifşa etmeden herhangi bir güvensiz ağ üzerinde birbiri ile haberleşmek istemektedir. Bu durumda simetrik şifreleme algoritması kullanarak birbirlerine iletecekleri gizli mesajları şifreleyerek iletirler. Şifreleme anahtarı sadece Can ve Bora tarafından bilindiğinden kötü niyetli kişiler bu haberleşmeleri dinleseler bile gizli mesajlara ulaşamazlar. Burada mesajın gizliliğini sağlayan, sadece ikisi arasında bilinen anahtardır. Bu şekilde haberleştikleri sürece

kullandıkları haberleşme kanalının bir önemi yoktur. Güvenli veya güvenilir olmayan bir haberleşme kanalı olması anlam ifade etmez. Simetrik anahtar sadece ikisi tarafından bilindiği ve üçüncü kişilerin eline geçmesi engellendiği sürece gizli mesajlarını başkalarına ifşa etmeden birbirlerine iletebilirler.

İlk uygulama alanının yanında, ikinci en yaygın uygulama alanı güvenli depolama olarak adlandırılabilir. Kişi veya kurumlar, gizli veri veya bilgiye sahip olabilir. Mesela, bir pazarlama firması için müşteri listesi değerli veri sınıfına girer. Herhangi bir içecek firması için çok sevilen bir içeceğin formülü değerli bilgi olarak kabul edilir. Çünkü hem müşteri listesi hem de içecek formülü rakip firmalara karşı avantaj sağlar. Bunların kötü niyetli kişi veya kurumların eline geçmesi engellenmelidir. Bu nedenle bu tür veri ve bilgilerin güvenli olarak depolanmaları ve saklanmaları gerekmektedir. Bu amaçla simetrik şifreleme algoritmaları kullanılabilir. Öncelikle veri sahibi kişi veya kurum simetrik bir anahtar üretir. Daha sonra simetrik şifreleme algoritması kullanarak saklamak istediği veriyi bu gizli anahtarla şifreler. Son olarak, bu şifreli metni uygun bir yerde depolar. Simetrik anahtarı da güvenli bir ortamda depolaması ve saklaması gerekmektedir. Çünkü şifrelenmiş verinin daha sonra şifresinin çözülmesi için bu anahtara ihtiyaç olacaktır. Böylece kötü niyetli kişiler gizli anahtara ulaşamadıkları sürece şifreli metni çözerek orijinal veriye ulaşamazlar.

Üçüncü uygulama alanı kimlik doğrulama olarak sıralanabilir. Birbiri ile haberleşmeyi planlayan iki kişi veya kurumun haberleşmeye başlamadan önce birbirlerinin kimliklerini doğrulamaları gerekmektedir. Bu doğrulamalar yapıldıktan sonra kişiler haberleşmeye başlayabilir. Kimlik doğrulamalarının yapılması için simetrik şifreleme algoritmaları kullanılabilir.

Özet

Bilgi güvenliği kavramı ve ihtiyacını açıklamak

Bilginin gizli ve değişmeden ulaştırılması insanlığın ilk yıllarından günümüze kadar oldukça büyük bir öneme sahip olmuştur. Geçmişte hükümdarlar komutanlarına önemli mesajlarını aktarabilmek için çeşitli yöntemler kullanmışlardır. Günümüzde bilgi teknolojilerindeki gelişmeye paralel olarak gizli veri aktarımı kritik bir öneme sahip olmuştur. Kriptografi bilim alanı bilginin gizli olarak paylaşılması ile ilgilenir.

Klasik şifreleme algoritmalarını açıklamak

Klasik algoritmalar, günümüz modern şifreleme algoritmalarına temel teşkil etmiştir. Geçmişten günümüze kullanılan şifreleme algoritmalarının açıkları ve eksiklikleri tespit edilerek yeni ve modern şifreleme algoritmaları geliştirilmiştir. Daha çok veri karıştırma yöntemleri ile çalışan klasik algoritmalardan bazıları Sezar şifreleme, Affine şifreleme, Monoalfabetik şifreleme ve Vigenere şifreleme olarak sayılabilir.

Dizi ve blok şifreleme arasındaki farkları sıralamak

Simetrik yöntemler dizi ve blok olmak üzere ikiye ayrılır. Dizi simetrik şifreleme yöntemleri bit temelli şifreleme ve çözme yapar. Bir bitlik açık metni yine bir bitlik şifrelenmiş metne dönüştürür. Blok şifreleme yöntemleri ise belirli uzunlukta bloklara bölünmüş açık metni belirli sayıda birbirini takip eden karışıklık ve yayılma işlemlerini kullanarak şifrelenmiş metne dönüştürür. Dizi şifreleme algoritmaları bit tabanlı oldukları için şifreleme ve çözme fonksiyonları basit ve hızlıdır. Dizi şifrelemede şifreleme ve çözme fonksiyonlarında kullanılacak anahtar dizilerinin her iki kullanıcıda da aynı olması gerekmektedir. Dizi şifrelemede kullanılan anahtar dizisi üreten fonksiyonlar başlangıç durumunun bilinmesi halinde aynı diziyi üretmek üzere tasarlanmışlardır.

Rastgele sayılar arasındaki farkları açıklamak

Kriptolojide rastgele sayıların büyük bir önemi vardır. Rastgele sayılar, gerçek, sözde ve kriptolojik olarak güvenli olmak üzere üç gruba ayrılır. Rastgele sayılar tekdüze dağılıma sahip ve bağımsız olmalıdır. Bağımsızlık, bir sonraki adımda üretilecek rastgele sayının önceki adımlarda üretilen sayılar ile ilişkisinin olmaması demektir. Para atışı sonucu elde edilecek rastgele bir sayının tura veya yazı gelme olasılığı önceki atışlardan bağımsız olarak %50'dir.

DES ve AES şifreleme yöntemlerinin çalışma prensiplerini tanımlamak

En yaygını olarak bilinen ve kullanılan simetrik blok şifreleme algoritmaları DES ve AES'dir. DES toplam 16 tur veya iterasyondan oluşan Feistel şifreleme yöntemi üzerine kurulmuştur. DES 56 bitlik gizli anahtar ve 64 bitlik blok uzunluğuna sahiptir. 56 bitlik gizli anahtar uzayının günümüzde yetersiz kalmasından dolayı güvenilir olarak kabul edilmez. AES algoritması 2000'li yılların başında DES'in yerine kabul edilmiştir. 128, 192 ve 256 bit olmak üzere 3 farklı uzunlukta gizli anahtar kullanılabilmektedir. Standartlarda kabul edilmiş birçok blok şifreleme modu vardır. Örnek olarak ECB, CBC, CFB, OFB ve CM modları gösterilebilir.

Kendimizi Sınayalım

1. DES şifreleme algoritmasının kullandığı blok boyutu kaç bittir?

a. 32
b. 48
c. 64
d. 128
e. 256

2. AES şifreleme algoritmasında kullanılabilecek anahtar boyutları aşağıdaki hangi seçenekte doğru verilmiştir?

a. 32/48/64
b. 48/56/64
c. 64/96/128
d. 128/192/256
e. 1024/2048/3072

3. Aşağıda verilen algoritmalarından hangisi bir dizi şifreleme algoritmasıdır?

a. DES
b. AES
c. 3DES
d. RC4
e. IDEA

4. DES algoritması kaç tur veya iterasyondan oluşur?

a. 8
b. 10
c. 12
d. 16
e. 32

5. AES şifreleme algoritması 128 bit uzunluğunda gizli anahtar kullanılması durumunda kaç tur veya iterasyondan oluşur?

a. 8
b. 10
c. 12
d. 14
e. 16

6. Aşağıdakilerden hangisi bir blok şifreleme modu **değildir?**

a. ECB
b. CBC
c. CFB
d. OFB
e. BCB

7. DES algoritmasında şifreleme ve şifre çözme için kullanılan anahtar uzunluğu kaç bittir?

a. 10
b. 16
c. 32
d. 56
e. 128

8. Toplam üç kişinin çalıştığı bir firma için simetrik şifreleme algoritması kullanılarak güvenli bir iletişim oluşturulmak istenirse kaç adet gizli anahtara gereksinim vardır?

a. 2
b. 3
c. 5
d. 10
e. 20

9. IDEA algoritmasında kullanılan anahtar uzunluğu kaç bittir?

a. 16
b. 32
c. 64
d. 128
e. 256

10. Aşağıda verilenlerden hangisi simetrik şifreleme algoritmalarının temel öğelerinden biri **değildir?**

a. Açık metin
b. Şifreleme fonksiyonu
c. Gizli anahtar
d. Çözme fonksiyonu
e. Doğrulama fonksiyonu

Kendimizi Sınayalım Yanıt Anahtarı

1. c	Yanıtınız yanlış ise "Data Encryption Standard" konusunu yeniden gözden geçiriniz.
2. d	Yanıtınız yanlış ise "Advanced Encryption Standard" konusunu yeniden gözden geçiriniz.
3. d	Yanıtınız yanlış ise "Dizi Şifreleme ve Blok Şifreleme" konusunu yeniden gözden geçiriniz.
4. d	Yanıtınız yanlış ise "Data Encryption Standard" konusunu yeniden gözden geçiriniz.
5. b	Yanıtınız yanlış ise "Advanced Encryption Standard" konusunu yeniden gözden geçiriniz.
6. e	Yanıtınız yanlış ise "Blok Şifreleme Metotları" konusunu yeniden gözden geçiriniz.
7. d	Yanıtınız yanlış ise "Data Encryption Standard" konusunu yeniden gözden geçiriniz.
8. b	Yanıtınız yanlış ise "Simetrik Şifreleme Algoritmaların Problemleri" konusunu yeniden gözden geçiriniz.
9. d	Yanıtınız yanlış ise "International Data Encryption Algorithm" konusunu yeniden gözden geçiriniz.
10. e	Yanıtınız yanlış ise "Giriş" konusunu yeniden gözden geçiriniz.

Sıra Sizde Yanıt Anahtarı

Sıra Sizde 1

Şifrelenen metin alıcı tarafından çözülerek açık metin elde edilir. Çözme fonksiyonu ile çözülen şifrelenmiş metin açık metni vermelidir. Eğer şifreleme fonksiyonu bire-bir değilse, alıcı elindeki şifreli karakterin hangi açık karaktere karşılık geldiğini bilemez. Eğer şifreleme fonksiyonu örten değilse, şifreli bir karakterin karşılığı açık karakter olmayacağından, alıcı bu karakterin karşılığı olan açık karakteri bilemez. Bu nedenle şifre çözmenin doğru çalışması için şifreleme fonksiyonları bire-bir ve örten olmalıdır.

Sıra Sizde 2

Sezar şifreleme algoritmasında açık metinde yer alan her harf alfabede üç ötelenir. Buna göre "hello" mesajını şifrelediğimizde elde edilen şifreli mesaj "KHOOR" olarak bulunur.

Sıra Sizde 3

Affine şifrelemede anahtarın iki bileşeni vardır. 23 harfli alfabe kullanıldığından, anahtarın *b* bileşeni 23 farklı değer alabilir. Anahtarın *a* bileşeni ise 23 ile aralarında asal olan ve 23'den küçük pozitif sayılar olabilir. Bu durumda *a* ise 22 farklı değer alabilir. Buna göre toplam 23×22 = 506 farklı anahtar kullanılabilir.

Sıra Sizde 4

DES, 3DES, AES ve IDEA simetrik algoritmalarına ek olarak Twofish, Blowfish, CAST ve Serpent gibi örnekler verilebilir.

Yararlanılan ve Başvurulabilecek Kaynaklar

Katz, J., Lindell Y. (2014). ***Introduction to Modern Cryptography***, CRC Press

Paar, C., Pelzl, J. (2010). ***Understanding Cryptography: A textbook for students and practitioners***, Springer Science & Business Media.

Stallings, W. (2011). ***Network Security Essentials: Applications and Standards***, Pearson Education.

Trappe, W., Washington, L.C. (2006). ***Introduction to Cryptography with Coding Theory***, Pearson Education.

Uçan, O. ve Osman, O. (2006). ***Bilgisayar Ağları ve Ağ Güvenliği***, Seçkin Yayınları.

4

Amaçlarımız

Bu üniteyi tamamladıktan sonra;

- Güvenlik servislerinin neler olduğunu ve ne sağladıklarını açıklayabilecek,
- Simetrik ve açık anahtar şifreleme yöntemleri arasındaki farkları ifade edebilecek,
- En yaygın kullanılan açık anahtar şifreleme algoritmalarını tanımlayabilecek,
- Dijital imzaların nasıl oluşturulduğunu ve kullanıldığını açıklayabilecek,
- Mesaj özetinin nasıl oluşturulduğunu ve kullanıldığını açıklayabilecek bilgi ve becerilere sahip olacaksınız.

Anahtar Kavramlar

- Açık Anahtar
- Gizli Anahtar
- RSA
- Dijital İmza
- Özet Fonksiyonu
- MD5
- SHA

İçindekiler

Açık Anahtar Şifreleme ve Mesaj Doğrulama

GİRİŞ

Simetrik anahtar şifreleme yöntemleri uzun yıllardır bir mesajın bir kullanıcıdan diğer bir kullanıcıya gizli bir şekilde ulaştırılmasında kullanılmıştır (Trappe ve Washington, 2006). Bankacılık ve bilgisayar teknolojilerinde yaşanan gelişmeye paralel olarak ortaya çıkan bazı gereksinimler simetrik şifreleme yöntemleri tarafından sağlanamamaktadır. Kullanıcılar arasında gizli anahtarların dağıtılması, mesaj içeriğinin değişime uğrayıp uğramadığının doğrulanması, mesajı oluşturan kişinin kimliğinin onaylanması gibi gereksinimleri sağlamak amacıyla 1976 yılında açık anahtar şifreleme yöntemi ortaya konmuştur (Stallings, 2011). Açık anahtar şifreleme yöntemlerinde kullanıcının birbiriyle ilişkili iki anahtarı vardır. Bu iki anahtar birbirinden bağımsız değildir. Aksine matematiksel olarak birbiri ile ilişkilidir. Bu anahtarlardan biri açık anahtar olarak adlandırılır. Açık anahtarın başkaları tarafından bilinmesinde hiçbir mahsur yoktur. Bu nedenle kullanıcılar açık anahtarlarını istedikleri ortamda yayınlayabilir. Açık anahtar, mesajların şifrelenmesinde ve dijital imzalarda mesajı gönderenin kimliğinin doğrulanmasında kullanılır. İkinci anahtar, gizli anahtar olarak bilinir. Gizli anahtarın sadece kullanıcının kendisi tarafından bilindiği kabul edilir. Gizli anahtarın ifşa olması durumunda gizlilik söz konusu değildir. Gizli anahtar, şifrelenmiş metinlerin çözülmesinde ve dijital imzaların oluşturulmasında kullanılır. Açık anahtarın aksine gizli anahtar, güvenli bir ortamda saklanmalı ve başkalarının bu anahtara erişimi engellenmelidir. Çünkü açık anahtar şifreleme algoritmalarının güvenliği, bu anahtarın gizliliğine bağlıdır.

Güvenlik sistemlerinin sağlaması gereken birçok güvenlik servisleri bulunur (Paar ve Pelzl, 2010). Farklı uygulamalar için değişik servislerin önemi vardır. Örneğin, İnternet üzerinden indirilen bir dosyanın tamamının indirilip indirilmediğini öğrenmek için mesaj bütünlüğü yeterlidir. Fakat çok önemli bir mesajın başkaları tarafından okunmaması isteniyorsa, gizlilik daha çok öneme sahip olmaktadır. İnternet üzerinden yapılacak alışverişlerde ise kredi kartı bilgisinin gizli bir şekilde gönderilmesi, istekte bulunan kişilerin kimliğinin doğrulanması ve yapılan isteğin kullanıcılar tarafından inkâr edilememesi önemlidir. Bu güvenlik servislerinden bazıları aşağıda verilmiştir.

Gizlilik: Sadece yetkili kişilerin mesajı okuyabilmesidir. Örneğin, Can arkadaşı Bora'ya bir mesaj göndermek istiyor. Bu mesajı sadece ve sadece Bora'nın okuyabilmesine gizlilik denir. Şifrelenmiş mesajı kötü niyetli kişiler elde etseler bile, açık metni okuyamamalıdırlar.

Mesaj bütünlüğü: Yetkisi olmayan kişilerin iletim halindeki mesaj içeriğinde hiçbir değişiklik yapamamalarıdır. Bora Can'dan gelen mesajı aldığında, mesaj içeriğinin kötü niyetli kişilerce değiştirilmediğinden emin olur.

Kimlik doğrulama: Mesajı oluşturan kişinin kimliğinin onaylanmasıdır. Bora mesajı aldığında, bu mesajın Can'dan geldiğinden emin olur.

İnkâr edememe: Mesajı oluşturan kişinin, oluşturduğu mesajı inkâr edememesidir. Ayrıca mesajı alan kişi, mesajın içeriğini değiştirerek başka mesaj aldığı iddiasında bulunamaz. Can Bora'ya gönderdiği mesajı inkâr edemez. Bora ise Can'dan başka bir mesaj aldığını iddia edemez.

Erişim kontrolü: Kullanıcılar kendilerine verilen yetkiler doğrultusunda servislerden faydalanmalıdır. Her kullanıcı kaynaklara, kendisine verilen yetkinin izin verdiği ölçüde erişebilir olmalıdır.

Kullanılabilirlik: Kullanıcıların, servisleri arzu ettikleri zaman kullanabilmesine imkân verilmelidir. Genel olarak, kaynaklara erişim yetkisi olan kullanıcıların erişim yetkisi oldukları zaman dilimlerinde bu kaynaklara erişebilmeleri anlamına gelir. Can'ın gönderdiği mesajın Bora'ya ulaşması kullanılabilirliğe bir örnektir.

Fiziksel güvenlik: Donanımın kötü niyetli kişiler tarafından fiziksel olarak zarara uğratılması engellenmelidir. Gerekli donanım güvenlik önlemleri alınmış olmalı ve çevresel faktörler ile doğal afetlere karşı korunaklı binalarda saklanmalıdır.

Denetim: Özel durumların kayıt altına alınması ile bir yanlış işlemin veya kötü niyetli kullanımın kim veya kimler tarafından yapıldığının tespit edilmesine imkân verilmelidir.

Yukarıdaki güvenlik servislerinin sağlanmasında kullanılan en yaygın yöntemin şifreleme olduğu söylenebilir. Kullanılan anahtar sayısına göre bu şifreleme algoritmaları simetrik anahtar şifreleme, açık anahtar şifreleme ve özet fonksiyonları olarak üç gruba ayrılır. Simetrik anahtar şifreleme aynı zamanda gizli anahtar şifreleme olarak da bilinir. Tek bir anahtar hem şifreleme hem de çözme için kullanıldığından simetrik olarak adlandırılır. Açık anahtar şifreleme, asimetrik anahtar şifreleme olarak da bilinir. Her kullanıcının birbiri ile ilişkili iki anahtarı vardır. Özet fonksiyonlarında ise anahtar kullanılmaz. Bu nedenle özet fonksiyonları anahtarsız şifreleme algoritmaları olarak isimlendirilir. Gizli anahtar şifreleme algoritmaları bit tabanlı operasyonlara dayanır. Açık anahtar şifreleme algoritmalarında matematiksel işlemler ağırlıklıdır. Bu yüzden simetrik şifreleme algoritmaları şifreleme ve çözme işlevlerini asimetrik şifreleme algoritmalarına göre daha hızlı yaparlar.

AÇIK ANAHTAR ŞİFRELEME ALGORİTMALARI

Açık anahtar şifreleme algoritmaları şifreleme ve çözme için farklı iki anahtar kullandıklarından asimetrik şifreleme olarak isimlendirilir. Teknolojik gelişmelere bağlı olarak simetrik şifreleme algoritmaları bazı güvenlik servislerini sağlamakta yetersiz kalmıştır. Gelişen teknoloji ve beklentilerle beraber güvenlik servislerinin nitelik ve niceliğindeki beklentiler de artmıştır. Bu nedenle, ilgili servislerin sağlanması için alternatif çözümlere ihtiyaç vardır. Simetrik şifreleme algoritmalarının yetersiz kaldığı durumlarda güvenlik servislerinin sunulması amacıyla özet fonksiyonları ve asimetrik şifreleme algoritmaları kullanılmaktadır. Simetrik şifreleme yöntemlerinde kullanılacak simetrik anahtarların kullanıcılara dağıtılması oldukça zordur. Simetrik anahtar şifreleme algoritmalarının en önemli problemi, gizli anahtarların dağıtılması olarak tanımlanan anahtar paylaşım problemidir. Simetrik anahtar şifreleme algoritması kullanarak haberleşmek isteyen iki kişiden biri tek kullanımlık bir oturum anahtarı üretir. Bu anahtarın şifreli mesajla beraber diğer kişiye iletilmesi gerekmektedir. Bu problem simetrik şifreleme algoritmalarının kullanımını zorlaştırmaktadır.

Yukarıda açıklanan gelişmeler ve simetrik şifreleme algoritmalarının problemleri nedeniyle alternatif yöntemler araştırılmıştır. Farklı bir teknik ile yukarıda açıklanan servislerin sağlanması ve gizli anahtarların dağıtılması gerekir. Bu açığı gidermek için açık anahtar şifreleme algoritmaları geliştirilmiştir. Diffie-Hellman-Merkel tarafından açık

anahtar şifreleme yöntemi ortaya konmuştur. Bu yöntemde simetrik şifrelemenin aksine her kullanıcının birbiri ile ilişkili bir açık ve bir gizli olmak üzere iki anahtarı vardır. Kullanıcı açık anahtarını herkes ile paylaşabilir fakat gizli anahtarını yalnızca kendisinin bilmesi gerekmektedir. Açık anahtar ve gizli anahtar matematiksel bir ilişki ile birbirlerine bağlanmıştır. Açık anahtar bilgisini kullanarak gizli anahtara ulaşmak imkânsızdır. Açık anahtar şifreleme algoritmalarında, açık ve gizli anahtardan herhangi biri şifreleme için kullanılabilir. Şifre çözme için, şifreleme için kullanılan anahtarın ilişkili olduğu diğer anahtar kullanılır. Eğer açık anahtar şifrelemek için kullanılmışsa, şifre çözme için o anahtarın karşılığı olan gizli anahtar kullanılır. Eğer şifreleme için gizli anahtar kullanılmışsa, bu şifreli mesajı çözmek için bu anahtarın karşılığı olan açık anahtar kullanılmalıdır.

Açık anahtar şifreleme yöntemleri, gerek dayandıkları matematiksel yöntemlerin uzun ve karmaşık hesaplamalar gerektirmesi, gerek anahtar uzunluklarının simetrik anahtar şifreleme yöntemlerine göre daha uzun olmasından dolayı gizli anahtar şifreleme algoritmalarına göre daha yavaş çalışmaktadırlar. Açık anahtar şifreleme yöntemleri daha çok mesaj bütünlüğü, kimlik doğrulama ve inkâr edememe gibi güvenlik servislerini sağlamak için kullanılır. Gizlilik ise daha hızlı olmalarından dolayı simetrik anahtar şifreleme algoritmaları ile sağlanır. Simetrik ve asimetrik anahtar şifreleme algoritmalarının birbirlerine göre avantaj ve dezavantajları vardır. Simetrik şifreleme algoritmaları daha hızlıdır. Ama anahtar paylaşım problemi vardır. Asimetrik şifreleme algoritmaları daha yavaş olmalarına rağmen anahtar paylaşım problemi yoktur. Bu nedenle simetrik şifreleme algoritmaları mesaj şifrelemek için kullanılır. Oturum anahtarı olan gizli anahtarın paylaşılması için ise asimetrik şifreleme algoritmaları kullanılır.

Açık anahtar şifreleme algoritmaları tek yönlü fonksiyonlar üzerine kurulmuştur. Tek yönlü fonksiyonlar prensip olarak, verilen girdiye karşılık çıktının kısa sürede hesap edilebilmesi; ancak bilinen çıktı değerine karşılık gelen girdi değerinin kolayca hesap edilememesine dayanmaktadır. Açık anahtar şifreleme yöntemlerinde üç farklı tek yönlü fonksiyon kullanılmıştır. Bu fonksiyonlar tam sayıyı asal çarpanlarına ayırma, ayrık logaritma ve eliptik eğriler fonksiyonlarıdır.

Tam sayıyı çarpanlarına ayırma ve ayrık logaritma 1970'li yılların ortasında ve eliptik eğriler ise 1980'li yılların ortasında sunulmuştur. Tam sayıyı asal çarpanlarına ayırma ve ayrık logaritma yöntemlerinde kullanılan anahtar uzunlukları 1024, 2048, 3072 bit gibi oldukça uzundur. Anahtar boyunun uzunluğu hem performans hem de güvenlik açısından önemlidir. Anahtar boyu uzadıkça, anahtar kümesinin eleman sayısı artar. Kaba kuvvet saldırılarının gerçekleştirilmesi zorlaşır. Dolayısıyla güvenlik artar. Fakat anahtar boyu arttıkça performans kötüleşir. Bu nedenle performans ve güvenlik birbiriyle çelişen amaçlardır. Anahtar boyu, güvenlik ve performansı en iyi dengeleyecek şekilde seçilmelidir. Eliptik eğri yöntemlerinin anahtar uzunlukları her iki yönteme göre daha kısadır.

Açık anahtar şifreleme algoritmalarının uygulanabilmesi için bazı şartları sağlamaları gerekmektedir. Öncelikle kullanıcılar, hem açık hem de gizli anahtarlarını kolaylıkla hesaplayabilmelidir. Asimetrik şifreleme algoritmaları kullanılarak şifreli mesaj değiştirmeye başlamadan önce haberleşecek kişiler, açık ve gizli anahtarlarını üretmelidirler. Açık anahtarlar yayınlanarak diğer kullanıcılar haberdar edilmelidir. Böylece ilgili kullanıcıyla güvenli haberleşmek isteyen kişiler kişinin açık anahtarını kullanabilir. İkinci olarak, şifreleme fonksiyonu ve ilgili anahtar kullanılarak şifreli mesaj kolaylıkla hesaplanmalıdır. Üçüncü gereksinim ise şifre çözme fonksiyonu ve ilgili anahtar kullanılarak şifreli metinden açık metin elde etmenin kolaylıkla yapılabilmesidir. Anahtarların üretilmesi, açık metnin şifrelenerek şifreli metnin elde edilmesi ve şifreli metnin çözülerek açık metnin hesaplanması işlemleri performans ile ilgilidir. Bu işlemler ne kadar hızlı yapılırsa, algoritmanın performansı o kadar iyidir.

Dördüncü gereksinim ise gizli anahtarın elde edilmesi ile ilgilidir. Hatırlanacağı gibi, açık anahtar şifreleme algoritmalarında açık anahtarlar herkes tarafından bilinmektedir. Bu nedenle kötü niyetli kişiler de bu anahtarları bilmektedir. Açık anahtardan gizli anahtarın elde edilmesi hesaplama açısından olanaksız olmalıdır. Yani açık anahtar verildiğinde, gizli anahtarın elde edilmesi hesaplama açısından imkânsız olmalıdır. Açık anahtara ek olarak, kötü niyetli kişiler başka bilgiler de elde edebilir. İki kişi güvenli haberleşse bile, kötü niyetli kişiler bu haberleşmeleri dinleyerek şifreli metinleri ele geçirebilirler. Ne kadar çok bilgi elde edilirse, gizli veriyi ele geçirmek o kadar kolaylaşacaktır. Bu nedenle beşinci gereksinim şöyle açıklanabilir: Kötü niyetli kişiler açık anahtarı ve şifreli metni elde etseler bile, gizli anahtara ulaşmaları hesaplama açısından olanaksız olmalıdır. Bu iki gereksinim ise algoritmanın güvenliği ile ilgilidir. Kullanılacak şifreleme algoritması hem performans açısından iyi olacak hem de güvenli olacaktır. Burada güvenlik, gizli anahtarın gizliliği ile ilgilidir. Bu anahtarı elde etmek ne kadar zorsa, algoritma o kadar güvenilir kabul edilir.

Açık anahtar şifreleme algoritmalarının son gereksinimi, açık ve gizli anahtarın şifreleme ve şifre çözme işlemleri için herhangi bir sırada yapılabilmesine olanak sağlaması olarak açıklanır. Bu algoritmaların en önemli özelliği, şifreleme ve çözme için anahtarlar herhangi bir sıra ile kullanılabilir. Bunu daha açık bir ifadeyle şöyle açıklayabiliriz. Bir mesaj açık anahtarla şifrelenip gizli anahtarla çözülebilir veya gizli anahtarla şifrelenip açık anahtarla çözülebilir. Bu son gereksinim ise kolay kullanılabilirlik ile alakalıdır. Yukarıda açıklanan iki özellik olan **performans** ve **güvenliğe** ek olarak üçüncü özellik **kolay kullanılabilirlik** özelliğidir. Eğer elimizde iki veya daha fazla şifreleme algoritması varsa, bunlardan birinin şifreleme algoritması olarak seçilmesi gerekmektedir. Bu seçimin belli kriterlere göre yapılması gerekir. Bu kriterler güvenlik, performans ve kolay kullanılabilirlik olarak sıralanır. Bu üç kriter veya şifreleme algoritmalarının sağlaması gereken özellikler birbirleriyle çelişen özelliklerdir. Biri iyileşirken diğeri veya diğer iki özellik kötüleşebilir. Bu nedenle bu üç özelliğin aynı anda iyileştirilmesi zordur.

En uygun şifreleme algoritmasını seçmek için kullanılan kriterler **güvenlik, performans** ve **kolay kullanılabilirliktir.**

SIRA SİZDE 1

Güvenlik, performans ve kolay kullanılabilirlik özelliklerinden biri veya ikisi iyileştirilmek istendiğinde, diğer özelliklerde kötüleşme olabilir. Güvenlik, performans ve kolay kullanılabilirlik özelliklerinin birlikte iyileştirilemeyeceğini ifade eden terim nedir?

Açık Anahtar Şifreleme Algoritmalarının Uygulama Alanları

Simetrik anahtar şifreleme algoritmaları gibi açık anahtar şifreleme algoritmaları da benzer uygulama alanlarına sahiptir. Öncelikle simetrik şifreleme algoritmaları açık anahtar şifreleme algoritmalarına göre daha hızlı olduklarından, bir mesajın gizli olarak alıcıya ulaşması için simetrik şifreleme algoritmaları kullanılır. Açık anahtar şifreleme algoritmalarının ise en önemli iki uygulama alanı vardır. Bunlardan birincisi oturum anahtarının kullanıcılar arasında güvenli bir şekilde paylaşılması, ikincisi ise dijital imza ya da diğer adıyla elektronik imza uygulamasıdır.

Simetrik şifreleme yöntemleri kullanarak gizli mesaj paylaşmak isteyen Can ve Bora adlarında iki kullanıcı olsun. Can gönderici olduğundan, bu haberleşme için oturum anahtarı oluşturur. Bu oturum anahtarını güvenli bir şekilde alıcı olan Bora'ya göndermesi gerekir. Bunun için açık anahtar şifreleme algoritması kullanır. Açık anahtar şifrelemede her kullanıcı kendi açık ve gizli anahtarlarını oluşturur. Öncelikle Can kendi gizli ve açık anahtar çiftini oluşturur. Üretmiş olduğu açık anahtarını bütün kullanıcıların erişebildiği sunucularda depolar. Bora Can'ın açık anahtarını sunucudan elde eder. Aynı şekilde Bora da gizli ve açık anahtar çiftini üretir. Açık anahtarını bütün kullanıcıların erişebilmesi için sunucuyla paylaşır. Can, Bora'nın açık anahtarını sunucudan elde eder. Can kendi

ürettiği oturum anahtarını Bora'ya göndermek istediğinden, oturum anahtarını Bora'nın açık anahtarı ile şifreler. Asimetrik şifreleme kullanarak şifrelenen bu oturum anahtarını Bora'ya gönderir. Şifrelenmiş oturum anahtarını çözmek için Bora'nın gizli anahtarına ihtiyaç vardır. Gizli anahtarı sadece Bora bildiğinden, Bora bu şifreli anahtarı çözer ve oturum anahtarına ulaşır. Bora'dan başkası şifre çözmek için ihtiyaç duyulan gizli anahtarı bilmediğinden, oturum anahtarına sadece Bora ulaşır ve oturum anahtarı gizlilik bozulmadan paylaşılmış olur. Açık anahtar şifreleme algoritmaları simetrik şifreleme algoritmalarının en önemli problemi olan anahtar paylaşım problemini yukarıda basitçe anlatılan şekilde çözer.

Açık anahtar şifreleme algoritmalarının en önemli ikinci uygulama alanı dijital veya elektronik imza olarak adlandırılır. Dijital imza konusu ünitenin sonraki bölümlerinde daha detaylı biçimde anlatılacaktır. Dijital imza, mesajı gönderen kullanıcının kimliğini doğrulamak için kullanılır. Kimlik doğrulama için değişik doğrulayıcılar kullanılabilir. Akıllı kartlar, güvenlik simgeleri ve kullanıcı adı ve şifresi gibi kimlik doğrulayıcılar olabilir. Bunların yanında dijital imza da kimlik doğrulamak için kullanılan yöntemlerden biridir. Diğer kimlik doğrulayıcılardan farklı olarak, dijital imza inkâr edilemezlik güvenlik servisi de sunar. Bazı durumlarda birbiri ile haberleşen iki kişi herhangi bir işlemin veya haberleşmenin bir parçası olduklarını inkâr edebilir. Örneğin, Can arkadaşı Bora'ya bir mesaj göndermiş olsun. İnkâr etme durumu iki farklı şekilde gerçekleşebilir. Can Bora'ya mesajı gönderdiğini inkâr edebilir. Bora ise Can'dan böyle bir mesaj aldığını veya gelen mesajı değil, içeriği farklı başka bir mesajı aldığını iddia edebilir. Bu tür ihtilafların oluşması durumunda, üçüncü kişilerce bu ihtilafların çözülmesi gerekir. İnkâr etme ihtilaflarına karşı inkâr edilemezlik servisleri sunan yöntemler kullanılmalıdır.

Açık anahtar şifreleme algoritmaları, oturum anahtarı paylaşımı ve dijital imzaya ek olarak başka alanlarda da kullanılabilir. Bunlardan biri güvenli veri depolamadır. Simetrik şifreleme algoritmaları gibi asimetrik şifreleme algoritmaları da gizli verinin güvenli saklanması için kullanılabilir. Burada ilk tercih edilen algoritmalar, hızlı olmalarından dolayı simetrik şifreleme algoritmalarıdır. Asimetrik şifreleme algoritmaları karmaşık olduklarından dolayı güvenli depolama için tercih edilmeyebilir. Güvenli veri saklamak için kullanıcı gizli veriyi kendi açık anahtarı ile şifreleyerek şifreli veriyi elde eder. Bu şifreli verinin şifresinin çözülerek orijinal veriye ulaşmak için açık anahtarın karşılığı olan gizli anahtara ihtiyaç vardır. Bu anahtarı ise sadece şifrelemeyi yapan kullanıcı bildiğinden, kötü niyetli kişilerin bu anahtara ve dolayısıyla orijinal gizli veriye ulaşmaları mümkün değildir.

Açık anahtar şifreleme algoritmaları oturum anahtarı paylaşmak, kimlik doğrulama, inkâr edilemezlik ve güvenli veri saklama amacıyla kullanılabilir.

Açık Anahtar Şifreleme Algoritmalarına Karşı Yapılan Saldırılar

Bütün şifreleme algoritmalarına karşı saldırılar gerçekleştirilebilir. Bu saldırıların amacı, gizli anahtarları ele geçirerek şifrelenmiş mesajlardan orijinal mesajlara ulaşmaktır. Açık anahtar şifreleme algoritmalarına karşı değişik saldırılar olabilir. Kötü niyetli kişilerin bu saldırıları gerçekleştirmeleri için üç şey gerekir.

Öncelikle saldırıları gerçekleştirmek için **motivasyon** gereklidir. Sebepsiz yere saldırıların gerçekleştiği düşünülemez. Her türlü saldırının arkasında bir motivasyon vardır. Eğlenmek için bile yapılmış olsa, saldırganların bir motivasyonu vardır. Bu motivasyonlar arasında tanınma, başkalarınca takdir edilme, politik sebepler, dini sebepler, para ve güç elde etmek gibi motivasyonlar sayılabilir.

İkinci olarak, kötü niyetli kişilerin saldırıları gerçekleştirmek için kullanacakları bir **metot** olmalıdır. Burada anlatılmak istenen kötü niyetli kişilerin saldırı yapacakları sistem veya algoritma hakkında bilgiye sahip olmaları, belli bir yeteneğe sahip olmaları, ataklar için gerekli araçlara ve yeterli maddi güce sahip olmaları olarak açıklanabilir. Saldırganlar

atak yapacakları sistemleri çok iyi tanımalı ve bu sistem hakkında yeterli bilgiye sahip olmalıdır. Şifreleme algoritmasına saldırılacaksa, algoritmanın nasıl çalıştığı bilinmelidir. Mümkün olduğunca bilgi ve veri elde edilmelidir. Yetenek çok önemlidir. Saldırıları gerçekleştirmek için bu konuda yetenekli olmalı ve yeterli bilgi ve tecrübeye sahip olunmalıdır. Ayrıca ihtiyaç duyulacak araç ve maddi imkânlara sahip olunmalıdır.

Son olarak, kötü niyetli kişilerin ihtiyaç duyacağı şey **fırsat** olarak sıralanabilir. Saldırılacak sistemde bir açık bulunmalıdır. Açıklar tehditlere yol açan zayıflıklardır. Saldırı yapacak kişi sistemde var olan açıkları tespit etmeye çalışır. Bu tür zayıflıklar olmadan saldırıların gerçekleştirilmesi çok zordur. Kötü niyetli kişilerin saldırıyı gerçekleştirecek zamana ihtiyaçları vardır. Ayrıca sisteme giriş yapabilecek ortamın olması gerekir.

Kötü niyetli kişilerin saldırıları gerçekleştirmek için ihtiyaç duydukları üç şey **motivasyon, metot** ve **fırsat** olarak sıralanabilir.

Yukarıda açıklanan gereksinimler, şifreleme algoritmalarına yapılacak saldırılar için kötü niyetli kişilerde bulunmalıdır. Bunların biri eksikse saldırının gerçekleşmesi beklenemez. Bu üç gereksinimin türü ve gerekçesi saldırganlara göre değişebilir. Amatörler için motivasyon eğlence olabilir. Ama kariyer suçluları için motivasyon politik ya da ekonomik sebepler olabilir. Kullanılacak metotlar da saldırganların sınıfına göre değişir. Benzer şekilde ihtiyaç duyulan fırsat saldırganların sınıfına ve saldırı türüne göre farklılık gösterir.

Açık anahtar şifreleme algoritmalarına karşı yapılabilecek değişik saldırılar vardır. Bunlardan birincisi, açık anahtar bilgisini kullanarak gizli anahtara ulaşmak şeklinde açıklanabilir. Bilindiği gibi açık anahtarlar herkes tarafından bilinir. Bu anahtarları elde etmek için herhangi bir çaba harcamaya gerek yoktur. Açık anahtar bilindiğinde gizli anahtar elde edilmeye çalışılabilir. Ama anahtarlar belli şartlara göre dikkatli seçilirse, açık anahtar bilgisinden gizli anahtarın elde edilmesi hesaplama açısından olanaksızdır denebilir. Benzer şekilde ikinci bir saldırı türü, açık anahtar bilgisi ve bu anahtarla şifrelenmiş şifreli metin bilgisinden yola çıkarak gizli anahtarı elde etmeye çalışmak olabilir. Kötü niyetli kişiler açık anahtar bilgisine sahiptir. Daha başarılı bir saldırı gerçekleştirmek için şifreli metinleri elde edebilirler. Bunun için haberleşmeleri dinleyerek, şifreli olarak iletilen mesajların şifreli metinlerini biriktirirler. Açık anahtar şifreleme algoritmalarında, açık anahtar ile beraber şifreli metin bilinse bile, gizli anahtarı elde etmek hesaplama açısından olanaksızdır.

Diğer saldırı türü, bütün şifreleme algoritmalarına karşı gerçekleştirilen en yaygın ataklardan biri olan kaba kuvvet atağıdır. Olası bütün anahtarlar sırayla denenerek gizli anahtar elde edilmeye çalışılır. Bu nedenle anahtar uzunluğu, bu tür saldırılara karşı yeterli güvenlik sağlayacak şekilde belirlenmelidir. Anahtar uzunluğu arttıkça performansın düşeceği de unutulmamalıdır.

Açık anahtar şifreleme algoritmalarının en yaygın uygulama alanlarından birinin, simetrik anahtar şifreleme algoritmalarında kullanılan oturum anahtarı paylaşımı olduğu belirtilmişti. Oturum anahtarı üretildikten sonra bu anahtar, karşı tarafın açık anahtarı ile şifrelenerek alıcıya gönderilmektedir. Oturum anahtarının uzunluğu önemlidir. Eğer anahtar uzunluğu küçük olan simetrik anahtar, açık anahtar şifreleme algoritması ile şifrelenmişse, *tahmin edilebilir mesaj atağı* ile bu anahtar elde edilebilir. Burada dikkat edilmesi gereken nokta şöyle açıklanabilir. Asıl amaç açık şifreleme algoritmasında kullanılan gizli anahtarı elde etmek değildir. Açık anahtar şifreleme algoritması ile şifrelenen oturum anahtarını ele geçirmektir. Tahmin edilebilir mesaj atağı bu amaçla kullanılan bir ataktır. Bu saldırıyı bir örnekle açıklamaya çalışalım. Can ve Bora'nın haberleşmek için simetrik şifreleme kullandıklarını varsayalım. Bunun için DES simetrik şifreleme algoritması kullanmaya karar verdiklerini düşünelim. Şifreleme için üretilen ve kullanılan oturum anahtarı 56 bitlik bir anahtardır. Bu oturum anahtarını Can üretir ve mesaj şifreleme için kullanır. Oturum anahtarını da Bora'ya güvenli bir şekilde göndermek için asimetrik şifreleme kullanarak Bora'nın açık anahtarı ile şifreler ve Bora'ya gönderir. Bilindiği gibi Bora'nın

açık anahtarı herkese açıktır. Can'ın Bora'ya gönderdiği bu şifreli anahtar mesajının bir kopyasını, kötü niyetli bir kişi haberleşmeyi dinleyerek elde edebilir. Bu durumda kötü niyetli kişinin elinde Bora'nın açık anahtarı ve Bora'nın açık anahtarı ile şifrelenmiş oturum anahtarının şifreli hali vardır. Kötü niyetli kişinin ayrıca Can'ın oturum anahtarını şifrelemek için kullandığı asimetrik şifreleme algoritmasının ne olduğunu bildiğini varsayalım. Genel olarak düşünülürse, 56 bit uzunluğundaki oturum anahtarının çok kısa bir anahtar olduğu söylenebilir. Bu anahtar 56 bit olup her bitin alabileceği değer ya 0 ya da 1'dir. Yani her biri için iki seçenek vardır. Bu durumda 56 bitlik bir anahtarın seçilebileceği anahtar kümesinde toplam 2^{56} anahtar vardır. Kötü niyetli kişi bu anahtarları sırasıyla şifreler. Bunun için Can'ın kullandığı asimetrik şifreleme algoritmasını ve Bora'nın açık anahtarını kullanır. Bu kümede yer alan toplam 2^{56} anahtarı sırasıyla şifreleyip elde ettiği şifreli anahtarı, Can ve Bora'nın haberleşmesini dinleyerek elde ettiği şifreli metin ile karşılaştırır. Eğer kendi hesapladığı bir şifreli metin Can ve Bora'yı dinleyerek elde ettiği şifreli metine eşitse, bu anahtarın Can'ın ürettiği oturum anahtarı olduğu anlaşılır. Tahmin edilebilir mesaj atağı, kaba kuvvet atağına benzemektedir. Şifrelenen mesaj, tahmin edilebilir bir mesajdır. Bu mesajın ne olduğu bilinmediğinden, olası bütün mesajlar (oturum anahtarları) sırayla şifrelenerek oturum anahtarı bulunmaya çalışılır.

SIRA SİZDE 2

56 bitlik bir oturum anahtarının açık anahtar şifreleme algoritması ile şifrelendiğini varsayalım. Tahmin edilebilir mesaj atağı kullanılarak bu oturum anahtarı elde edilmeye çalışılmaktadır. Bu durumda kötü niyetli kişi en iyi durumda, en kötü durumda ve ortalama olarak kaç şifreleme yaparak oturum anahtarını elde edebilir?

RSA

Diffie-Hellman'ın ortaya koydukları prensipleri yerine getirmek üzere 1977 yılında Ron Rivest, Adi Shamir ve Leonard Adleman RSA algoritmasını sundular (Paar ve Pelzl, 2010). Algoritma adını, öneren araştırmacıların soyadlarının ilk harflerinden almaktadır. RSA, eliptik eğriler yöntemiyle, daha kısa anahtarlar kullanmasına rağmen en yaygın olarak kullanılan ve bilinen açık anahtar şifreleme yöntemidir. Kısa metinlerin şifrelemesinde, dijital imza oluşturmada ve simetrik yöntemler için gerekli gizli anahtarın kullanıcılara dağıtılmasında kullanılır. Prensip olarak, iki büyük sayıyı çarpmanın kolay olması, ancak büyük bir sayıyı faktörlerine ayırmanın zor olması prensibi üzerine kurulmuştur. RSA bir açık anahtar şifreleme algoritması olduğundan hızı düşüktür. Bu nedenle kısa metinlerin şifrelenmesi için kullanılabilir ve uzun metinlerin şifrelenmesi için kullanılması performans açısından çok uygun değildir. RSA şifreleme algoritması bir blok şifreleme algoritmasıdır. Şifrelenecek blokların uzunluğu değişkenlik gösterebilmektedir.

RSA algoritması için gerekli açık ve gizli anahtarların oluşturulması aşamasında aşağıdaki adımların uygulanması gerekmektedir. Bu işlemleri RSA algoritmasını kullanarak güvenli haberleşmek isteyen her kullanıcı gerçekleştirir.

- p ve q gibi iki büyük asal sayı seçilir.
- n değeri p ve q sayılarının çarpımı olarak hesaplanır. Yani $n = p \times q$.
- Euler sayısı (p-1) ile (q-1) değerlerinin çarpımı olarak hesaplanır. Euler sayısı $\emptyset$ ile gösterilir. Bu nedenle $\emptyset(n) = (p\text{-}1)\times(q\text{-}1)$ olarak bulunur.
- $\emptyset(n)$ değeri yani Euler sayısı ile aralarında asal olmak üzere bir açık anahtar belirlenir. Açık anahtar e simgesi ile gösterilir. Açık anahtar 1'den büyük, $\emptyset(n)$ değerinden küçüktür ve $\emptyset(n)$ değeri ile aralarında asaldır, yani ortak bölenlerinin en büyüğü 1'dir. Açık anahtar bu şartlara göre seçilir.
- $e \times d = 1$ **mod** $\emptyset(n)$ şartını sağlayacak şekilde d gizli anahtarı hesaplanır.

Hem gönderen hem de alıcı bu işlemleri yaptıktan sonra kendilerine ait gizli ve açık anahtarı elde ederler. Açık anahtarın iki bileşeni vardır. Açık anahtar (e, n) ikilisi olarak ilan edilir. Her kullanıcı kendi açık anahtarını, bu iki bileşeni içerecek şekilde ilan eder. Gizli anahtarın da iki bileşeni vardır. Gizli anahtar (d, n) ikilisi olarak gizli bir şekilde saklanır.

RSA algoritmasında kullanılan şifreleme ve şifre çözme fonksiyonlarını şöyle açıklayabiliriz. Eğer x açık metin, y şifrelenmiş metin, n iki büyük asal sayının çarpımı ($n = p \times q$), e açık anahtar ve d gizli anahtar olarak kabul edilirse, RSA algoritmasında şifreleme ve çözme işlemleri aşağıdaki gibi uygulanır:

Şifreleme fonksiyonu: $y = x^e$ **mod** n
Çözme fonksiyonu: $x = y^d$ **mod** n

Açık anahtar şifreleme algoritması olan RSA algoritmasında açık ve gizli anahtarların nasıl seçilip hesaplandığını bir örnekle anlayalım. Konunun anlaşılması için işlemleri çok küçük asal sayılarla yapalım. Asal sayılar, sadece kendisi ve 1 sayısına bölünebilen 1'den büyük pozitif tam sayılardır. İki asal sayı olarak $p = 13$ ve $q = 17$ seçilsin. Bu durumda $n = p \times q = 13 \times 17 = 221$ olarak hesaplanır. Euler sayısı $\emptyset(n) = (p\text{-}1) \times (q\text{-}1) = 12 \times 16 = 192$ olarak hesaplanır. Açık anahtar 1'den büyük ve $\emptyset(n)$ değerinden küçük olacak şekilde $\emptyset(n)$ değeri ile aralarında asal olan bir değer olarak seçilebilir. Buna göre açık anahtar, $e = 5$ olarak seçilebilir. Gizli anahtar ise $e \times d = 1$ **mod** $\emptyset(n)$ şartını sağlayacak şekilde d = 77 olarak hesaplanır. Çünkü 5×77 = 1 **mod** 192'dir. Bu hesaplamalara göre açık anahtar (5, 221) ve gizli anahtar (77, 221) olarak elde edilmiş olur. Bu örnekte kullanılan asal sayılar çok küçük sayılardır.

Anahtar üretmeye ek olarak, şifreleme ve çözme fonksiyonlarının nasıl çalıştığını da bir örnekle açıklamaya çalışalım. Mesaj şifrelenirken takip edilecek işlemleri kısaca gözden geçirelim. Şifrelenecek mesaj öncelikle bir sayıya çevrilir. Bunun için mesaj içindeki her harf alfabede bu harfe karşılık gelen pozisyon sayısı ile temsil edilir. Şifrelenecek mesaj M ise, sayıya çevrilen mesaja m diyelim. Daha sonra m sayısı ile n sayısı karşılaştırılır. Eğer m sayısı n sayısından küçükse problem yoktur. Tersi durumunda, yani m sayısı n sayısından büyük veya eşitse m sayısı, her bir parçası n sayısından küçük olacak şekilde parçalara bölünür. Son olarak, bu parçalanmış sayılar şifreleme fonksiyonu ile şifrelenir.

Kullanıcı Can'ın yukarıda belirtilen adımları takip ederek açık anahtarını 5 ve gizli anahtarını 77 olarak belirlediği kabul edilirse, kendisine RSA kullanarak gizli bir mesaj göndermek isteyen kullanıcı Bora, şifrelenmiş metni hesap etmek için öncelikle Can'ın açık anahtarını bilmelidir. Can'ın açık anahtarı herkese ilan edildiğinden Bora bu anahtarı bilmektedir. Bora'nın göndereceği mesajın sayısal karşılığının 12 olduğunu varsayalım. Orijinal açık metnin sayı karşılığı olan 12 sayısı $n = 221$ sayısından küçüktür. Bu nedenle 12 sayısının küçük parçalara ayrılmasına gerek yoktur. Bu durumda Bora, 12 sayısını şöyle şifreler: $y = 12^5$ **mod** 221 = 207. Bora bu şifreli mesajı Can'a gönderir. Can, şifrelenmiş metinden açık metni elde etmek için gizli anahtarını kullanmalıdır. Can RSA çözme fonksiyonunu kullanarak $x = 207^{77}$ **mod** 221 = 12 değerini elde eder. Son olarak, sayısal değerler karşılıkları olan harflerle yer değiştirilerek açık metin elde edilmiş olur.

Verilen örnekten anlaşılacağı üzere gerekli hesaplamaların yapılması için uzun zaman gerekebilir. Çünkü RSA algoritmasında, hem anahtarların üretilmesinde hem de şifreleme ve çözmede, üs alma ve modüler hesaplama gibi uzun zaman gerektiren işlemler yapılmaktadır. Gerçekte kullanılan n sayısının yaklaşık 300 basamaktan büyük olduğu düşünülürse gerek anahtarların hesaplanması gerek şifreleme ve çözme fonksiyonlarının hızlandırılması için bazı yöntemler sunulmuştur. **Çin Kalan Teoremi, hızlı üs hesaplama** ve **küçük açık anahtar seçme** gibi yöntemlerin kullanılması RSA algoritmasını hızlandırmak için tavsiye edilmiştir.

RSA algoritmasının hızlandırılması için kullanılabilecek yöntemler **Çin Kalan Teoremi, hızlı üs alma** ve **küçük açık anahtar seçme** olarak sayılabilir.

RSA algoritmasında $p = 5$ ve $q = 7$ verildiğine göre açık ve gizli anahtar olarak kullanılabilecek anahtarları hesaplayınız.

SIRA SİZDE 3

RSA asimetrik şifreleme algoritması genel olarak mesaj şifreleme ve çözme, dijital imza ve anahtar paylaşımı için kullanılabilir. Bu açık anahtar algoritmasının yanında başka algoritmalar da vardır. Bunlardan biri Diffie-Hellman şifreleme algoritmasıdır.

Diffie - Hellman Şifreleme Algoritması

Bu algoritma ilk defa 1976 yılında Whitfield Diffie ve Martin Hellman tarafından önerilmiştir. Diffie - Hellman şifreleme algoritmasının uygulama alanı RSA'ye göre daha sınırlıdır. Açık anahtar veya asimetrik şifreleme algoritması olan Diffie-Hellman, aslında anahtar değişimi protokolü olarak bilinir. Bu nedenle Diffie-Hellman şifreleme algoritması iki kullanıcı arasında gizli bir oturum anahtarının oluşturulması için kullanılır. Değiştirilmiş Diffie-Hellman algoritması başka uygulamalarda kullanılabilir. Özelleştirildiği işlem olan anahtar paylaşımı konusunda diğer algoritmalara göre daha başarılı bir algoritmadır. Diffie-Hellman şifreleme yöntemi ile gizli anahtar oluşturan herhangi iki kişi, simetrik şifreleme algoritması ve bu gizli anahtarı kullanarak mesajları şifreleyip birbirlerine iletebilirler. Bu algoritmanın en önemli problemi, öncesinde kimlik doğrulama yapılması gerekliliğidir. Kullanıcılar, birbirlerinin kimliğini mutlaka doğruladıktan sonra oturum anahtarı oluşturmaya başlamalıdır. Diffie-Hellman şifreleme algoritmasının güvenliği ayrık logaritma hesaplanmasının zorluğuna dayanmaktadır. RSA şifreleme algoritmasının güvenliği ise verilen bir n sayısının çarpanlarına ayrılmasının zorluğuna dayanmaktadır.

İlerleyen kısımlarda tüm ayrıntılarıyla anlatılacak olan yöntemin kavranması için metaforik olarak renkli boyaları kullanalım. Gizli mesaj paylaşmak isteyen kullanıcılar herkesin bileceği şekilde ortak bir renkte boya seçerler. Daha sonra her bir kullanıcı, diğer kullanıcıların bilmeyeceği, sadece kendisinin bileceği başka bir renk boyayı seçerek bunu ortak renkteki boya ile karıştırır. Kullanıcılar elde ettikleri karışımı gizli mesaj paylaşacağı diğer kullanıcılara gönderirler. Birbirlerinin karışımlarını elde eden kullanıcılar kendi gizli renkli boyalarını karışıma ilave ederler. Sonuç olarak elde edilen karışımlar, her iki kullanıcının kendisinin ve mesajlaşacağı kullanıcının gizli ve ortak renk seçimini barındırır. Her bir kullanıcının seçmiş olduğu gizli rengi ne karşı kullanıcı ne de kötü niyetli başka kişiler tahmin edemezler.

Metafordan yola çıkarak Can ve Bora isimli iki kullanıcının Diffie-Hellman şifreleme algoritmasını kullanarak nasıl gizli anahtar oluşturduklarını açıklamaya çalışalım. Can ve Bora ortaklaşa p gibi bir büyük asal sayı belirler. Sonra bu asal sayıdan küçük olacak şekilde p asal sayısının primitif kökü olan bir g sayısını seçerler. Can ve Bora p ve g sayılarını bilmektedir. Primitif kök kavramı şöyle açıklanabilir. Bir p asal sayısının primitif kökü olan g sayısının 1'den başlayarak p-1'e kadar olan üslerini hesapladıktan sonra **mod** p'ye göre denklerini bulursak, 1'den p-1'e kadar olan bütün sayıları karışık bir sırada elde ederiz. Bu şartı sağlayan g değerleri p asal sayısının primitif kökleri olarak adlandırılır. Örneğin, 19 asal sayısının primitif kökleri 2, 3, 10, 13, 14 ve 15 sayılarıdır.

İki kullanıcının ortaklaşa kararlaştırdıkları p ve g sayıları herkes tarafından bilinen açık değerlerdir. Bunların bilinmesinin bir mahsuru yoktur. Can bir gizli anahtar seçer. Bu anahtara A diyelim. Aynı şekilde Bora bir gizli anahtar seçer. Buna B diyelim. Can $T = g^A$ **mod** p değerini hesaplar. Bora ise $V = g^B$ **mod** p değerini hesaplar. Daha sonra Can T değerini Bora'ya, Bora ise V değerini Can'a gönderir. Değiştirilen bu T ve V değerleri geneldir ve herkes tarafından bilinmesinde bir mahsur yoktur. Fakat A ve B değerleri gizlidir. Can $K = V^A$ **mod** p değerini hesaplar. Benzer şekilde Bora $K = T^B$ **mod** p değe-

rini hesaplar. Dikkat edilirse, hem Can hem de Bora aynı K değerini hesaplamış olurlar. Hesaplanan bu K değerine sadece Can ve Bora tarafından bilinen gizli anahtar veya oturum anahtarı denir. Bu şekilde iki kullanıcı, sadece kendilerinin bildiği bir gizli anahtarı oluşturmuş olurlar.

Diffie-Hellman algoritmasında üs hesaplama kolay iken, ayrık logaritmaları hesaplamak zordur. Bu nedenle, herkes tarafından bilinen genel veya açık değerler olan p, g, T ve V değerleri verildiğinde, gizli anahtarlar olan A ve B değerleri hesaplanamaz.

Diffie-Hellman anahtar değişim algoritmasını basit bir örnekle açıklayalım. Can ve Bora $p = 23$ ve $g = 5$ değerlerini seçer. Algoritmaya göre p asal sayı ve g bu asal sayının primitif kökü olmalıdır. Can'ın seçtiği gizli anahtar 2, Bora'nın seçtiği gizli anahtar ise 4 olsun. Can $T = 5^2$ **mod** 23 = 2 değerini hesaplar ve Bora'ya gönderir. Bora $V = 5^4$ **mod** 23 = 4 değerini hesaplar ve Can'a gönderir. Can $K = 4^2$ **mod** 23 = 16 değerini bulur. Benzer şekilde Bora $K = 2^4$ **mod** 23 = 16 değerini bulur. Hem Can hem de Bora aynı K değerini 16 olarak hesaplarlar. Bu $K = 16$ anahtarı sadece Can ve Bora'nın bildiği gizli bir anahtardır.

SIRA SİZDE 4

Diffie-Hellman örneğinde gizli anahtarlar sırasıyla 3 ve 5 seçildiğinde, Can ve Bora'nın elde edeceği gizli anahtarı bulunuz.

ElGamal Şifreleme Sistemi

Taher ElGamal tarafından 1985 yılında ayrık logaritma üzerine kurulan bir açık anahtar şifreleme yöntemidir. Diffie-Hellman algoritmasında olduğu gibi, ElGamal algoritmasının güvenliği de ayrık logaritmaların hesaplanmasının zorluğuna dayanmaktadır. ElGamal şifreleme algoritmasını bir örnekle aşağıdaki gibi açıklayabiliriz.

Can bir p asal sayısı seçer. Diyelim ki, $p = 7$ olarak seçilsin. Can bu asal sayının primitif kökü olan g sayısını seçer. Bu değerin $g = 2$ olduğunu varsayalım. Daha sonra Can kendi gizli anahtarı olan a değerini seçer. Can'ın gizli anahtarı $a = 5$ olsun. Can $A = g^a$ **mod** p değerini hesaplar. Bu örnekte $A = 2^5$ **mod** 7 = 4 olarak hesaplanır. Burada p, g ve A değerleri genel ve açık değerlerdir. Herkes tarafından bilinmesinde mahsur yoktur. Ama a anahtarı gizli anahtardır ve sadece Can bilmektedir. Bora m mesajını ElGamal şifreleme algoritmasını kullanarak şifreleyip Can'a göndermek istemektedir. Bu mesajın $m = 6$ olduğunu varsayalım. Bora kendi gizli anahtarı olan b anahtarını seçer. Bora'nın gizli anahtarı $b = 4$ olsun. Bora $C = g^b$ **mod** p değerini hesaplar. Bu örnekte $C = 2^4$ **mod** 7 = 2 olarak hesaplanır. Bora ayrıca $D = m \times A^b$ **mod** p değerini hesaplar. Örnekte, $D = 6 \times 4^4$ **mod** 7 = 3 olarak bulunur. Bora C ve D şifreli mesajlarını Can'a gönderir. Can orijinal mesajı hesaplamak için önce C^a değerinin **mod** p'ye göre çarpımsal tersini hesaplar. Bu değeri bulmak için önce 2^5 **mod** 7 = 4 değeri bulunur. 4'ün **mod** 7'ye göre çarpmaya göre tersi 2'dir. Çünkü $4 \times 2 = 1$ **mod** 7'dir. Daha sonra bulunan bu değer D ile çarpılıp mod 7'ye göre eşiti bulunur. Örnekte, $D = 3$ olduğundan $m = 3 \times 2$ **mod** 7 = 6 olarak orijinal mesaj bulunur. Bora'nın gönderdiği mesajı Can elde etmiş olur.

Yukarıda açıklanan RSA, Diffie-Hellman ve ElGamal açık anahtar şifreleme algoritmalarına ek olarak başka açık anahtar şifreleme algoritmaları da vardır. Bunlar arasında eliptik eğri şifreleme algoritması, dijital imza algoritması ve Paillier şifreleme sistemi gibi algoritmalar sayılabilir. Dijital imza algoritması aşağıdaki bölümde anlatılacaktır. Bu algoritma sadece dijital imza servisi sunmak için geliştirilmiş bir algoritmadır. Eliptik eğri şifreleme algoritması şifreleme ve şifre çözme, dijital imza ve anahtar paylaşımı için kullanılabilir. Eliptik eğri şifreleme algoritması diğer algoritmalar ile aynı seviyede güvenliği daha kısa anahtar uzunluğu ile sağlar. Bu nedenle performansı daha iyidir. Fakat diğer şifreleme algoritmalarına göre güvenliği henüz kanıtlanmamıştır. RSA algoritmasına göre güven derecesi daha düşüktür.

Açık anahtar şifreleme algoritmalarının temel olarak altı bileşeni vardır. Bunlar açık metin kümesi, şifreli metin kümesi, şifreleme fonksiyonu, şifre çözme fonksiyonu, açık anahtar ve gizli anahtar olarak sıralanabilir. Güvenlikleri, bu algoritmaları kırmak için yapılan hesaplamaların zorluğuna dayanır. Anahtar uzunluğu güvenlikleri açısından çok önemlidir. Matematiksel fonksiyonlara dayandıklarından simetrik şifrelemeye göre daha yavaştırlar. Gizli anahtar şifreleme algoritmaları bit tabanlı basit operasyonlara dayandığından daha hızlıdır.

DİJİTAL İMZA

Bir metnin kimin tarafından yazıldığını ve içeriğin kendi bilgisi dâhilinde olduğunu kanıtlamak için, metni oluşturan kişi tarafından imzalanması gerekir. Bankacılıkta kullanılan çekler, ticari sözleşmeler, mektuplar ve dilekçeler gibi birçok yasal sorumluluk taşıyan işlemlerde imza atılarak kimlik bilgisi ve metin içeriği doğrulanır. Elektronik ortamda bir mesajın kime ait olduğunu kanıtlamak için bir açık şifreleme algoritması olan dijital imza kullanılır. Örneğin, bir kişi oluşturduğu metni dijital olarak imzalamak isterse, metnin arkasına kendi gizli anahtarını kullanarak şifrelediği metnin özetini ekler. Karşı tarafa hem orijinal mesajını hem de dijital imzasını gönderir. Mesajı alan kullanıcı, gönderenin kimliğini doğrulamak için, dijital imzayı gönderenin açık anahtarını kullanarak çözer. Çözme işlemi sonunda elde ettiği metin özeti ile orijinal metnin özetini karşılaştırır. Eğer bu özetler arasında bire bir eşleşme var ise gönderenin kimliği doğrulanmış olur. Çünkü şifrelenmiş dijital imzayı çözmek için kullanılan açık anahtara karşılık gelen gizli anahtar sadece mesajı gönderen kullanıcıda olabilir. Dijital imza günlük hayatta kullanılan ıslak imzadan farklı olarak her seferinde farklı bir değere sahip olmaktadır. Dijital imza fonksiyonunun bir girdisinin açık metin olmasından dolayı metinlerin farklı olması durumunda her seferinde farklı imzalar üretilecektir.

Kimlik doğrulama protokolleri birbiri ile haberleşen iki kişiyi, kötü niyetli üçüncü kişilere karşı korumaktadır. Fakat bu tür protokoller, haberleşen bu iki kişiyi birbirine karşı korumaz. Haberleşen bu iki kişi arasında inkâr etme ihtilafları oluşabilir. Dijital imza hem mesajlaşmada kimlik doğrulamayı sağlayarak haberleşen iki kişiyi, kötü niyetli üçüncü kişilere karşı hem de haberleşen kişileri inkâr etme ihtilaflarında birbirlerine karşı korumaktadır.

Dijital imzaların gereksinimleri şöyle açıklanabilir. Dijital imzanın, imzalanan metne bağlı bir örüntüsü olmalıdır. Dijital imza benzersiz olmalıdır. Dijital imzaları üretmek hesaplama açısından kolay olmalıdır. Göndericiden gelen imzaları tanımak ve doğrulamak kolay olmalıdır. Göndericinin oluşturduğu dijital imzayı kötü niyetli kişiler oluşturamamalıdır. Gönderici dijital imzanın bir kopyasını kolaylıkla oluşturarak saklayabilmelidir.

Dijital imzada bütün metin yerine metnin özeti imzalanır. Neden?

SIRA SİZDE 5

Basit bir dijital imza protokolü aşağıda verilen adımlardan oluşur:

- Kullanıcı Can ilk önce bir açık ve gizli anahtar çifti oluşturur. Kullanıcılar birden çok açık ve gizli anahtar çiftlerine sahip olabilir. Önemli olan şifreleme için hangi anahtar kullanıldıysa, çözme için bu anahtarın karşılığı olan anahtarın kullanılmasıdır. Kendisine ait olan açık anahtarı iletişime geçmek istediği kullanıcı Bora'ya gönderir. Açık anahtar herkese ilan edilebilir.
- Sonraki adımda Can iletmek istediği orijinal metni oluşturur ve bir özet fonksiyonu kullanarak bu mesajın özetini bulur. Sonra bu ileti özetini kendi gizli anahtarını kullanarak şifreler. Hem orijinal metni hem de dijital imzasını (ileti özetinin gizli anahtarla asimetrik şifreleme kullanarak şifrelenmiş hali) Bora'ya gönderir.

- Bora öncelikle Can'ın açık anahtarını kullanarak imzayı çözer. Kendisine gelen metnin, aynı özet fonksiyonunu kullanarak özetini bulur. Hesapladığı bu özet ile dijital imzadan elde ettiği özeti karşılaştırır. Eğer bu özetler birbirine eşitse, gönderilen metnin gerçekten Can tarafından oluşturulduğuna emin olunur. Eğer özetler birbirine eşit değilse, Bora bu durumda mesajın Can tarafından oluşturulduğundan emin olamaz.

RSA Dijital İmza Protokolü

RSA dijital imza protokolü RSA şifreleme algoritmasına dayanmaktadır. En yaygın olarak bilinen ve kullanılan dijital imza protokolüdür (Paar ve Pelzl, 2010). RSA algoritmasının en yaygın uygulama alanlarından birisi dijital imzadır. Eğer açık metin ile birlikte dijital imzanın da oluşturulması isteniyorsa aşağıda verilen adımlar uygulanır:

- Can öncelikle RSA anahtarlarını oluşturur. Açık anahtarını dijital imzasını göndermek istediği Bora'ya gönderir.
- Can bir özet fonksiyonu kullanarak imzalamak istediği metnin ileti özetini hesaplar. Daha sonra RSA çözme fonksiyonu kullanarak dijital imzasını oluşturur. Yani kendi gizli anahtarı ile ileti özetini şifreler.
- Can hem açık metni hem de bu metnin dijital imzasını Bora'ya gönderir.
- Bora, Can'dan kendisine gelen mesajın gerçekten Can'dan gelip gelmediğini doğrulamak için RSA şifreleme fonksiyonunu kullanarak dijital imzayı açar.
- Kendisine gelen metnin özetini hesaplar. Açma işlemi sonunda elde ettiği ileti özeti ile kendisinin hesapladığı ileti özetini karşılaştırır. Eğer bire bir eşleşme var ise mesajın Can'dan geldiği doğrulanır.

Dijital imzayı basit bir örnekle açıklamaya çalışalım. Can'ın açık anahtarı 5, gizli anahtarı 5, n değeri 35, $\emptyset(n)$ değeri 24 ve açık metin değeri ise 214 olsun. Can öncelikle bir özet fonksiyonu kullanarak bu mesajın ileti özetini hesaplamalıdır. Özet fonksiyonunun **mod** 10 olduğunu varsayalım. Gerçek hayatta **mod** operatörü, özet fonksiyonu olarak kullanılmaz. Örneği basitleştirmek için özet fonksiyonu olarak seçilsin. 214 mesajının bu özet fonksiyonuna göre özeti, 214 **mod** 10 = 4 olarak hesaplanır. Daha sonra bu özeti RSA şifreleme fonksiyonunu kullanarak, kendi gizli anahtarı ile şifreler. Yani dijital imza, 4^5 mod 35 = 9 olarak hesaplanır. Can hem orijinal mesaj olan 214'ü hem de bu mesajın dijital imzası olan 9'u Bora'ya gönderir. Bora öncelikle gelen mesajın özetini hesaplar. Bunun için aynı özet fonksiyonunu kullanarak ileti özetini 4 olarak hesaplar. Daha sonra RSA şifre çözme fonksiyonunu kullanarak Can'ın açık anahtarı ile dijital imzayı çözer. Elde ettiği özet, 9^5 **mod** 35 = 4 olarak hesaplanır. Dijital imzayı çözerek elde ettiği bu özet olan 4 ile gelen mesajdan hesapladığı özet olan 4'ü karşılaştırır. Bunların birbirine eşit olduğunu görür. Böylece gelen mesajın Can tarafından oluşturulduğundan emin olur.

RSA dijital imzalamasına ek olarak, daha önce açıklanan ElGamal şifreleme algoritması da dijital imza için kullanılabilir.

Dijital İmza Algoritması

Dijital imza algoritması (DSA–Digital Signature Algorithm) ayrık logaritma prensibine göre tasarlanmıştır (Stallings, 2013). Fakat ElGamal dijital imza protokolüne göre daha yaygın olarak kullanılmaktadır. DSA algoritması, sadece dijital imza üretmek amacıyla tasarlanmıştır. RSA ve ElGamal algoritmalarında olduğu gibi şifreleme amaçlı kullanılmaz. DSA ile üretilen imzalar sabit uzunluktadır. DSA mesajın tamamını değil özetini imzaladığı için daha kısa ve sabit uzunlukta dijital imzalar oluşturabilmektedir. DSA anahtar üretme parametrelerinin değişmesi durumunda imza boyutları farklılık göstermektedir. Örneğin, p değeri 1024 bit ve q değeri 160 bit uzunluğunda ise, imza uzunluğu 320 bit

olur. Eğer p değeri 2048 bit ve q değeri 224 bit uzunluğunda ise, imza uzunluğu 448 bit olur. DSA yönteminde imza oluşturmak için gerekli anahtarlar aşağıda verilen adımlar takip edilerek üretilir:

- Bir p asal sayısı 2^{1023} değerinden büyük ve 2^{1024} değerinden küçük olmak üzere seçilir.
- $p - 1$ değerinin asal böleni ve 2^{159} değerinden büyük ve 2^{160} değerinden küçük olmak üzere bir q sayısı belirlenir. Bu q sayısının basit köklerinden biri g değeri olarak belirlenir.
- Rastgele bir d sayısı 0'dan büyük ve q'dan küçük olmak üzere belirlenir. Bu gizli bir değerdir.
- $y = g^d$ **mod** p hesaplanır. Bu anahtar kullanıcının açık anahtarıdır.

Kullanıcının açık anahtarı (p, q, g, y) ve gizli anahtarı (d) olarak belirlenir. DSA imza üretimi ise aşağıdaki gibi açıklanabilir:

- Kullanıcı Can, imza oluşturmak için öncelikle oluşturduğu mesajın özet değerini bulur. Bunun için bir özet fonksiyonu kullanır. Eğer mesaj M ise bu mesajın özeti $H(M)$ ile gösterilsin.
- 0'dan büyük ve q'dan küçük olmak üzere rastgele tek kullanımlık anahtar k belirlenir. Bu anahtar da gizlidir. Sadece Can tarafından bilinir.
- $r = (g^k \textbf{ mod } p) \textbf{ mod } q$ olmak üzere hesaplanır. Ayrıca $s = ((H(M) + d \times r)\ k^{-1}) \textbf{ mod } q$ olmak üzere hesap edilir. Can'ın hesapladığı r ve s değerleri mesaj imzasıdır.

Can oluşturduğu açık metni (M) ve bu metne ait olan dijital imzayı (M, (r, s)) Bora'ya gönderir. Bora bu mesaj ve imzasını aldıktan sonra imzayı doğrulamalıdır. Bunun için DSA imza doğrulama işlemini gerçekleştirir. Bora kendisine iletilen (M, (r, s)) mesajının gerçekten Can'dan geldiğini doğrulamak için aşağıdaki adımları takip eder. Bora öncelikle Can'ın açık anahtarına yani (p, q, g, y) değerlerine ulaşmalıdır. Sonra gerekli hesaplamaları yapar. Açık anahtar bilindiğinden, Bora bu anahtara kolayca ulaşır. Bora daha sonra aşağıdaki hesaplamaları yapar.

- $w = s^{-1}$ **mod** q değerini hesaplar.
- $c = w \times H(M)$ **mod** q ve $d = w \times r$ **mod** q değerlerini hesaplar.
- $v = (g^c \times y^d \textbf{ mod } p) \textbf{ mod } q$ değerini hesaplar.

Bora hesapladığı bu v değerini imza içeriğinde bulunan r değeri ile karşılaştırır. Bu iki değer birbirine eşit ise imza doğrulanır; değilse imza geçerli değildir.

Farklı iki mesajın ileti özetlerinin aynı olması ne tür problemlere neden olur?

SIRA SİZDE 6

ÖZET FONKSİYONLARI

Özet fonksiyonu, değişken uzunlukta bir mesajı girdi olarak alır ve sabit uzunlukta bir çıktı mesajı üretir (Trappe ve Washington, 2006). Bu çıktı mesaj özeti, *ileti özet* veya *özet* gibi terimlerle ifade edilir. Özet fonksiyonları dijital imza oluşturulması, parolaların saklanması, İnternet üzerinden indirilen bir dosyanın içerik olarak tam ve doğru indirildiğinin doğrulanması veya mesajın iletim sırasında yetkisi olmayan kişiler tarafından içeriğinin değiştirilip değiştirilmediğinin kontrol edilmesi gibi birçok alanda kullanılmaktadır. Özet fonksiyonları bu işlevlerini herhangi bir anahtar kullanmadan yerine getirir. Açık anahtar şifreleme algoritmaları iki, simetrik şifreleme algoritmaları ise bir anahtar kullanır. Fakat özet fonksiyonları anahtar kullanmadığından, anahtarsız fonksiyonlar olarak bilinirler.

Dijital imzalamada bütün metin imzalanabilir. Bunun anlamı, bütün metnin şifrelenmesidir. Şifreleme için açık anahtar şifreleme algoritmaları kullanılır. Bu durumda uzun bir metin için mesajın sonuna, verimsiz şekilde metin boyutu kadar dijital imzanın eklenmesi gerekmektedir. Bunun iki önemli dezavantajı vardır. Birinci dezavantajı, gereksiz

yere mesaj boyutunu iki katına çıkarmak suretiyle daha uzun bir mesajın ağ üzerinden gönderilmesi gerekmesidir. İkincisi ise dijital imza oluşturmak ve kontrol etmek için gereken zamanın uzamasıdır. Bu dezavantajlara ek olarak, hem mesajın hem de imzanın bazı bloklarının yerlerinin değiştirilmesi sonucu güvenlik açığı oluşabilmektedir. Uzun şifrelenmiş metin yerine kısa bir mesaj özetinin oluşturulması, yukarıda bahsedilen problemleri ortadan kaldırmak için önerilmiştir. Herhangi bir boyutta verilen bir metnin daha kısa ve sabit uzunlukta özeti elde edilebilir. Bütün mesaj yerine bu özet şifrelenerek mesaj imzalanmış olur.

Özet fonksiyonlarının kullanılması durumunda basit bir dijital imza oluşturma ve doğrulama protokolü aşağıda verilen adımlardan oluşmaktadır. Açıklanacak protokolde veri gizliliği önemsenmeyip, sadece iletilen mesajın iletim sırasında değişime uğrayıp uğramadığı ve mesajı oluşturan kullanıcının kimliğini kontrol etmek amaçlanmıştır.

- Kullanıcı Can iletmek istediği mesajı oluşturur ve mesajın özet fonksiyonu çıktısını elde eder. Yani ileti özetini bulur. Oluşturduğu mesajın sonuna özet değerini kendi gizli anahtarı ile şifreleyerek ekler. Hem mesajı hem de şifrelenmiş özet değerini alıcı Bora'ya gönderir.
- Bora ilk olarak Can'ın açık anahtarı ile şifrelenmiş özet değerini çözer. Sonra mesajı kullanarak özet değerini hesaplar. Çözülen mesaj ile hesaplanan özet değeri eşit ise, hem mesajın değişmediği hem de Can'ın kimliği doğrulanmış olur.

Özet fonksiyonları bazı özelliklere sahip olmalıdır. Öncelikle özet fonksiyonu mesaj uzunluğundan bağımsız olmalıdır, girdi olarak değişken uzunlukta mesaj alabilmelidir. Ayrıca, özet fonksiyonu için performans önemlidir, kısa bir zaman zarfı içerisinde çıktı üretmelidir. Mesaj boyu ne olursa olsun, hızlı bir şekilde ileti özeti hesaplanabilmelidir ve özet değeri sabit uzunlukta olmalıdır. Mesaj içeriğinde bir karakterin değişmesi halinde bile özet fonksiyonu çok farklı değerler üretmelidir.

Yukarıda verilen genel özellikler yanında özet fonksiyonları, güvenli olmaları açısından aşağıda verilen üç özelliğe sahip olmalıdır.

- **Ön–görüntü direnci (Tek yönlülük**): Elde edilen özet değerini kullanarak bu özete ait mesajın ne olduğunu hesaplamak imkansız olmalıdır. Özet fonksiyonları tek yönlü fonksiyonlar olarak adlandırılır. Bir mesaj verildiğinde bu mesajın özetinin hesaplanması kolay olmalıdır. Fakat bir özet verildiğinde, bu özetten yola çıkarak orijinal mesajı hesaplamak imkânsız olmalıdır. Bu özellik tek yönlülük olarak adlandırılır.
- **İkinci ön–görüntü direnci (Zayıf çakışma direnci):** Aynı özet değerine sahip iki farklı mesajın bulunması zor olmalıdır. Bu durumda kötü niyetli kişinin elinde bir mesaj ve özet değeri var ise, kolayca aynı özet değerine sahip başka bir mesajı oluşturamaması gerekmektedir. İleti özetleri benzersiz olmalıdır. Bir mesajın içinde sadece bir bitlik bir değişiklik yapılsa bile, hesaplanacak özet değeri bir önceki özet değerinden farklı olmalıdır.
- **Çakışma direnci (Güçlü çakışma direnci):** Eğer iki farklı mesaj için aynı özet değerinin bulunması zor ise, bu durum güçlü çakışma direnci olarak adlandırılır. Bu durumda kötü niyetli kişinin her iki mesajı oluşturma serbestliği vardır.

İki türlü özet algoritması vardır. Birinci türde sadece özet değeri üretmek amacı ile tasarlanmış MD ve SHA ailesi algoritmalar vardır. Bu algoritmalar, Merkle-Damgard yöntemini kullanır. Bahsedildiği üzere özet fonksiyonların değişken uzunluktaki mesajlar için sabit uzunlukta özet değeri üretmeleri gerekmektedir. Mesaj belirli uzunlukta bloklara bölünür ve özet fonksiyonuna gönderilir. Son blok parçasından sonra elde edilen fonksiyon çıktısı özet değeri olarak kabul edilir.

Ronald Rivest tarafından geliştirilen MD4 algoritması bu grupta yer almaktadır. 32 bit değişkenler ve mantıksal fonksiyonlar (AND, OR ve XOR) kullanılarak geliştirilmiştir. MD5, SHA, WHIRLPOOL ve RIPEMD gibi özet fonksiyonların hepsi MD4 algoritması üzerine inşa edilmiştir. 1991 yılında MD5 algoritması geliştirilmiştir. MD5, 128 bit uzunluğunda mesaj özeti üretmektedir. Ancak içerdiği zayıflıklarından dolayı 1995 yılında yerini SHA ailesine terk etmiştir. SHA-0 ve SHA-1 algoritmaları 160 bitlik mesaj özeti üretmektedir. Sonraki yıllarda SHA-224, SHA-256, SHA-384 ve SHA-512 olmak üzere dört farklı sürümü çıkmıştır.

İkinci grupta ise simetrik blok şifreleme algoritmaları kullanılarak elde edilen özet fonksiyonları yer almaktadır. Blok simetrik şifreleme algoritması kullanılarak elde edilen özet fonksiyonu, benzer şekilde mesajı bloklara böler. Mesaj özeti oluşturmak için hem mesaj bloğunu hem de şifrelenmiş metni fonksiyon girdisi olarak kullanır. Birçok alternatif çözümü vardır. Bunlardan Matyas–Meyer–Oseas olarak bilinen yöntemde bir önceki blok için oluşturulmuş şifrelenmiş metin bir sonraki blok için şifreleme algoritmasında girdi olarak kullanılır. En son bloktan sonra elde edilen şifrelenmiş metin, mesaj özeti olur.

MD5 algoritmasında güvenlik açıklarının ortaya çıkmasından sonra SHA algoritması standart olarak kabul edilmiş ve yaygın olarak kullanılmaya başlanmıştır. SHA-0 olarak bilinen ilk sürümde bazı güvenlik açıklarının ortaya çıkmasından sonra SHA-1 olarak bilinen yeni sürümü 1995 yılında kullanılmaya başlanmıştır. SHA-1 fonksiyonu 160 bit uzunluğunda özet değeri üretmektedir. 2002 yılında SHA-1 revize edilerek SHA-2 kullanılmaya başlamıştır. SHA-2 fonksiyonunun 224, 256, 384 ve 512 bit uzunluğunda olmak üzere dört faklı uzunlukta özet değeri üreten sürümleri vardır. Bu sürümler SHA-224, SHA-256, SHA-384 ve SHA-512 olarak bilinir. NIST uzun yıllar süren yarışma sonucunda 2012 yılında SHA-3 algoritmasını belirlemiştir (Paar ve Pelzl, 2010).

Özet fonksiyonlarında özeti hesaplanacak metin *n* bit uzunluğunda bloklar şeklinde göz önüne alınır. Özet fonksiyonun girdileri bloklar şeklindedir. Bu fonksiyonlar tekrarlamalı olarak çalışırlar. En son tekrarlamadan sonra mesaj özeti elde edilir. En basit özet fonksiyonu bit tabanlı XOR operasyonudur. Modüler aritmetik, özet fonksiyonu olarak kullanılmamalıdır. Farklı iki mesajın modüler aritmetikten sonra aynı değeri vermesi yüksek olasılıktır. Örneğin, özet fonksiyonunun **mod** 5 olduğunu varsayalım. Özeti çıkarılmak üzere 25, 30, 32 ve 35 gibi dört farklı mesaj olsun. Bu mesajlar imzalanmak istendiğinde, bunların ileti özetlerinin bulunması gerekir. Bu durumda 25 **mod** 5 = 0; 30 **mod** 5 = 0; 32 **mod** 5 = 2 ve 35 **mod** 5 = 0 olarak özetler hesaplanır. Bu durumda birinci, ikinci ve dördüncü mesajların özetleri birbirine eşit çıkar. Dolayısıyla bu üç mesajın dijital imzası aynıdır ve benzersizlik özelliği ihlal edilmiş olur. Bu nedenle, modüler aritmetik özet fonksiyonu olarak kullanılmamalıdır.

Özet

Güvenlik servislerinin neler olduğunu ve ne sağladıklarını açıklamak

Simetrik şifreleme yöntemleri uzun yıllardır bir mesajın gizli bir şekilde iletilmesinde kullanılmaktadır. Fakat teknolojik gelişmelere paralel olarak mesaj bütünlüğü, kimlik doğrulama ve inkâr edilemezlik gibi bazı güvenlik servislerini sağlayacak ve kullanıcılar arasında gizli anahtar dağıtılması gibi hizmetleri yerine getirebilecek özelliklere sahip değildir. Açık anahtar şifreleme yöntemleri ve prensipleri, simetrik yöntemlerin bu açıklarını kapatmak amacıyla ilk olarak 1976 yılında ortaya konmuştur.

Simetrik ve açık anahtar şifreleme yöntemleri arasındaki farkları ifade etmek

Günümüze kadar açık anahtar şifreleme prensiplerini sağlamak için, tam sayıyı çarpanlarına ayırma, ayrık logaritma ve eliptik eğriler olmak üzere üç farklı yöntem sunulmuştur. Açık anahtar şifreleme yöntemlerinde simetrik yöntemlerin aksine her kullanıcının bir açık ve bir gizli olmak üzere iki anahtarı vardır. Açık anahtar şifreleme algoritmaları şifreleme ve dijital imza doğrulamada kullanılır. Açık anahtar şifreleme yöntemlerinin hepsi tek yönlü fonksiyonları yapı taşı olarak kullanmıştır.

En yaygın kullanılan açık anahtar şifreleme algoritmalarını tanımlamak

En yaygın açık anahtar şifreleme algoritmaları RSA, Diffie-Hellman Şifreleme Algoritması ve ElGamal Şifreleme Sistemi olarak sayılabilir. RSA ve Diffie-Hellman Şifreleme Algoritması tam sayıyı çarpanlarına ayırma, ElGamal Şifreleme Sistemi ise ayrık logaritma üzerine kurulmuştur. RSA ve ElGamal algoritmalarında kullanılan anahtar uzunluklarının, yeterli seviyede güvenlik sağlamak için 1024 bit veya daha uzun olmaları gerekmektedir.

Dijital imzaların nasıl oluşturulduğunu ve kullanıldığını açıklamak

Günlük hayatta bir mesajın kim tarafından yazıldığının göstergesi olarak mesajın altına imza atılır. Bir kişinin imzasının sadece kendisi tarafından atıldığı kabul edilir. Gerçek imza ve sahte imza arasındaki farklar kriminoloji metotları yardımı ile tespit edilebilmektedir. Kişilerin imzaları birbirinden farklıdır ve ömür boyu aynı imzayı kullanmak zorundadırlar. Benzer şekilde dijital imzalar, elektronik ortamda oluşturulan mesajların kime ait olduğunu kanıtlamak için kullanılır. Dijital imza bir açık anahtar şifreleme algoritmasıdır. Kullanıcı, göndermek istediği mesajın arkasına dijital imzasını ekleyerek alıcıya ulaştırır. RSA ve ElGamal gibi hem şifreleme yapan hem de dijital imza oluşturan yöntemlerin yanında DSA gibi sadece dijital imza oluşturmak amacıyla tasarlanmış algoritmalar da mevcuttur. Temel prensip olarak kullanıcı kendi gizli anahtarını kullanarak imzasını oluşturur ve alıcı, mesaj sahibinin açık anahtarını kullanarak kimliğini doğrular. Dijital imza algoritmaları girdi olarak hem mesajı hem de kullanıcının gizli anahtarını kullanır. Gizli anahtar her seferinde aynı olmasına rağmen mesaj farklı olacağı için kullanıcının dijital imzası ıslak imzanın aksine her seferinde değişir.

Mesaj özetinin nasıl oluşturulduğunu ve kullanıldığını açıklamak

Bir mesajın içeriğinin değiştirilip değiştirilmediğinin tespit edilmesi mesaj bütünlüğü olarak adlandırılır. Özet fonksiyonlar, bir mesajın içeriğinin yetkisi olmayan kişiler tarafından değiştirilip değiştirilmediğini kontrol etmek ve dijital imzaların daha kısa uzunlukta üretilmesi amacıyla kullanılır. Özet fonksiyonları tek yönlü fonksiyonlar üzerine kurulmuştur. Özet değeri bilinen bir mesajın içeriğini elde etmek imkânsızdır. Özet fonksiyonlarının farklı uzunluktaki mesajlar için sabit uzunlukta mesaj özetleri üretmeleri gerekmektedir. İyi bir özet fonksiyonu, mesajda tek bir karakterin değişmesi durumunda bile çok farklı özetler üretmelidir.

Kendimizi Sınayalım

1. MD5 özet fonksiyonu kaç bit uzunluğunda özet değeri üretir?

a. 64
b. 128
c. 160
d. 256
e. 512

2. Güvenli veri aktarımı için aşağıda verilen algoritmalardan hangisi birbiri ile ilişkili iki anahtar kullanır?

a. DES
b. 3DES
c. AES
d. RSA
e. IDEA

3. Aşağıdakilerden hangisi bir güvenlik servisi **değildir?**

a. Gizlilik
b. Mesaj bütünlüğü
c. Kimlik doğrulama
d. Doğruluk
e. Erişim kontrolü

4. Dijital imza oluşturmak için aşağıdaki hangi anahtar kullanılır?

a. Açık anahtar
b. Gizli anahtar
c. Bir kullanımlık anahtar
d. Oturum anahtarı
e. Yabancı anahtar

5. Dijital imzayı doğrulamak için aşağıdaki hangi anahtar kullanılır?

a. Açık anahtar
b. Yabancı anahtar
c. Gizli anahtar
d. Oturum anahtarı
e. Bir kullanımlık anahtar

6. Özet fonksiyonları bir mesajın özet değerini hesaplarken aşağıdaki hangi anahtarı kullanır?

a. Açık anahtar
b. Yabancı anahtar
c. Gizli anahtar
d. Oturum anahtarı
e. Anahtar kullanmaz

7. Aşağıdaki algoritmalardan hangisi bir özet fonksiyonu **değildir?**

a. MD5
b. RSA
c. SHA
d. WHIRLPOOL
e. RIPEMD

8. Aşağıdaki güvenlik servislerinden hangisi sadece yetkili kişilerin mesajı okuyabilmesi olarak tanımlanır?

a. Gizlilik
b. Mesaj bütünlüğü
c. Kimlik doğrulama
d. Erişim kontrolü
e. Fiziksel güvenlik

9. RSA algoritmasında $p = 5$ ve $q = 7$ olarak seçilirse, aşağıdakilerden hangisi açık anahtar olarak kullanılabilir?

a. 1
b. 2
c. 3
d. 7
e. 9

10. Aşağıdakilerden hangisi bir açık anahtar şifreleme algoritması **değildir?**

a. DSA
b. RSA
c. IDEA
d. ElGamal
e. Diffie-Hellman

Kendimizi Sınayalım Yanıt Anahtarı

1. b	Yanıtınız yanlış ise "Özet Fonksiyonu" konusunu yeniden gözden geçiriniz.
2. d	Yanıtınız yanlış ise "Açık Anahtar Şifreleme" konusunu yeniden gözden geçiriniz.
3. d	Yanıtınız yanlış ise "Giriş" konusunu yeniden gözden geçiriniz.
4. b	Yanıtınız yanlış ise "Dijital İmza" konusunu yeniden gözden geçiriniz.
5. a	Yanıtınız yanlış ise "Dijital İmza" konusunu yeniden gözden geçiriniz.
6. e	Yanıtınız yanlış ise "Özet Fonksiyonu" konusunu yeniden gözden geçiriniz.
7. b	Yanıtınız yanlış ise "Özet Fonksiyonu" konusunu yeniden gözden geçiriniz.
8. a	Yanıtınız yanlış ise "Giriş" konusunu yeniden gözden geçiriniz.
9. d	Yanıtınız yanlış ise "Açık Anahtar Şifreleme Algoritmaları" konusunu yeniden gözden geçiriniz.
10. c	Yanıtınız yanlış ise "Açık Anahtar Şifreleme Algoritmaları" konusunu yeniden gözden geçiriniz.

Sıra Sizde Yanıt Anahtarı

Sıra Sizde 1

Bu durumu açıklamak için kullanılan terim "güvenlik üçgeni" terimidir. Üçgenin köşeleri güvenlik, performans ve kolay kullanılabilirliği temsil eder. Aynı anda üç köşede bulunulamaz. Bu nedenle aynı anda bu üç özelliği sağlamak zordur.

Sıra Sizde 2

Bu durumda 56 bit uzunluğunda anahtarların oluşturduğu anahtar kümesinde toplam 2^{56} anahtar vardır. En iyi durumda sadece bir şifreleme ile oturum anahtarını elde edebilir. Eğer kötü niyetli kişi çok şanslı ise, ilk şifrelediği anahtar oturum anahtarı olarak seçilmiş anahtar olabilir. Ama bu oldukça küçük bir ihtimaldir. En kötü durumda ise toplam anahtar sayısı kadar, yani 2^{56} kez şifreleme yapmalıdır. Bu durumda kötü niyetli kişinin aradığı oturum anahtarı en son şifrelediği anahtar olabilir. Ortalama olarak ise, kötü niyetli kişi $2^{56}/2$ kez şifreleme yapmalıdır. Yani ortalama 2^{55} şifreleme yaparak oturum anahtarını elde edebilir.

Sıra Sizde 3

Öncelikle $n = 5 \times 7 = 35$ olarak hesaplanır. Sonra $\emptyset(n) = 4 \times 6 = 24$ olarak bulunur. Açık anahtar e 1'den büyük ve 24'den küçük olmalıdır. Ayrıca açık anahtar 24 ile aralarında asal olmalıdır. Buna göre $e = 5$ açık anahtar olarak seçilebilir. Açık anahtar 5 ise, $5 \times d = 1$ **mod** 24 olacağından, gizli anahtar $d = 5$ olarak hesaplanır. Sonuç olarak, seçilebilecek anahtarlar (5, 35) açık anahtar ve (5, 35) gizli anahtar olarak elde edilir. Başka anahtarlar da seçilebilir.

Sıra Sizde 4

Can $T = 5^3$ **mod** 23 = 10 değerini hesaplar ve Bora'ya gönderir. Bora $V = 5^5$ **mod** 23 = 20 değerini hesaplar ve Can'a gönderir. Can $K = 20^3$ **mod** 23 = 19 değerini bulur. Benzer şekilde Bora $K = 10^5$ **mod** 23 = 19 değerini bulur. Gizli anahtar 19 olarak hesaplanır.

Sıra Sizde 5

Dijital imza için açık anahtar şifreleme algoritmaları kullanılır. Bu algoritmalar gizli anahtar algoritmalarına göre daha yavaş algoritmalardır. Bütün metnin imzalanması, bütün metnin açık anahtar şifreleme algoritması ile şifrelenmesi demektir. Şifreleme algoritmasının yavaş olmasından dolayı imzalama çok yavaş olabilir. Bu nedenle orijinal metnin özeti alınıp imzalanarak performans iyileştirilir.

Sıra Sizde 6

Dijital imzalar her mesaj için farklı olmalıdır. Dijital imzalar ileti özetleri şifrelenerek elde edildiğinden farklı mesajların ileti özetleri farklı olmalıdır ki, dijital imzaları da farklı olsun. Eğer farklı iki mesajın ileti özetleri aynı ise dijital imzaları da aynı olur. Bu durumda benzersizlik özelliği sağlanamamıştır.

Yararlanılan ve Başvurulabilecek Kaynaklar

Paar, C., Pelzl, J. (2010). ***Understanding Cryptography: A textbook for students and practitioners,*** Springer Science & Business Media.

Stallings, W. (2013). ***Cryptography and Network Security: Principles and Practices,*** Pearson Education.

Stallings, W. (2011). ***Network Security Essentials: Applications and Standards,*** Pearson Education.

Trappe, W., Washington, L.C. (2006). ***Introduction to Cryptography with Coding Theory,*** Pearson Education.

5

Amaçlarımız

Bu üniteyi tamamladıktan sonra;

- Simetrik şifreleme yöntemi ile anahtar dağıtımını ifade edebilecek,
- Açık anahtar şifreleme yöntemi ile anahtar dağıtımını açıklayabilecek,
- Sertifikaları tanımlayabilecek ve sertifika kullanımını açıklayabilecek,
- Tek kullanımlık parola ve biyometrik kimlik doğrulama yöntemlerini tanımlayabilecek

bilgi ve becerilere sahip olacaksınız.

Anahtar Kavramlar

- Anahtar Dağıtımı
- Aradaki Adam Saldırısı
- Sertifikalar
- X.509
- Açık Anahtar Altyapısı
- Kerberos
- Biyometrik Kimlik Doğrulama Yöntemleri

İçindekiler

Anahtar Dağıtımı ve Kullanıcı Kimlik Doğrulama

GİRİŞ

Kriptografik şifreleme algoritmaları simetrik ve asimetrik şifreleme algoritmaları olmak üzere ikiye ayrılır. Simetrik şifreleme gizli anahtar şifreleme, asimetrik şifreleme ise açık anahtar şifreleme olarak bilinir. Simetrik şifreleme yöntemi ile güvenli bir iletişim kurulması için her iki kullanıcının aynı anahtara sahip olmaları gerekmektedir. Bu anahtar her iki kullanıcıya güvenli bir iletişim kanalı üzerinden aktarılmalıdır. Simetrik şifreleme yöntemlerinin güvenliği, kullanılan anahtarın gizliliğine bağlıdır. Anahtarın kötü niyetli kişiler tarafından ele geçirilmesi durumunda yapılacak iletişim artık güvenilir olarak kabul edilmez. Asimetrik şifreleme yöntemlerinde her kullanıcının bir açık ve bir gizli olmak üzere birbiri ile ilişkili bir anahtar çifti vardır. Gizli anahtarın sadece sahibi tarafından bilinmesi gerekirken, açık anahtarın diğer kullanıcılar tarafından bilinmesinde hiçbir güvenlik zafiyeti yoktur. Açık anahtarını üreten kullanıcı bu anahtarını haberleşmek istediği bütün kişiler ile paylaşabilir veya ortak bir sunucuda diğer kullanıcıların erişimine sunabilir.

Anahtar dağıtımı kullanıcılar arasında güvenli iletişim kurmak için gerekli gizli anahtarların kullanıcılara dağıtılmasını kapsar (Katz ve Lindell, 2014). Şifreleme algoritmalarının güvenliği gizli anahtarların yetkisi olmayan kullanıcıların eline geçmemesine bağlıdır. Bu nedenle anahtar dağıtımı güvenli bir şekilde yapılmalıdır. En genel haliyle anahtarların dağıtılması dört farklı yöntem ile yapılır. Bu yöntemler aşağıdaki açıklanmıştır (Stallings, 2011):

I. Kullanıcılardan bir tanesi simetrik şifreleme için gerekli gizli anahtarı oluşturur ve fiziki yollar kullanarak güvenli şekilde iletişim kurmak istediği diğer kullanıcıya ulaştırır. Bu, pratikte uygulanması zor ve zaman alıcı bir yöntemdir.
II. Bütün kullanıcılar tarafından güvenilir kabul edilen üçüncü bir parti gizli anahtarı üretir ve iletişimi yapacak kullanıcılara fiziki yollar kullanarak ulaştırır. Hem üçüncü partiye gereksinim olmasından hem de fiziksel temas gerektirdiğinden, bu yöntem tercih edilmez.
III. Her iki kullanıcının önceden paylaştığı bir gizli anahtar var ise yeni oluşturulacak oturum anahtarı, kullanıcının biri tarafından oluşturulur ve diğer kullanıcıya kriptografik yöntemler kullanılarak güvenli bir şekilde ulaştırılır.
IV. Güvenli iletişim kurmak isteyen kullanıcılar, diğer bir üçüncü parti ile güvenli bağlantıları var ise, anahtar üçüncü parti tarafından oluşturulur ve güvenli bir şekilde kullanıcılara ulaştırılır.

I. ve II. yöntemler ancak ağda az sayıda kullanıcının olması ve bunlar arasında mesafelerin kısa olması durumunda uygulanabilir. Ama kullanıcı sayısının artması ve kullanıcı-

ların farklı coğrafik konumlarda olması durumunda III. ve IV. yöntemleri kullanmak daha yönetilebilir çözümler sunar.

Bir bilgisayar ağında *n* adet kullanıcı olduğunu varsayalım. Bu kullanıcılar kendi aralarında karşılıklı olarak güvenli haberleşmek istediklerinde toplam $n\times(n-1)/2$ adet gizli anahtarın üretilmesine ihtiyaç vardır. Çünkü birinci kullanıcının *n*-1 anahtara, ikinci kullanıcının *n*-2 anahtara, üçüncü kullanıcının *n*-3 anahtara ihtiyacı olacaktır. Eğer bir firmada 100 çalışan var ise, her çalışanın bilgisayarında diğer iş arkadaşları ile simetrik şifreleme algoritmaları kullanarak güvenli bir iletişim kurmak için 99 adet gizli anahtarı saklaması gerekmektedir. Bu durumda toplamda 4.950 adet farklı gizli anahtarın oluşturulması gerekmektedir. Çalışan sayısının daha fazla olması durumunda anahtar dağıtımı artık yönetilebilir olmaktan çıkacaktır. Diğer bir sorun ise ağa yeni katılan kullanıcı için ağdaki diğer kullanıcılar ile paylaşılmak üzere *n* adet yeni anahtarın oluşturulması ve diğer kullanıcılara dağıtılması gerekliliğidir.

Haberleşmenin güvenli olmasının yanında kim ile haberleştiğini bilmenin de büyük bir önemi vardır. Anahtar dağıtımında veya herhangi bir haberleşmede, haberleşen iki kişi birbirlerinin kimliklerini doğrulamalıdır. Kimlik doğrulama yapıldıktan sonra haberleşmeye ve veri iletimine başlanmalıdır. Günlük hayatta kimlik doğrulama için en yaygın olarak kullanılan araç fotoğraflı kimlik kartlarıdır. Fiziksel temasın söz konusu olduğu durumlarda, fotoğraflı kimlik kartları kimlik doğrulama için kullanılabilir. Fakat sanal dünyada kimlik doğrulama için farklı yöntemler geliştirilmelidir. Teknolojinin gelişmesiyle beraber kimlik doğrulama için kullanılan teknikler de gelişmiştir. Bu amaçla yazılım veya donanım-tabanlı yöntemler kullanılmaktadır.

ANAHTAR DAĞITIMI

Bu bölümde anahtar dağıtımı için kullanılan yöntemler açıklanacaktır. Bu amaçla kullanılan yöntemlerin başında simetrik şifreleme, asimetrik şifreleme ile merkezi ve merkezi olmayan anahtar dağıtımı gibi yöntemler gelmektedir.

Simetrik Şifreleme ile Anahtar Dağıtımı

Anahtar Dağıtım Merkezi (ADM) ile kullanıcıların paylaştığı ana anahtar ve güvenli iletişim kurmak isteyen iki kullanıcı arasında kullanılmak üzere oluşturulan oturum anahtarı olmak üzere iki farklı anahtar vardır. Ana anahtar ADM ile kullanıcılar arasında uzun süre paylaşılır ve kullanıcılara güvenli iletişim sağlamak amacıyla kullanılır. Bu anahtarın sadece ADM ile kullanıcı tarafından bilinmesi gerekir. Bunlardan başkası tarafından anahtarın bilinmesi durumunda güvenli iletişimden bahsedilemez. Oturum anahtarı ise kullanıcılar arasında kısa süreli güvenli iletişim oluşturmak amacıyla kullanılır. Her haberleşme veya mesaj için bir oturum anahtarı üretilir. Haberleşmeden sonra bu anahtar artık bir daha kullanılmaz. Oturum anahtarlarının kullanım süreleri, ana anahtarlara göre çok daha kısadır. Kötü niyetli kişilerin oturum anahtarını ele geçirmesi halinde, farklı oturumlarda farklı anahtarlar kullanıldığı için, oluşacak zarar en aza indirgenmiş olur. Çünkü bir oturum anahtarı ile sadece bir mesaj şifrelenir. Kötü niyetli kişiler tarafından bir tek mesaj ele geçirilse bile diğer mesajlar hala güvendedir.

Anahtar Dağıtım Merkezi Kullanarak Anahtar Dağıtımı

Bu yöntemde bütün kullanıcılar tarafından güvenli kabul edilen bir ADM vardır. Burada ADM'nin güvenilir olduğu varsayımı yapılır. Her bir kullanıcının ADM ile gizli bir anahtar paylaştığı kabul edilir. Bu anahtarı kullanıcılar, ADM ile güvenli iletişim kurmak için kullanır. Sistemde kayıtlı Can ve Bora adında iki kullanıcının olması ve aralarında güvenli bir oturum anahtarı oluşturmak istemeleri durumunda aşağıda verilen adımlar takip edilir:

I. Can kendi kimliğini ve iletişime geçmek istediği Bora'nın kimliğini ADM'ye gönderir.
II. ADM ilk olarak Can ile Bora arasında kullanılacak oturum anahtarını oluşturur. Daha sonra ADM oluşturduğu oturum anahtarını, Can'ın daha önce ADM ile paylaştığı gizli anahtarı kullanarak şifreler ve Can'a gönderir. Bu mesaja ek olarak oturum anahtarının, Bora'nın gizli anahtarı ile şifrelenmiş halini de gönderir.
III. Her iki mesajı alan Can, daha önce ADM ile paylaştığı gizli anahtarı kullanarak birinci mesajı çözer ve oturum anahtarını elde eder. İkinci mesajı ise hiçbir işlem yapmadan Bora'ya iletir.
IV. Bora ise Can'dan aldığı mesajı, daha önce ADM ile paylaştığı gizli anahtarı kullanarak çözer ve oturum anahtarını elde eder.

Bundan sonra Can ile Bora arasında iletişim ADM tarafından oluşturulan ve kullanıcılara güvenli şekilde dağıtılan oturum anahtarı üzerinden devam eder. Can ve Bora güvenli haberleşme için bu oturum anahtarını kullanır. Çünkü bu anahtarı sadece Can, Bora ve güvenilir ADM bilmektedir. Ağda n adet kullanıcının olması durumunda her bir kullanıcı için bir adet ve ADM'de de n adet olmak üzere toplam $2n\times$ n kadar anahtar üretilmesi ve saklanması gerekmektedir. Ağa yeni bir kullanıcı katılması durumunda ADM ile yeni kullanıcı arasında paylaşılmak üzere 1 adet anahtar oluşturulur. Oluşturulan anahtar hem ADM hem de yeni kullanıcıda saklanmalıdır. Diğer kullanıcıların herhangi bir işlem yapmalarına gerek yoktur.

Bu yöntem pasif saldırılara karşı güvenlidir ama aktif saldırı olması durumunda güvenlik zafiyeti barındırmaktadır. Bu yöntemin diğer bir dezavantajı da güvenliğin tek noktaya bağlı olmasıdır. ADM sunucusundaki ana anahtarların ele geçirilmesi durumunda sistemdeki bütün anahtarların ifşa olduğu kabul edilir. Bütün kullanıcılar için yeni anahtarların oluşturulması ve dağıtılması gerekir. Ana anahtar güvenliği ADM'ye bağlıdır. Burada bir güvenlik zafiyeti oluşması demek bütün ana anahtarların gizliliğinin ortadan kalkması anlamına gelir.

Merkezi Olmayan Anahtar Dağıtımı

Kullanıcı sayısının az ve kullanıcılar arasındaki coğrafi mesafelerin kısa olması durumunda ADM olmadan anahtar dağıtımı mümkündür. Güvenilir bir ADM olması yukarıda bahsedilen güvenlik açıklarına sebep olabilmektedir. Merkezi Olmayan Anahtar Dağıtımı yönteminde bir kullanıcının diğer bütün kullanıcılar ile güvenli iletişim sağlamak üzere paylaştığı bir anahtar olduğu kabul edilir. Kullanıcılar, bu anahtar sayesinde yeni oturum anahtarları oluşturabilmektedir. Merkezi olmayan anahtar dağıtımı yöntemi ile Can ve Bora arasında güvenli bir oturum anahtarı oluşturmak için aşağıda verilen adımlar takip edilir:

I. Can güvenli iletişim kurmak istediği Bora'ya kimliğini ve oluşturduğu rastgele bir sayıyı açık olarak (herhangi bir kriptografik yöntem kullanmadan) gönderir.
II. Bora yeni oturum anahtarını, kendi kimliğini, Can'ın oluşturduğu rastgele sayının bir artırılmış halini ve kendi oluşturduğu rastgele bir sayıyı Can ile paylaştığı anahtarı kullanarak şifreli bir şekilde iletir.
III. Can, Bora ile paylaştığı anahtarı kullanarak mesajı çözer ve böylece mesajın gerçekten Bora'dan geldiğini doğrular ve yeni oturum anahtarını elde eder. Aynı zamanda kendisi tarafından oluşturulan rastgele sayının doğruluğunu kontrol eder.
IV. Son olarak Can, Bora'nın oluşturmuş olduğu rastgele sayının bir artırılmış halini, yeni oturum anahtarını kullanarak şifrelenmiş bir şekilde Bora'ya gönderir. Böylece Bora gerçekten Can ile iletişim içinde olduğunu doğrular. Bu durumda Can ve Bora birbirlerinin kimliğini doğrulamış olurlar.

Bu yöntem bir ADM olmadan kullanıcılar arasında oturum anahtarlarını oluşturmayı mümkün kılar. Ancak *n* kullanıcısı olan bir ağda her bir kullanıcıda *n-1* adet anahtarın saklanması ve toplamda $n \times (n-1)/2$ anahtar çifti oluşturulması gerekmektedir. Yeni bir kullanıcın ağa katılmasıyla, *n* adet anahtarın üretilmesi ve bu anahtarların fiziki yollar ile diğer bütün kullanıcılara dağıtılması gerekmektedir.

Asimetrik Şifreleme ile Anahtar Dağıtımı

Asimetrik şifreleme veya açık anahtar şifreleme yöntemlerini uygulayabilmek için her kullanıcının, bir adet açık ve bir adet gizli olmak üzere birbiri ile ilişkili bir anahtar çifti oluşturması gerekmektedir. Simetrik şifreleme yöntemlerinde bit tabanlı operasyonlar kullanılarak gizlilik sağlanır. Açık anahtar şifreleme yöntemleri, dayandıkları karışık ve uzun matematiksel işlemlerden dolayı simetrik şifreleme yöntemlerine göre yavaştırlar. Bu yüzden uzun mesajların şifrelemesinde tercih edilmezler. Ancak güvensiz bir ortamda iki kullanıcı arasında AES veya 3DES gibi simetrik yöntemler için gerekli gizli oturum anahtarının oluşturulmasında ve kullanıcılara dağıtılmasında kullanılabilir. Anahtar dağıtımında en yaygın kullanılan yöntem, basit ve pratik olmasından dolayı asimetrik şifreleme algoritmalarıdır. En basit yöntemlerden bir tanesi Merkel tarafından ortaya konmuştur. Bu yöntem ile Can ve Bora arasında gizli bir oturum anahtarı oluşturmak için sırasıyla aşağıda verilen adımlar takip edilir:

I. Can öncelikle bir adet açık ve bir adet gizli olmak üzere anahtar çifti oluşturur. Güvenli iletişim kurmak istediği Bora'ya hem açık anahtarını hem de kendi kimliğini gönderir.
II. Bora AES veya 3DES gibi simetrik yöntemler için gerekli gizli oturum anahtarını oluşturur. Daha sonra oluşturduğu oturum anahtarını Can'ın açık anahtarını kullanarak şifreler ve gönderir.
III. Can sadece kendisinin bildiği kabul edilen gizli anahtarını kullanarak gelen mesajı çözer ve oturum anahtarını elde eder.
IV. Can ile Bora arasındaki iletişim bundan sonra simetrik yöntemlerden biri ve oturum anahtarı kullanılarak devam eder.

SIRA SİZDE 1

Bora AES algoritması için gerekli bir gizli oturum anahtarı oluşturmak isterse, anahtar uzunluğu ne olmalıdır?

Aradaki Adam Saldırısı

Aradaki adam saldırısı bütün açık anahtar şifreleme algoritmalarına karşı kullanabilen bir saldırı türüdür. Aradaki adam saldırısını gerçekleştirebilmek için iletişim ağının ele geçirilmesi gerekmektedir.

Aradaki adam saldırısı, bütün asimetrik veya açık anahtar şifreleme algoritmalarına karşı kullanılabilen bir saldırı türüdür (Paar ve Pelzl, 2010). Kötü niyetli bir kullanıcının, açık anahtar yöntemleri ile güvenli bir iletişim kurmak isteyen kullanıcıların arasına girerek, onların açık anahtarı yerine kendi açık anahtarını göndermesi ile uygulanır. Saldırıyı gerçekleştirebilmek için kötü niyetli kişinin iletişim ağını ele geçirmesi gerekir. Bu saldırının nasıl uygulanabileceği aşağıda kısaca açıklanmıştır. Bu senaryoda Can ve Bora iyi niyetli iki kullanıcıyı, Cem ise kötü niyetli kullanıcıyı temsil etmektedir. Can ve Bora aralarında bir oturum anahtarı oluşturmak isterken, Cem, Can ve Bora arasında oluşturulan iletişim kanalına girerek her ikisi ile birer gizli anahtar oluşturur.

I. Can öncelikle bir adet açık ve bir adet gizli olmak üzere bir açık anahtar çifti oluşturur. Güvenli iletişim kurmak istediği Bora'ya hem açık anahtarını hem de kendi kimliğini gönderir.
II. Kötü niyetli kullanıcı Cem, Can'ın gönderdiği mesajı yakalar ve kendi açık anahtarı ile Can'ın açık anahtarını değiştirir. Yeni oluşturduğu mesajı Bora'ya iletir. Bora mesajın Can'dan geldiğini düşünür. Ancak açık anahtarın Cem'e ait olduğunu fark edemez.
III. Bora oturum anahtarını oluşturur ve aldığı mesajın içinde bulunan açık anahtar, yani Cem'e ait anahtar ile şifreler.
IV. Cem iletilen mesajı alır ve kendisine ait gizli anahtar ile çözer. Böylece Can ile Bora arasında güvenli iletişim sağlamak amacı ile oluşturulan oturum anahtarını elde eder.
V. Cem elde etmiş olduğu oturum anahtarını Can'ın açık anahtarını kullanarak şifreler ve Can'a gönderir. Can ise gelen mesajı, Bora'dan geliyormuş gibi algılar ve mesajı çözerek oturum anahtarına ulaşır.

Bundan sonra Can ile Bora arasında güvenli veri iletişimi oluşturulan oturum anahtarı ve simetrik yöntemlerden biri kullanılarak yapılır. Ancak kötü niyetli Cem oturum anahtarına sahip olduğu için, Can ile Bora arasında iletilen bütün güvenli mesaj trafiğini ele geçirmiş olur. Can'ın Bora'ya gönderdiği mesajı ele geçirip çözer ve mesajı okuyabilir. Sonra Bora ile arasında oluşturduğu anahtarla şifreleyerek Bora'ya gönderir. Benzer senaryoyu Bora Can'a mesaj gönderdiği zaman da uygular. Güvenli bir oturum anahtarı oluşturmak isteyen kullanıcıların açık anahtarlarının kimlik denetimi yapılması ile bu saldırı önlenebilir. Kullanıcılara ait açık anahtarların sertifika kullanarak karşı tarafa aktarılması bu problemi ortadan kaldırılır. Anahtar dağıtımında aradaki adam saldırısına dikkat edilmesi gerekir. Eğer anahtar dağıtımı algoritmaları veya protokolleri kimlik doğrulaması olmadan uygulanırsa, aradaki adam saldırılarına maruz kalabilirler. Bu nedenle bu tür saldırılara karşı kimlik doğrulamasının mutlaka yapılması gerekmektedir.

Sertifikalar

Aradaki adam saldırısında görüldüğü gibi kullanıcıların açık anahtarları için kimlik doğrulaması gerekmektedir. Bu amaçla sertifika kullanan çözümler ortaya konmuştur. Sertifika bir açık anahtarı, bir kişi, uygulama veya servis ile ilişkilendirmek için kullanılan bir dijital dokümandır. Sertifikaların yönetimi güvenilir üçüncü partiler tarafından yapılır. Güvenilir üçüncü partilere sertifika otoritesi denir. Sertifikaların güvenliği bu sertifika otoritelerine bağlıdır. Bir varlığın kimliği, dijital imzası kullanılarak doğrulanabilir. Sertifikalar en basit haliyle sertifika sahibinin açık anahtarı, kimliği ve dijital imzasından oluşur. Dijital imza, sertifika sahibinin gizli anahtarı kullanılarak açık anahtarının ve kimliğinin şifrelenmesi ile elde edilir. Bir başka kullanıcının sertifikasını alan kişi, dijital imza ile kimlik bilgisini karşılaştırarak doğrulama yapar. Eğer imza içerisindeki kimlik bilgisi ile gönderenin kimlik bilgisi eşleşmez ise kimlik doğrulaması yapılamadığı için oturum anahtarı oluşturma yöntemi, anahtar üretilmeden sonlandırılır. Kimlik doğrulaması yapılırsa, oturum anahtarı oluşturma süreci başlatılır. Şekil 5.1'de X.509 sertifika yapısı gösterilmektedir (Stallings, 2011).

Şekil 5.1

X.509 sertifika yapısı

Versiyon
Seri Numarası
Sertifika Algoritması: • Algoritma • Parametreler
Yayımlayan
Geçerlilik Süresi: • Başlangıç süresi • Bitiş Süresi
Konu
Konunun Açık Anahtarı: • Algoritma • Parametreler • Açık Anahtar
Dijital İmza

Şekil 5.1'de yapısı verilen bir X.509 sertifikasında 1, 2 ve 3 olmak üzere versiyon numarası, sertifikayı tanımlamak için yayımlayıcı adı ve eşsiz bir sayı, sertifikayı imzalamak için kullanılan algoritma ve parametreleri, sertifika yayımlayanın adı, sertifikanın geçerlilik süresi, sertifikanın kim için düzenlendiği, sertifika düzenlenene ait açık anahtar ve algoritma ve son olarak da sertifika otoritesinin gizli anahtarı kullanılarak elde edilmiş dijital imza bulunmaktadır.

Sertifika oluşturmak için iki farklı yöntem vardır. Birinci yöntemde kullanıcı kendisine ait açık anahtar çiftini oluşturur ve açık anahtarını imzalatmak için sertifika otoritesine gönderir. Bu yöntemin adımları aşağıdaki gibidir:

I. Can bir adet açık ve bir adet gizli olmak üzere açık anahtar çifti üretir ve açık anahtarını ve kimliğini sertifika otoritesine iletir.
II. Sertifika otoritesi öncelikle Can'ın kimliğini denetler. Sonra kendi gizli anahtarını kullanarak Can'ın kimliğini ve açık anahtarını şifreleyerek dijital imza üretir.
III. Sertifika otoritesi Can için açık anahtarı, kimliği ve imzadan oluşan sertifikayı oluşturur ve bu sertifikayı Can'a gönderir.

Bu yöntemde açık anahtarı denetlemek için her seferinde kimliği doğrulanmış bağlantı kurmak gerekmektedir. Aksi halde aradaki adam saldırısına açıktır. Açık anahtar çiftlerinin sertifika otoriteleri tarafından üretildiği alternatif bir çözüm ortaya konmuştur. Bu yöntemin adımları aşağıdaki gibidir:

I. Can sertifika elde etmek için sertifika otoritesine istekte bulunur.
II. Sertifika otoritesi Can'ın kimliğini denetler. Can için açık ve gizli anahtar çiftini oluşturur. Kendi gizli anahtarını kullanarak Can'ın kimliğini ve açık anahtarını şifreleyerek dijital imzasını oluşturur. Can'ın kimliği, açık anahtarı ve sertifika otoritesinin imzasından oluşan sertifikayı üretir.
III. Sertifika otoritesi sertifikayı ve Can'ın gizli anahtarını güvenli bir iletişim kanalı kullanarak iletir.

Bu yöntemin avantajı sadece sertifika üretim safhasında bir kez kimliği doğrulanmış bağlantıya ihtiyaç duymasıdır. Ama sadece kullanıcının bilmesi gerektiği kabul edilen gizli anahtarın bir başkası tarafından üretilmesi bu yöntemin dezavantajıdır. Açıklanan avantaj ve dezavantaj dikkate alınarak kimlik doğrulama yöntemi seçilmelidir.

SIRA SİZDE 2

Sertifikaların içinde yer alan bilgilerden biri dijital imzadır. Sertifikalarda yer alan bu dijital imza nasıl oluşturulur?

AÇIK ANAHTAR ALTYAPISI

Açık anahtar altyapısı veya kısaca PKI (Public Key Infrastructure) açık anahtar şifreleme yöntemleri için gerekli servisleri kapsar. Açık anahtar altyapısının kapsadığı bu servis-

ler kullanıcıların, programların ve sistemlerin kullandığı sertifikaların üretilmesinden, yayımlanmasından, saklanmasından, yönetilmesinden ve kaldırılmasından sorumludur. PKI'nın sertifika yayımlamak, sertifika iptal etmek, sertifika iptal listelerini oluşturmak ve basmak, sertifika ve iptal listelerini saklamak ve erişime açmak ve anahtar yaşam döngüsünü yönetmek üzere temel işlevleri vardır. SSL, S/MIME, VPN ve PGP gibi teknolojiler PKI altyapısını kullanmaktadır.

Sertifika yayımlamak: Sertifika otoritesi sertifika isteğinde bulunan kullanıcının kimliğini doğrulayarak imzalar. Buna ek olarak sertifika için geçerlilik süresi belirler ve üretilen sertifikayı depolama alanına gönderir.

Sertifika iptal etmek: Kullanıcıya ait gizli anahtarın ifşa olması veya çalışanın işten ayrılması gibi durumlarda sertifikaların geçerlilik süreleri dolmadan iptal edilmeleri gerekebilir. Bu gibi durumlarda, iptal edilecek sertifikanın numarasının, sertifika iptal listelerine (Certificate Revocation List–CRL) eklenmesi sağlanır.

Sertifikaların ve iptal listelerinin saklanması ve erişime açılması: En yaygın yöntem, LDAP erişimi ile bir klasör servisi kullanmaktır. Ancak X.500 ile uyumlu HTTP, FTP veya e-posta seçenekleri de kullanılabilir.

Anahtar yaşam döngüsünü yönetmek: Aynı anahtarın uzun süre kullanılması güvenlik açıklarına neden olabileceği için anahtarların belirli aralıkla yenilenmesi gerekmektedir.

Dünya üzerinde sertifika yayımlayan ve iptal eden tek bir sertifika otoritesi olması birçok problemi ortadan kaldırabilir. Ancak gerek güvenlik, gerek coğrafi şartlardan dolayı bu mümkün değildir. Bu yüzden sertifika otoriteleri hiyerarşik bir yapıda şekillenmişlerdir. En üstte bulunan otorite kök sertifika otoritesi ve altında yer alanlar ise yayımlayıcı sertifika otoritesi olarak adlandırılır. PKI ile ilgili standartlar, PKI tanımlayıcı ve PKI uygulayıcı olmak üzere iki ayrı kategoriye ayrılmaktadır.

PKI tanımlayıcı standartlar

- X.509,
- PKIX ve
- PKCS olarak sıralanır.

PKI uygulayıcı standartlar ise

- S/MIME,
- SSL ve TLS ile
- IPSec

olarak sıralanabilir.

X.509 sertifikasını destekleyen protokol ve standartlara örnek veriniz.

SIRA SİZDE 3

KULLANICI KİMLİK DOĞRULAMA VE YÖNTEMLERİ

Kimlik doğrulama, kullanıcıların iddia ettikleri kişi olup olmadıklarını ispat etmek için kullanılır. Bir kişinin fotoğraflı kimliğine bakarak onun kimliğini doğrulama yöntemi, bir sınav ortamında bina girişlerinde uygulanan bir yöntemdir. Kimlik kartları, sürücü belgesi ve pasaport gibi kimlikler, kimlik doğrulama için kullanılabilir. Fakat bu yöntemde kişilerin birbirleriyle fiziksel olarak iletişim halinde olmaları gerekmektedir. Telefon görüşmesi yaparken bir kişinin sesinden onun kim olduğunu tanıyabilmek için o kişi ile önceden bir yerde karşılaşmış olmak veya o kişiyi daha önceden tanımak gerekmektedir. Teknolojik gelişmeyle birlikte, kullanıcıların kimliklerini sanal ortamlarda doğrulamak için çok daha farklı yöntemlerin kullanılması gerekmektedir. Bu yöntemler sadece kullanıcının kendisi ve doğrulama otoritesinin bildiği bir parola, tek kullanımlık parola üreten bir yazılım veya donanım ya da parmak izi gibi biyometrik yöntemler olmak üzere üç grupta toplanabilir.

Kullanıcının kimlik bilgisi iki parçadan oluşur. Birinci parça, herkesin bilmesinde bir sakınca olmayan kullanıcı adı olarak isimlendirilir. Kullanıcı adı herkese açık bir bilgi olarak kabul edilir. İkinci parça ise kimlik bilgisini doğrulamak üzere sadece kullanıcının ve doğrulama otoritesinin bilmesi veya sahip olması gereken ve başkaları ile kesinlikle paylaşılmaması gereken bir şifredir. Kullanıcının bildiği bir parola, sahip olduğu bir akıllı kart veya kullanıcıya ait fiziksel bir özellik olabilir. Gizli olması gereken şifre parola gibi kullanıcın bildiği, akıllı kart gibi sahip olduğu veya kullanıcıya ait fiziksel bir özellik olabilir. İkinci kısım ise birinci kısmın aksine gizli olmalıdır. Parola, sadece kullanıcının kendisinin bildiği kabul edilen ve uzun yıllardır en yaygın olarak kullanılan kimlik doğrulama yöntemlerinden biridir. Parolaların çeşitli yollarla kötü niyetli kişiler tarafından kolayca ele geçirilmesi ve bu nedenle sık aralıklarla değiştirilen parolaların unutulması, bu yöntemin zayıf yönlerinden biridir. Sadece parola kullanılarak kimlik doğrulama, tek faktör kimlik doğrulamaya bir örnektir. İki veya daha fazla yöntem kullanılarak yapılan kimlik kontrol işlemi, çoklu faktör kimlik doğrulama olarak adlandırılır. Akıllı kart veya biyometrik yöntemler kullanılarak yapılan kimlik doğrulama parolaya göre daha güvenlidir. Fakat her iki yöntem de kullanıcıya ek maliyet getirmektedir.

Kullanıcı Adı ve Parola

En yaygın ve kolay uygulanabilen kimlik doğrulama yöntemi kullanıcı adı ve parola çiftinden oluşur. Kullanıcı girmiş olduğu kullanıcı adının gerçekten kendisine ait olduğunu kanıtlamak için doğru parolayı da bilmek zorundadır. Eğer kullanıcı adı ve parola eşleşiyorsa erişim izni verilir. Fakat eşleşme olmazsa kullanıcı kimliğini doğrulatamadığı için sisteme erişimi engellenir. Kullanıcı adları, genelde kullanıcıların tam isimlerini anımsatacak şekilde seçilir. Ele geçirilmesi zor bir parola oluşturmak için aşağıda verilen kurallara uymak gerekir.

Güçlü bir parola aşağıda verilen özelliklere sahip olmalıdır:

- En az sekiz karakter uzunluğunda olmalıdır.
- Parola oluştururken {a, b, c, …, z}, {A, B, C, …, Z}, {0, 1, 2, …, 9} ve {?, @, !, #, %, $} karakter kümelerinin her birinden en az bir karakter kullanılmalıdır.
- Sözlükte yer alan kelime içermemelidir.
- Ad, soyad ve doğum tarihi gibi kişisel bilgiler içermemelidir.
- Belirli zaman aralıklarında yenilenmelidir.
- Önceden kullanılan parolalardan farklı olmalıdır.
- Aynı parola birden çok kimlik doğrulama sisteminde kullanılmamalıdır.
- Hatırlanması kolay ama başkaları tarafından tahmin edilmesi zor olacak şekilde uzun seçilmelidir.

Parola kullanmanın oluşturacağı güvenlik açıkları olabilir. Can isimli kullanıcı parolasını kullanarak kimlik doğrulama yapmak istediğinde, kötü niyetli kişi kullanılan parolayı görebilir. Parolalar gerektiğinde hatırlamak veya kullanmak üzere bilgisayarda bir dosya içinde saklanabilir. Bu durumda bilgisayara erişim sağlayan kötü niyetli kişi bu dosyaya erişerek parolaları öğrenebilir. Parolalar çok dikkatli seçilmelidir. Yukarıda açıklanan özelliklere göre seçilmeyen parolalar çok kolaylıkla elde edilebilir. Kötü niyetli kişi bir takım denemeler yaparak parolayı elde edebilir. Mesela, parola sözlükte yer alan bir kelime olarak seçilmiş olsun. Bu durumda kaba kuvvet saldırısı uygulanarak parola çok sayıda deneme yapılarak elde edilebilir. Bunun için sözlükte yer alan bütün sözcükler tek tek denenir. Bu denemeler sonucunda gerçek parola bulunabilir. Bir başka problem hatırlanması zor parolalar seçildiğinde görülebilir. Bu durumda kullanıcılar parolalarını kolay hatırlamak için bir yerlere not edebilirler. Bu kayıtın kötü niyetli kişilerin eline geçmesi durumunda parolanın gizliliği ortadan kalkmış olur.

Farklı kimlik doğrulama sistemleri için birbirinin aynısı olmayan parolalar tercih edilmelidir. Aynı parolanın farklı yerlerde kullanılması durumunda, parolayı ele geçiren kötü

niyetli kişi bu sistemlerin hepsine giriş yapabilir. Farklı parolaların kullanılması durumunda ise bütün parolaların hatırlanması gerekir.

Parola güvenliğini artırmak için parolaların belli aralıklarla değiştirilmesi gerekir. Eğer kötü niyetli kişi parolayı ele geçirirse, bu parola sadece parolanın değiştirileceği zamana kadar kullanılabilir. Kullanıcı, parolasını kısa zaman aralıkları içerisinde değiştirirse, parolanın ele geçmesi durumunda kötü niyetli kişilerin vereceği zarar en aza indirgenmiş olur. Çok kısa aralıklarla parolanın değiştirilmesinin olumsuz sonuçları da olabilir. Parolalar sıklıkla değiştirilirse, hatırlanması zor olur. Bu durumda kullanıcılar hatırlanması kolay parola seçme eğiliminde olurlar veya hatırlamak için sürekli parolalarını not ederler. Kullanıcılar bu nedenle aynı parolayı uzun süre kullanma eğiliminde olurlar. Bu eğilimin önüne geçmek için güvenlik sistemleri, kullanıcıların parolalarını belli aralıklarla değiştirmelerini zorunlu kılar. Bu durumda sistem ayrıca kullanıcının daha önce kullandığı parolaları da kontrol ederek önceden kullanılmamış bir parola seçmesini sağlar.

SIRA SİZDE 4

Can kendine bir parola seçecektir. Parola altı karakterden oluşacaktır. Karakterler Türkçe alfabede yer alan 29 harf içinden seçilecektir. Bir harf birden fazla kullanılabilir. Sadece küçük harf kullanılacaktır. Bu şartlara göre Can'ın seçebileceği kaç farklı parola vardır?

Kullanıcı adı ve parola üzerine inşa edilmiş birçok yöntem vardır:

- Lokal depolama
- Merkezi depolama
- Kerberos
- Bir kullanımlık parola

Lokal Depolama

İlk bilgisayar sistemleri çok kullanıcılı olarak tasarlanmamıştır. Fiziksel olarak bilgisayara erişimi olan kişiler bütün yazılım, donanım ve kullanıcı dosyalarını kontrol edebiliyordu. Bu durum beraberinde birçok güvenlik zafiyeti getirmişti. Bu problemi ortadan kaldırmak amacı ile her kullanıcının kullanıcı adı ve parolasını girerek, sadece kendilerine verilen yetkilerce erişim hakkı sunan sistemlere geçiş yapıldı. Bu sistemlerde kullanıcı adları ve parolaları bir dosyada açık olarak saklanmaktaydı ve bir sistem yöneticisi kullanıcı parolalarını oluşturmak ve dağıtmak ile görevlendirilmişti. Parolaların saklandığı dosyaya kötü niyetli kişiler tarafından kolayca ulaşılması birçok problemi de beraberinde barındırıyordu. Kullanıcı parolalarının saklandığı dosyanın şifrelenmesi sistemin güvenliğini artırmıştı ama kullanılan şifreleme algoritmalarının çok güçlü olmamasından dolayı kaba kuvvet veya sözlük saldırısı yöntemleri ile kötü niyetli kullanıcılar tarafından parolaların elde edilmesi mümkün olabilmekteydi. İlk kullanılan şifreleme algoritmaları geleneksel algoritmalar olup günümüz modern şifreleme algoritmalarına göre daha düşük seviyede güvenlik sağlamaktadırlar. Bunlarla şifrelenen parola dosyaları kolayca kırılarak parolalara ulaşmak mümkündü. Bu şifrelerin kırılması için olası bütün anahtarların sırayla denenmesi yeterlidir. Sistemlerin fiziksel olarak da korunması gerektiğinden merkezi çözümler, lokal çözümlerin yerini aldı.

Merkezi Depolama

Parolaların uzak bir merkezde saklanması güvenliği artırdı. Ancak bunun yanında yeni problemlerin doğmasına sebep oldu. Bu durumda kullanıcının girmiş olduğu parolanın güvenli olmayan bir ağ üzerinden sunucuya iletilmesi gerekir. Telnet ve FTP gibi protokoller, parolaları şifrelemeden açık bir şekilde ağ üzerinde iletirler. Kullanıcı ile merkezi sunucu arasında oluşan bağlantıyı dinleyen kötü niyetli bir kişi, parolaları zahmetsizce elde etme imkânı bulur.

Parolaların bir merkezde depolanması için önerilen ilk çözümler hem yeniden gönderme (replay) hem de aradaki adam saldırılarına maruz kalabiliyorlardı. Bu saldırıları bertaraf etmek için hem kullanıcının hem de sunucunun birbirlerini doğrulamaları gerekiyordu. Bu amaçla kimlik doğrulama yöntemleri olan CHAP ve MS-CHAP protokolleri kullanılabilir. Bu protokoller aşağıda verilen adımlardan oluşur:

- Kullanıcının sunucuya bir erişim isteği göndermesi durumunda sunucu kullanıcıya rastgele bir sayı üreterek gönderir.
- Kullanıcı sunucudan gelen rastgele sayının bir artırılmış halini ve parolasını özet fonksiyonuna gönderir. Özet fonksiyonundan elde ettiği çıktıyı sunucuya iletir.
- Sunucu rastgele sayıyı ve kullanıcının parolasını bildiği için özet değerini oluşturur. Kendi ürettiği değer ile kullanıcıdan gelen değeri karşılaştırarak kullanıcının kimliğini doğrular. Eşleşme var ise kullanıcıya erişim izni verilir. Eğer eşleşme yoksa erişim izni verilmez.

CHAP ve MS-CHAP protokollerinin ilk sürümlerinde, yalnızca kullanıcı kimliği sunucu tarafından üretilen rastgele sayı kullanılarak kontrol edilir. Sunucunun kimliğini kontrol etmek için benzer bir şekilde kullanıcının ürettiği rastgele sayı şifrelenmiş bir şekilde sunucuya iletilir. Şifrelenmiş sayıyı elde etmek için sunucu veri tabanında var olan parolayı kullanır ve rastgele sayıyı bir artırarak kullanıcıya gönderir. Bu şekilde sunucu kullanıcıya kimliğini kanıtlar.

Kerberos

Kerberos MIT tarafından geliştirilen bilet-tabanlı bir ağ kimlik doğrulama yöntemidir.

Kerberos bilet-tabanlı bir ağ kimlik doğrulama yöntemidir. MIT (Massachusetts Institute of Technology) tarafından Athena projesinin bir parçası olarak geliştirilmiştir. Adını Yunan mitolojisinde yer alan üç başlıklı muhafız bir köpekten almaktadır. Kerberos, simetrik şifreleme algoritmaları üzerine kurulmuştur ve güvenilir üçüncü kişi yapısına gereksinim duymaktadır. Kerberos standardında parola önemli bir yere sahiptir. Fakat sertifikalar (açık anahtar şifreleme algoritmaları) kullanılarak da kimlik doğrulama yapılabilir. Dağıtık mimariye sahip bilgisayar sistemlerinde yetkisi olmayan kullanıcılar servislerden faydalanmak veya yetkili kullanıcılar kendilerine verilen hakların dışına çıkmak isteyebilir. Sisteme bağlı her bir sunucu için ayrı ayrı kimlik doğrulama protokolü yerine Kerberos merkezi kimlik doğrulama imkânı sunmaktadır. Aradaki adam saldırısı gibi saldırılara karşı koymak için sunucular ve kullanıcıların karşılıklı olarak kimlik doğrulaması yapmaları gerekmektedir. Günümüzde Kerberos'un dördüncü ve beşinci sürümleri yaygın olarak kullanılmaktadır. Dördüncü sürüm güvenlik, güvenilirlik, saydamlık ve ölçeklenebilirlik gereksinimlerini destekler. Beşinci sürüm, bir önceki sürümde görülen güvenlik açıklarını kapatmak amacıyla geliştirilmiştir. İlk üç sürüm sadece MIT'de kullanılmıştır ve artık hiçbir yerde kullanılmamaktadır. Windows işletim sisteminin son sürümleri ağ kimlik doğrulama protokolü olarak Kerberos kullanırlar.

Uzaktan sistem kaynaklarına erişmek performans için önemlidir. Bu nedenle sisteme giriş yapan Can uzaktaki kaynaklara erişmek ister. Bu kaynakların Can'ın kimliğini doğrulaması gerekir. Bu nedenle Kerberos, ağ kimlik doğrulama yöntemi olarak kullanılır. Eğer Kerberos gibi bir ağ kimlik doğrulama yöntemi kullanılmazsa, ortaya güvenlik riskleri çıkabilmektedir. Herhangi bir kullanıcı, belli bir sisteme veya bilgisayara uzaktan erişerek farklı bir kullanıcı gibi hareket edebilir. Kötü niyetli kullanıcı, ağı dinleyerek sunucuya girip işlemleri kesintiye uğratabilir.

Sadeleştirilmiş haliyle Kerberos aşağıdaki adımlardan oluşmaktadır;

I. Kullanıcı, kimlik doğrulama sunucusuna kendisinin ve bilet sağlayıcı sunucusunun kimliğini gönderir.
II. Kimlik doğrulama sunucusu, kullanıcıya farklı servisler için gerekli biletleri almak üzere kullanıcının parolasıyla şifrelenmiş olan bir *Bilet Sağlayıcı Bilet* gönderir. *Bi-*

let Sağlayıcı Bilet kimlik doğrulama sunucusu ve bilet sağlayıcı sunucu arasında paylaşılan gizli anahtar ile şifrelenir. *Bilet Sağlayıcı Bilet*, kullanıcının ve bilet sağlayıcı sunucusunun kimliği ve biletin ne kadar süre ile geçerli olacağını gösteren zamandan oluşmaktadır.

III. Kullanıcı bilet sağlayıcı sunucuya hangi servisten faydalanmak istiyorsa onun kimliğini, kendi kimliğini ve *Bilet Sağlayıcı Bileti* gönderir.

IV. Bilet sağlayıcı sunucu, kullanıcıya gerekli doğrulama işlemini yaptıktan sonra istediği serviste kullanmak üzere *Bilet* gönderir. Gönderilen *Bilet*, servis ve bilet sağlayıcı sunucusu arasında paylaşılan anahtar ile şifrelenir. *Biletin* içerisinde kullanıcının kimliği, servis sunucusunun kimliği ve biletin geçerlilik süresi vardır.

V. Kullanıcı iletişime geçmek istediği servis sunucusuna elde etmiş olduğu *Bileti* göndererek istekte bulunur ve servisten yararlanmaya başlar.

Kullanıcı ağda bulunan bir servisten yararlanmak istediğinde birinci ve ikinci adımları takip ederek kendisinin ve bilet sağlayıcı sunucusunun kimliğini kimlik doğrulama sunucusuna gönderir. Sunucu ise kimlik doğrulaması yaptıktan sonra kullanıcıya bir *Bilet Sağlayıcı Bilet* ulaştırır. Böylece kullanıcı farklı servislerden faydalanmak istediğinde, açmış olduğu oturum süresince artık bir daha parola girmek zorunda değildir. Kimlik doğrulama sunucusu oluşturduğu veriyi kullanıcının parolasını kullanarak elde ettiği gizli anahtar ile şifreler ve böylece kullanıcıya gönderdiği mesajın sadece kullanıcı tarafından çözülmesini sağlar. Ayrıca kimlik doğrulama sunucusu *Bilet Sağlayıcı Bileti*, bilet sağlayıcı sunucusu ile paylaştığı gizli anahtar ile şifrelediği için ne kullanıcı ne de kötü niyetli kişiler bilet içindeki veriyi değiştiremezler. Yeniden gönderme saldırılarını önlemek için bilet içerisinde geçerlilik süresi vardır. Bu yüzden kullanıcı ve sunucu zamanları senkronize olmalıdır. Kullanıcı ile sunucu saatleri arasındaki oluşabilecek en çok beş dakikalık fark ihmal edilebilir kabul edilmektedir.

Yeniden gönderme atağını açıklayınız.

SIRA SİZDE 5

Bir Kullanımlık Parola

Kullanıcılar yeterince bilinçli olmadıkları zaman kolay hatırlanabilir parolalar oluşturmakta ve parolaları bir kâğıda yazarak saklamaktadırlar. Bunlara ek olarak, oluşturdukları bir parolayı birden fazla sistemde kimlik doğrulaması amacıyla kullanmaktadırlar. Parolaların kullanıcılar tarafından oluşturulması, sistemleri, sözlük ve yeniden gönderme saldırısı kullanan kötü amaçlı yazılımlara açık bırakmaktadır. Özellikle GSM şifrelemesinde kullanılan tek kullanımlık kod çözümüne benzer yöntemler, parolaların kullanıcılar tarafından değil de bir protokole göre üretilmesini sağlayarak bu problemin ortadan kaldırılmasını hedeflemiştir. Kullanıcı her kimlik doğrulatma işlemi için farklı parola girmek zorundadır. Bu çözümde hem kullanıcı hem de sunucunun senkronize olarak aynı parolayı üretmesi gerekmektedir. Bir kullanımlık parolalar zamana bağlı olarak üretilebilmektedir.

Bankacılık uygulamalarında yaygın olarak kullanılan bu yöntemde, parola üretecek fonksiyon, girdi parametresi olarak kullanıcının kimlik doğrulatma anındaki zamanını alır. Hem kullanıcı hem de sunucu aynı fonksiyon ve zaman değerini kullandıkları için birbirlerinden bağımsız olarak aynı parolayı üretmiş olurlar. Kullanıcı belirli bir süre aralığında üretilen parolasını girmek zorundadır. Sürenin aşılması durumunda yeni bir parola üretilmesi gerekir. Kullanıcı akıllı kart veya cep telefonu gibi donanım ya da yazılım çözümlerinden birini kullanarak bir kullanımlık parola üretebilir. Bankacılık uygulamaları, kullanıcıdan parolaya ek olarak PIN kodunu girmesini de ister. Böylece iki faktör kimlik doğrulama ile sisteme erişim izni verilir. Tek faktör kimlik doğrulamaya oranla iki faktör kimlik doğrulama daha güvenlidir.

Açık Anahtar Şifreleme ile Kimlik Doğrulama

Dijital sertifika, bir kimliği (kişi, bilgisayar, program) bir açık anahtar ile ilişkilendirir. Basitçe bir dijital sertifikada sertifika sahibinin kimliği, açık anahtarı ve sertifikayı yayımlayan kuruluşun gizli anahtarı kullanılarak oluşturulmuş imza bölümleri vardır. Dijital sertifika kullanarak kimlik doğrulaması yapan bir protokolün adımları aşağıda verilmiştir;

I. Kullanıcı sunucuya kimlik doğrulama isteği gönderir.
II. Sunucu kullanıcıya rastgele ürettiği bir sayıyı iletir.
III. Kullanıcı sadece kendisinde olan gizli anahtar ile sunucudan gelen sayıyı şifreler ve sunucuya gönderir.
IV. Sunucu kullanıcının açık anahtarını bildiği için kullanıcıdan gelen mesajı çözer ve karşılaştırma yapar. Eğer kendi ürettiği sayı ile kullanıcıdan gelen sayı eşleşirse kullanıcının kimliği doğrulanmış olur. Eğer eşleşme sağlanamazsa, kimlik doğrulaması yapılamaz ve erişim izni verilmez.

Açık anahtar şifreleme kullanarak kimlik doğrulaması yapan protokollerden en yaygın olanı Secure Socket Layer (SSL)/Transport Layer Security (TLS) olarak bilinir. Bu protokolle hem sunucunun kimliğini kullanıcıya hem de kullanıcının kimliğini sunucuya doğrulatması gerekir. Doğrulatma işlemi başarı ile gerçekleşirse, sunucu ve kullanıcı arasında güvenli iletişim kurmaları için gerekli oturum anahtarı protokolün sonunda oluşturulur. Sunucu, bir sertifika otoritesinden kendisi için bir sertifika üretmesini ister ve üretilen sertifikayı Web sunucusunda saklar. Basitçe SSL/TLS protokolü aşağıdaki adımları kapsamaktadır.

I. Kullanıcı bağlantı kuracağı Web sunucusun adresini tarayıcıya yazar ve sunucuya istek gönderilir.
II. Sunucu kullanıcıdan gelen isteği alır almaz kendi sertifikasını gönderir.
III. Kullanıcının tarayıcısı kendisinde bulunan sertifika otoritesi sertifikalarını kullanarak sunucunun sertifikasını onaylar.
IV. Kullanıcı, simetrik oturum anahtarı oluşturur ve sunucunun açık anahtarını kullanarak şifreler.
V. Sunucu kullanıcıdan gelen şifrelenmiş mesajı, sadece kendisinde olan gizli anahtar ile çözer ve oturum anahtarını elde eder. Kullanıcı ve sunucu arasında güvenli bir iletişim kurmak için gerekli oturum anahtarı oluşturulmuş olur. Bundan sonra güvenli veri aktarımı 3DES veya AES gibi simetrik şifreleme yöntemlerinden biri seçilerek devam eder.

Biyometrik Yöntemler

Biyometrik yöntemler insanların fizyolojik veya davranışsal özelliklerinin belirli ölçütlere göre belirlenmesine ve daha sonra kimlik doğrulaması için karşılaştırılması üzerine kurulmuştur.

Kullanıcı parolalarının kötü niyetli kişiler tarafından farklı birçok yöntem kullanılarak elde edilmesinin yaygınlaşmasıyla alternatif çözüm arayışları hızlandı. **Biyometrik yöntemler** insanların fizyolojik veya davranışsal özelliklerinin ölçülmesine dayanmaktadır. Bütün biyometrik yöntemler deneye dayalı (heuristic) yaklaşımlar üzerine kurulmuştur. Örneğin, bir kişinin ıslak imzasında kişinin ruh haline ve bulunduğu ortama göre farklılıklar gözlemlenebilmektedir. Biyometrik kimlik doğrulama için kullanılacak hem fiziksel hem de davranışsal özelliklerin kişiye özgü ve eşsiz olmaları gerekmektedir. Bir başka deyişle, farklı iki kişinin aynı özelliğe sahip olma olasılığının çok düşük olması gerekir. Aksi durumda kimlik doğrulama çok güvenilir olmaz. Biyometrik özellikler fizyolojik özellikler (pasif) ve davranışsal özellikler (aktif) olmak üzere iki grupta incelenir.

Fizyolojik özellikler aşağıdaki gibi sıralanabilir:

- Parmak izi
- Yüz
- Kulak
- Retina

- İris
- El geometrisi
- Damar yapısı
- Koku

Davranışsal özellikler arasında aşağıdaki özellikler sayılabilir:

- Ses
- El yazısı
- Tuş vuruşu
- Dudak hareketi
- Yürüyüş tarzı

Yukarıdaki özelliklere ek olarak biyometrik kimlik doğrulama olarak kullanılabilecek diğer özellikler neler olabilir?

SIRA SİZDE 6

Biyometrik kimlik doğrulama sistemlerinde kayıt olma ve kimlik doğrulama olmak üzere iki temel işlem vardır. Kayıt olma işleminde kullanıcılara ait referans özellikler bir donanım ile elde edilir ve kullanıcının kimliği ile birlikte sistemde saklanır. Kimlik doğrulama için kullanıcı her başvurduğunda elde edilecek değerler ile sistemde saklanan değerler karşılaştırılır ve eşleşme olması durumunda kullanıcının kimliği doğrulanır. Her bir biyometrik yöntem için farklı bir algoritma kullanılarak karşılaştırma işlemi yapılır.

Biyometrik kimlik doğrulama yöntemlerinde, parola kullanan yöntemlerde olduğu gibi kullanıcının bir şey hatırlaması veya taşıması gerekli değildir. Biyometrik özelliklerin kopyalanması veya bir başka kişiye aktarılması neredeyse imkânsız olduğu için daha güvenilir çözümler sunar. Bir kişiye ait biyometrik veri, kaza veya yanma gibi durumların dışında değiştirilemez.

Bazı özel durumlarda (eli veya gözü olmayan kişiler gibi) biyometrik veri elde edilmesi mümkün değildir. Yaşlanma veya hastalık gibi sağlık durumlarında bazı biyometrik verilerde deformasyon görülebilmektedir. Biyometrik verilerin çok güvenli şekilde korunması gerekmektedir. Eğer kullanıcılara ait veriler çalınırsa, kullanıcılara ait biyometrik özellikler değiştirilemeyeceği için güvenlik zafiyetine sebep olur.

Biyometrik kimlik doğrulama sistemleri fiziksel ve davranışsal özellikleri kullanan bilgisayar destekli sistemlerdir. Fiziksel ve davranışsal özellikler kişilere özgü eşsiz özelliklerdir. Çok farklı fiziksel ve davranışsal özellikler olduğundan, hangi özelliğe göre biyometrik kimlik doğrulama yapılacağı uygulamaya göre seçilir. Ayrıca her sistemin avantaj ve dezavantajlarına göre bir değerlendirme yapılmalıdır.

Çok yaygın olarak kullanılan iki biyometrik yöntem, parmak izi okuma ve yüz tanımadır. Parmak izi okuma sistemleri genel olarak ucuz ve güvenilir sistemlerdir. Bu nedenle çok yaygın olarak kullanılmaktadır. İki kişinin parmak izlerinin aynı olma olasılığı çok düşüktür. Bazı sebeplerden dolayı insanların bir kısmının parmak izi kullanılamamaktadır. Yüz tanıma ise ucuz olmasına rağmen parmak izi kadar güvenilir değildir.

Biyometrik yöntemler, yüksek maliyet gerektiren bir donanıma ihtiyaç duymaları ve bazı fizyolojik özelliklerin günümüz teknolojisiyle kopyalanabilmesinin mümkün hale gelmesinden dolayı diğer yöntemlere göre daha az tercih edilmektedir. Bu yöntemler askeri alanlar, havaalanları ve hastaneler gibi giriş ve çıkışların kritik bir öneme sahip olduğu özel durumlarda tercih edilmektedir.

Damar yapısının biyometrik kimlik doğrulama yöntemi olarak nasıl kullanıldığını açıklayınız.

SIRA SİZDE 7

Özet

AMAÇ 1 *Simetrik şifreleme yöntemi ile anahtar dağıtımını ifade etmek*

Bir bilgisayar sisteminde kullanıcı sayısının artmasıyla birlikte kullanıcılar arasında güvenli bir iletişim kurmak için gerekli gizli anahtarların yönetimi içinden çıkılmaz bir hal alır. Günümüz şartlarında kullanıcıların çok farklı coğrafi konumlarda bulunmalarından dolayı gizli anahtarların fiziki yollar aracılığıyla ulaştırılması imkânsız hale gelmiştir. Merkezi olan ve olmayan anahtar dağıtımı ile kullanıcılara gizli anahtar ulaştırma yöntemleri mevcuttur. Her iki yöntemde de kullanıcılar sahip oldukları ana anahtarlar sayesinde gizli oturum anahtarlarını simetrik şifreleme algoritmaları kullanarak gizli bir şekilde karşı tarafa iletebilmektedirler.

AMAÇ 2 *Açık anahtar şifreleme yöntemi ile anahtar dağıtımını açıklamak*

Açık anahtar şifreleme yöntemleri ile kullanıcılar arasında oturum anahtarının paylaştırılması mümkündür. Kullanıcı ilk olarak gizli bir iletişim oluşturmak için gerekli oturum anahtarını üretir. Sonra iletişime geçmek istediği kullanıcının açık anahtarını kullanarak oturum anahtarını şifreler ve karşı tarafa iletir. Mesajı alan kullanıcı, kendi gizli anahtarını kullanarak mesajı çözer ve oturum anahtarını elde eder. Bundan sonra kullanıcılar arasındaki iletişim, oturum anahtarı kullanarak simetrik şifreleme algoritmaları ile devam eder.

AMAÇ 3 *Sertifikaları tanımlamak ve sertifika kullanımını açıklamak*

Kötü niyetli kişilerin aradaki adam ve yeniden gönderme saldırılarına karşı dijital sertifikalar kullanılır. Sertifika bir açık anahtarı, bir kişi, uygulama veya servis ile ilişkilendirmek için kullanılan bir dijital dokümandır. Sertifikalar ülkelerin sorumlu kamu ve güvenilir özel kurumları tarafından yönetilir. Kerberos parola-tabanlı bir ağ kimlik doğrulama sistemidir. Kullanıcıların elde ettikleri biletleri kullanarak her seferinde parola girmeleri gereksinimini ortadan kaldırmıştır. Parola yerine sertifika kullanarak da doğrulama yapabilir. En yaygın olarak dördüncü ve beşinci sürümleri kullanılmaktadır.

AMAÇ 4 *Tek kullanımlık parola ve biyometrik kimlik doğrulama yöntemlerini tanımlamak*

Kullanıcının ağ üzerinden bir servisten faydalanmak istemesi durumunda, kendisini sisteme tanıtması gerekmektedir. Kullanıcıya kimlik doğrulama sistemi tarafından doğrulama yapıldıktan sonra onun için belirlenmiş haklar ölçüsünde kullanım izni verilmelidir. Uzun yıllardır yaygın olarak kullanıcı adı ve parola yöntemi kullanılmaktadır. Bu yöntemde sisteme giriş yaparken kullanıcı adı ve geçerli parola girilmesi gerekmektedir. Kullanıcılar, parolalarını unutmamak için bir kâğıda yazmak, parolası içerisinde kendi adını veya doğum tarihini kullanmak gibi yöntemlerle kötü niyetli kişilerin işlerini kolaylaştırırlar. Kullanıcıların bu kullanım hatalarını ortadan kaldırmak için tek kullanımlık parola ve biyometrik yöntemler ile kimlik doğrulama yöntemleri geliştirilmiştir. Kullanıcının sahip olduğu bir donanım veya yazılım aracı ile elde ettiği tek kullanımlık parolayı belirlenen zaman aralığında sisteme girerek kimlik doğrulaması gerçekleştirilebilmektedir. Bu yöntemde kullanıcının bilgisayarı ile sunucunun bilgisayarı senkronize olmalıdır. Sunucuya gelen tek kullanımlık parolanın aynısı sunucu tarafından da üretilmelidir. Biyometrik yöntemler kullanıcıların fizyolojik ve davranışsal özelliklerini kullanarak doğrulama yapar. Biyometrik özelliklerin her insan için farklı olmasından dolayı kullanıcıları birbirinden ayırt etmek mümkündür.

Kendimizi Sınayalım

1. Aşağıda verilenlerden hangisi fizyolojik (pasif) biyometrik özelliklerden biri **değildir?**

a. Parmak izi
b. Damar yapısı
c. İris
d. El yazısı
e. Retina

2. Aşağıda verilenlerden hangisi davranışsal (aktif) biyometrik özelliklerden biri **değildir?**

a. Ses
b. El
c. Yüz
d. Tuş vuruşu
e. Dudak hareketi

3. Güçlü bir parola aşağıda verilen özelliklerden hangisine sahip olmalıdır?

a. Sadece küçük harfler kullanılmalıdır.
b. Kullanıcıya ait doğum tarihi gibi kişisel bilgiler içermelidir.
c. Belirli zaman aralıklarında yenilenmelidir.
d. Sözlükte geçen bir kelime içermelidir.
e. Önceden kullanılmış parolalara benzemelidir.

4. Aşağıdakilerden hangisi X.509 sertifikası içerisindeki bilgilerden biri **değildir?**

a. Seri numarası
b. Başlangıç süresi
c. Bitiş süresi
d. Açık anahtar
e. Gizli anahtar

5. Bir firmada 100 çalışan olması ve her çalışanın diğer çalışanlarla bir simetrik şifreleme algoritması kullanarak güvenli iletişim kurması durumunda sistemde toplam kaç adet farklı gizli anahtar üretilmesi gerekmektedir?

a. 100
b. 200
c. 1.000
d. 2.000
e. 4.950

6. Bir firmada 100 çalışan olması ve yeni bir çalışanın işe alınmasından sonra her çalışanın diğer çalışanlarla bir simetrik şifreleme algoritması kullanarak güvenli iletişim kurması durumunda sistemde toplam kaç adet yeni gizli anahtar üretilmesi gerekmektedir?

a. 100
b. 200
c. 1.000
d. 2.000
e. 4.950

7. Aşağıda verilenlerden hangisi PKI altyapısını **kullanmaz?**

a. SSL
b. S/MIME
c. Telnet
d. VPN
e. PGP

8. Can kendine bir parola seçecektir. Parola yedi karakterden oluşacaktır. Karakterler Türkçe alfabede yer alan 29 harf içinden seçilecektir. Bir harf birden fazla kullanılabilir. Büyük ve küçük harf kullanılabilir. Bu şartlara göre Can'ın seçebileceği kaç farklı parola vardır?

a. 29
b. 58
c. 29^2
d. 29^7
e. 58^7

9. Aşağıdakilerden hangisi açık anahtar altyapısının işlevlerinden biri **değildir?**

a. Sertifika yayımlamak
b. Parola oluşturmak
c. Sertifika iptal etmek
d. Anahtar yaşam döngüsünü yönetmek
e. Sertifikaların saklanması ve erişime açılması

10. Gizli anahtar oluşturmak isteyen iki kullanıcının arasına girerek her ikisi ile kendi arasında anahtar oluşturmak olarak tanımlanan saldırı aşağıdakilerden hangisidir?

a. Aradaki adam
b. Yeniden gönderme
c. Kaba kuvvet
d. Sözlük
e. Telekulak

Yaşamın İçinden

Parmak izi ile pasaporttan geçiş bugün başlıyor!

Dünyada birçok ülke tarafından kullanılan parmak izi ile 15 saniyede pasaport kontrolünün yapıldığı Biyometrik Otomatik Geçiş sistemi deneme amaçlı olarak Atatürk Havalimanı'nda bugün başlıyor.

Atatürk Havalimanı Dış Hatlar terminalinde ikisi gidiş katında, ikisi de geliş katında olmak üzere dört pasaport kontrol noktasında uygulama, deneme amaçlı olarak bugünden itibaren başlayacak. Bu sistemle sahte pasaport kullanımı ve zaman zaman oluşan uzun kuyrukların tamamen ortadan kalkacağı, pasaport polisi sayısının da asgariye ineceği belirtildi.

Parmak iziyle geçiş!

Yolcular özel hazırlanan bankolarda parmak izlerini taratacak. Sistem parmak izini kontrol ettikten sonra eşleşmenin sağlanmasıyla kapıyı açarak geçişi sağlayacak. Biyometrik bu kontrol sisteminde, insan işgücü kullanılmayacağı gibi işlemler çok hızlı ve güvenli olarak gerçekleşecek. Sistem başarılı olursa, gidiş ve geliş yönünde dörder biyometrik kabin daha eklenecek, önümüzdeki yılsonunda ise sayı gidişte 12, gelişte de 12'ye çıkacak.

İkinci adım yüz tanıma sistemi!

Sistemin başarılı olmasıyla birlikte ikinci aşama olan yüz tanımaya geçilecek. Yolcunun parmak izinin yanı sıra farklı kamera açılarından çekilecek görüntü ile yüz tanıma sistemde eşleştirilecek.

Kaynak: Faik KAPTAN – Murat ÇAKIR / İSTANBUL DHA 22 OCAK 2015. http://goo.gl/bmZ8q2

Kendimizi Sınayalım Yanıt Anahtarı

1. d	Yanıtınız yanlış ise "Biyometrik Yöntemler" konusunu yeniden gözden geçiriniz.
2. c	Yanıtınız yanlış ise "Biyometrik Yöntemler" konusunu yeniden gözden geçiriniz.
3. c	Yanıtınız yanlış ise "Kullanıcı Adı ve Parola" konusunu yeniden gözden geçiriniz.
4. e	Yanıtınız yanlış ise "Sertifikalar" konusunu yeniden gözden geçiriniz.
5. e	Yanıtınız yanlış ise "Anahtar Dağıtımı" konusunu yeniden gözden geçiriniz.
6. a	Yanıtınız yanlış ise "Anahtar Dağıtımı" konusunu yeniden gözden geçiriniz.
7. c	Yanıtınız yanlış ise "Açık Anahtar Altyapısı" konusunu yeniden gözden geçiriniz.
8. e	Yanıtınız yanlış ise "Kullanıcı Adı ve Parola" konusunu yeniden gözden geçiriniz.
9. b	Yanıtınız yanlış ise "Açık Anahtar Altyapısı" konusunu yeniden gözden geçiriniz.
10. a	Yanıtınız yanlış ise "Aradaki Adam Saldırısı" konusunu yeniden gözden geçiriniz.

Sıra Sizde Yanıt Anahtarı

Sıra Sizde 1

AES simetrik şifreleme algoritmasında anahtar boyu 128, 192 veya 256 bit olabilir. Sabit bir anahtar boyu yoktur. DES simetrik şifreleme algoritmasında anahtar boyu 64 bittir ama etkin olarak 56 biti kullanılır.

Sıra Sizde 2

Dijital imzayı sertifika otoritesi oluşturur. Dijital imza asimetrik şifreleme ile elde edilir. Sertifika otoritesi sertifikayı kendi gizli anahtarı ile şifreleyerek elde eder ve sertifikaya ekler.

Sıra Sizde 3

X.509 sertifikasını destekleyen protokol ve standartlar arasında TLS/SSL, S/MIME, IPSec, HTTPS, LDAP ve EAP sayılabilir.

Sıra Sizde 4

Verilen şartlara göre parolanın birinci karakteri için toplam 29 seçenek vardır. İkinci karakter için yine 29 seçenek vardır. Kısaca altı karakterin her biri için 29 seçenek vardır. Bu nedenle seçilebilecek toplam parola sayısı 29^6 olarak bulunur.

Sıra Sizde 5

Yeniden gönderme (replay) saldırıları veri iletişimi sırasında veri paketlerinin kötü niyetle tekrar edilmesi veya geciktirilmesi olarak tanımlanabilir. Ele geçirilen veri paketlerinin sunucuya tekrar geri gönderilmesi olarak da açıklanabilir.

Sıra Sizde 6

İmza, vücut kokusu ve DNA eşleşme bu özellikler arasında sayılabilir.

Sıra Sizde 7

Damar yapısı her insan için farklıdır. Damar yapısı, farklı kişiler için elde, kolda ve yüzde farklıdır ve farklı dağılım gösterir. Bu nedenle kimlik doğrulama için kullanılabilir.

Yararlanılan ve Başvurulabilecek Kaynaklar

Katz, J., Lindell Y. (2014). ***Introduction to Modern Cryptography***, CRC Press.

Paar, C., Pelzl, J. (2010). ***Understanding Cryptography: A textbook for students and practitioners***, Springer Science & Business Media.

Stallings, W. (2011). ***Network Security Essentials: Applications and Standards,*** Pearson Education.

AĞ YÖNETİMİ VE BİLGİ GÜVENLİĞİ

6

Amaçlarımız

Bu üniteyi tamamladıktan sonra;

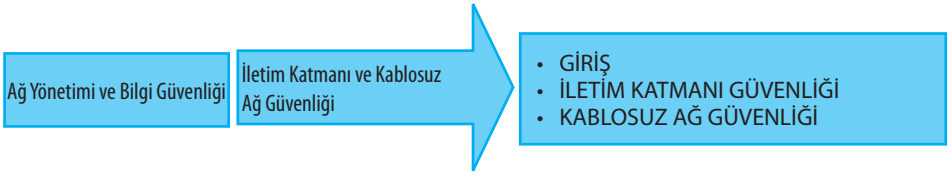
- İnternet ortamındaki güvenlik sorunlarını tanımlayabilecek,
- Güvenli soket katmanı ve iletim katmanı güvenliği kavramlarını açıklayabilecek,
- HTTPS ve SSH kullanım alanlarını tanımlayabilecek,
- IEEE 802.11 ve IEEE 802.11i kablosuz ağ standartlarını tanımlayabilecek,
- Kablosuz uygulama protokolü ve kablosuz iletim katmanı güvenliği kavramlarını açıklayabilecek

bilgi ve becerilere sahip olacaksınız.

Anahtar Kavramlar

- İnternet Güvenliği
- Güvenli Soket Katmanı
- İletim Katmanı Güvenliği
- HTTPS
- SSH
- Kablosuz Ağ Standardı
- Kablosuz Ağ Güvenliği

İçindekiler



İletim Katmanı ve Kablosuz Ağ Güvenliği

GİRİŞ

Teknolojik gelişmelerle beraber İnternet kullanımı yaygınlaşmıştır. İnternet erişimine sahip bireylerin ve kurumların sayısı her geçen gün artmaktadır. İnternet kullanımı ile kişiler ve şirketler ticari faaliyetlerini Web sayfaları üzerinden gerçekleştirmektedirler.

İnternet ve Web teknolojileri kullanıcılara birçok avantaj sunmaktadır. Kaynakların ortak kullanımı bunlardan en önemlisidir. Bu teknolojilerle kısıtlı kaynaklar en verimli şekilde kullanılabilir hale gelmektedir. Bir ağ ile birbirine bağlanan kaynakların birçok kullanıcıya açılması ile verimli kullanılmaları sağlanabilir. Bu teknolojilerin diğer bir avantajı ise kaynaklara uzaktan erişime imkân vermesidir. Ağa bağlı kullanıcılar farklı konumlardan kaynaklara erişim sağlayabilirler.

Yukarıda bahsedilen avantajlarının yanında Web sayfaları farklı şekillerde gerçekleşebilecek tehditlere açıktırlar. Kişiler veya kurumların bu tehditlerin ne kadar önemli olduğu konusunda farkındalıkları arttıkça, güvenli Web servislerine olan ihtiyaç artacaktır. Bu ünitede Web üzerinden gerçekleşecek ticari işlemleri de ilgilendiren ve standart haline gelmiş üç güvenlik protokolü açıklanacaktır. Bu kavramlar sırasıyla SSL/TLS, HTTPS ve SSH olarak bilinir.

Kablosuz ağlar modern iletişim araçları için artan bir öneme sahiptir. Geçmişte sadece dizüstü bilgisayarlar için gerek duyulan kablosuz ağlar artık her gün kullanılan cep telefonu, televizyon, otomobiller ve akıllı ev cihazları için vazgeçilmez olmuştur. İletişim araçlarındaki gelişmeye ve kullanıma paralel olarak kablosuz ağ güvenliği artan öneme sahiptir. Kablosuz ağlar veriyi, belirli frekans aralıklarında hava aracılığıyla radyo dalgaları olarak iletir. Dolayısıyla iletilen verinin, kablosuz ağ ile aynı frekansta çalışan bir alıcıya sahip kötü niyetli kişi tarafından dinlenebilmesi mümkün hale gelmektedir. Kötü niyetli kişi veri trafiğini dinlediği gibi aynı zamanda karıştırıcılar (jammer) kullanarak yetkili iki kişi arasında gerçekleştirilecek iletişime de engel olabilmektedirler. Ünitenin ikinci kısmında kablosuz ağ güvenliği için gerekli şifreleme algoritmaları, kullanıcı kimlik doğrulama ve mesaj bütünlüğü üzerinde durulacaktır ve kablosuz ağ standardı IEEE 802.11 incelenecektir.

İLETİM KATMANI GÜVENLİĞİ

Kablolu bilgisayar ağları kapsadığı coğrafik alana ve boyuta göre Yerel Alan Ağı (Local Area Network – LAN) ve Geniş Alan Ağı (Wide Area Network – WAN) olmak üzere ikiye ayrılır. LAN'lar ev, okul, kurum binası gibi daha sınırlı alanlarda bulunan bilgisayar, telefon ve yazıcı gibi ağ aygıtlarını birbirine bağlar. WAN'lar ise çok farklı coğrafik bölge-

lerdeki donanımları birbirine bağlar. LAN'lar daha küçük alanlarda hizmet verdikleri için WAN'lara göre daha hızlıdır. LAN oluşturmak için gerekli maliyet WAN'a göre daha azdır. Bilgisayar ağları topolojilerine göre;

- Yıldız (Star)
- Halka (Ring)
- Ortak Yol (BUS)
- Örgü (Mesh)

olmak üzere 4 gruba ayrılır.

Bir ağda cihazların nasıl iletişim kuracakları Açık Sistemler Arabağlaşımı (Open Systems Interconnection – OSI) modeli tarafından tanımlanmıştır. Bu model 7 adet katmandan oluşur;

- Fiziksel: Veri bitlerinin alıcıya nasıl iletileceğinden sorumludur.
- Veri Bağlantısı: Uç düğümler arasında verinin hatasız bir şekilde transferini sağlar.
- Ağ: Verinin iletileceği ağ üzerinde en uygun yolu belirler.
- İletim: Verinin hangi protokoller kullanılarak iletileceğini belirler.
- Oturum: Uç düğümler arasında bağlantının oluşturulması, kullanılması ve sonlandırılmasından sorumludur.
- Sunum: Verinin biçimsel düzenlemesinin yapıldığı katmandır.
- Uygulama: Ağ bağlantısını kullanacak programdır.

Bu bölümde öncelikle Web uygulamalarının sebep olabileceği sorunlar açıklanacaktır. Daha sonra güvenli soket katmanı üzerinde durulacak ve mimari yapısı tanımlanacaktır. Son olarak bu katman içinde yer alan protokoller ve iletim katmanı güvenliği kavramları açıklanacaktır.

Web Güvenliği Kavramı

Web, İnternet veya intranetler üzerinde çalışan bir istemci/sunucu uygulamasıdır. Web kavramı ile beraber daha önce bilgisayar ve ağ güvenliği konularında üzerinde durulmayan yeni güvenlik tehditleri ortaya çıkmıştır:

- Teknolojide yaşanan gelişmelerin bir sonucu olarak Web bir kurumun veya şirketin ticari faaliyetleri açısından daha çok öneme sahip olmaktadır. Kurumların sunmuş oldukları Web servislerinde ortaya çıkabilecek sorunlar, hem maddi hem de itibar kayıplarına sebep olabilmektedir.
- Web sunucular kurumların merkezi bilgisayar sistemlerine dışarıdan erişmek için bir giriş noktasıdır. Dolaysıyla Web sunucuların sebep olabileceği güvenlik problemleri kurumun tüm bilgisayar sistemi için tehdit oluşturmaktadır.
- Web kullanıcıların karşılıklı iletişim kurabildikleri bir ortamdır. Sunucular üzerinden gerçekleştirilen Web yayınları, geleneksel yöntemler ile karşılaştırıldığında saldırılara daha açıktır.
- Web sunucularının donanımsal açıdan yapılandırılması ve yönetilmesi güvenlik sorunlarına yol açmaz. Buna rağmen arka planda çalışan yazılım son derece karmaşık olabilmekte ve güvenlik açıkları içerebilmektedir.
- Web güvenliği hakkında yeterli bilgi sahibi olmayan kullanıcılar risklerin farkında olmadıkları için oluşacak tehditlere karşı gerekli korunma araçlarına sahip değildirler.

Web güvenliği tehditleri dört farklı grupta incelenebilir:

I. Gizliliğe karşı tehditler arasında ağın gizli bir şekilde dinlenmesi, sunucu veya istemci verisinin çalınması gösterilebilir. Bu tehditlerin getireceği sonuçlar bilgi kaybı ve gizlilik ihlalidir. Şifreleme algoritmaları ve Web vekil sunucular bu tehditlere karşı geliştirilen çözümlerdir.

II. Bütünlüğe yönelik tehditler arasında kullanıcı verisinin, iletim halindeki mesajın ve belleğin kötü amaç için değiştirilmesi yer almaktadır. Bu tehditler gerçekleşirse bilgi kaybı, sistemin ele geçirilmesi ve diğer saldırılara karşı savunmasız kalma gibi durumlar ortaya çıkabilir. Bu saldırılara karşı korunmak için kriptografik özet fonksiyonları kullanılır.

III. Hizmet engellemeye yönelik tehditler arasında kullanıcı iş parçacıklarının sonlandırılması, disk veya belleğin kapasitelerinin üzerinde kullanılmaya çalışılması ve gerçek olmayan istekler ile sistemi meşgul etme sayılabilir. Bu tehditler yetkili kullanıcıların gerektiğinde servislere erişmelerine engel olurlar.

IV. Kimlik doğrulama işlemine yönelik tehditler arasında meşru kullanıcıların kimliğine bürünme ve veri sahteciliği gösterilebilir. Bu tehditlerin amacı, kötü niyetli kullanıcıların yetkileri dışında başka kullanıcılara ait bilgilere ulaşmalarıdır. Güçlü parola yönetimi ve biyometrik yöntemler gibi daha güvenilir kimlik doğrulama yöntemleri bu tehditlerin gerçekleşmesini önlemede kullanılabilir.

Güvenlik tehditlerini pasif ve aktif saldırılar olmak üzere iki gruba ayırmak mümkündür. Web tarayıcısı ve sunucusu arasındaki veri iletimini gizli dinlemek bir pasif saldırı örneğidir. Aktif saldırılara örnek olarak başka bir kullanıcının kimliğine bürünme ile sunucu ve istemci arasındaki mesajları değiştirme verilebilir.

Web güvenliğini sağlamak için çeşitli çözümler vardır. Bu çözümlerin sağladığı servisler benzer olmakla birlikte, kullandıkları yöntemler farklıdır. Temel farklılık, uygulama alanları ve protokollerin TCP/IP kümesindeki yerlerinden kaynaklanır.

Güvenli Soket Katmanı (Secure Socket Layer–SSL)

SSL Web-tabanlı uygulamalar için bir güvenlik sağlama tekniğidir. Güvenlik denince temel olarak anlaşılan gizlilik, mesaj bütünlüğü ve kimlik doğrulamasıdır. SSL kriptografik yöntemler, dijital imzalar, özet fonksiyonlar ve sertifikalar kullanarak güvenliği sağlar.

Gizlilik, mesaj bütünlüğü ve kimlik doğrulama terimlerini açıklayınız.

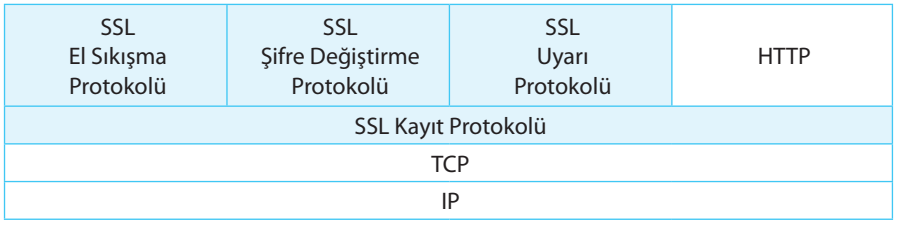
SIRA SİZDE 1

SSL Mimarisi

SSL, TCP'nin uçtan uca güvenli bir hizmet sunmasını sağlamak amacıyla tasarlanmıştır. SSL iki katmanda yer alan protokollerden oluşmaktadır. Şekil 6.1'de SSL protokolünün TCP/IP üzerine nasıl yerleştiği gösterilmiştir.

Şekil 6.1

SSL Protokol Yığını



SSL kayıt protokolü çeşitli üst katman protokollerine temel güvenlik hizmetlerini sağlar. Özellikle istemci/sunucu etkileşimi için hizmet transferi sağlayan HTTP protokolü SSL üstünde çalışabilir. SSL'in bir parçası olarak tanımlanan üç üst katman protokolü El Sıkışma, Şifre Değiştirme ve Uyarı protokolleridir. SSL oturumu ve SSL bağlantısı iki önemli SSL kavramıdır.

SSL'de yer alan üst katman protokolleri el sıkışma, şifre değiştirme ve uyarı protokolleridir.

- **SSL bağlantısı:** SSL bağlantısı sunucu ve istemci arasında gerekli servisi sağlayan bir iletim aracıdır. SSL ile oluşturulan bağlantılar belirli bir süre sonra sonlandırılır ve her bir bağlantı tek bir oturum ile ilişkilidir.
- **SSL oturumu:** İstemci ve sunucu arasında güvenli bir iletim kanalı kurmak için gerekli parametrelere karar verilir. Oturumlar el sıkışma protokolü tarafından oluşturulur ve birden fazla bağlantı arasında paylaşılabilir bir dizi kriptografik güvenlik parametreleri tanımlarlar. Oturumlar her bağlantı için yeni güvenlik parametreleri müzakerelerini önlemek için kullanılır.

Bir oturum durumunu tanımlamak için gerekli bazı parametreler aşağıdaki verilmiştir:

- Oturum Tanımlayıcısı: Sunucu tarafından seçilen aktif veya devam ettirilebilir oturum durumlarını tanımlayan rastgele oluşturulmuş bir bayt dizisidir.
- Veri Sıkıştırma Metodu: Şifrelemeden önce veri sıkıştırmak için kullanılan algoritmadır.
- Şifreleme yönteminin belirlenmesi: Mesaj Doğrulama Kodu (Message Authentication Code–MAC) hesaplamada kullanılan toplu veri şifreleme algoritmasını ve karma algoritmayı tanımlar.
- Ana Sır: İstemci ile sunucu arasında paylaşılan 48 baytlık sırdır.
- Yenilenebilir: Bir oturumun yeni bağlantılar başlatmak için kullanılıp kullanılamayacağını belirlemek için kullanılır.

Bir bağlantı durumu aşağıdaki parametreler ile tanımlanır:

- Rastgele sayı: Her bağlantı için sunucu ve istemci tarafından rastgele oluşturulmuş bayt dizileridir.
- Sunucuya ait MAC gizli anahtarı: Sunucu tarafından istemciye iletilecek veri için MAC operasyonlarında kullanılan gizli anahtardır.
- İstemciye ait MAC gizli anahtarı: İstemci tarafından sunucuya iletilecek veri için MAC operasyonlarında kullanılan gizli anahtardır.
- Gizli Anahtar: Sunucu ve istemci arasında iletilecek verinin gizlenmesi için kullanılacak simetrik şifreleme algoritması anahtarıdır.
- Başlatma Vektörleri (Initialization Vectors – IV): Bu alan ilk olarak SSL el sıkışma protokolü tarafından başlatılır.
- Sıra Numaraları: Her iki taraf, her bağlantıda alınan ve iletilen mesajlar için farklı sıra numaraları tutar.

SSL Kayıt Protokolü

SSL kayıt protokolünün sunduğu iki servis gizlilik ve mesaj bütünlüğü olarak adlandırılır.

SSL kayıt protokolü, bağlantılar için Gizlilik ve Mesaj Bütünlüğü olmak üzere iki farklı güvenlik servisi sağlar. El sıkışma protokolü, Gizlilik servisinin sağlanması amacıyla, SSL yüklerinin şifrelenmesi için gerekli gizli anahtarı tanımlar. Benzer şekilde Mesaj Bütünlüğü servisinin sağlanması amacıyla el sıkışma protokolü, mesaj doğrulama kodu (MAC) oluşturmak için gerekli gizli anahtarı tanımlar.

Kayıt protokolü iletilecek veriyi belirli uzunlukta bloklar halinde parçalar ve sıkıştırma fonksiyonuna gönderir. Daha sonra elde edilen çıktıya MAC uygulanır. Son olarak elde edilen veri şifrelenir ve başlık eklenerek TCP bölümü olarak iletilir. İletişim kanalının diğer tarafında alıcı gelen şifrelenmiş veriyi çözer. Mesaj bütünlüğü kontrol edilir. Eğer hata yoksa, bölünmüş parçalar birleştirilerek üst seviye katmanlara gönderilir.

Protokolde gerçekleşen işlemlerden ilk adım uygulama katmanından gelen mesajı parçalara ayırmadır. Oluşturulacak her bir bloğun boyutu 2^{14} baytı geçemez. Daha sonra isteğe bağlı olarak sıkıştırma işlemi uygulanır. Normalde sıkıştırma işleminin amacı verinin boyutunu azaltmaktır. Ama bazı durumlarda mesajın boyutunun küçük olması sebebiyle sıkıştırma işleminin sonunda gerçek boyuttan daha büyük boyutlu mesajlar

elde edilebilir. Sıkıştırma işlemi sonunda elde edilecek verinin boyutu artıyor ise en fazla 1024 bayt olmasına izin verilir. Sıkıştırma algoritmaları beklendiği gibi veri kaybına sebep olmamalıdır.

Bir sonraki adım sıkıştırılmış veri üzerinden gizli anahtar kullanılarak MAC hesaplanmasıdır. Hem MAC hem de sıkıştırılmış mesaj, simetrik şifreleme algoritmalarından biri kullanılarak şifrelenir. Şifreleme içerik uzunluğunu 1024 bayttan fazla arttıramaz. Toplam uzunluk 2^{14} + 2048 baytı geçemez.

Dizi şifrelemede sıkıştırılmış mesaj ile beraber MAC şifrelenir. MAC hesap edildikten sonra şifreleme işlemi sıkıştırılmış veri ve MAC üzerinde gerçekleştirilir. Blok şifreleme işleminde şifreleme işlemine başlamadan önce MAC değerinden sonra dolgu eklenir. Dolgu eklemenin amacı şifrelenecek verinin toplam boyutunu şifreleme blok uzunluğunun bir sonraki katına tamamlamaktır. Dolgu miktarı bir bayt ile gösterilir ve bu bayttan sonra dolgu baytları yer alır.

SSL kayıt protokolü işleminin son adımı aşağıdaki alanları içeren bir başlık hazırlamaktır: İçerik Tipi (8 bit), Başlıca Sürüm (8 bit), İkincil Sürüm (8 bit) ve Sıkıştırılmış Uzunluk (16 bit).

Şifre Değiştirme Protokolü

Şifre değiştirme protokolü SSL kayıt protokolünü kullanan üç protokolden en basit olanıdır. Bu protokol değeri 1 olan ve bir bayttan oluşan bir mesaj içerir. Bu mesajın tek amacı bekleyen durumun güncel durumun içine kopyalanmasını sağlamaktır. Bunun sonucunda bağlantıda kullanılacak şifre paketi güncellenir.

Uyarı Protokolü

Uyarı protokolü SSL ile ilgili uyarıları iletmek için kullanılır. SSL kullanan diğer uygulamalarda olduğu gibi uyarı mesajları sıkıştırılır ve şifrelenir. Bu protokoldeki her mesaj 2 bayttan oluşur. İlk bayt mesajın şiddetini iletmek için iki farklı değerden birini alabilir. Bu değerler uyarı (1) ve ölümcül (2) değerleridir. Eğer değer ölümcül ise SSL acilen bağlantıyı sonlandırır. Aynı oturumdaki diğer bağlantılar devam edebilir, fakat aynı oturumda yeni bir bağlantı oluşturulmaz. İkinci bayt belirli uyarıları belirten bir kod içerir.

Uyarı protokolünde ilk baytın aldığı 1 ve 2 değerlerinin önemini açıklayınız.

SIRA SİZDE 2

El Sıkışma Protokolü

SSL'nin en karmaşık kısmı **el sıkışma protokolü**dür. Bu protokol, istemci ve sunucunun birbirlerinin kimliklerinin doğrulamasını sağlar. Ayrıca veri transferinde gönderilecek mesajı gizlemek için kullanılacak şifreleme ve MAC algoritması ile şifreleme anahtarlarına karar verilmesini sağlar. El sıkışma protokolü herhangi bir uygulama verisi iletilmeden önce kullanılır. El sıkışma protokolü istemci ve sunucu tarafından karşılıklı iletilen bir dizi mesajı içerir. Tüm mesajlar aşağıdaki alanlara sahiptir:

- Tür: 10 farklı mesaj türünden hangisi olduğunu belirtir.
- Uzunluk: Bayt cinsinden mesajın uzunluğunu belirtir.
- İçerik: Mesajla ilişkili parametrelerden oluşur.

İstemci ve sunucu arasındaki değişim dört evreli olarak görülebilir.

Birinci evre *güvenlik kabiliyetlerinin kurulması* evresidir. Bu evre mantıksal bağlantı başlatmak ve onunla ilgili güvenlik yeteneklerini kurmak için kullanılır. Alışveriş *client_hello* mesajı gönderen istemci tarafından başlatılır. Bu mesaj aşağıdaki parametrelere sahiptir:

El sıkışma protokolünde istemci ve sunucu arasındaki değişim; güvenlik kabiliyetlerinin kurulması, sunucu kimlik doğrulaması ve anahtar değişimi, istemci kimlik doğrulaması ve anahtar değişimi ve bitiş evreleri olmak üzere dört evreden oluşur.

- Sürüm: İstemci tarafından kullanılabilecek en yüksek SSL sürümünü belirtir.
- Rastgele: İstemci tarafından üretilen 32-bit zaman damgası ve 28 bayt içeren rastgele yapıdır. 28 bayt güvenli rastgele sayı üreticisi tarafından üretilir. Bu değerler bağlantıya özeldir ve anahtar değişiminde tekrar saldırılarını (replay) önlemek için kullanılır.
- Oturum Kimliği: Değişken uzunlukta oturum tanımlayıcısını gösterir. Sıfırdan farklı değer, istemcinin var olan bağlantı parametrelerini güncellemek veya bu oturumda yeni bir bağlantı oluşturmak istediğini belirtir. Sıfır değeri, istemcinin yeni bir oturumda yeni bir bağlantı kurmak istediğini gösterir.
- Şifre Kümesi: Azalan tercih sırasına göre, istemci tarafından desteklenen şifreleme algoritmalarını içeren bir listedir. Listenin her bir elemanı hem anahtar değişim algoritmasını hem de şifreleme algoritmasını tanımlar.
- Sıkıştırma Metodu: İstemci tarafından desteklenen sıkıştırma metotlarının listesini gösterir.

İstemci *client_hello* mesajını gönderdikten sonra aynı parametreleri içeren *server_hello* mesajını bekler. *server_hello* mesajı için şu kurallar geçerlidir: Sürüm alanı istemci tarafından önerilen sürümlerin en düşüğünü ve sunucunun desteklediği sürümlerin en yükseğini içerir. Sunucu tarafından üretilen rastgele alan istemcinin ürettiği rastgele alandan bağımsızdır. Eğer istemcinin oturum kimliği alanı sıfırdan farklı ise aynı değer sunucu tarafından da kullanılır. Aksi takdirde sunucunun oturum kimliği alanı, yeni oturum için yeni bir değer içerir. Şifre kümesi alanı sunucunun istemcinin önerdiği şifreleme algoritmalarından seçtiği tek bir şifre paketini gösterir. Sıkıştırma metodu alanı, istemcinin önerdiği sıkıştırma metotlarından sunucunun seçtiği metodu içerir.

İkinci evre *sunucu kimlik doğrulaması ve anahtar değişimi* evresi olarak adlandırılır. Kimlik doğrulaması gerekiyorsa, sunucu sertifikasını göndererek bu aşamaya başlar. Mesaj X.509 sertifikaları içerir. Anonim Diffie-Hellman hariç, anahtar değişim metotlarının hepsinde sertifika mesajı gereklidir. Sabit Diffie-Hellman kullanıldığında sertifika mesajı sunucunun anahtar değişim mesajı gibi hareket eder.

Üçüncü evre *istemci kimlik doğrulaması ve anahtar değişimi* evresidir. *server_done* mesajı alındıktan sonra, istemci sunucunun geçerli bir sertifika sağladığını doğrulamalı ve *server_hello* parametrelerinin kabul edilebilir olduğunu kontrol etmelidir. Doğrulama ve kontrol işlemleri istenildiği şekilde sonuçlanırsa, istemci sunucuya bir veya daha fazla mesaj gönderebilir.

Son evre ise *bitiş* evresi olarak adlandırılır. Bu evre güvenli bir bağlantı kurulmasını tamamlar.

İletim Katmanı Güvenliği (Transport Layer Security–TLS)

TLS, SSL'nin İnternet standart sürümünü oluşturma amacıyla gerçekleştirilen bir standardizasyon girişimidir. TLS, önerilen İnternet standardı olarak RFC 5246'da tanımlanmıştır. Öncelikli hedefi iletişimde bulunan iki uygulama arasında gizliliği ve veri bütünlüğünü sağlamaktır. TLS temel olarak iki protokolden oluşmaktadır. Bu protokoller *TLS kayıt protokolü* ve *TLS el sıkışma protokolü* olarak adlandırılmıştır.

TLS kayıt protokolü bağlantı güvenliği sağlar ve iki temel özelliğe sahiptir. Birinci özellik bağlantı özel olmasıdır. Veri şifreleme için simetrik kriptografi kullanılır. Simetrik şifreleme anahtarları her bağlantı için yeniden oluşturulur ve diğer bir protokol tarafından karar verilmiş bir anahtara bağlıdır. Kayıt protokolü şifreleme olmadan da kullanılabilir. İkinci özellik ise bağlantı güvenilir olmasıdır. Mesaj taşıma anahtarlı MAC kullanarak mesaj bütünlük denetimi sağlar. Güvenli özet fonksiyonları, MAC hesaplamaları için kullanılır. Kayıt protokolü MAC olmadan kullanılabilir. Ama bu durum sadece diğer protokoller, kayıt protokolünü güvenlik parametrelerini karar vermek amacıyla kullanıyorsa gerçekleşir. TLS kayıt protokolü ayrıca çeşitli üst düzey protokolleri kapsülleme için kullanılır.

TLS el sıkışma protokolü istemci ve sunucunun birbirlerinin kimlik doğrulaması yapmasına olanak verir. Ayrıca uygulama protokolü veri almadan veya göndermeden önce şifreleme algoritmalarının ve kriptografik anahtarların müzakere edilmesini sağlar. El sıkışma protokolü üç temel özelliği olan bağlantı güvenliği sağlar. Birincisi eşdüzeylinin kimliği doğrulanabilir. Kimlik doğrulama isteğe bağlı olabilir ama eşdüzeylilerden en az biri için genellikle gereklidir. İkincisi ise paylaşılan sırrın müzakeresi güvenlidir. Müzakere edilen sır, gizlice elde etmek isteyenler için ulaşılmazdır. Üçüncüsü ise müzakere güvenilir olmasıdır. Hiçbir saldırgan iletişimin taraflarınca fark edilmeden müzakere iletişimini değiştiremez.

TLS'nin bir avantajı uygulama protokolünün bağımsız olmasıdır. Yüksek seviyeli protokoller, TLS protokolünün üzerinde şeffaf bir şekilde yer alabilirler. TLS protokolünün temel amaçları aşağıda verilmiştir:

- Kriptografik güvenlik: TLS iki taraf arasında güvenli bir bağlantı kurmak için kullanılır.
- Birlikte çalışabilirlik: Bağımsız programcılar birbirlerinin kod bilgilerini bilmeden kriptografik parametreleri değiştirmeyi sağlayan TLS kullanan uygulamalar geliştirmelidir.
- Geliştirilebilirlik: TLS gerektiğinde yeni açık anahtarlar ve şifreleme yöntemlerinin dâhil edilebildiği bir çerçeve sağlamayı amaçlamaktadır. Bu aynı zamanda iki alt amacın gerçekleşmesini de sağlayacaktır. Bu amaçlardan birincisi, yeni protokol oluşturma ihtiyacının önlenmesidir. İkinci alt amaç ise tümüyle yeni bir güvenlik kütüphanesi oluşturma ihtiyacından kaçınılmasıdır.
- Bağıl verim: Özellikle açık anahtar işlemleri olmak üzere kriptografik işlemler yoğun şekilde CPU kullanırlar. Bu nedenle TLS protokolü sıfırdan kurulacak bağlantı sayısını azaltmak için isteğe bağlı oturumları önbelleğe alan bir düzen geliştirmiştir. Ek olarak ağ aktivitesinin azaltılması için çalışılmıştır.

Güvenli Hipermetin İletim Protokolü (Secure Hypertext Transfer Protocol–HTTPS)

HTTP protokolü kullanılarak yapılan veri iletimi güvenli değildir. Kredi kartı bilgisi ve kullanıcı şifreleri gibi hassas bilgilerin açık olarak paylaşılması güvenlik zafiyeti oluşturur. Ortaya çıkan bu güvenlik zafiyetini önlemek için **HTTPS** önerilmiştir. HTTPS, Web tarayıcısı ile sunucusu arasında güvenli iletişim sağlamak amacıyla HTTP ve **SSL** protokollerinin beraber kullanılması ile oluşturulmuştur. Tüm modern Web tarayıcılar HTTPS yeteneğine sahiptirler. Bir Web tarayıcı kullanıcısının göreceği temel fark URL adresinin **http://** yerine **https://** ile başlamasıdır. Normal HTTP bağlantısı 80 numaralı bağlantı noktasını kullanır. Eğer HTTPS kullanılacaksa, bağlantı noktası numarası 443 olur.

HTTPS, SSL ve **HTTP** protokollerini kullanarak Web tarayıcı ve Web sunucu arasında güvenli bir iletişimin alt yapısını oluşturur.
HTTPS kullanıldığında iletişimin aşağıda verilen bileşenleri şifrelenir:
- İstenen dokümanın URL adresi,
- Doküman içeriği,
- Tarayıcı formların içeriği,
- Tarayıcıdan sunucuya, sunucudan tarayıcıya gönderilen çerezler,
- HTTP başlığının içeriği

Bağlantı Başlatma

HTTPS için HTTP istemcisi gibi davranan üstlenici aynı zamanda TLS istemcisi gibi davranır. İstemci uygun bir bağlantı noktasından sunucuya bir bağlantı başlatır ve TLS el sıkışma başlatmak için *TLS ClientHello* gönderir. *TLS ClientHello* bittiği zaman, istemci ilk HTTP isteğini başlatabilir. Tüm HTTP verisi TLS uygulama verisi olarak gönderilir. HTTPS'de üç seviye bağlantı vardır. HTTP düzeyinde, HTTP istemcisi bir sonraki katmana bağlantı isteği göndererek, HTTP sunucusundan bağlantı istemiş olur. Sonraki en düşük katman TCP'dir. Ama aynı zamanda TLS/SSL de olabilir. TLS düzeyinde, TLS sunucu ve TLS istemci arasında bir oturum kurulur. Bu oturum bir veya birden fazla bağlantıyı destekleyebilir. TLS'nin bağlantı kurma isteği sunucu tarafındaki TCP öğesiyle istemci tarafındaki TCP öğesi arasında bir TCP bağlantısı kurulmasıyla başlar.

Bağlantı Sonlandırma

Bir HTTP istemci veya sunucu HTTP kaydına *Connection: close* satırını dâhil ederek bir bağlantının kapandığını gösterebilir. Bu satır ilgili kayıt teslim edildikten sonra bağlantının kapanacağını gösterir. HTTPS bağlantısını kapatma, TLS bağlantısının kapatılmasını, bu durumda ilgili TCP bağlantısının sonlandırılmasını gerektirir. TLS düzeyinde, bir bağlantıyı her iki tarafta uygun şekilde kapatmak için *close_notify* uyarısının TLS uyarı protokolü tarafından gönderilmesi gerekir. TLS uygulamaları bir bağlantıyı kapatmadan önce kapatma uyarıları değiştirmeyi başlatmalıdır. HTTP istemcileri TCP bağlantısının *close_notify* ve *Connection: close* uyarıları olmaksızın sonlandırılması durumu ile başa çıkmak zorunda kalabilirler. Sunucudaki programlama hatası veya iletişim hatası TCP bağlantısının aniden sonlanmasına neden olabilir. Ayrıca beklenmeyen TCP sonlanması bir çeşit saldırının göstergesi de olabilir. Bu durum gerçekleştiğinde HTTPS istemcisinin güvenlik uyarısı oluşturması gerekir.

Güvenli Kabuk (Secure Shell–SSH)

SSH, şifreleme kullanarak güvenli olmayan bir ağ üzerinde uzaktan bağlanma ve diğer ağ hizmetlerini güvenli şekilde gerçekleştirmeyi sağlayan bir protokoldür.

Telnet ve FTP sırasıyla uzaktaki bir bilgisayarda oturum açmak ve dosya aktarmak amacıyla kullanılan uygulama katmanı protokolleridir. Bu protokoller herhangi bir kriptografik koruma olmadan, düz metin şeklinde veri iletimini gerçekleştirirlerdi. Bu nedenle IP adresi kandırması, şifre koklama ve gizli dinleme gibi saldırılara açık durumdaydılar. **SSH** uzaktan oturum açma işlemlerinde saldırılardan korunmak için Helsinki Teknoloji Üniversitesi öğrencileri tarafından 1995 yılında tasarlanmıştır. SSH1 ve SSH2 olmak üzere iki sürümü vardır. SSH2 daha güvenlidir. SSH kimlik doğrulama ve şifreleme algoritmaları kullanarak iki bilgisayar arasında güvenli bir bağlantı oluşturur. Aynı zamanda veri sıkıştırmayı destekler. Güvenli dosya transferi (SFTP) ve dosya kopyalama (SCP) protokolleri SSH üzerine inşa edilmiştir.

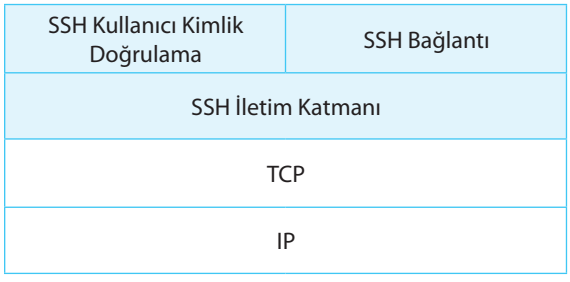
SIRA SİZDE 3

Telnet ve FTP protokollerine karşı yapılabilecek saldırılara örnekler veriniz.

SSH istemci-sunucu mimarisine sahip bir ağ protokolüdür. *SSH iletim katmanı protokolü*, *SSH kullanıcı kimlik doğrulama protokolü* ve *SSH bağlantı protokolü* olmak üzere üç protokole ayrılır. Şekil 6.2'de SSH protokolünün TCP/IP üzerine nasıl yerleştiği gösterilmiştir.

Şekil 6.2

SSH Protokol Yığını



SSH iletim katmanı protokolü sunucu kimlik doğrulama, veri gizliliği ve veri bütünlüğü hizmetlerini sağlar. Ayrıca ileri gizlilik özelliği vardır. Bu, bir anahtarın bir oturum sırasında tehlikeye atılması durumunda, önceki oturumların güvenliğinin etkilenmemesi demektir. Bu katman isteğe bağlı olarak sıkıştırma sağlar. SSH kullanıcı kimlik doğrulama protokolü istemcinin sunucuya kimlik doğrulaması yapabilmesi için gerekli araçları sağlar.

SSH bağlantı protokolü birden çok mantıksal iletişim kanalını bir SSH bağlantısı üzerinden çoklar. Bağlantı protokolü iletim katmanı protokolünün üzerinde çalışır ve güvenli kimlik doğrulama bağlantısının kullanımda olduğunu varsayar. Güvenli kimlik doğrulama bağlantısı tünel olarak isimlendirilir ve bağlantı protokolü tarafından belirli sayıda mantıksal kanalı çoklamak için kullanılır.

KABLOSUZ AĞ GÜVENLİĞİ

Kablosuz ağlar kablo yerine radyo dalgaları aracılığıyla bir tablet veya diz üstü bilgisayarı ve cep telefonu, kulaklık gibi mobil cihazları bir ağa veya birbirlerine bağlamak için kullanılır. Kablosuz ağ cihazları tasarsız (ad-hoc) ve tasarlı (infrastructure) olmak üzere iki farklı mod ile bağlanırlar. Tasarsız mod için herhangi bir erişim noktası veya yönlendirici olmadan bir cihaz ile başka bir cihaz arasında bir bağlantı oluşturulur. İnternet bağlantısı olan cihaz üzerinden diğer cihazlar için bağlantı oluşturulur. Bu yüzden cihazlar arasında veri herhangi bir başka cihaza gerek kalmadan karşı cihaza aktarılır. Çok güvenilir olmamakla birlikte maliyetinin düşük olmasından dolayı bir ev içerisindeki cihazlar için tercih edilebilir. Tasarlı modda ise cihazlar bir erişim noktası (access point) üzerinden bağlanırlar. Bütün veri erişim noktası üzerinden aktarılır. Verinin korunması amacıyla iletişim şifrelenmiş halde iletilir. Çok sayıda cihazın olması ve daha güvenilir bir bağlantıya ihtiyaç olduğunda tercih edilir.

Kablosuz ağlar kişisel ve yerel alan ağları olmak üzere ikiye ayrılır. Kablosuz kişisel alan ağlar (Wireless Personal Area Network – WPAN) cihazların 10 metre civarı içerisinde oldukları, çoğu zaman birbirlerini direkt görmesi ve aktarılacak verinin çok büyük olmaması gibi durumlarda tercih edilir. İlk başlarda bir cep telefonundan başka bir telefona resim veya müzik gibi dosyaların paylaşılması amacıyla geliştirilmiştir. Uygulama alanı genişleyerek araç içi uygulamalarda ve telefon ile kulaklık veya hoparlör gibi cihazları birbirine bağlama amacı ile kullanılmaya başlamıştır. WPAN standardının kullanıldığı teknolojilerin başında ZigBee ve Bluetooth gelmektedir. Bluetooth teknolojisi bu alanda önemli bir yol alarak hem veri aktarım hızlarını hem de cihazlar arasında olabilecek maksimum mesafeyi oldukça artırmıştır. Başlıca Bluetooth cihazlarda saptanan güvenlik açıkları Bluejacking, Bluebugging, Bluesnarfing, Aradaki adam saldırısı, Tekrarlama saldırısı ve Hizmet engelleme saldırısıdır.

Kablosuz yerel ağlar (Wireless Local Area Network - WLAN) mimarisinde kapsama alanları hücre olarak adlandırılan alt gruplara bölünür ve her bir hücreden bir erişim noktası sorumludur. Kablosuz yerel alan ağlarda güvenilir bir iletişim kurulabilmesi için IEEE 802.11 standardı geliştirilmiştir. IEEE 802.11i kablosuz yerel alan ağları için kimlik doğrulama, veri bütünlüğü, veri gizliliği ve anahtar yönetimi alanlarında güvenlik satandartlarını belirler. Kablosuz Uygulama Protokolü (Wireless Application Protocol–WAP) kablosuz telefon ve benzeri cihazları kullanan mobil kullanıcılara İnternet ve benzeri bilişim hizmetlerine erişmesine imkân sağlar. WAP güvenliği temel olarak kablosuz iletim katmanı güvenliği (Wireless Transport Layer Security - WTLS) tarafından sağlanır.

Kablosuz ağların sağladığı hareket esnekliği, kablolama maliyetinin azalması ve erişim kolaylığı yanında barındırdığı zafiyetler vardır. Kablosuz ağlara yönelik saldırılar aktif veya pasif olmak üzere iki gruba ayrılır. Pasif saldırılarda amaç iletilen verinin elde edilmesine yöneliktir. Aktif saldırı ise güvenli bir şekilde kablosuz iletişim kurmaya çalışan yetkili iki kullanıcının arasında oluşturmak istediği iletişimi bozmaya veya verinin değiştirilmesine yönelik saldırılardır. Kablosuz ağların aşağıda bahsedilen güvenlik zafiyetleri mevcuttur:

- Kablosuz ağlarda iletişim kolaylıkla yetkisiz kişiler tarafından dinlenebilir.
- Radyo sinyalleri kolaylıkla karıştırılabilir veya kötü amaçlı sinyaller iletişime eklenebilir.

- Cep telefonu ve gömülü sistemler gibi cihazların yeterli hesaplama kabiliyeti olmadığı için bazı şifreleme algoritmalarının çalıştırılmasında sorunlar yaşanabilir.
- İstemcilerin yetkisiz erişim noktalarına bağlanması mümkün olabilmektedir.

IEEE 802.11 Kablosuz Yerel Alan Ağlarına Genel Bakış

IEEE 802 yerel alan ağları (LAN) konusunda standartlar geliştiren bir komitedir. Kablosuz yerel alan ağları (WLAN) için bir standart olan IEEE 802.11'in amacı protokoller ve iletim özelliklerini geliştirmektir. Farklı frekanslarda ve farklı veri aktarım hızlarında WLAN talebi hızla artmıştır. IEEE 802.11 çalışma grubu, sürekli genişleyen bir standartlar listesi yayınlamıştır. Aşağıda IEEE 802.11 standardında tanımlanan bazı anahtar terimler sıralanmıştır.

İstasyon (Kablosuz istemci): MAC ve fiziksel katman açısından IEEE 802.11 standardı ile uyumlu herhangi bir aygıttır.

Erişim Noktası: İstasyon işlevine sahip ve ilişkili istasyonlar için kablosuz ortam üzerinden dağıtım sistemine erişim sağlayan herhangi bir öğedir.

Temel Hizmet Kümesi: Tek bir koordinasyon işlevi tarafından kontrol edilen istasyonların kümesinden oluşur.

Dağıtım Sistemi: Genişletilmiş servis seti oluşturmak için temel servis setlerinin kümesi ile yerel alan ağlarını birbirine bağlamak için kullanılan sistemdir.

IEEE 802 Protokol Mimarisi

IEEE 802 standartları fiziksel katman, ortam erişim denetimi katmanı ve mantıksal bağlantı denetimi katmanından oluşur.

IEEE 802.11 standartları katmanlı protokoller kümesi yapısı içinde tanımlanır. Bu yapı tüm **IEEE 802** standartları için kullanılır ve üç katmandan oluşur. Birinci katman *fiziksel katman* olarak adlandırılır. IEEE başvuru modelinin en alt seviye katmanıdır. Sinyallerin kodlanması ve kodlarının çözülmesi işlevi ve bitlerin iletimi ve alımı işlevlerini gerçekleştiren katmandır. İletim ortamının özelliklerini belirler. IEEE 802.11 protokolünde bu katman ayrıca frekans bantları ve anten özelliklerini de tanımlar. İkinci katmana ise *ortam erişim denetimi katmanı* denir. Bütün yerel alan ağları ağın iletim kapasitesini paylaşan cihazlardan oluşmaktadır. Bu kapasiteyi düzenli ve verimli kullanmak amacıyla iletim ortamına kontrollü erişim gerekmektedir. Bu görev, ortam erişim denetimi katmanınındır. Bu katman veriyi bir üst katman olan *mantıksal bağlantı denetimi katmanı* üzerinden Ortam Erişim Kontrolü (Media Access Control-MAC) hizmet veri birimi ismi verilen bloklar olarak alır. Bu katmanın gerçekleştirdiği üç temel işlev vardır. Bunlardan birincisi iletim işleminde veriyi adres ve hata algılama alanları ile birlikte MAC protokol veri birimi olarak da bilinen çerçeve içine birleştirmektir. İkinci işlevi ise alım işleminde çerçeveyi parçalarına ayırma, adres tanıma ve hata ayıklama işlemini gerçekleştirmedir. Son işlevi ise yerel alan ağı iletim ortamına erişimi yönetmedir.

MAC protokol veri birimi çerçevesi aşağıdaki alanlardan oluşur:

MAC Kontrol: MAC protokolünün işleyişi için gerekli protokol kontrol bilgilerini içerir.

Hedef MAC Adres: MAC protokol veri birimi için yerel alan ağı içindeki ulaşılacak fiziksel adresi gösterir.

Kaynak MAC Adres: MAC protokol veri birimi için yerel alan ağı içindeki kaynak fiziksel adresi gösterir.

MAC Hizmet Veri Birimi: Bir üst katmandan gelen veriyi içerir. MAC hizmet veri biriminden önce verilen alanlar MAC başlığı, daha sonra gelen alanlar MAC sonlandırma bilgisi olarak adlandırılır.

Döngüsel Artıklık Denetimi (Cyclic Redundancy Check – CRC): Döngüsel artıklık denetimi dijital veride iletim sırasında bir hatanın oluşup oluşmadığını tespit etmek için kullanılır. Tüm MAC protokol veri birimi kullanılarak CRC değeri hesaplanır ve çerçeveye

eklenerek gönderilir. Alıcı aynı veri birimi ile CRC değerini tekrar hesaplar ve göndericinin CRC değeri ile karşılaştırır. Karşılaştırma sonucunda iletim sırasında değişime uğramış bitler tespit edilebilir.

Üçüncüsü ise *mantıksal bağlantı denetimi katmanı* olarak adlandırılmıştır. Veri bağı denetim protokollerinde veri bağı öğesinin görevi çoğu zaman CRC kullanarak hataları tespit etmek ve hasarlı çerçeveleri tekrar göndermektir. Bu görevler ortam erişim denetimi katmanı ve mantıksal bağlantı denetimi katmanı arasında paylaşılmıştır. Hataları bulma işlemini ortam erişim denetimi katmanı gerçekleştirirken, hatalı çerçeveleri gönderme işlemi mantıksal bağlantı denetimi katmanının görevidir. Mantıksal bağlantı denetimi katmanı bu görevi gerçekleştirirken gönderilme işlemi başarıyla tamamlanmış çerçevelerin kaydını tutar ve başarısız çerçeveleri tekrar gönderir.

IEEE 802.11 Ağ Bileşenleri ve Mimari Modeli

Bir kablosuz yerel alan ağının en küçük yapı taşı aynı MAC protokolünü kullanan ve aynı paylaşılan kablosuz ortama erişim için yarışan kablosuz istasyonlardan oluşan temel hizmet kümesidir. Temel hizmet kümesi izole olarak kalabileceği gibi erişim noktası kullanarak omurga dağıtım sistemine de bağlanabilir. Erişim noktası bir köprü görevi görür. Temel hizmet kümesi içindeki istasyonlar birbirleri ile doğrudan iletişimde bulunmazlar. Aynı hizmet kümesi içindeki bir diğer istasyona MAC çerçevesi göndermek istediklerinde öncelikle bu çerçeve erişim noktasına gönderilir, daha sonra erişim noktası bu çerçeveyi ilgili istasyona iletir. Eğer bir istasyon başka bir temel hizmet kümesi içindeki istasyona çerçeve göndermek istiyorsa, bu çerçeve erişim noktası üzerinden dağıtım sistemine gönderilir. Dağıtım sistemi çerçeveyi ilgili temel hizmet kümesine ulaştırır. Eğer bir temel hizmet kümesindeki istasyonlar birbirleri ile doğrudan iletişime geçen mobil istasyonlar ise bu hizmet kümesine bağımsız temel hizmet kümesi adı verilir. Bu durumda iletişimi sağlamak için erişim noktasına ihtiyaç yoktur. İki temel hizmet kümesi coğrafi olarak örtüşüyor olabilir. Bu durumda bir istasyon aynı anda birden fazla temel hizmet kümesinin kapsama alanında yer alabilir. Ayrıca istasyonlar ile temel hizmet kümeleri arasındaki ilişki dinamiktir. İstasyonlar kapanabilir, bir temel hizmet kümesinin kapsama alanına girebilir veya bu alandan çıkabilir.

IEEE 802.11 Hizmetleri

IEEE 802.11 kablolu yerel alan ağlarındaki işlevselliğin eşdeğerine ulaşmak için gerekli, kablosuz yerel alan ağları tarafından sağlanması gereken dokuz hizmet tanımlanır. Bu hizmetler aşağıdaki gibi iki farklı bakış açısı ile değerlendirilebilir:

- Hizmet sağlayıcı, istasyonlar veya dağıtım sistemi olabilir. İstasyon hizmetleri erişim noktalarını da içeren her 802.11 istasyonunda uygulanır. Dağıtım hizmetleri temel hizmet kümeleri arasında gerçekleştirilir.
- Hizmetlerden üçü IEEE 802.11 yerel alan ağına erişimi ve gizliliği denetlemek için kullanılır. Diğer altı hizmet ise MAC hizmet veri birimlerinin istasyonlar arasında teslimatı için kullanılır.

Mesajların dağıtım sistemi içindeki işlemlerinde iki temel hizmet gereksinimleri bulunmaktadır. Bu hizmetler *dağıtım* ve *tümleştirme* işlemleridir. Dağıtım MAC protokol veri birimlerinin bir temel hizmet kümesindeki istasyondan diğer bir temel hizmet kümesindeki istasyona ulaşmak için dağıtım sistemini kullanmaları gerektiğinde ihtiyaç duyulan birincil hizmettir. Tümleştirme hizmeti kablosuz bir ağdaki istasyonla kablolu bir ağdaki istasyon arasındaki veri transferi işleminin mümkün olmasını sağlar. Bu hizmet, veri alışverişinde gerekli adres çevrimi ve ortam dönüştürme işlemleri ile ilgilenir.

Bir mesajın bir dağıtım sistemi içerisinde teslimatını gerçekleştirmek için dağıtım hizmetinin hedef istasyonun yerini bilmesi gerekmektedir. Mesajın istenen istasyona ulaşması için hangi erişim noktasına yönlendirilmesi gerektiği bilinmelidir. Bu nedenle bir istasyonun kendi temel hizmet kümesindeki erişim noktası ile ilişkisini sürdürmesi gerekir. Bu noktada üç hizmet söz konusudur. *Bağlama* hizmeti, istasyon ile erişim noktası arasındaki başlangıç ilişkisini kurar. Bir istasyonun bir kablosuz yerel alan ağı içinde çerçeve gönderebilmesi ve alabilmesi için kimliğinin ve adresinin bilinmesi zorunludur. Bu amaçla istasyon temel hizmet kümesi içindeki erişim noktası ile bir ilişki kurmak zorundadır. Daha sonra erişim noktası bu bilgileri genişletilmiş hizmet kümesindeki diğer erişim noktaları ile paylaşır. *Yeniden bağlama* hizmeti, bir erişim noktasında kurulmuş bir ilişkiyi mobil cihazın yer değiştirmesinden dolayı başka bir erişim noktasına taşıma işlemini gerçekleştirir. *Ayrışma* hizmeti, istasyonun veya erişim noktasının var olan bir bağlantının bittiği konusunda yaptığı bilgilendirmedir.

IEEE 802.11i Kablosuz Yerel Alan Ağı Güvenliği

Kablolu ağlar ile kablosuz ağlar arasında temel olarak iki fark bulunmaktadır. Birincisi, kablolu ağlarda bir cihazın bir ağda yer alabilmesi için cihazın fiziksel olarak o ağa bir kablo aracılığıyla bağlanması gerekir. Başka bir ifade ile bir istasyonun bir ağa eklenmesi işlemi gözlemlenebilir bir eylemdir. Kablosuz ağlarda böyle bir durum söz konusu değildir. İkinci fark ise, kablolu ağda bir istasyonun başka bir istasyondan mesaj alabilmesi için fiziksel olarak o ağda bağlı olması gerekir. Kablosuz ağda ise radyo aralığında yer alan herhangi bir istasyon mesaj alabilir. Bu durumda kablolu ağ fiziksel bir bağlantı gereksinimi ile belirli bir seviyede gizlilik sağlar. Ancak bu özellik kablosuz ağlar için geçerli değildir. Bu farklılıklar kablosuz yerel alan ağları için dayanıklı güvenlik hizmetleri ve mekanizmalarına olan ihtiyacı arttırmıştır. 802.11 standardının güvenlik özellikleri zayıflıklar içermekteydi. Bu nedenle 802.11i çalışma grubu kablosuz yerel alan ağlarının güvenlik sorunlarını çözmek için yeni bir takım özellikler geliştirmişlerdir. 802.11i standardının son sürümü *Dayanıklı Güvenlik Ağı* (Robust Security Network –RSN) şeklinde isimlendirilmiştir.

IEEE 802.11i Hizmetleri

802.11i RSN güvenlik şartnamesi aşağıdaki hizmetleri tanımlar:

Kimlik doğrulama: Kablosuz bağlantı üzerinden istemci ile erişim noktası arasında kullanılacak geçici anahtarları üreten ve karşılıklı kimlik doğrulama sağlayan sunucu ile kullanıcı arasındaki değişimi tanımlamak için kullanılan protokoldür.

Erişim denetimi: Bu hizmet, doğrulama hizmetinin kullanımını mecbur kılar, mesajların uygun şekilde yönlendirilmesini sağlar ve anahtar değişimini gerçekleştirir. Çeşitli doğrulama protokolleri ile beraber çalışabilir.

Mesaj bütünlüğü ile gizlilik: MAC düzeyindeki veriler, kötü niyetli kişiler tarafından iletilecek verinin okunmamasını ve değiştirilmemesini sağlamak amacıyla ileti bütünlük kodu ile birlikte şifrelenir.

IEEE 802.11i Operasyon Aşamaları

IEEE 802.11i Dayanıklı Güvenlik Ağı'nın operasyonu temelde beş farklı evrede değerlendirilebilir. Gerçekte kaç evreden oluştuğu iletişimin bitiş noktaları ve yapılandırmasına bağlıdır. Bu farklı yapılandırmalar şu şekilde olabilmektedir:

- **Yapılandırma 1.** Aynı temel hizmet kümesinde yer alan iki kablosuz istasyonun erişim noktası kullanarak iletişimde bulunması.
- **Yapılandırma 2.** Aynı bağımsız temel hizmet kümesinde yer alan iki istasyonun doğrudan birbirleriyle iletişimde bulunması.

- **Yapılandırma 3.** Farklı temel hizmet kümelerinde yer alan iki istasyonun kendi erişim noktalarını kullanarak dağıtım sistemi üzerinden iletişim gerçekleştirmesi.
- **Yapılandırma 4.** Bir kablosuz istasyonun kablolu bir ağda bulunan bir istasyonla erişim noktası ve dağıtım sistemi kullanarak iletişimde bulunması.

IEEE 802.11i güvenliği, sadece bir istasyonun kendi erişim noktası ile güvenli iletişim gerçekleştirmesi ile ilgilidir. Birinci ve ikinci yapılandırmada her bir istasyonun erişim noktası ile güvenli iletişim kurması amaçlanır. Üçüncü yapılandırmada IEEE 802.11 seviye güvenliği dağıtım sistemi düzeyinde sağlanmamaktadır. Sadece temel hizmet kümeleri içerisindeki güvenlik sağlanır. Dördüncü yapılandırmada da aynı şekilde güvenlik sadece istasyon ve onun erişim noktası arasında verilmektedir. Beş farklı evre aşağıdaki şekilde tanımlanabilir.

Keşif: Doğrulama sunucusu kendi IEEE 802.11i güvenlik politikasını yayınlar. Bir istasyon bu bilgiyi kullanarak iletişim kurmak istediği kablosuz yerel alan ağı için bir erişim noktası belirler. İstasyon, sunulan seçeneklerden bir şifreleme paketi ve doğrulama mekanizması kullanan bir erişim noktası ile iletişim kurar.

Doğrulama: Bu aşamada istasyon ve doğrulama sunucusu birbirlerine kimliklerini kanıtlar. Erişim noktası doğrulama işlemi başarılı oluncaya kadar doğrulama sunucusu ve istasyon arasındaki doğrulanmamış mesaj trafiğini engeller. Erişim noktası istasyon ile doğrulama sunucusu arasındaki trafiği iletmek dışında doğrulama işleminin gerçekleşmesine karışmaz.

Anahtar yönetimi: Erişim noktası ve istasyon şifreleme anahtarlarının üretilmesi ve yerleştirilmesini sağlamak için çeşitli işlemler gerçekleştirir. Bu işlemler sadece erişim noktası ve istasyon arasında yapılır.

Korumalı veri transferi: Çerçeveler erişim noktası aracılığıyla son istasyonlar arasında gönderilir. Güvenli veri transferi sadece istasyon ve erişim noktası arasında gerçekleştirilir. Uçtan uca güvenlik hizmeti verilmez.

Bağlantı sonlandırma: Bu aşamada güvenli bağlantı sonlandırılır ve bağlantı özgün durumuna geri döner.

Bu evreleri daha detaylı aşağıdaki gibi açıklayabiliriz. Keşif evresinin amacı istasyon ile erişim noktasının birbirlerini tanımaları, güvenlik parametreleri üzerinde anlaşmaları ve bu parametreleri kullanarak gelecekteki iletişim için ilişki kurmalarıdır. Bu aşamada istasyon ve erişim noktası tek yönlü trafiği korumak amacıyla gizlilik ve MAC protokol veri birimi bütünlük protokolleri, doğrulama metodu ve şifreleme anahtar yönetim yaklaşımı gibi alanlarda kullanılacak teknikleri belirler. Keşif aşaması üç değiştirme işlemi içerir. Birincisi, ağ ve güvenlik özelliklerinin belirlenmesidir. Bu değişim sırasında istasyonlar iletişim kurulacak ağın varlığını keşfederler. İkincisi, açık sistem kimlik doğrulamasıdır. Hiçbir güvenlik sağlamayan bu çerçeve dizisinin amacı basitçe IEEE 802.11 durum makinesine geriye dönük uyumluluk sağlamaktır. Üçüncüsü bağlama işlemidir ve amacı kullanılacak bir dizi güvenlik adımları üzerinde anlaşmaktır.

Doğrulama evresi, kimlik doğrulama için dağıtım sisteminde yer alan kimlik doğrulama sunucusu ile istasyon arasında karşılıklı kimlik doğrulama sağlar. Doğrulama sadece yetkili istasyonların ağı kullanmasını sağlamak ve bir istasyona meşru bir ağla iletişim kurduğu güvencesini vermek amacıyla tasarlanmıştır.

Anahtar yönetimi aşamasında çeşitli şifreleme anahtarları oluşturulur ve istasyonlara dağıtılır. İki çeşit anahtar bulunmaktadır. İkili anahtarlar, istasyon ve erişim noktası arasındaki iletişimde kullanılır. Grup anahtarlar çoklu iletişimlerde kullanılmaktadır. İkili anahtarlar sınırlı bir zaman içinde kullanılabilen diğer anahtarların dinamik olarak oluşturulduğu bir ana anahtar ile başlayan bir hiyerarşi oluştururlar. Hiyerarşinin en üst düzeyinde kullanılacak iki farklı seçenek vardır. Önceden paylaşılmış anahtar erişim noktası ve

istasyon arasında paylaşılan ve IEEE 802.11i kapsamı dışında yüklenen bir anahtardır. Diğer seçenek is AAAK olarak da bilinen ana oturum anahtarıdır. Bu anahtar IEEE 802.11X protokolü tarafından doğrulama aşamasında üretilmiştir. Gerçek anahtar üretim metodu kullanılan kimlik doğrulama metodunun detaylarına bağlıdır. Her iki durumda da erişim noktasının her bir istasyonla paylaştığı benzersiz bir anahtar vardır. Bu ana anahtardan türetilmiş, erişim noktası ve istasyon arasında paylaşılan tüm anahtarlar da benzersizdir. Her istasyon herhangi bir zamanda bir anahtar kümesine sahipken, her erişim noktası her bir istasyonla iletişim için ayrı anahtar kümelerine sahiptir.

İkili ana anahtar, ana anahtardan türetilmiştir. Eğer önceden paylaşılan anahtar kullanılmışsa, bu anahtar ikili ana anahtar olur. Eğer ana oturum anahtarı kullanılmışsa, ikili ana anahtar bu anahtardan türetilir. Doğrulama aşamasının sonuna kadar erişim noktası ve istasyon ikili ana anahtarın birer kopyasına sahip olurlar.

İkili ana anahtar, ikili geçici anahtarı üretmek için kullanılır. İkili geçici anahtar, karşılıklı kimlik doğrulaması yapıldıktan sonra istasyon ile erişim noktası arasındaki iletişimde kullanılan üç anahtarı içerir. İkili geçici anahtarı oluşturmak için ikili ana anahtar ile erişim noktası ve istasyonun MAC adreslerine HMAC-SHA-1 fonksiyonu uygulanır. İstasyon ve erişim noktası adreslerini ikili geçici anahtar üretiminde kullanmak sahte kimlik saldırısı ve oturum kaçırmaya karşı koruma sağlar. İkili geçici anahtar aşağıdaki üç anahtardan oluşur:

1. *EAPOL anahtar onay anahtarı:* Dayanıklı güvenlik ağının kurulumu sırasında istasyondan erişim noktasına denetim çerçevelerinin veri kaynağının özgünlüğünü ve bütünlüğünü destekler.
2. *EAPOL anahtar şifreleme anahtarı:* Bazı dayanıklı güvenlik ağı birleşme işlemlerinde anahtarlar ve verinin gizliliğini korur.
3. *Geçici anahtar:* Kullanıcı trafiğinde gerçek korumayı sağlar.

Grup anahtarları bir istasyonun birden fazla istasyona MAC protokol veri birimi gönderdiği çoklu iletişimde kullanılır. Grup anahtarı hiyerarşisinin en üst düzeyinde grup ana anahtarı bulunur. Grup ana anahtarı bir çeşit anahtar üretici anahtardır ve diğer girdilerle birlikte grup geçici anahtarını oluşturur. Erişim noktası ve istasyon bilgileri kullanılarak üretilen ikili geçici anahtarın aksine, grup geçici anahtarı erişim noktasında üretilir ve ilişkili istasyonlara dağıtılır. Grup geçici anahtarları hâlihazırda oluşturulmuş ikili anahtarlar kullanılarak güvenli bir şekilde dağıtılır. Herhangi bir aygıt ağı terk ettiğinde grup geçici anahtarı değiştirilir.

Korumalı veri transferi aşamasında, IEEE 802.11i MAC protokol veri birimleri ile aktarılan veriyi korumak için iki protokol tanımlanmıştır. Bunlar geçici anahtar bütünlüğü protokolü ve CCMP olarak adlandırılmıştır. CCMP mesaj bütünlüğü ve veri gizliliği hizmetlerini gerçekleştirmektedir. Geçici anahtar bütünlüğü protokolü de aynı iki hizmeti sağlar. Veri gizliliği MAC protokol veri birimi ile mesaj bütünlüğü kodunun RC4 kullanılarak şifrelenmesiyle sağlanır. Mesaj bütünlüğü hizmetinde bu protokol 802.11 MAC çerçevesinde veri alanından sonra mesaj bütünlüğü kodu ekler. Mesaj bütünlüğü kodu Michael algoritması tarafından üretilir. 64 bit uzunluğunda olup, kaynak ve hedef fiziksel adresleri, veri alanı ve anahtar bilgilerinin Michael algoritması tarafından girdi olarak kullanılmasıyla oluşturulur.

Kabloya Eşdeğer Gizlilik (Wired Equivalent Privacy–WEP)

1999 yılında standartlaştırılan 802.11 kablosuz ağ protokolü için gerekli kimlik doğrulama, şifreleme ve veri bütünlüğü işlemleri için WEP protokolü tanımlanmıştır. WEP ağ yapılandırmasının ve uygulamasının pratik olması amacıyla tasarlanmıştır. WEP'nin kablolu bir ağa eşdeğer güvenlik sağlayacağı varsayılıyordu. Hem anahtar uzunluğunun yetersiz olması hem de barındırdığı zafiyetlerden dolayı yayınlanmasını takip eden birkaç yıl içerisinde kolayca kırılabilir olduğu gösterildi. Kullanılması güvenlik zafiyetlerine sebep olacağı için daha güvenilir olan WAP protokolüne geçiş yapıldı.

Kablosuz Uygulama Protokolü (Wireless Application Protocol –WAP)

Kablosuz uygulama protokolü evrensel ve açık standart bir protokoldür. Kablosuz telefonlar, çağrı cihazları ve kişisel dijital asistanların İnternet ve Web dâhil olmak üzere telefon ve bilgi hizmetlerine ulaşmasını sağlamak için kullanılır. WAP, bütün kablosuz ağ teknolojileri ile çalışabilmek üzere tasarlanmıştır. Bu protokol IP, XML, HTML ve HTTP gibi İnternet standartlarına dayanmaktadır. Aynı zamanda güvenlik olanakları içermektedir.

Veri hizmetleri için cep telefonları ve terminalleri kullanmanın cihazlar ve bu cihazları bağlayan ağlardan kaynaklanan bazı sınırlamaları vardır. Cihazların ara yüzleri, işlem gücü, bellek miktarı ve pil ömürleri sınırlıdır. Kablosuz ağlar kablolu bağlantılara göre nispeten düşük bant genişliği, yüksek gecikme ve öngörülemeyen kullanılabilirlik ve istikrara sahiptir. Ayrıca kablosuz ağlara bağlanan kullanıcılar farklı beklentilere sahiptir. Örneğin, mobil cihazların kullanımının kişisel bilgisayarlara göre çok kolay olması beklenir. WAP bütün bu sorunlara çözüm olması amacıyla geliştirilmiştir. Aşağıdaki konular kablosuz uygulama protokolünde ayrıntıları ile belirlenmiştir:

- WWW programlama modeline dayanan bir programlama modeli,
- XML'e bağlı kalan bir biçimlendirme dili (Kablosuz İşaretleme Dili),
- Mobil, kablosuz terminal için uygun küçük tarayıcı,
- Hafif iletişim protokolü yığını ve
- Kablosuz telefon uygulamaları için bir çerçeve.

WAP istemci, ağ geçidi ve orijinal sunucu olmak üzere üç unsura dayanmaktadır. HTTP protokolü, ağ geçidi ve orijinal sunucu arasında içerik aktarmak için kullanılır. Ağ geçidi, kablosuz etki alanı için bir vekil sunucu gibi hareket eder. WAP özelliklerine sahip bir mobil kullanıcı Web içeriğini sıradan bir Web sunucuda görebilir. Web sunucusu, standart Web protokol yığını (HTTP/TCP/IP) kullanılarak iletilen HTML kodlu sayfalar şeklinde içerik sağlar. HTML içeriği bir HTML filtresinden geçmelidir. Filtre, HTML içeriğini Kablosuz İşaretleme Dili (Wireless Markup Language–WML) içeriğine çevirir. Vekil, WML içeriğini daha kompakt bir form olan ikili WML içeriğine dönüştürür ve WAP protokol yığını kullanarak kablosuz ağ üzerinden mobil kullanıcıya sunar. Eğer Web sunucusu doğrudan WML içeriği üretme yeteneğine sahipse, WML, TCP/IP kullanılarak vekile teslim edilir. WML vekil tarafından ikili WML durumuna dönüştürülür ve WAP protokolleri kullanılarak mobil düğüme iletilir.

WAP mimarisi, mobil düğümün sınırlamaları (küçük ekran boyutu, sınırlı giriş yeteneği) ve kablosuz dijital ağların düşük veri hızları gibi iki temel problem ile başa çıkmak amacıyla tasarlanmıştır.

Kablosuz İşaretleme Dili (Wireless Markup Language–WML)

WML sınırlı bant genişliği, sınırlı ekran boyutu ve sınırlı kullanıcı giriş özelliğine sahip cihazlarda verileri sunmak için içerik ve biçim tanımlamak için tasarlanmıştır. Bu dil telefon tuş takımı gibi mobil, kablosuz cihazlarda yaygın olarak kullanılan aygıtlarla çalışabilmek için geliştirilmiştir. Web tarayıcı, HTML ile kodlanmış Web sayfaları şeklindeki içeriği kişisel bilgisayarlar için sağlar. HTML ile kodlanmış Web sayfalarını kablosuz cihazlar için uygun olacak WML format ve içeriğine çevirmek için, özellikle grafik ve animasyon bilgileri olmak üzere birçok bilgi sayfadan çıkarılır. WML, Web sayfasının özünü yakalamaya yönelik metin tabanlı bilgi sunar. Bu bilgi aynı zamanda mobil cihaz kullanıcılarının kolay erişimi için organize edilir.

WAP Mimarisi

WAP mimarisi beş katmanlı bir modeldir. Her katman iyi tanımlanmış ara yüzler vasıtasıyla diğer katmanlara işlev ve hizmet sağlar. Mimari katmanların her biri üstteki katmanlar ve diğer hizmet ve uygulamalar tarafından erişilebilir. Bu hizmetler iki kategoride değerlendirilebilir. Bunlar güvenlik hizmetleri ve hizmet bulgulama katmanlarıdır. Güvenlik hizmetleri arasında kriptografik kütüphaneler, kimlik doğrulama, güvenli iletim ve güvenli taşıyıcı sayılabilir. Hizmet bulgulama hizmetleri arasında dış işlevsellik ara yüzü, sağlama, navigasyon bulgulama ve hizmet arama sayılabilir.

Kablosuz İletim Katmanı Güvenliği (Wireless Transport Layer Security–WTLS)

WTLS istemcisi olarak değerlendirilebilecek mobil cihaz ile WAP ağ geçidi arasında güvenlik hizmetleri sunar. TLS Web tarayıcı ve Web sunucular arasında kullanılan bir güvenlik protokolüdür ve WTLS protokolünün temelini oluşturur. WTLS mobil cihazlarda kullanılacağı için daha verimli olmalıdır ve bu nedenle daha az mesajlaşma içerir. Uçtan uca güvenlik sağlamak amacıyla istemci ile ağ geçidi arasında WTLS, ağ geçidi ile hedeflenen sunucu arasında TLS kullanılır. Aşağıdaki özellikler WTLS tarafından karşılanır:

Veri bütünlüğü: İstemci ve ağ geçidi arasında gönderilen verinin başkaları tarafından değiştirilmediğinden emin olmak için mesaj bütünlüğü doğrulaması yöntemleri kullanılır.

Gizlilik: İletim halindeki verinin üçüncü şahıslar tarafından okunmamasını garanti etmek amacıyla şifreleme algoritmaları kullanılır.

Kimlik doğrulaması: Her iki tarafın (istemci ve ağ geçidi) kimlik doğrulaması için dijital sertifikalar kullanılır.

Hizmet engelleme koruması: Başarılı bir şekilde doğrulanmayan ve yeniden yönlendirilen mesajları algılar ve reddeder.

WTLS Oturumları ve Bağlantıları

Güvenli oturum ve güvenli bağlantı iki önemli WTLS kavramıdır. Oturum, istemci ve sunucu arasında bir birleşmedir. Oturumlar el sıkışma protokolü tarafından oluşturulur. Oturumlar birden fazla bağlantı tarafından paylaşılabilen kriptografik güvenlik parametreleri dizisi tanımlar. Oturumlar her bağlantı için yeni güvenlik parametrelerinin müzakere edilmesini önlemek için kullanılır. Bağlantılar geçicidir ve tek oturumla ilişkilidir.

WAP Uçtan Uca Güvenlik

WAP istemci, WAP ağ geçidi ve Web sunucu içeren temel WAP iletim modeli güvenlik boşlukları içerir. Mobil cihaz WAP ağ geçidi ile güvenli bir WTLS oturumu kurar. WAP ağ geçidi ise Web sunucusu ile güvenli bir SSL veya TLS oturumu oluşturur. Ağ geçidi içinde çeviri sürecinde veri şifreli değildir. Bu nedenle ağ geçidi verinin riske atıldığı bir nokta olarak düşünülebilir. Mobil istemci ve Web sunucu arasında uçtan uca güvenlik sağlayan çeşitli yaklaşımlar bulunmaktadır. İlk yaklaşım, istemci ve sunucu arasında TLS kullanımından faydalanmaktır. Güvenli TLS oturumu uç noktalar arasında kurulur. WAP ağ geçidi TCP düzeyinde ağ geçidi olarak görev yapar ve uç noktaları arasındaki trafiği taşımak için birlikte iki TCP bağlantısını ekler. TCP kullanıcı veri alanı (TLS kayıtları) ağ geçidini geçerken şifreli kalır, yani uçtan uca güvenlik sağlanır. Diğer bir yaklaşım da WAP ağ geçidinin basit bir yönlendirici gibi davranmasıdır. Bu durumda güvenlik IP düzeyinde IPsec protokolü kullanılarak sağlanır.

Özet

AMAÇ 1 *İnternet ortamındaki güvenlik sorunlarını tanımlamak*

Verinin İnternet gibi korumasız bir ağ üzerinden iletilmesi önemli güvenlik tehditlerine sebep olur. Bu güvenlik tehditlerinden birisi ağın dinlenmesidir ve gizli kalması gereken bilginin kötü niyetli kişilerin ellerine geçmesi anlamına gelir. Diğer bir tehdit ise ağ üzerinden gönderilen verinin bütünlüğünün korunamamasıdır. Bu durum veri kaybına yol açar. Önlenmesi en zor tehditlerden birisi sahte istekler ile sistemi meşgul etmedir ve bu tehdit gerçekleşirse sistemin belli bir süre hizmet vermesi engellenmiş olur. Başkasının kimliğine bürünme şeklinde kendini gösteren diğer bir tehdit kimlik doğrulama işlemini tehlikeye atar. Çözümü kriptografik yöntemlerdir.

AMAÇ 2 *Güvenli soket katmanı ve iletim katmanı güvenliği kavramlarını açıklamak*

Güvenli soket katmanı veri bütünlüğünün sağlanması, gizlilik ihlallerinin giderilmesi ve kimlik doğrulama işleminin en iyi şekilde tamamlanabilmesi için kullanılan bir güvenlik uygulamasıdır. Şifreleme yöntemleri, dijital imzalar ve sertifikalar kullanarak görevini yerine getirir. İki katman halinde yerleşen dört protokolün bir araya gelmesi ile oluşmuştur. Bu protokoller kayıt protokolü, el sıkışma protokolü, şifre değiştirme protokolü ve uyarı protokolüdür. İletim katmanı güvenliği, güvenli soket katmanının İnternet standart sürümü şeklinde düşünülebilir. Bir takım farklarla beraber güvenli soket katmanının özelliklerini taşır. Temel amacı iletişimde bulunan iki taraf arasında mesaj bütünlüğünün ve gizliliğin sağlanmasıdır.

AMAÇ 3 *HTTPS ve SSH kullanım alanlarını tanımlamak*

HTTPS, HTTP ile SSH'ın birleştirilmesi ile Web tarayıcı ve Web sunucu arasındaki iletişimin güvenli olması amacıyla oluşturulmuştur. HTTPS,URL adresi, doküman içeriği, tarayıcı formların içeriği, çerezler ve HTTP başlığının içeriğini şifreler. SSH uzaktan oturum açmada ortaya çıkma ihtimali olan tehditlerden korunmak için tasarlanan bir protokoldür. SSH tarafından güvenli bir bağlantı, kimlik doğrulama ve şifreleme algoritmaları kullanılarak gerçekleştirilir. Aynı zamanda veri sıkıştırma, dosya transferi ve dosya kopyalama hizmetlerinde güvenlik sağlar.

AMAÇ 4 *IEEE 802.11 ve IEEE 802.11i kablosuz ağ standartlarını tanımlamak*

IEEE 802.11 kablosuz yerel alan ağları için oluşturulan standartları belirler. Kablolu yerel alan ağlarındaki işlevselliğe ulaşmak için sağlanması gereken hizmetleri tanımlar. Hizmetlerden üçü yerel alan ağına erişimi ve gizliliği tanımlamak için kullanılır. Diğer altı hizmet ise istasyonlar arasında hizmet veri birimlerinin teslimatı için oluşturulmuştur. Kablolu ağlar fiziksel bağlantı gereksinimleri ile bir derece güvenlik sağlayabilmektedirler. Buna karşılık kablosuz ağlar aynı gereksinime sahip olmadıklarından güvenlik tehditlerine daha açık durumdadırlar. 802.11 kablosuz ağ standardı güvenlik açısından çeşitli zayıflıklar içerir. 802.11i standardı bu güvenlik zafiyetlerini gidermek için geliştirilmiştir. Kimlik doğrulama, erişim denetimi, mesaj bütünlüğü ve gizlilik gibi hizmetleri sunar.

AMAÇ 5 *Kablosuz uygulama protokolü ve kablosuz iletim katmanı güvenliği kavramlarını açıklamak*

Evrensel ve açık standart olan kablosuz uygulama protokolü, kablosuz telefonlar çağrı cihazları gibi cihazların İnternet hizmetlerine ulaşması için geliştirilmiştir. Mümkün olduğunca var olan İnternet standartlarına dayanmaktadır. Mobil cihazların donanım yeteneklerinin daha az olmasından kaynaklanan bir takım sorunları vardır. Bu sorunları çözebilmek için kablosuz uygulama protokolü; XML'e bağlı kalan bir biçimlendirme dili, mobil ve kablosuz terminaller için uygun küçük tarayıcı ve hafif iletişim protokolü yığını gelişmiştir. Kablosuz iletim katmanı güvenliği protokolü mobil cihazlar ile WAP ağ geçidi arasında güvenlik hizmetleri sunar. Bu protokolün temeli Web tarayıcı ile sunucu arasında güvenli bağlantı oluşturmayı sağlayan TLS protokolüdür.

Kendimizi Sınayalım

1. Aşağıdakilerden hangisi Web kavramının ortaya çıkardığı ve güvenlik sorunlarına sebep olan durumlardan biri **değildir?**

a. İletişimin iki yönlü olması
b. Web sunucuların kurumların bilgisayar sistemlerine ulaşmak için bir atlama noktası olarak düşünülebilmesi
c. Güvenlik konularında eğitilmemiş kullanıcıların Web-tabanlı sistemlerin temel müşterileri olmaları
d. Web-tabanlı sistemlerin dünyanın her yanında şirketlerde ve kurumlarda kullanılması
e. Arka planda çalışan gelişmiş ve karmaşık yazılımın güvenlik açıklarının fazla olması

2. Aşağıdakilerden hangisi Web güvenliği tehditlerinin incelendiği gruplardan birisi **değildir?**

a. Gizliliğe yönelik tehditler
b. Web-tabanlı sistemleri kullanan şirketlere yönelik tehditler
c. Kimlik doğrulamaya yönelik tehditler
d. Bütünlüğe yönelik tehditler
e. Hizmet engellemeye yönelik tehditler

3. Aşağıdakilerden hangisi SSL'yi oluşturan protokollerden birisi **değildir?**

a. Dosya Aktarımı Protokolü
b. Kayıt Protokolü
c. Uyarı Protokolü
d. Şifre Değiştirme Protokolü
e. El Sıkışma Protokolü

4. Aşağıdakilerden hangisi TLS protokolünün temel amaçlarından birisi **değildir?**

a. Kriptografik güvenlik
b. Maliyeti düşürmek
c. Bağıl verim
d. Geliştirilebilirlik
e. Birlikte çalışabilirlik

5. HTTPS'nin bağlantı noktası numarası kaçtır?

a. 80
b. 135
c. 20
d. 53
e. 443

6. Aşağıdakilerden hangisi SSH'yi oluşturan protokollerden birisidir?

a. Şifre değiştirme
b. Kayıt
c. IP
d. Kullanıcı kimlik doğrulama
e. Uyarı

7. Aşağıdakilerden hangisi IEEE 802.11 standardında sağlanması gereken hizmetlerden **değildir?**

a. Kimlik doğrulama
b. Dağıtım
c. Tümleştirme
d. Bağlanma
e. Yeniden bağlanma

8. IEEE 802.11i dayanıklı güvenlik ağının operasyonlarının doğru sıralaması aşağıdakilerden hangisidir?

a. Doğrulama – Korumalı Veri Transferi – Keşif – Anahtar Yönetimi – Bağlantı Sonlandırma
b. Doğrulama – Anahtar Yönetimi – Keşif – Korumalı Veri Transferi – Bağlantı Sonlandırma
c. Keşif – Doğrulama – Anahtar Yönetimi – Korumalı Veri Transferi – Bağlantı Sonlandırma
d. Bulgulama – Anahtar Yönetimi – Korumalı Veri Transferi – Doğrulama – Bağlantı Sonlandırma
e. Keşif – Anahtar Yönetimi – Korumalı Veri Transferi – Bağlantı Sonlandırma – Doğrulama

9. Aşağıdakilerden hangisi IEEE 802.11i standardının sağladığı temel hizmetlerden **değildir?**

a. Kimlik doğrulama
b. Yeniden bağlanma
c. Erişim denetimi
d. Mesaj bütünlüğü
e. Gizlilik

10. Aşağıdaki konulardan hangisi kablosuz uygulama protokolünde (WAP) ayrıntıları ile **belirlenmemiştir?**

a. WWW programlama modeline dayanan bir programlama modeli
b. Mobil, kablosuz terminal için uygun küçük tarayıcı
c. XML'e bağlı kalan bir biçimlendirme dili (Kablosuz İşaretleme Dili)
d. Kablo bağlantılarının nasıl gerçekleştirileceği
e. Hafif iletişim protokolü yığını

Kendimizi Sınayalım Yanıt Anahtarı

1. d	Yanıtınız yanlış ise "Ağ Güvenliği Tehditleri" konusunu yeniden gözden geçiriniz.
2. b	Yanıtınız yanlış ise "Ağ Güvenliği Tehditleri" konusunu yeniden gözden geçiriniz.
3. a	Yanıtınız yanlış ise "Güvenli Soket Katmanı" konusunu yeniden gözden geçiriniz.
4. b	Yanıtınız yanlış ise "İletim Katmanı ve Güvenliği" konusunu yeniden gözden geçiriniz.
5. e	Yanıtınız yanlış ise "HTTPS" konusunu yeniden gözden geçiriniz.
6. d	Yanıtınız yanlış ise "Güvenli Kabuk" konusunu yeniden gözden geçiriniz.
7. a	Yanıtınız yanlış ise "IEEE 802.11 Kablosuz Yerel Alan Ağlarına Genel Bakış" konusunu yeniden gözden geçiriniz.
8. c	Yanıtınız yanlış ise "IEEE 802.11i Kablosuz Yerel Alan Ağı Güvenliği" konusunu yeniden gözden geçiriniz.
9. b	Yanıtınız yanlış ise "IEEE 802.11i Kablosuz Yerel Alan Ağı Güvenliği" konusunu yeniden gözden geçiriniz.
10. d	Yanıtınız yanlış ise "Kablosuz Uygulama Protokolü" konusunu yeniden gözden geçiriniz.

Sıra Sizde Yanıt Anahtarı

Sıra Sizde 1

Gizlilik bir mesajın sadece bu mesaja erişim hakkı olan kullanıcılar tarafından okunabilmesidir. Mesaj bütünlüğü ise mesajın içeriğinin yetkisiz kişilerce değiştirilememesidir. Kimlik doğrulama ise mesajı oluşturan kişinin kimliğinin doğrulanmasıdır.

Sıra Sizde 2

Bu baytın 1 ve 2 değerleri almasının farklı anlamları vardır. Bu değerlere göre ya uyarı verilir ya da bağlantı kesilir. İlk baytın değeri 1 ise uyarı verilir, 2 olması durumunda ise SSL hemen bağlantıyı sonlandırır.

Sıra Sizde 3

Örnek saldırılar arasında Telnet oturumuna müdahale, Telnet vasıtasıyla sunuculara saldırılar, parolaların elde edilmesi ve dinleme gibi saldırılar sayılabilir.

Yararlanılan ve Başvurulabilecek Kaynaklar

Anonim. Web Sitesi: http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/wpa-(wi-fi-protected-access--wi-fi-korumal%C4%B1-eri%C5%9Fim) Erişim tarihi: 15.11.2016.

Introduction to Secure Sockets Layer, White Paper, Cisco Systems.

Kaufman, C., Perlman, R. ve Speciner, M. (2002). ***Network Security Private Communication in a Public World,*** USA: Prentice Hall.

Özdemir, B. (2008). ***Kablosuz Yerel Alan Ağı Güvenliği Kılavuzu,*** TÜBİTAK UEKAE

Stallings, W. (2013). ***Cryptography and Network Security Principles and Practice,*** United Kingdom: Pearson.

Stallings, W. (2011). ***Network Security Essentials: Applications and Standards,*** United Kingdom: Pearson Education.

Wang, J. (2009). ***Computer Network Security: Theory and Practice,*** USA: Springer.

7

Amaçlarımız

Bu üniteyi tamamladıktan sonra;

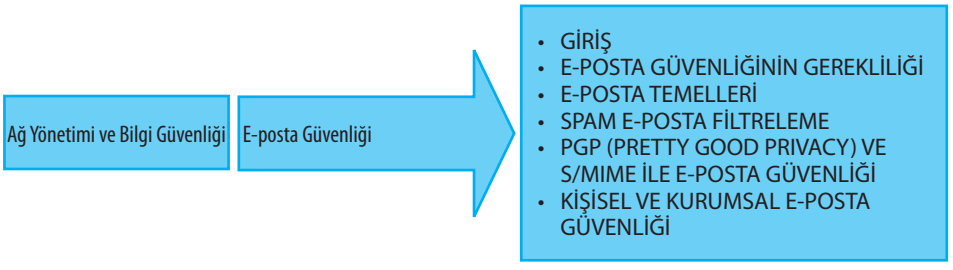
- E-posta güvenliği kavramını ve ihtiyacını açıklayabilecek,
- Sunucu tarafından spam e-posta yollanmasına neden olan güvenlik açıklarını betimleyecek,
- Spam filtrelerin temel çalışma prensiplerini açıklayabilecek,
- PGP e-posta aşamalarını açıklayabilecek,
- Temel e-posta güvenlik gereksinimlerini listeleyebilecek

bilgi ve becerilere sahip olacaksınız.

Anahtar Kavramlar

- SMTP
- SPAM
- SPF
- PGP
- Simetrik Anahtar
- Asimetrik Anahtar
- Özet Fonksiyon

İçindekiler



E-posta Güvenliği

GİRİŞ

İnsanoğlunun evrimini hızlandıran en önemli olgu, hiç şüphesiz iletişim ve bu iletişim esnasında paylaşılan bilginin birikimi ve kullanıma geçirilmesidir. Çağlar boyunca iletişimin şekli ve yöntemleri değişmekte, iletişimin önemi sürekli artmakta, gerek toplumsal gerek sosyal statüler, iletişim sonucu edinilen bilgi ve deneyimlere bağlı şekillenmektedir. Günümüz enformasyon çağında da durum değişmemiş aksine iletişim yöntemleri ve araçları günden güne katlanarak çeşitlenmiştir. Bilginin en önemli güç unsuru haline gelmesi, bilginin veriye dönüşümü ve bu verinin iki taraflı iletimi esnasında oluşabilecek güvenlik açıkları, kolaylıkla kötü niyetli üçüncü taraflarca kullanılabilmekte ve veriyi üretenle kullananlar için tehlike yaratmaktadır. İletişim ortamındaki veriye dönüşmüş bilgi, bir savaş zamanındaki stratejik bir karar veya bankalar arası bir ticaretin finansal kriterleri gibi kurumları veya devletleri etkileyen öneme sahip olabilir. Ancak iki kişi arasındaki günlük bir iletişimin içeriği de her iki uçta bulunanlar için kişisel öneme sahip olup, aynı güvenlik ölçütlerinin ve yöntemlerinin uygulanmasını gerekli kılmaktadır. Bir başka deyişle güvenlik ölçütleri ve buna bağlı önlemler kişiden veya kurumdan bağımsızdırlar. Zira e-postalarda paylaşılan iş hayatı, ilişki durumu, sağlık koşulları, finansal yapı gibi kişiye özel bilgilerin istenmeyen kişilerin eline geçmesi, kişilik haklarının ihlaline neden olabilecek sonuçlar doğurabilmektedir.

1971 yılında ilk e-posta denemesiyle ortaya çıkan ve günümüzün olmazsa olmaz iletişim biçimi olan e-posta, yaklaşık 40-50 yıllık bir süreç içerisinde hemen her bireyin yaşamının ayrılmaz parçası haline gelmiş ve daha önceki çoğu iletişim mekanizmalarının (mektup, teleks, telgraf, faks) öneminin azalmasına, hatta ortadan kalkmasına neden olmuştur. E-posta, alıcı ve gönderici tabanlı iki uçlu bir uygulama gibi gözükse de, verinin üretilip alıcıya ulaştığı noktaya kadar birçok protokol ve bu protokollerin desteklendiği ağ katmanları ve sunucular üzerinde koşan yazılımlarla bu altyapının sürekliliği sağlanmaktadır. Bu mekanizmanın herhangi bir noktasındaki güvenlik açığı ise kolaylıkla kötü amaçlı kullanıcıların, iletişimin şeklini ve içeriğini değiştirmesine neden olacağından bu ünitede hem kullanıcı, hem de sunucu tabanlı güvenlik açıklarına ve bunların önlenebilmesi için geliştirilen yöntemlere değinilecektir.

E-posta, uygulama tabanlı birçok protokol sayesinde gerçekleşebilmekte ve her protokol, kendi tanımlarını e-posta verisinin önüne ekleyerek çalışmaktadır. İşte bu aşamada her e-posta için bir üstbilgi de yaratılmakta ve mesaja eklenmektedir. Şekil 7.1'de hemen her gün karşılaşılan bir e-postanın üst bilgisi görülmektedir. Belki şu aşamada verilen üst bilgi içerisinde geçen ifadeler (Örneğin; "Received", "SMTP", "SPF", "sender") sizlere

bir şey ifade etmeyecektir ancak, ünitenin ilerleyen bölümleriyle bu ifadelerin ne anlama geldiğini göreceksiniz. Bu yüzden aynı üst bilgi, ünitenin ortalarında tekrar edilecektir. İşte bu sayede hem e-posta protokolünün temel noktalarını hem de buna bağlı güvenlik açıklarını irdelemek kolaylaşacaktır.

Şekil 7.1

Tipik bir e-posta üstbilgisi

```
Received: from edge3.anadolu.edu.tr (212.175.41.140) by
 casarray.anadolu.edu.tr (212.175.41.200) with Microsoft SMTP Server
(TLS) id 14.1.438.0; Tue, 6 Dec 2016 03:55:59 +0300
Received-SPF: Fail (edge3.anadolu.edu.tr: domain of admin@claims.org
does not designate 86.127.213.174 as
 permitted sender) identity=mailfrom; client-ip=86.127.213.174;
receiver=edge3.anadolu.edu.tr;
 envelope-from=”admin@claims.org”; x-sender=”admin@claims.org”;
 x-conformance=spf_only; x-record-type=”v=spf1”
Authentication-Results:  edge3.anadolu.edu.tr;  dkim=none  (message
not signed) header.i=none; spf=Fail smtp.mailfrom=admin@claims.org;
dmarc=fail (p=none dis=none) d=claims.org
```

Bir e-posta uygulaması kullanılarak (Örneğin; Outlook, Gmail vb.) oluşturulan bilgi, öncelikle bir e-posta servisine yönlendirilmekte ve bu e-posta servisi de ağ katmanları ve bunlara bağlı protokoller çerçevesinde veriyi, alıcının e-posta sunucusuna yollamaktadır. Alıcının çalıştırdığı posta uygulaması da bu posta sunucusunu belirli aralıklarla kontrol etmekte ve sunucuda yeni e-posta gördüğünde bunu kullanıcıya iletmektedir. E-posta iletişimi, gönderici ile alıcı sunucu arasında Basit Posta İletim Protokolü (Simple Mail Transfer Protocol – SMTP) ile tanımlanan protokol ile sağlanmaktadır. Alıcı taraftaki kullanıcılar da, Posta Ofisi Protokolü (Post Office Protocol 3 – POP3) veya İnternet Mesaj Erişim Protokolü (Internet Message Access Protocol – IMAP) gibi yaygın uygulama protokolleriyle mesajlarına ulaşabilmektedirler. İşte tüm bu protokoller arası ve ağ katmanları arası oluşabilecek güvenlik açıklarına karşı güvenlik önlemleri bu ünitenin konusunu oluşturmaktadır.

Başlangıçta, e-posta güvenliğinin temel kavramları tartışılacak ve günümüz e-posta altyapısından kaynaklanan tehditlere değinilecektir. Bu tehditlerin nasıl işlediğinin anlaşılabilmesi için de SMTP protokolünün irdelenmesi oldukça faydalı olacaktır. Böylece bu protokolün çalıştırıldığı, gerek uçlardaki istemciler, gerekse merkezdeki sunucularda ne tür güvenlik açıkları olduğu ve bunların kötü niyetli kullanıcılar tarafından nasıl istismar edildiği anlatılacaktır. Sunucularda oluşan güvenlik açıkları ve bunların giderilmesine yönelik bilgiler verilecektir. Bu bilgiler ışığında Şekil 7.1'de verilen e-posta üstbilgisini anlamak daha kolay olacaktır.

Ünitenin ilerleyen bölümlerinde uçtan uca en önemli e-posta güvenlik mantığını sunan Pretty Good Privacy (PGP) yapısı anlatılacaktır. Böylece bu ünite, bir anlamda tüm İnternet güvenliği kavramlarının pekişmesini sağlayacak bir platform gibi düşünülebilir. Zira iki taraflı güvenli iletişimin temel kavramları olan "veri şifrelemesi", "kimlik doğrulama", "mesaj bütünlüğü" ve "inkâr edememe" güvenlik servisleri PGP tarafından sağlanmakta ve PGP bu servislerin istendiğinde tümünü istendiğinde bir bölümünü içeren çözümler sunmaktadır.

Her ne kadar PGP uygulamaları sayesinde iki taraflı güvenli iletişim sağlansa da, e-posta güvenliği konuları içerisinde zararlı e-posta olarak nitelendirilebilecek taklit/oltalama e-postaları ve aldatmaca e-postalarına değinmek konu bütünlüğü açısından son derece önemlidir. Zira bu tip zararlı e-postalar, bilgisayar sistemlerinde önemli güvenlik açıkları yaratmakta ve arka kapılar oluşturarak DOS (Denial of Service) saldırı-

ları için sistemin hem kendisine hem de başka sistemlere tehdit oluşturmasına zemin hazırlamaktadır.

Güvenilir bir e-posta sisteminden bahsettiğimizde, güvenli e-posta uygulamaları gerekli şifreleme ve özet (hash) teknikleriyle veri ve kullanıcı bütünlüğünü korurken, sunucular kendi güvenlik önlemlerini almakta, sistemin kesintisiz ve güvenli çalışmasını sağlamaktadırlar. Ayrıca zararlı e-posta denilebilecek spam e-postalar, gerek sunucularda gerekse uygulama noktalarında yakalanabilmekte ve kullanıcıya ulaşmadan yok edilmektedir. Bu ünitede, tüm bu noktalara değinilecek ve günümüzde bir e-postanın güvenlik kavramları çerçevesindeki iletimi ve sürdürülebilir bir e-posta sisteminin sağlanabilmesi için zararlı mekanizmalarla nasıl savaşıldığı irdelenecektir.

E-POSTA GÜVENLİĞİNİN GEREKLİLİĞİ

Günümüzde bilgisayar virüslerinin ve bilgisayarlarda güvenlik açığı yaratacak "açık kapı", **"truva atı"** gibi zararlı program parçacıklarının çok büyük bir kısmı e-postalar aracılığıyla yayılmaktadır. E-posta her ne kadar sadece iki taraflı bir iletişim biçimi olsa da bu iletişimin yaygınlığı ve etkileşimi göz önünde bulundurulduğunda suiistimale oldukça yatkın bir ortam gözler önüne serilmektedir. E-posta güvenliğinin gerekliliklerinin anlaşılabilmesi ve açık noktaların doğru irdelenebilmesi için de olası tehditlerin ve bu tehdit unsurunu yaratacak profillerin iyi belirlenmesi şarttır. E-posta trafiğinde başlıca kötü niyetli kullanıcılar aşağıdaki şekilde gruplandırılabilir:

Truva Atı: Zararlı kodlar barındıran ve çoğunlukla kullanıcının iradesi dışında bilgisayarın işlem yapmasını sağlayan küçük boyutlu programlardır. Terim, adını Antik Yunan mitolojisinden almıştır. Truva atları kullanıcıya ilginç ve çoğunlukla işe yarar programlar içerisinde gönderilmekte ve bu program çalıştırıldığında zararlı program da çalışmaya başlamaktadır.

- **Spam e-posta üreticileri**: Spam e-posta terimi, temelde kullanıcıların istemi dışında kendi e-posta sunucularına gelen çoğunlukla reklam içerikli mesajlar için kullanılmaktadır. Spam mesajları, genelde aynı içeriğe sahip yüksek miktarlardaki kopyaların İnternet ortamına dağılması ve bu mesajı alma talebinde bulunmayan kişilere ulaşması sonucu İnternet trafiğinde sıkışma ve kullanıcı tarafında zaman kaybına yol açar. Spam e-posta üreticileri, daima kendi gerçek adreslerini gizlemek ve geri dönüşlere engel olmak istemektedirler. Bunun en temel nedenlerinden birisi yayımcıların milyonlarca e-posta adresini yasal veya yasa dışı yöntemlerle ele geçirmeleri ve gerçek olmayan kullanıcılara da mesajı göndermeleridir. Bu mesajların ilgili hedeflere teslim edilememesi durumunda, saldırganların kendilerine de çok miktarda "Teslim Edilemedi" bilgilendirme e-postası döneceğinden, e-posta sunucularında sorun yaşanması kaçınılmaz olacaktır.
- **Dolandırıcılar:** İnternet ortamı bir iletişim aracı olmaktan öte bir yaşam biçimi olmaya başladığından beri birçok kullanıcı kendi ticari faaliyetlerini çevrimiçi ortamlar üzerinden sürdürmektedirler. Paranın ve kazancın olduğu her ortam gibi bu iletişim mecrası da dolandırıcıların ağzını sulandırmakta ve tuzaklarına düşürdükleri kullanıcılardan tüzel kişi kılığında gerek maddi gerek manevi çıkar sağlamaktadırlar. Dolandırıcıların en temel isteği kendi gerçek kimliklerini saklamak ve karşısındaki kullanıcının açık noktalarını yakalayarak kendi çıkarları doğrultusunda kanunsuz yarar sağlamaktır.
- **Bilgisayar Solucanları:** Bilgisayar solucanları, kendilerini kopyalayarak başka bilgisayarlara yayılma işlevine sahip zararlı küçük boyutlu program parçacıklarıdır. E-posta aracılığıyla yayılabilmekte ve bilgisayarlarda açık kapıları keşfederek bilgisayarların güvenilirliğini tehdit etmektedirler. Ayrıca bu program parçacıkları büyük saldırılar için kullanılabilmekte ve İnternet trafiğinde sorun yaratabilmekte, yasal kullanıcıların işlerini yapmaları engellenebilmektedir. 2016 yılında Fransa'daki bir hizmet barındırma firmasına yapılan saldırıda anlık 1 Tb/s trafik ölçülmüştür. Yani solucanlarla yayılmış bir saldırı platformu harekete geçirilerek saniyede 1,000 Gigabit veri, ilgili firmanın sunucularını çalışamaz hale getirmiştir.

- **Oltacılar:** İnternet ortamında oltacılar diye adlandırılan kötü niyetli kullanıcılar başkalarının kullanıcı adı ve şifrelerini elde etmek üzere küçük program parçacıklarını veya kodlarını e-posta yoluyla dağıtmakta ve buna aldanan kişilerin şifrelerini elde etmektedirler. E-postalarda son derece kişisel bilgiler olduğundan bu tür hileler, genelde e-posta şifrelerini veya ticari değeri olan kullanıcı haklarını elde etmeye yönelik tehditler barındırmaktadır. Oltacılar, kendi kimliklerini gizleyerek farklı yasal bir karaktere bürünmeyi amaçlamakta ve amaçlarına uygun çok yüksek miktarda e-posta üreterek kullanıcılara yollamaktadır. Temel amaç, olabildiğince fazla sayıda bilinçsiz e-posta kullanıcısına ulaşarak bilgilerini ele geçirmektir.

Tüm bu tehdit unsuru profillerin en önemli ortak noktası, hiç şüphesiz, tanınırlığın olabildiğince engellenmesi ve olabildiğince yüksek miktarda tehdit unsuru barındıran yasa dışı e-postanın İnternet ortamına sunulmasıdır. Bir başka deyişle kötü niyetli e-posta kullanıcıları hem kendilerini gizlemeyi hem de olabildiğince çok kullanıcıya ulaşmayı amaç edinmekte ve tüm İnternet kaynaklarını bu amaçlar için kullanmaktadırlar.

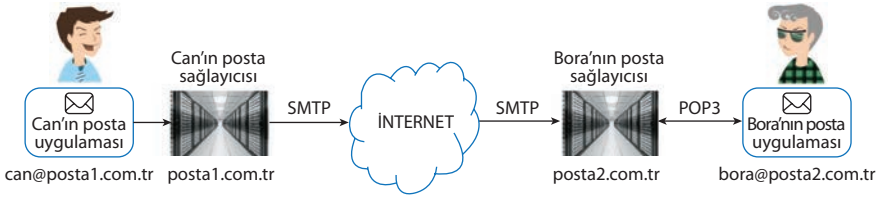
E-POSTA TEMELLERİ

Günümüz İnternet altyapısı açık bir ağ sistemi olup yasal ancak hile barındırabilecek her türlü iletişimin sağlanabildiği bir platformdur. Böylesi açık bir platformda gönderici ve alıcı arasında bir e-posta güvenliğinden bahsedebilmek için bir e-postanın göndericiden alıcıya nasıl ulaştığını anlamak ve bu iletişim esnasında oluşabilecek güvenlik açıklarını irdelemek konu bütünlüğü için son derece gereklidir. Giriş bölümünde bahsedildiği üzere e-posta, iki kullanıcı arasında gerçekleşen bir iletişim yapısı sunmaktadır. Bu mekanizmayı anlayabilmek için yasal bir e-posta hesabına sahip alıcı ve gönderici kullanıcılar olan Can ile Bora arasında bir e-posta iletişimi kurgulansın. Can'ın gönderdiği e-postanın Bora'ya ulaşması senaryosuna göz atalım.

Can, Bora'ya bir e-posta yollamak istediğinde hem kendisinin bir e-posta adresine sahip olması hem de Bora'nın e-posta adresini bilmesi gerekir. Can'ın bir e-posta adresi yoksa Hotmail, Gmail, Yahoo! veya Anadolu Üniversitesi gibi bir e-posta sağlayıcısından kendisine geçerli bir e-posta adresi temin etmesi gerekir. Can kendisine **can@posta1.com.tr** e-posta adresini alır. Burada **posta1.com.tr** Can'ın postalarının tutulacağı veya Can'ın Bora'ya gönderdiği e-postaların İnternet ağına çıkacağı e-posta sunucusunu tanımlamaktadır. Can başlangıçta bir e-posta uygulaması kullanarak posta metnini hazırlar ve alıcı adresine Bora'nın e-posta adresini (**bora@posta2.com.tr**) yazarak metni yollar. Can ve Bora arasındaki e-posta iletişimi Şekil 7.2'de sunulmaktadır.

Şekil 7.2

Can Bora'ya bir e-posta yollar



Can'ın kullandığı e-posta uygulaması sayesinde posta, Can'ın posta sağlayıcısına ulaşır ve diğer kullanıcılardan gelen postaların olduğu kuyruğa girer. Burada **posta1.com.tr** posta sunucusu Can'ın postasını SMTP (Simple Mail Transfer Protocol) ile şekillendirir ve **posta2.com.tr** posta sunucusuyla bir TCP (Transmission Control Protocol) bağlantısı kurar. TCP ile yollanan SMTP mesajı **posta2.com.tr** sunucusunda depolanır. Bora'nın posta uygulaması bu sunucuyla bağlantı kurar ve gelen postayı sunucudan alır. Burada POP3 (Post Office Protocol 3) kullanılabileceği gibi IMAP (Internet Message Access Protocol) de postanın sunucudan alınıp okunmasını sağlamaktadır.

Can ile Bora'nın iletişimi esnasında tüm güvenlik gereksinimlerinin posta sunucuları tarafından sağlanması bir seçenek olabilir. Yani posta1 sunucusu posta2 sunucusuyla güvenli bir bağlantı kurabilir ve bu iletişim esnasında üçüncü şahısların bu haberleşmede kulak misafiri olması engellenebilir. Zaten bu da günümüz posta sunucularının sağladığı bir yöntem olarak karşımıza çıkmaktadır. Ancak bilginin öneminin gittikçe arttığı günümüzde Can tarafından şifrelenmemiş bir mesajın posta1 sunucusuna kadar iletişimi esnasında oluşabilecek bir güvenlik açığı iletişimi riske atabilir. Ayrıca gönderilen bilgi posta1 sunucusu tarafından güvenlik önlemleri doğrultusunda şifrelenmiş olsa bile Can'ın posta1 sunucusuna ne ölçüde güvenmesi gerektiği tartışma konusudur.

Bireysel güvenlik ihlalleri ortaya çıkabileceği gibi, hiç şüphesiz, e-posta sunucularının da karşılaştığı önemli başka güvenlik sorunları vardır. Bunlardan en önemlisi, posta sunucularının kötü amaçlı kullanıcılar ve spam mesaj üreticilerine bilmeden aracılık ediyor olmalarıdır. Bu güvenlik açığı, SMTP açık yönlendirme desteği olan posta sunucularında görülmektedir. Bu zafiyetin anlaşılabilmesi için SMTP protokolüne değinmek faydalı olacaktır.

SMTP Protokolü

SMTP protokolü, 1982 yılında e-posta haberleşmesini sağlamak için tasarlanmış ve adının da çağrıştırdığı gibi oldukça basit bir protokoldür. Bu protokolde tüm iletişim, ASCII temelli komutlar sayesinde gerçekleşir. Can'ın e-posta uygulaması SMTP istemci, e-posta sağlayıcısı da sunucu görevi üstlenmiştir. İstemciler SMTP sunucuyla **TCP** 25 numaralı portu kullanılarak iletişime geçilebilmektedir.

İnternet'te iletişim **TCP/IP** temelli beş katmanlı bir yapı içerisinde gerçekleşmektedir. İstemci/sunucular kendilerine özgü tanımlanmış IP adresleriyle iletişim kurarlar. Bu adreslerde İnternet ağına ulaşmak isteyen her program farklı bir tanımlayıcıya ihtiyaç duymaktadır. Port, bir IP adresi üzerinde farklı iletişim diyaloglarının ayrılması için kullanılan 0 ile 65.535 arasında sayıdır.

Aşağıda tipik bir SMTP bağlantısı ve diyalog görülmektedir. Burada İ: istemci S: SMTP sunucusunu ifade etmektedir.

```
S: 220 posta1.com.tr
İ: HELO posta1.com.tr
S: 250 Hello posta1.com.tr pleased to meet you
İ: MAIL FROM: <can@posta1.com.tr>
S: 250 can@posta1.com.tr ... sender ok
İ: RCPT TO: <bora@posta2.com.tr>
S: 250 can@posta1.com.tr ... recepient ok
İ: DATA
S: 354 Enter mail, end with "." on a line by itself
İ: Bora sinemaya gidelim mi?
İ: Saat 19.00 seansında indirim var
İ: .
S: 250 Message accepted for delivery
İ: QUIT
S: 221 posta1.com.tr closing connection
```

Bu diyalogdan anlaşılacağı üzere istemci TCP 25 numaralı portu kullanarak bir SMTP sunucusu ile iletişime geçebilir ve istediği şekilde e-posta oluşturup yollayabilir. Burada MAIL FROM komutundan sonra yazılacak adres, göndericinin adresi olarak belirecek ve alıcı, ilgili adresten bir e-posta aldığını anlayacaktır. Yukarıdaki örnekte Can ile Bora arasında bir e-posta iletişimi sağlanmıştır. Bora e-posta kutusunda gördüğü postanın Can'dan geldiğini anlayabilir. Can'ın e-posta sunucusuyla Bora'nın e-posta sunucusu da birbirleriyle TCP 25 portu üzerinden haberleşmektedirler. Bir başka deyişle TCP 25 numaralı portu SMTP posta iletişimi için hem kullanıcıların hem de sunucuların kullandıkları porttur. TCP 25 numaralı portu kullanan tüm SMTP uygulamalarında, gerek istemci gerek sunucu, hiçbir güvenlik sorgulaması beklenmez. Eğer sunucu tarafı TCP 25 numa-

ralı portu destekleyen SMTP haberleşmeye açık bir sistem sunuyorsa, her istemci bu port üzerinden rahatlıkla SMTP mesajı üretebilir ve istediği adrese bu mesajları gönderebilir.

Bir Güvenlik Açığı: SMTP Geçiş (SMTP Relaying)

Spam e-postaların, kullanıcının isteği ve iradesi dışında gelen ve genelde reklam içerikli e-postalar olduğundan bahsedilmişti. Ayrıca spam e-postalar, içerisinde kötü amaçlı yazılımları da barındırabilmektedir. Bu tip e-postalar bazen bilgisayarın, kullanıcısının iradesi dışında işlemler yapmasına neden olurken, bazen de kullanıcının kişisel verilerinin ele geçmesini sağlayan arka kapıları açan program parçacıklarını da bilgisayarlara yerleştirmektedir. Spam e-posta oluşturma ve dağıtımı, bilgisayar korsanlarının ve e-ticaret firmalarının en çok kullandıkları yöntemlerden biridir. Spam e-posta üreticisinin en önemli isteği de kendini gizlemektir. Peki, bu işlem nasıl gerçekleştirilmektedir? En basit şekliyle bir spam e-posta yollayıcısı kaynak adrese kendi adresini yazmayarak Can'ın adresini yazabilir ve istediği tür bir mesajı, reklamı veya kötü amaçlı bir yazılımı rahatlıkla Bora'ya yollayabilir. Böylece Bora yine Can'dan bir e-posta geldiğini zannederek kötü amaçlı kullanıcının e-postası ile karşılaşacaktır. Bu yöntem "SMTP geçişi" olarak adlandırılmaktadır. Yakın zamana kadar spam e-posta üreticileri için bu yöntem vazgeçilmez olmuştur ve spam e-postaların yayılması için hemen her e-posta sunucusu SMTP geçişine bilmeyerek aracılık etmiştir.

SMTP geçişini bir örnekle açıklayalım. Bir SMTP e-posta sunucusu TCP 25 numaralı port ile kendisine bağlanan bir uygulama tarafından SMTP kurallarına uygun komutlarla oluşturulmuş veri alırsa, ilgili e-postayı İnternet ortamına yollamakta ve alıcı sunucular da bu e-postaları gerçek alıcılarına ulaştırmaktadırlar. Reklam amaçlı e-postalar yaratan Vampir adlı kullanıcının Bora'ya aşağıdaki şekilde hazırlanmış bir e-posta gönderdiğini düşünelim.

```
S: 220 posta1.com.tr
İ: HELO posta1.com.tr
S: 250 Hello posta1.com.tr pleased to meet you
İ: MAIL FROM: <can@posta1.com.tr>
S: 250 can@posta1.com.tr ... sender ok
İ: RCPT TO: <bora@posta2.com.tr>
S: 250 can@posta1.com.tr ... recepient ok
İ: DATA
S: 354 Enter mail, end with "." on a line by itself
İ: Bora yeni çıkan Vampir markalı çikolatadan mutlaka yemelisin
İ: .
S: 250 Message accepted for delivery
İ: QUIT
S: 221 posta1.com.tr closing connection
```

Yukarıdaki örnekte oluşturulan e-posta Bora'ya ulaştığında, Bora bu e-postanın Can'dan geldiğini sanacak ve içinde Vampir marka çikolatadan yemesinin iyi olacağı şeklinde bir mesajla karşılaşacaktır. İşte, her türlü e-posta mesajını nereden geldiğine bakmaksızın işleyerek alıcıya yönlendiren posta1.com.tr sunucusu SMTP geçişi yapmaktadır. Bir başka deyişle, isteyen her spam e-posta üreticisi posta1.com.tr sunucusunu kullanarak istediği kadar e-postayı istediği kimselere gönderebilmektedir. Buna izin verildiği ölçüde spam e-postaların sayısı çoğalmakta, ağ trafiği artmakta ve kullanıcılara yönelen tehditler ve reklam bombardımanı nedeniyle kullanıcıların siber güvenliği tehlikeye atılmaktadır.

Spam üreticilerinin en temel korkusu tanınmaktır. Spam e-postaları gönderen kötü niyetli kullanıcılar kendilerini gizlemek ve yolladıkları e-postaların gerçek bir kullanıcıdan geldiği izlenimini vermek isteyeceklerdir. Bu hedefi sağladıkları ölçüde spam e-postaları alan kullanıcılar, sanki gerçek kişilerden geliyormuşçasına, bu e-postaları açacaklar ve hatta içlerindeki zararlı kodları da çalıştıracaklardır.

Yasal bir e-posta trafiği için SMTP geçişinin kesinlikle engellenmesi gerekmektedir. Bu nedenle hemen tüm e-posta sunucuları SMTP geçişin önünü kesmektedir. SMTP geçişin nasıl engellenebileceğini sorguladığınızda çok büyük bir olasılıkla çözümü de bulabileceksiniz. SMTP geçişe izin veren sunucular (Örneğin, posta1.com.tr veya posta2.com.tr sunucuları) sıklıkla ürettikleri yasa dışı trafik sebebiyle İnternet ortamında kolaylıkla tanınmaya başlanmakta ve bu sunuculardan gelen e-postalara güven azalmaktadır. Bir başka deyişle, bu sunucular diğer sunucuların oluşturduğu kara listeye girmektedir. Kara listeye giren sunucuların da ticari itibarları günden güne azalmaktadır. SMTP geçişi, bir e-posta sunucusunda tanımlı olmayan kullanıcıların başvurduğu bir yöntemdir. Spam e-posta tasarlayanlar veya bilgisayarlara bulaşmış spam e-posta yollayan virüsler kendi kayıtlı oldukları e-posta sağlayıcılarının sunucularını kullandıkları takdirde ürettikleri trafik ve içerik yüzünden hemen fark edilecekler ve çok güvendikleri tanınmazlık profilini kaybedeceklerdir. İşte bu temel noktadan yola çıkıldığında, her SMTP e-posta sunucusu yalnızca kendisine kayıtlı kullanıcılarına hizmet verir ve diğer tüm istekleri reddederse SMTP geçişi engellenebilir.

SMTP portu için uzun zamandır yeni bir standart belirlenmiş olup, TCP 25 numaralı port yerine genelde tüm iletişimde TCP 587 numaralı port kullanılmaktadır. Bu port üzerinden iletişim kuran bir uygulamadan kimlik denetimi istenmekte ve kimlik bilgileri şifrelenerek iletilmektedir. Sunucu, TCP 25 numaralı portu kullanan bir SMTP isteği ile karşılaşırsa, bu isteği yanıtsız bırakmaktadır. Yalnızca TCP 587 numaralı portu kullanan isteklere cevap vermektedir. Bu iletişim için şifreli bir haberleşme altyapısı kullanılmakta ve kullanıcılardan kullanıcı adı ve şifre talep edilmektedir. Eğer kullanıcı adı ve şifre, servis listesinde bulunan kullanıcı adı ve şifre ile örtüşmezse, ilgili kullanıcının istemi gerçekleştirilmemektedir. Bu durumda e-posta SMTP protokolü çerçevesinde doğru kodlanmış da olsa, alıcısına ulaştırılmak üzere İnternet ağına yönlendirilmemektedir.

Google firması tarafından sunulan e-posta hizmetleri için smtp.gmail.com adresi kullanılmaktadır. Windows komut satırı kullanarak SMTP portu üzerinden smtp.gmail.com adresine bağlanabilir misiniz? Bu bağlantıda TCP 25 ve TCP 587 numaralı portlar kullanıldığında nasıl bir geri dönüş olacaktır?

SIRA SİZDE 1

Türkiye'deki en geniş kapsamlı ağ işletim altyapısını elinde bulunduran Türk Telekom, ülkemiz kaynaklı yüksek oranda üretilen spam e-postanın önüne geçebilmek ve kötücül trafiği azaltmak üzere TCP 25 numaralı portu kullanan istemci paketlerini engellemektedir. Artık TCP 25 numaralı SMTP portunun kullanılması hemen hemen olanaksızdır. Ancak e-iletişim teknolojilerindeki en önemli gerçeklerden birisi, uygulanan her türlü kısıtın ve güvenlik engelinin üzerinden aşılacak teknolojinin kısa zamanda yaratılabilmesidir. Bu iki taraflı hırsız polis tarzı engel koyma ve engel kırma programcılığı bir yandan iletişim teknolojilerinin çok büyük bir devingenlikle gelişimini sağlamakta, bir yandan da İnternet güvenliği ve regülasyonları gibi iş sahalarının açılmasına neden olmaktadır.

Gönderen Teyit Politikası (Sender Policy Framework – SPF)

E-posta gönderici sunucularında geçiş engellemesi oldukça önemli bir güvenlik önlemi olup, spam e-posta trafiğini bir ölçüde rahatlatmıştır. Ancak sadece spam trafiği üretebilmek için kurulmuş bir e-posta sunucusu, hiç şüphesiz kendisi üzerinden bu trafiğe izin verecek ve her türlü e-postanın dağıtımı için oldukça kullanışlı bir kaynak olacaktır. Bu spam kaynağının da, hiçbir önlem alınmadığı durumda belirlenmesi son derece güçtür. Böylesi bir trafiğin de önünün kesilmesi ancak farklı bir yaklaşımı ve korunma mekanizmasının üretilmesini gerekli kılmıştır. Gönderen Teyit Politikası (Sender Policy Framework – SPF) bu bağlamda ortaya çıkmıştır.

SPF bir açık standart olup gönderici adresinin yasal olmayan yolla kullanımının önüne geçilmesi için üretilmiş bir çözümdür. Halen SPF sürüm 1 kullanımdadır. Bu yöntem, göndericinin mesaj gönderdiği etki alanının yetkili bir etki alanı olduğunu betimlemekte ve yetkisiz etki alanlarından gelen e-postaların doğrudan çöpe atılmasını sağlamaktadır. Bu koruma mekanizmasının tam olarak anlaşılabilmesi için TCP/IP tabanlı bir ağ ortamında veri paketlerinin oluşturulması ve yönlendirilmesinde büyük öneme sahip etki alanı kavramına değinmek konu bütünlüğü açısından yararlı olacaktır.

İnternet, uçtan uca paket trafiğinin protokollerinin ve mekanizmalarının tanımlandığı bir iletişim ortamıdır. Her iletişim noktasının kendine ait tekil bir IP adresi bulunmaktadır. Bu IP adresleri aslında etki alanları bağlamında tanımlanmış özel adreslerdir. Temel olarak İnternet, etki alanları iletişimidir denebilir. Ev kullanıcısı kendi İnternet sağlayıcısının tanımladığı etki alanı ile iletişime geçerken, Anadolu Üniversitesi tarafından sağlanan İnternet bağlantısını kullanan bir öğrenci Anadolu Üniversitesi'nin etki alanını kullanarak e-posta üretip gönderebilmektedir. Tüm bu etki alanları, Alan Adı Sistemi (Domain Name System – DNS) kayıtları vasıtasıyla birbirleriyle iletişim halindedir. Etki alanı sorgulaması, e-posta göndericisinin veya SMTP sunucusunun yasal bir e-posta göndericisi olup olmadığını belirlemede kullanılabilir.

Şekil 7.3

Anadolu Üniversitesi etki alanı SPF kayıtları

```
v=spf1 include:spf.anadolu.edu.tr include:spf.protection.outlook.com include:sharepointonline.com -all
```

Gönderici, bir e-posta oluşturduğu zaman, bu e-postayı mutlaka bir etki alanı içerisinden göndermesi gerekmektedir. Eğer etki alanı sunucularına ilgili etki alanlarından SMTP kullanarak e-posta göndermeye yetkili sunucular tanıtılırsa, bu sunucular dışında SMTP mesajı üreten tüm sunucuların mesajları spam olarak etiketlenebilir. Bir başka deyişle, SPF bir etki alanı içerisinde yetkili SMTP göndericilerini tanımlamaktadır ve gönderici kısmında yetkilendirilmemiş bir etki alanı adresine rastlandığında, ilgili e-posta spam olarak değerlendirilmektedir. Etki alanı içerisinde bu kayıtlar genelde TXT kayıtları olarak saklanmaktadır. Bu koruma yönteminde "FROM" adresi, yani göndericinin adresi, başlangıçta bir SMTP diyalog içerisinde yollanır. Eğer sunucu bu mesajın etki alanını kabul etmezse, istemci tarafa ret mesajı gelir. Öte yandan sunucu, TXT dosyalarını kontrol edip "FROM" kısmında yazılan etki alanının kayıtlar içerisinde izin verilen bir etki alanı olduğunu teyit ederse, mesajın geri kalan kısımları da kabul edilir. Daha sonra, e-postanın gönderilen adrese ulaşmaması durumunda gön-

dericiye uyarı mesajı sağlanabilmesi amacıyla geri dönüş adresine de "FROM" kısmında yazılan adres kopyalanmaktadır. Bu sayede bir spam üreticisi farklı bir etki alanına ait geri dönüş adresi ile bir e-posta ürettiği takdirde, SPF kullanan sistem tarafından kolaylıkla reddedilecektir. Şekil 7.3 içerisinde Anadolu Üniversitesi'nin TXT dosyası görülmektedir.

Şekil 7.3 içerisindeki kayıt incelendiğinde:

- **v=spf1**: SPF sürüm bilgisini ifade etmektedir. Burada SPF sürüm 1 kullanılmaktadır.
- **include:spf.anadolu.edu.tr**: Yetkilendirilmiş sunucu olan spf.anadolu.edu.tr sunucusu ile gönderilen SMTP dosyaları kabul edilmektedir.
- **include:spf.protection.outlook.com**: Yetkilendirilmiş sunucu olan spf.protection.outlook.com sunucusu ile gönderilen SMTP dosyaları kabul edilmektedir.
- **include:sharepointonline.com:** Yetkilendirilmiş sunucu olan sharepointonline.com sunucusu ile gönderilen SMTP dosyaları kabul edilmektedir.
- **-all:** Yukarıda belirlenen yetkilendirilmiş sunucular dışındaki tüm sunucuların bu etki alanından e-posta gönderme yetkileri kaldırılmıştır.

Yetkilendirilmiş sunucular ayrıca bir MX sorgusuyla listelendiği takdirde TXT kaydı içerisinde görülen sunucular Şekil 7.4. ile gösterilmektedir. Burada "Pass" "+" olarak görülen sunucular izin verilen sunucu listelerini, "Fail" "–" olarak görülen sunucular ise izin verilmeyen sunucuları göstermektedir. Bunlardan başka, kayıtlarda "SoftFail" "~" olarak görünen sunuculardan gelen mesajlar ise gelen kutusuna iletilecek ancak spam olarak değerlendirilecektir. Şekil 7.4'de anadolu.edu.tr, Şekil 7.5'de ise "google.com" etki alanı SPF kayıtları sorgulanması sonucu oluşan tablolar gösterilmektedir.

Şekil 7.4

MX sorgusu sonucu Anadolu Üniversitesi etki alanı SPF kayıtları

Prefix	Type	Value	PrefixDesc	Description
v	version	spf1		The SPF record version
+	include	spf.anadolu.edu.tr	Pass	The specified domain is searched for an 'allow'.
+	include	spf.protection.outlook.com	Pass	The specified domain is searched for an 'allow'.
+	include	sharepointonline.com	Pass	The specified domain is searched for an 'allow'.
-	all		Fail	Always matches. It goes at the end of your record.

Şekil 7.5

MX sorgusu sonucu Google.com etki alanı SPF kayıtları

Prefix	Type	Value	PrefixDesc	Description
v	version	spf1		The SPF record version
+	include	_spf.google.com	Pass	The specified domain is searched for an 'allow'.
~	all		SoftFail	Always matches. It goes at the end of your record.

Siz de merak ettiğiniz bir SMTP sunucusu için SPF sorgulaması yapabilirsiniz. Örnek olarak http://mxtoolbox.com adresine giderek Hotmail.com SPF kayıtlarını sorgulayınız ve çıkan tabloları yorumlayınız.

İNTERNET

SPAM E-POSTA FİLTRELEME

SMTP sunucuları, SMTP geçişini engelledikleri ölçüde spam trafiğinin bir kısmının önünü kesmektedirler. Ancak spam e-postalar sadece SMTP geçişe izin veren sunucularla yayılmazlar. Kötü niyetli kullanıcılar kendi e-posta sunucularını sistemlere tanımlayıp bu sunucular üzerinden spam e-postalar yayabilmektedirler. Bunların da önüne SPF filtreleme ile geçilmektedir. Ancak yine de tümüyle spam e-postalardan kurtulmak mümkün olmamaktadır. Yasal sunuculardan da spam e-posta yaymak olasıdır. Böylesi bir sunucu, trafiğin el verdiği ölçüde, gerek reklam içeren metinleri gerekse başka spam e-posta üretebilecek programları veya bilgisayarlarda arka kapı oluşturabilecek zararlı kodları e-postalara ekleyip alıcılara yollamaktadır. Hemen herkesi bir şekilde zaman ve bazen de veri kaybına uğratan bu gereksiz e-postalarla başa çıkmanın bir yolu da, bu tip e-postaları sezebilme yeteneğine sahip programlar kullanmaktır. Bu tür programlara Spam engelleyici/yok edici programlar denmekte ve bunlar hem sunucularda hem de istemcilerde çalışmaktadırlar.

Spam engelleyiciler genelde istatistiksel yöntemler kullanmaktadır. Ancak spam karakteristiklerinin sürekli değişmesi ve yakalanmaya karşı yeni metotlar ortaya çıkması sonucu bu algoritmalar da öğrenebilme ve adapte olabilme yeteneğine sahip olmalıdırlar. Bu algoritmalar, e-postaların içeriğine ve üstbilgilerine bakarak ve kullanıcıların tepkilerini dikkate alarak her e-postaya belirli bir aralıkta puan vermektedirler. Bu puanlamada belirli bir seviyenin üzerine çıkan e-postalar spam olarak damgalanıp, kullanıcının etkileşiminden çıkarılmaktadırlar. Spam e-posta filtreleme algoritmaları bir e-posta için spam kararı verince, genellikle bu e-postayı silmek yerine kullanıcının gözü önünden kaldırmaktadırlar. Zira ne kadar gelişkin bir algoritma kullanılırsa kullanılsın, küçük de olsa hata payı vardır. Temelde iki tip hata görülmektedir:

1. Yanlış Pozitif Hata: Gerçekte spam olmayan e-postaya spam kararı vermek anlamına gelir ve oldukça kritik hatalar olup veri kaybına neden olabilmektedir.
2. Yanlış Negatif Hata: Gerçekte spam olan e-postaya spam-değil kararı vermek anlamına gelir. Birçok kontrolden geçmeyi başararak kullanıcıya ulaşan bu tür spam e-postalar genel olarak pek zararlı değildir ve sadece kullanıcının zaman kaybına neden olmaktadır.

Yanlış Negatif ve Yanlış Pozitif hata oranları spam filtrelerin güvenilirliği için önemli parametrelerdir. Her ne kadar az rastlansa da, her e-posta kullanıcısının geçmişte beklediği bir e-postanın spam damgası yediği ve ilgili e-postaya ulaşamadığı olmuştur. Bu durumda kullanıcının mağduriyetinin önüne geçmek için tüm spam damgası yiyen e-postalar silinmeden önce belirli bir klasörde depolanmaktadır ve bu klasör de kullanıcının her an kontrol edebileceği biçimde etkileşime sokulmaktadır. Bu mekanizma Yanlış Pozitif hataların kullanıcıları ciddi biçimde etkilememesi için düşünülmüştür. Google, Hotmail, Yahoo! vb. e-posta sunucularında mutlaka bir spam klasörü bulunmakta ve ara sıra kullanıcıların bu klasörleri kontrol etmesi gerektiği vurgulanmaktadır.

Bu ünite kapsamında bir spam engelleyici programın tüm detaylarıyla nasıl çalıştığını incelemeye çok gerek olmamakla beraber basit birkaç noktaya değinilerek, bir spam engelleyici programın çalışma prensiplerinin nasıl şekillendiğini anlamak faydalı olacaktır. Her normal e-posta gibi spam e-postanın da kendine göre belli başlı tanımlayıcıları vardır. Örneğin, reklam amaçlı e-postalar Amerika kıtasında bulunan bir etki alanındaki sunucudan gönderildiğinde, e-postanın varış zamanı Türkiye içinden gönderilen e-postalardan

farklı olmaktadır. Ayrıca postaların içerisinde çokça kullanılan ticari terimler, konu başlığı, gönderenin adresi de teker teker kontrol edilerek daha önceki spam e-postalarla aynı karakteristiğe sahip özelliklerle karşılaştırılmaktadır. Şekil 7.6'da bir e-postanın üstbilgisi görülmektedir (aynı üstbilgi ünitenin başında da verilmişti). Bu üst bilgi incelendiğinde mesajın claims.org etki alanından geldiği ve mesaj saatinin 03.55 olduğu görülmektedir. Ayrıca bu üstbilgi SPF kayıtlarını da içermektedir. Burada SPF kayıtlarından FAIL (geçemedi) bilgisi görülmektedir.

Siz de size gelen bir e-postanın üstbilgisinin nasıl açılacağını öğrenerek bu üstbilgi bölümünde ne tür bilgiler olduğuna bakın.

İNTERNET

Şekil 7.6

Tipik bir e-posta üstbilgisi

```
Received: from edge3.anadolu.edu.tr (212.175.41.140) by
 casarray.anadolu.edu.tr (212.175.41.200) with Microsoft SMTP
Server (TLS) id 14.1.438.0; Tue, 6 Dec 2016 03:55:59 +0300
Received-SPF: Fail (edge3.anadolu.edu.tr: domain of admin@claims.
org does not designate 86.127.213.174 as
 permitted sender) identity=mailfrom; client-ip=86.127.213.174;
receiver=edge3.anadolu.edu.tr;
 envelope-from="admin@claims.org"; x-sender="admin@claims.org";
x-conformance=spf_only;
 x-record-type="v=spf1"
Authentication-Results: edge3.anadolu.edu.tr; dkim=none (message
not signed) header.i=none; spf=Fail smtp.mailfrom=admin@claims.org;
dmarc=fail (p=none dis=none) d=claims.org
```

Spam e-posta filtreleme tekniklerinde en çok başvurulan yöntemlerden birisi de, gerek reklam amaçlı gerek kötü niyetli oluşturulan e-postaların başlıklarında bulunabilecek ortak karakteristik özellikler veya e-postalar içerisinde sıkça tekrarlanan kelimelerin kontrol edilmesidir. Örneğin bir alıcıya gelen postalar içerisinde "ucuz", "avantaj" vb. sıkça rastlanan ifadeler değerlendirilerek bir spam katsayısı çıkartılabilir. Bu katsayı kullanıcının da belirleyebileceği bir limitin üzerine çıkarsa, gelen e-posta spam olarak nitelendirilir ve genelde silinmeden özel bir klasör içerisine kopyalanır. Kullanıcı istediği takdirde bu klasöre göz atarak olası yanlışlıkların önüne geçebilir.

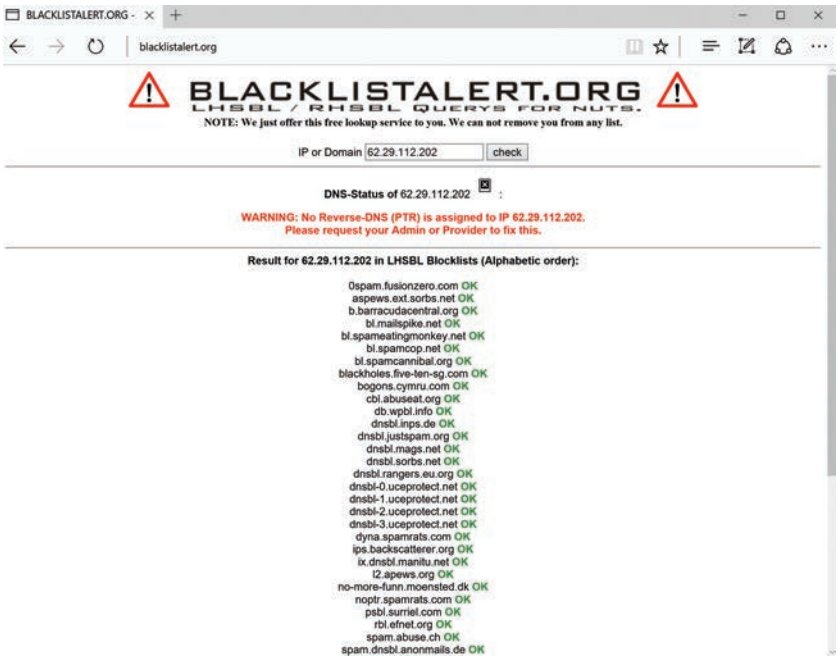
Bir önceki bölümde belirtildiği üzere spam e-postalar genelde belli başlı SMTP sunucular vasıtasıyla yayılmaktadır. Bu e-postalardan ve üretilen trafikten zarar gören gerçek kullanıcılar ve bunlara hizmet veren servis sağlayıcıları, gelen yüksek miktardaki spam e-postanın nereden geldiğine bakarak ilgili adresleri kara liste adı altında sınıflandırmaktadırlar. Eğer bir SMTP sunucu kara listeye girmişse, bu sunucunun ürettiği paketler genelde içeriğine bakılmaksızın diğer sunucular tarafından spam olarak değerlendirilmektedir. Günümüz İnternet trafiğinde kara listeler son derece önemlidir. Birçok yetkili kuruluş bu listeleri hem güncellemekte hem de içeriklerinin geliştirilmesi için çalışmaktadır. Şekil 7.7'de bir alanın kara liste taraması sonucu gösterilmiştir.

Kara liste İngilizce "blacklist" olarak adlandırılmaktadır. İnternette bir araştırma yapınız ve şu anda kullanmakta olduğunuz e-posta sunucusunun kara listede olup olmadığını kontrol ediniz.

İNTERNET

Şekil 7.7

62.29.112.202 IP adresi ile yapılan bir kara liste sorgulaması.



PGP (PRETTY GOOD PRIVACY) VE S/MIME İLE E-POSTA GÜVENLİĞİ

Ünitenin şimdiye kadar olan bölümünde e-posta güvenliği kapsamında kullanıcıların gerek zaman gerek veri kaybıyla sonuçlanması muhtemel spam e-posta sorununa karşı alınabilecek önlemlerden bahsedilmiştir. Bu kapsamda SMTP sunucularında olası engelleme yöntemleri üzerinde durulmuştur. Ayrıca dünya çapında oluşturulan proaktif mücadeleye yardımı dokunabilecek, yoğun spam e-posta adreslerinin listelerinin tutulmasının bu mücadelede etkin bir rol oynayacağından bahsedilmiştir. Ancak e-postanın temel varoluş nedeni kullanıcıların ürettikleri mesajları ve paylaşmak istedikleri verileri, alıcı tarafa sorunsuz iletebilmeleri ve bu iletişim esnasında gerek gönderici gerekse de alıcı açısından paylaşılan bilginin bir başkası tarafından değiştirilmemiş olmasına duyulan güvendir. Ayrıca bazı yazışmalarda sadece verinin korunması değil, bu verinin gizlenmesi de önemli bir gereklilik olabilir. Kullanıcıların e-posta sistemini kullanabilmeleri için güven duymaya ihtiyaçları vardır. Temel ihtiyaç ve hak olan mahremiyetin iletişimde önemi yadsınamaz.

İnternet'in günümüzdeki yaygın kullanımının bir hayal olduğu ve e-posta iletişiminin daha emekleme aşamasındaki zamanlarda güven kavramıyla sadece verinin kaybolmadan göndericiden alıcıya ulaşması anlaşılmaktaydı. Bu yüzden SMTP protokolü tanımlanırken gönderilecek postanın sadece ASCII karakterlerden oluşması ve bu verinin göndericiden alıcıya kayıpsız ulaşması planlanmıştı. Ancak iletişimin bu hızlı devinimi ve İnternet'in yaşamın vazgeçilmezi olmasıyla birlikte elektronik veri iletişimi, bireylerin tüm özel yaşamsal bilgilerinin taşındığı bir ortam haline gelmiştir. Dolayısıyla başlangıçta tanımlanan, sadece verinin doğru biçimde iletiminin sağlandığı güven kavramının boyutu ve kapsamı da genişlemek ve değişmek zorunda kalmıştır. Güven kavramının içerisine gizlilik, kimlik doğrulama, mesaj bütünlüğü, inkâr edilememe gibi kavramlar da dâhil olmuştur.

İngilizce "Pretty Good Privacy" teriminin Türkçe karşılığı "Oldukça İyi Gizlilik" olarak tanımlanabilir. 1991 yılında Phil R. Zimmermann tarafından tanımlanan ve geliştirilen açık kaynak kodlu bu bilgisayar algoritması, gönderilen ve alınan verilerin şifrelenmesini ve şifrelenen mesajların yeniden açılmasını sağlamaktadır. Adı, oldukça ilginç biçimde, tasarlandığı dönemdeki popüler bir radyo programından esinlenerek konulmuştur. Adı "*Ralph's Pretty Good Grocery*" olan radyo programının Türkçe karşılığı "*Ralph'in oldukça iyi bakkal dükkanı*"dır.

Zimmermann kendi döneminin aktivistlerinden olup, bu algoritmayı ve algoritmayı işleten programı açık kaynak kodlu olarak yayınlamıştır. Sağladığı güvenlik altyapısı Amerikan hükümeti gibi diğer hükümetlerin de ilgisini çekmiş ve kısa zamanda yaygınlaşması sonucu beklenmedik şekilde Zimmermann'ı Amerikan yargı sistemiyle karşı karşıya getirmiştir. Zira Amerikan senatosunun dayattığı güvenlik politikasında, her güvenlik yazılımında açık bir arka kapı bırakılması istenmekteydi. Bu açık nokta, terörist eylemlere karşı önlem alınması için bir gereklilik olarak tanımlanmaktaydı. Bu nedenle Phil Zimmermann hakkında lisanssız silah ihracatı yapmak suçlamasıyla dava açılmıştır. Ancak bu suçlamaların hepsinden beraat eden Zimmermann'ın algoritması günümüzde yüksek bir ticari değere sahiptir. Bu program e-posta güvenliği yanında dosyaların, klasörlerin, veri bankalarının ve disk birimlerinin de güvenliğini sağlamak için kullanılabilmektedir.

Gerçekten adından anlaşılacağı üzere bu yöntem oldukça güvenilebilir bir iletişim altyapısı sağlamaktadır. E-posta göndericisi ve alıcısı her noktada güvenliğin dört ana ilkesiyle korunmaktadırlar. Bu yüzden PGP, sunucular yerine uç istemcilerde, yani gönderici ve alıcı tarafta çalışmaktadır. Bu protokolleri bizzat e-postayı yollayan ve e-postayı alan kullanıcılar kendi başlarına uygulayabilmektedirler. Ancak kavraması biraz zaman alacak olan bu metodun zorlu aşamalarını kullanıcıya hissettirmeden yapabilen eklentiler oldukça yaygındır. Bu eklentileri, kullanmaktan hoşlandığınız bir e-posta programına kolaylıkla adapte edip PGP'nin sağladığı güvenlik platformuna sahip olabilirsiniz. Ancak göz önünde bulundurulması gereken en önemli nokta, PGP'nin e-posta iletişimini sağlamakla yükümlü olmadığıdır. E-posta yine SMTP tabanlı sunucular arasında transfer edilmektedir. Fakat e-posta gönderme ve alma sürecinde verinin güvenliği PGP tarafından sağlanmaktadır.

PGP ile hemen hemen aynı koruma mekanizması öneren Güvenli Çok-amaçlı İnternet Posta Uzantısı (Secure Multipurpose Internet Mail Extension – S/MIME), İnternet Mühendisliği Görev Gücü (Internet Engineering Task Force – IETF) tarafından önerilen e-posta güvenliği standardıdır. S/MIME ilk olarak 1995 yılında önerilmiş, son sürümü ise 1999 yılında yayınlanmıştır. Üçüncü sürüm ile önerilen standart, kişisel kullanımdan çok şirketlerin başvurduğu bir yöntem olarak göze çarpmaktadır. S/MIME ile PGP arasındaki en belirgin fark, S/MIME protokolünde anahtar paylaşımının güvenlik otoriteleri tarafından yapılıyor olması, ancak PGP'nin ise anahtarları kendi algoritmalarıyla üretmesi ve bu anahtarları bir merkezi dağıtım platformuna yüklemesidir.

Daha önceki ünitelerde de bahsedildiği üzere veri ve ağ güvenliği denilince çok temel güvenlik servislerinin göz önünde bulundurulması gerekmektedir. Bu güvenlik servislerini yeniden hatırlamak e-posta iletişiminde hangi güvenlik ilkelerinin koşulsuz sağlanması gerektiğini de gözler önüne serecektir.

- **Gizlilik:** Göndericinin oluşturduğu veriye sadece gönderici ve alıcı erişebilecektir. İletişim esnasında verinin başka kullanıcılar tarafından ele geçirilmesi durumunda yorumlanması gizlilik ilkesini yok edeceğinden, veri sadece alıcı ve vericinin çözebileceği şekilde şifrelenmelidir.
- **Kimlik Doğrulama:** Ağ üzerinde mesajı oluşturan gönderici ve mesajı alan alıcı birbirlerine gerçek gönderici ve alıcı olduklarını kanıtlayabilmelidirler. Ağ üzerin-

de kötü amaçlı uygulama geliştiren kullanıcılar, kendilerini gizlerse veya mesajın bir başka gerçek kullanıcı tarafından gönderildiğine ikna edebilirlerse kimlik doğrulama güvenlik ihlali ortaya çıkacaktır.

- **Mesaj bütünlüğü ve inkâr edilememe:** Yasal bir kullanıcının yolladığı mesaj, yasal bir alıcıya ulaştığı takdirde bu mesajın gönderici tarafından inkâr edilememesi ve mesaj içeriğinde değişiklik olmadığının garanti edilmesi gerekir. Günümüzde kâğıt ve ıslak imza ile haberleşme ve mesajlaşma, yerini sayısal imza ve bu imzayla güvene alınmış e-posta iletişimine bırakmaktadır. Bürokraside de her metnin kim tarafından oluşturulduğunun ve metnin kime gönderildiğinin inkâr edilemeyecek bir altyapıda hazırlanması ve iletişimin bu kanuni çerçeve içerisinde gerçekleşmesi gerekmektedir.

PGP ve S/MIME aynı temeller üzerine şekillendiğinden, bu temellerin, ilk önerildiği platform olan PGP üzerinden anlatılması konu bütünlüğü açısından yararlı olacaktır. PGP uygulaması gönderici ve alıcı arasındaki mesajlaşmada yukarıda temel nitelikleri verilen güvenlik servislerini sağlayacak şekilde geliştirilmiş ve bir standart haline gelmiştir. Bu esnada akıllara şu soru gelmektedir. Basit bir e-posta ile yukarıda verilen temel kavramlar nasıl bağdaşırlar? Biraz derinlemesine düşünüldüğünde bu temel güvenlik kavramlarını, Can ile Bora'nın iletişimine kolaylıkla uyarlayabiliriz. Can e-posta uygulamasını açıp bir mesaj yazdığında bu mesaj, kişisel bir değere sahip olacaktır. Bu postanın gerek SMTP sunucularından geçerken, gerek Bora'ya iletilirken gizlilik ilkesi gereği kimse tarafından açılıp deşifre edilememesi gerekmektedir. Bunun için PGP, hem asimetrik hem de simetrik şifreleme mekanizmalarını çalıştırmaktadır. Bu şifrelenmiş mesajın Bora'ya ulaşmasıyla birlikte Bora'nın aklına gelebilecek ikinci soru gelen mesajın gerçekten Can tarafından gönderilmiş olup olmadığıdır. Zira Bora, bu esnada farklı kullanıcılardan gelen birçok spam e-posta ile de uğraşmaktadır. PGP, asimetrik şifreleme yöntemiyle kimlik doğrulama ilkesini de şüpheye yer bırakmadan sağlamaktadır. Ancak bu esnada her iki kullanıcının kafasında yeni bir soru oluşabilir: Alınan mesaj gönderilen mesaj ile gerçekten aynı mıdır? Mesaj bütünlüğü güvenlik servisi çerçevesinde tanımlanan bu sorun, yine mesaja eklenen bir tür imza ile çözümlenmektedir. Bu imza aynı zamanda, Can ile Bora arasında daha sonra oluşabilecek bir anlaşmazlık sonucu Can'ın mesajı gönderdiğini inkâr etmesinin de önüne geçmektedir. Peki, PGP tüm bu güvenlik gereksinimlerini nasıl karşılamaktadır? Bundan sonraki bölümlerde şifreleme yöntemleriyle mesajın nasıl güvenlik altına alındığı, sayısal imza ile de mesaj bütünlüğünün ve inkâr edilemezlik servisinin nasıl sağlandığı açıklanacaktır.

E-posta Şifreleme

Son istatistikler incelendiğinde (Email Statistical Report 2015–2019) dünya çapındaki günlük e-posta trafiğinin yaklaşık 216 milyar adet olduğu görülmekte ve bu sayının 2019 yılında 250 milyara ulaşacağı tahmin edilmektedir. Ancak bu rapordaki en etkileyici nokta, e-posta hesap sayısının kullanıcı sayısından fazla olmasıdır. Bir başka deyişle kullanıcıların birden fazla e-posta hesabına sahip olduğu görülmektedir. Muhtemelen farklı hesaplar farklı amaçlar için kullanılmaktadır. Bu denli yoğun bir iletişim ortamında da e-posta içeriğinin güvenliğini sağlamak için hem simetrik hem de açık anahtarlama yolunun kullanıldığı şifreleme yöntemlerine başvurulmaktadır. Daha önceki ünitelerde değinilen bu kavramların e-posta güvenliğine uygulanmasıyla bilgilerinizin pekişeceğini umuyoruz.

Simetrik şifreleme, bilinen en etkili şifreleme mekanizması olup şifre anahtarının uzunluğu oranında şifrelenen mesajın çözülmesi için harcanacak zaman artmaktadır.

Günümüzde en az 128 bit uzunluğunda simetrik anahtarlama yöntemiyle uygulanan şifreleme oldukça yeterli bir güvenlik ölçütü sağlamaktadır. Burada simetrik şifre dendiğinde mesajın şifrelenmesi ve tekrar şifresinin çözülmesi için aynı anahtarın kullanılması gerekliliği anlaşılmalıdır. PGP uygulandığında simetrik anahtar sadece ilgili e-postaya özgü olarak üretilecek ve bir daha aynı anahtar kullanılmayacaktır. Burada 128 bit boyutlu bir anahtar ile ne kastedildiğini tekrar gözden geçirmekte fayda vardır. Gerek şifreleme anahtarlarının, gerekse tüm mesajların ikili sistemle kodlandığı bir ortamda iki bitlik bir şifre 00, 01, 10 ve 11 olmak üzere toplamda dört farklı olasılık sunacaktır. Eğer iki bit ile şifrelenmiş bir mesajı çözmek isterseniz, olası tüm şifreleri, yani dört farklı kombinasyonu tek tek deneyerek mesajın içeriğini çok kısa zamanda herkesin anlayabileceği biçimde çözebilirsiniz. Bu yönteme kaba kuvvet yöntemi denmektedir. Ancak 128 bit uzunluğunda bir anahtar toplamda 2^{128} = 340282366920938 463463374607431768211456 farklı şifre üreteceğinden her bir olası şifreyi deneyerek mesajı çözmek, ne kadar güçlü bir bilgisayar kullanılırsa kullanılsın, oldukça uzun bir zaman alacaktır. Burada bahsedilen zamanın milyonlarca yıl seviyesinde olduğunu belirtmekte fayda vardır.

1 nanosaniyede (1 nanosaniye = 0.000000001 saniye) 1 şifrenin denendiği bir bilgisayar ortamında 64-bit ile şifrelenmiş bir mesajı çözmek en kötü ihtimalle ne kadar zaman alır?

SIRA SİZDE 2

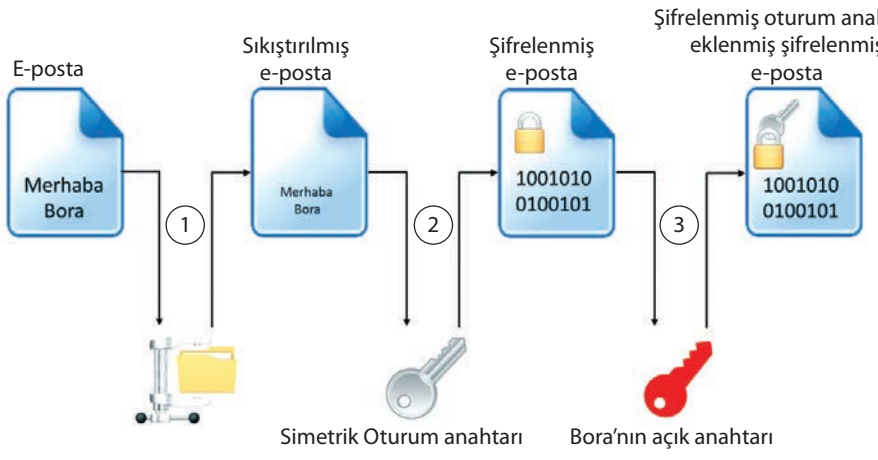
E-posta, simetrik anahtarla şifrelendikten sonra tekrar orijinal metne dönüşmesi için aynı anahtarın alıcı tarafa da ulaştırılması gerekmektedir. Aksi takdirde alıcının bu e-postayı okuyabilme ihtimali, e-postayı ele geçiren herhangi bir kullanıcıyla aynı olacaktır. PGP öncesi en büyük sorun, şifre anahtarının alıcıya nasıl gönderileceği konusuydu. Bu anahtar şifrelenmeden gönderilirse, yolda bunu ele geçiren kötü niyetli kullanıcı rahatlıkla metnin orijinalini elde edebilecekti. İşte bu noktada asimetrik anahtarla şifreleme yöntemi kullanılmaktadır. Simetrik anahtar, alıcı tarafın açık anahtarı kullanılarak şifrelenir ve mesajın içerisine eklenir. Böylelikle bu anahtar alıcının dışındaki kullanıcılara geçse de, kendilerinde gizli anahtar olmayacağı için gerçek anahtarı deşifre etmek neredeyse imkânsız olacaktır.

Can Bora'ya bir e-posta yollarken, bu e-postanın PGP algoritması kullanılarak şifrelenmesini Şekil 7.8 üzerinden incelemek, şifreleme mantığının anlaşılmasına kolaylık sağlayacaktır. Algoritmanın adımları şu şekilde sıralanabilir:

1. PGP uygulamasında e-posta öncelikle sıkıştırılır. Zira sıkıştırma işlemi şifreleme işleminden çok daha hızlı bir işlemdir. Böylelikle sıkıştırılmış metin daha kısa zamanda şifrelenecek ve tüm işlemlerde hız artacaktır. Ayrıca sıkıştırma işlemi güvenliğin artmasına da katkıda bulunmaktadır. Şifre çözme için geliştirilen algoritmalarda düz metinler içerisindeki ardışık harfler ve kelimeler bulunmaya çalışılmaktadır. Ancak sıkıştırma işlemi bu yöntemlerin doğru çalışmasını engellemektedir.
2. Sıkıştırılmış e-posta, sadece bu e-posta için üretilen simetrik anahtar kullanılarak şifrelenir. Bu anahtara oturum anahtarı denmektedir ve bu anahtar rastgele üretilmiştir. Rastgele işleminin çok büyük önemi vardır. Eğer oturum anahtarı belirli bir algoritma kullanılarak üretilmiş olsa, bu şifreyi kırmak isteyen kullanıcılar da rahatlıkla aynı algoritmayı kullanarak oturum anahtarını elde edebilirler. Rastgele oturum anahtarı hem kullanıcının klavye ile etkileşimi hem de zamana bağlı olarak elde edilen değerlere göre üretilmektedir. Dolayısıyla aynı algoritma kullanılsa bile aynı rastgele değeri ve aynı şifreyi elde etmek neredeyse olanaksızdır.

Şekil 7.8

PGP ile e-postanın şifrelenmesi



Simetrik oturum anahtarı kullanılarak IDEA algoritmasının kullanılması, PGP'nin temel şifreleme alt yapısını oluşturmaktadır. IDEA (International Data Encryption Algorithm), DES algoritmasının geliştirilmiş bir şeklidir. Önceleri PES algoritması olarak anılsa da, gelişimler sonucu günümüzün kırılması en zor algoritmalarından birisi olarak kabul edilmektedir. IDEA şu anda serbestçe kullanılan bir şifreleme yöntemidir ve DES gibi blok şifreleme yöntemi kullanır. Ancak DES algoritmasında 56-bit uzunlukta anahtar kullanılırken, IDEA en az 128 bit uzunluğunda anahtar kullanarak kaba kuvvetle çözümü zorlaştırmaktadır.

3. Simetrik oturum anahtarıyla şifrelenmiş metin dosyasının açılması için yine aynı anahtara ihtiyaç duyulmaktadır. Bu anahtarın da alıcı tarafa, yani Bora'ya, büyük bir gizlilik içerisinde iletilmesi gerekmektedir. İşte burada asimetrik anahtarların kullanıldığı açık anahtarlı şifreleme sistemi işin içine girmektedir. Zira simetrik anahtarın da şifrelenerek gönderilmesi gerekmektedir. Oturuma özgü rastgele oluşturulmuş simetrik anahtar, alıcının açık anahtarıyla tekrar şifrelenip e-posta içerisine eklenmektedir. Burada merak oluşturan iki konu vardır. Bunlardan ilki, neden bütün sıkıştırılmış e-postanın alıcının açık anahtarıyla şifrelenmediğidir. Diğeri ise, Bora'nın açık anahtarının nereden öğrenileceği konusudur.

Daha önceki ünitelerde simetrik ve asimetrik anahtarlarla şifreleme üzerinde oldukça detaylı bilgiler verilmiştir. Simetrik anahtarlar, aynı tip algoritmalar kullanılarak hem şifrelemeye hem de şifrenin açılmasına olanak tanımakta ve bu işlem oldukça hızlı gerçekleşmektedir. Genelde 128-bit ve 256-bit anahtarların kullanıldığı bu algoritmalar hızlıdırlar ve az işlemci gücü gerektirmektedirler. Ancak asimetrik anahtarların elde edilmesi rastgele 128-bit uzunluğunda simetrik anahtarların elde edilmesi kadar kolay değildir. Ayrıca asimetrik anahtarlar simetrik anahtarlardan çok daha uzun olmaktadır. Bu yüzden asimetrik algoritma kullanılarak, yani açık anahtarla uzun verilerin şifrelenmesi ve gizli anahtarla şifrenin çözülmesi, çok karmaşık işlemler ve yüksek işlemci potansiyeli gerektirmektedir. Bu yüzden simetrik anahtar şifrelemenin avantajlarını kullanarak, simetrik anahtarı da asimetrik şifreleme ile korumak hem hız hem de daha az kaynak tüketimi sağlamaktadır.

Şimdi, Bora'nın açık anahtarının nereden öğrenileceği konusuna cevap arayalım. Bu sorunun arkasında yatan temel problemi anlamak için şu soruyu sormak gerekir: Eğer

Can Bora yerine, Bora sandığı başka bir kullanıcının açık anahtarını kullanarak simetrik anahtarı şifrelerse ne olur? Böyle bir durumda hem Bora bu mesajı açamaz, hem de diğer kullanıcı kendi gizli anahtarı ile simetrik şifreyi çözer ve şifrelenmiş tüm metnin içeriğini rahatlıkla okuyabilir. Daha önce bahsedildiği gibi bu problem "Ortadaki Adam" saldırısı olarak anılır. Bu tip bir saldırı oluşturmak için özel güvenlik açığı programlarına ulaşmak son derece kolaydır.

Can'ın elde etmeye çalıştığı Bora'nın açık anahtarının, gerçekten Bora tarafından üretildiğinin, yani bu anahtarın gerçekten Bora'nın açık anahtarı olduğunun sınanması için güvenlik sertifikaları kullanılmaktadır. Bir sertifika çok temel anlamda kişinin açık anahtarının yetkili bir otorite tarafından güvenlik altına alınmış halidir. Yani bütün anahtar alış verişi içerisine ayrı bir kurum daha dâhil olmaktadır. Güvenilir üçüncü parti olarak anılan bu kurumlar devlet kurumları veya özel sektör kuruluşlarıdır ve hiçbir şekilde güvenliğinden kuşku duyulmayacak otoritelerdir. Aslında günlük yaşamda ve İnternet ortamında hemen her işlemde, farkında olmadan, bu sertifika otoriteleriyle iletişim halindeyiz. Bu iletişim bazen bilinçli bazen de bilinçsiz bir şekilde gerçekleşmektedir. Örneğin, bir bankanın İnternet sitesini kullanarak kredi kartınıza ait bir hareketi izlemek istemeniz durumunda bu bilgilerin tam gizlilik içerisinde gerçekleşmesi ve "ortadaki adam"ın bu bilgi trafiğini hiçbir şekilde izleyememesi en temel güvenlik gereksinimidir. İnternette bir arama motorundan arama yaparken bile sertifika otoritelerinin sağladığı güvenlik platformu kullanılmaktadır. Eğer İnternet tarayıcısının adres kısmı https:// ile başlıyorsa, o sırada mutlaka açık anahtar alışverişi yapılmış anlamına gelmektedir. Şekil 7.9'da sık karşılaşılan sertifika sağlayıcıların logoları görülmektedir.

Şekil 7.9

Sık rastlanan sertifika sağlayıcı otoriteler

Sertifika sağlayıcısı kendi güvenlik sertifikalarını ve bu sertifikaların geçerlilik sürelerini başlangıçta hem Can'a hem de Bora'ya gönderir. Hemen her kullanıcının bilgisayarı bu güvenlik sertifikalarını tutar ve haberleşme esnasında karşı tarafın açık anahtarının nereden alınacağına bu sertifikalara bakarak karar verir. Eğer Can Bora'ya mesaj yollayacaksa Bora'nın sertifika sağlayıcısına başvurur ve Bora'nın açık anahtarını bu sertifika sağlayıcısından alır. Bu anahtar tümüyle güvenilir bir anahtardır ve mesajın oturum anahtarını açık anahtar ile şifreleyerek mesajın içerisine ekler. Tüm bu sertifikalar ve sertifika hizmetlerinin de bir standarda göre sağlanması ve yürütülmesi gerekmektedir. Uluslararası Telekomünikasyon Birliği (International Telecommunication Union–ITU) ve IETF, bu standartların geliştirilmesi ve sağlanması görevlerini üstlenen kurumlar olup standartların ortak bildirgelerini belirlemişlerdir [RFC 1422]. Bu standartlar tümüyle halka açık olup, RFC 1422 belgeleri incelendiğinde isteyen kullanıcıların bu standarda göre sertifika üretmesini ve kullanmasını sağlamaktadırlar. Tablo 7.1'de bir sertifikanın bazı önemli alanları gösterilmiştir (RFC 1422'den alınmıştır). Şekil 7.10'da örnek bir sertifika görülmektedir. Bu sertifika incelendiğinde imza algoritmasının SHA256 olduğu ve 2.048 bitlik ortak anahtarın sertifikası olduğu görülmektedir.

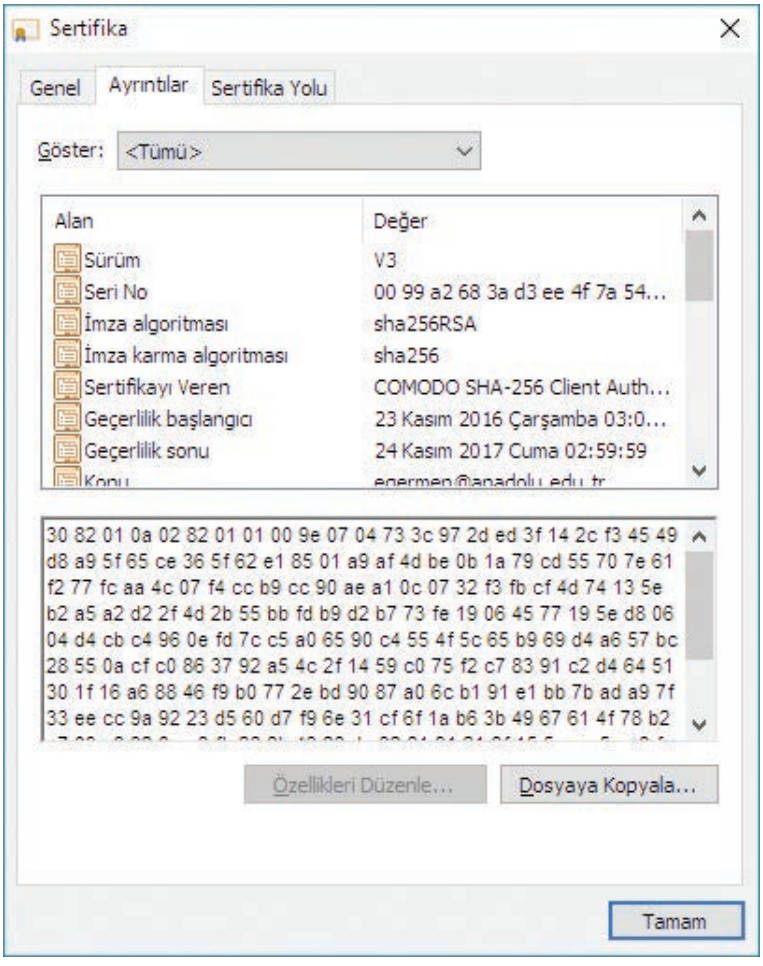
Tablo 7.1
Bir sertifikanın bazı temel alanları

Alan Adı	Açıklama
Sürüm	Sertifikanın X 509 sürüm numarası
Seri No	Her sertifika üreticisinin belirlediği özgün sertifika numarası
İmza Algoritması	Sertifika sağlayıcısının bu imza için belirlediği algoritma
Sertifikayı Veren	Sertifika sağlayıcısının kimlik bilgisi
Geçerlilik Başlangıcı	Sertifikanın geçerli olduğu sürenin başlangıç tarihi
Geçerlilik Sonu	Sertifikanın geçerli olduğu son tarih

SIRA SİZDE 3

Kullanıcıların anahtarlarının saklandığı sertifikaları görüntülemek isterseniz ne yapmanız gerekir?

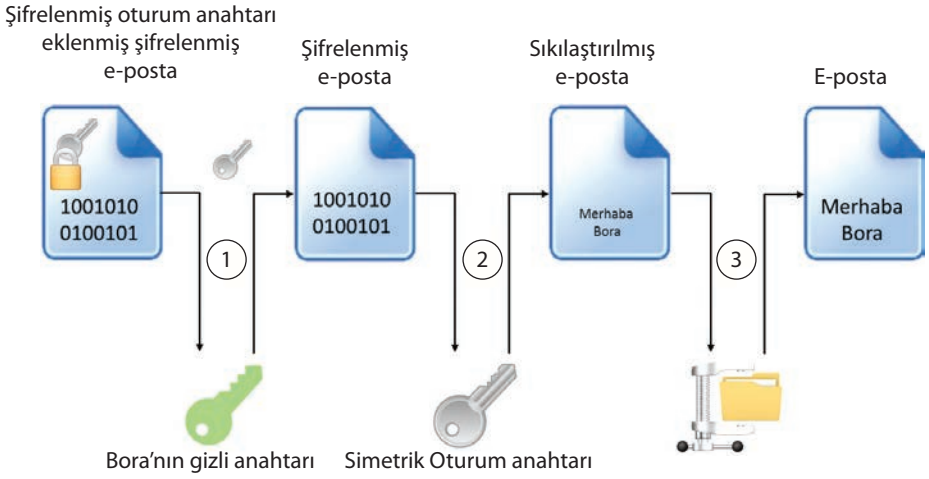
Şekil 7.10
Örnek sertifika



S/MIME protokolünde gizli ve açık anahtarların üretimi ve dağıtımı sertifika sağlayıcılarına bırakılırken, PGP için bu anahtarların yaratılması özel PGP yazılımı tarafından gerçekleştirilmekte ve güvenli anahtar değişimi PGP servislerine bırakılmaktadır.

Şifrelenmiş E-postanın Açılması

Alıcı (Bora) e-postayı aldıktan sonra şifreleme için yapılan tüm işlemlerin sürecini tersine çalıştırarak gelen e-postanın içerisindeki bilgiye erişebilmektedir. Şekil 7.11 tersine işleyen bu süreci tanımlamaktadır. Algoritmanın adımları şu şekilde sıralanabilir:



Şekil 7.11

PGP ile şifrelenmiş e-postanın şifresinin çözümü

1. Bora kendisinin açık anahtarı ile şifrelenmiş simetrik anahtarı çözecek yegâne kullanıcıdır. Çünkü asimetrik şifreleme yönteminde veri bir kullanıcının açık anahtarıyla şifrelendiğinde ancak bu kullanıcının gizli anahtarı sayesinde çözülebilmektedir. Açık anahtarın yetkili sertifika sağlayıcılarından temin edildiği açıklanmıştı. Ancak gizli anahtarın Bora'ya nasıl ulaştırıldığı tekrar bir güvenlik sorusunu akla getirmektedir. Hiç şüphesiz açık anahtarı üreten kurum yine bu gizli anahtarı da üretmektedir. Eğer bu anahtar İnternet üzerinden yollanırsa, ortadaki adam denilen kötü amaçlı kullanıcılar anahtarı rahatlıkla ele geçirebilir ve tekrar kendilerini anahtarın sahibi gibi tanıtabilirler veya hiçbir şey olmamış gibi Can ile Bora arasındaki trafiği izlerken, bu trafikte şifrelenmiş simetrik oturum anahtarının şifresini kırarak tüm veriyi deşifre edebilirler. İşte bu yüzden gizli anahtarın doğru kişiye ulaşması, bütün sistemin güvenliği için önemlidir. Bu gizli anahtarı kullanacak firma, kuruluş veya kullanıcılar, gerekli güvenlik aşamalarından geçirilmektedirler. Eğer kullanıcı kendisinin güvenilirliğini kanıtlayabilirse gizli anahtar genelde bir kurye ile çoğunlukla elektronik iletişim ortamı dışında bir ortam üzerinden iletilmektedir. Ancak deneme amaçlı ve çok büyük gizlilik önemine sahip olmayan uygulamalar için sertifika sağlayıcılar, oluşturdukları sertifikalarla birlikte gizli anahtarları da İnternet ortamından kullanıcıya ulaştırmaktadır. Bora kendisinin gizli anahtarını kullanarak e-posta içerisine gömülü simetrik oturum anahtarının şifresini açar ve elinde şifrelenmiş bir veri ile bu veriyi şifreleyen anahtar bulunur. Artık yalnızca simetrik şifre çözme algoritmasını işletmesi gerekmektedir.
2. Bora elindeki simetrik oturum anahtarını ve IDEA algoritmasını kullanarak sıkıştırılmış veriyi elde eder. Sıkıştırılmış veri, şifreleme algoritmasının çözümünü daha da kolaylaştırmakta ve daha önce de bahsedildiği üzere sistemin güvenliğini arttırmaktadır.
3. Son aşamada e-postanın geleneksel yöntemlerle sıkıştırılmış hali elde edildiğinden aynı yöntemler kullanılarak sıkıştırılmış dosya açılabilmekte ve Can'ın Bora'ya gönderdiği veri başkasının eline geçmiş olması endişesi yaşanmadan yeniden oluşturulmaktadır.

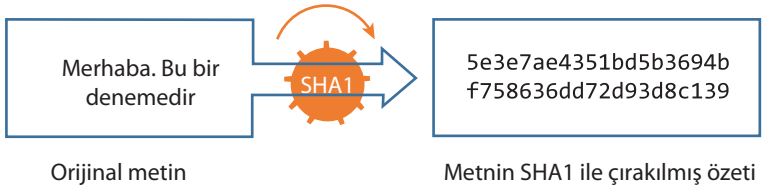
Kimlik Doğrulama ve Dijital İmza

SMTP, Can ile Bora arasında iletişimi sağlarken PGP şifreleme algoritmaları, verinin güvenli biçimde gönderici ve alıcı arasındaki iletişimin gerçekleşmesini sağlamaktadır. Ancak bu işlemler sırasında, fark edileceği üzere, sadece veri güvenliği sağlanmakta, fakat kullanıcı kimliği garanti altına alınmamaktadır. Can'ın yerine onun şakacı arkadaşı Burak, Bora'nın açık anahtarını kullanarak, sanki mesajı Can yolluyormuş gibi davranırsa, Burak ondan gelen mesajı Can'dan gelmiş gibi algılayabilir. Dijital İmza yöntemi bu güvenlik açığını ortadan kaldırmak için kullanılır. PGP dijital imza ile gönderenin kimliğini de güvenceye almaktadır. PGP ile dijital olarak imzalanan e-postanın diğer bir avantajı ise dijital imza kullanılan durumda inkâr edilmezlik servisinin de sağlanıyor olmasıdır. Bunu bir örnekle şöyle açıklayabiliriz: Can, Cumartesi günü Bora'ya gönderdiği e-postada Pazartesi günü birlikte sinemaya gideceklerini söylemiş olsun. Pazartesi günü Bora sinemaya gittiğinde Can'ın oraya gelmediğini fark ettiğinde Can'a mesaj atarak nerede olduğunu sorar. Can gönderdiği mesajla kesinlikle öyle bir e-posta yollamadığını, bu e-postanın şakacı arkadaşı Burak tarafından yollandığını düşündüğünü söylediğinde Bora'nın aksini iddia etme şansı yoktur. Bora ya tek başına sinemaya girmeye veya eve geri dönmeye karar verir. Ancak Can Bora'ya dijital imzalı bir mesajı PGP içerisinde yollamış olsaydı, Bora, Can ile olan arkadaşlığını tekrar gözden geçirmeye karar verecektir. Çünkü dijital imzalı bir e-posta kesinlikle gönderenin kimliğini garanti altına almaktadır. Dijital imza, PGP metodolojisi içinde özet değerinin bulunmasıyla ve bu özet değerin şifrelenmesi ve mesaja eklenmesiyle sağlanmaktadır.

Dijital imza, e-postaya eklenmiş ve dosyaların güvenliği için oluşturulmuş sayısal kodlardır. E-posta içerisinde imza olmadığı takdirde e-postanın göndericisini ispat etmek son derece güçtür. Bir e-postanın dijital olarak imzalanması aşamasında öncelikle tüm e-postanın özet değeri çıkarılmaktadır. Bu özet değeri, bir özetleme algoritması sonucu elde edilen belli uzunluktaki sayısal değerlerin bir araya gelmesinden oluşur. SHA özetleme algoritmaları gereksinimler doğrultusunda evrimleşmeye devam etmektedir ve günümüzde 512-bit uzunlukta özet çıkaran algoritmaların kullanıldığı görülmektedir. Şekil 7.12'de örnek bir metin ve bu metnin SHA1 algoritmasıyla çıkarılan gerçek 128-bitlik özeti görülmektedir.

Şekil 7.12

SHA1 algoritmasıyla özet çıkarma



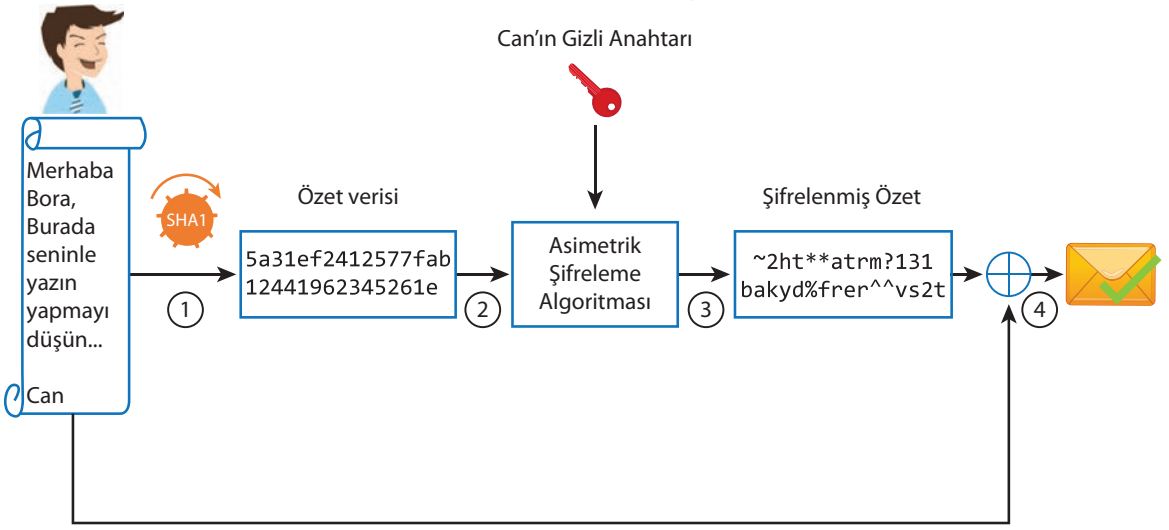
SIRA SİZDE 4

SHA1 algoritması 128-bit uzunluğunda özet çıkarabilmektedir. Bu algoritmayla en fazla kaç verinin farklı özeti çıkarılabilir?

Dijital imza, seçilmiş bir özet algoritmasının çalıştırılmasıyla başlar. Daha sonra sırasıyla asimetrik şifreleme ile bu özetin şifrelenmesi ve şifresinin çözülmesi işlemleri PGP tarafından gerçekleştirilir. Dijital imzanın e-postaya eklenmesi işlemleri Şekil 7.13 ile daha iyi anlaşılacaktır.

Şekil 7.13

Dijital imza ile imzalanmış e-postanın oluşturulması



Şekil 7.13'de görüleceği gibi Can Bora'ya bir e-posta yazar. Ancak e-postayı imzalamak için sırasıyla:

- Tüm e-posta verisi bir özetleme algoritmasından geçirilerek bu veriye ait bir özet ortaya çıkarılır.
- Bu özet verisi Can'ın gizli anahtarı ile şifrelenir.
- Şifrelenmiş özet verisi Can'ın e-postasına eklenir.
- Hem e-posta hem de şifreli özet verisi SMTP sunucusuna gönderilir ve bu posta Bora'nın adresine iletilir.

Neden Can'ın gönderdiği e-postanın tümü değil de sadece özet verisi asimetrik şifreleme metoduyla şifrelenmektedir?

SIRA SİZDE 5

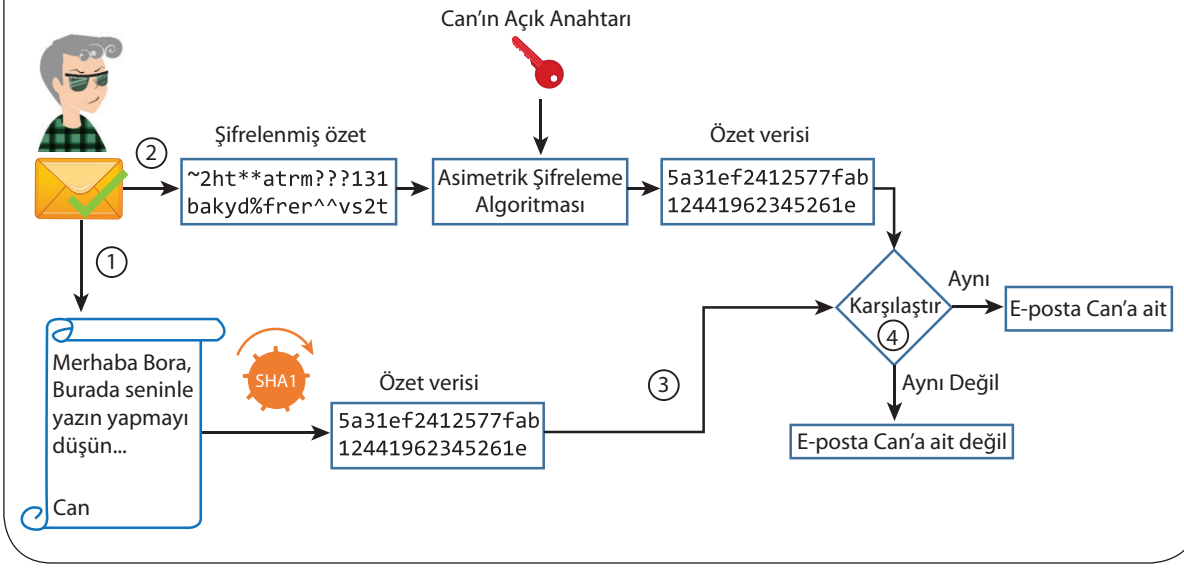
Bu postanın Bora'ya ulaşmasından sonra tüm süreç ters yönde işletilerek gelen e-postanın postada belirtildiği gibi Can'dan mı yoksa başkasından mı geldiği anlaşılır. Ancak bu işlemde Can'ın gizli anahtarı yerine açık anahtarı kullanılmaktadır. Şekil 7.14 süreci anlamayı kolaylaştıracaktır.

- Bora, Can'dan gelen e-postayı aldığında bu posta içerisinde hem Can'ın yolladığı veri hem de Can'ın kendi gizli anahtarı ile şifrelediği özet verisi bulunmaktadır. Öncelikle Can tarafında çalışan PGP uygulaması daha sonra Bora'nın tarafında çalışarak Can'ın e-postasını tekrar çıkartır.
- PGP ayrıca postanın içerisine eklenmiş şifreli özet dosyasını da çıkartır. Bu dosya Can'ın gizli anahtarı ile şifrelenmiş olduğundan, Can'ın açık anahtarı kullanılarak eski haline döndürülebilir. Bora'nın PGP uygulaması Can'ın anahtar dağıtıcısına başvurarak Can'ın açık anahtarını elde eder ve bu anahtar yardımıyla özet verisini çözer.
- Özet verisi çıkarma algoritmaları veriden her zaman aynı özeti çıkaracağından Bora, Can'ın yolladığı mesajın özetini Can'ın kullandığı aynı algoritmayı kullanarak elde eder.

- Son olarak Bora'nın PGP uygulaması hem Can'ın açık anahtarıyla çözülmüş özet verisini hem de Can'ın mesajından elde edilen özet verisini karşılaştırır. Her iki veri de eşitse Bora mesajın Can'dan geldiğine emin olacaktır.

Şekil 7.14

Sayısal imzalanmış e-posta denetimi



Tüm bu işlemler sonucu PGP metodu içerisinde elde edilen iki adet özet verisinin aynı olması iki temel noktayı garantilemektedir. Can'ın açık anahtarının şifresini çözebileceği tek veri Can'ın gizli anahtarı ile şifrelediği metindir. Bu yüzden Can bundan sonra bu mesajı kendisinin gönderdiğini hiçbir zaman inkâr edemez. Zira Can'ın gizli anahtarı sadece kendisinin kullanabileceği bir gizliliğe ve güvene sahiptir. İkinci temel nokta ise, her iki özet verisinin eşit olduğu durumda mesajın kesinlikle Can tarafından yazıldığı ve hiçbir aradaki adam tarafından değiştirilmediğinin garanti altına alınmış olmasıdır. Eğer bu veri ortadaki adam tarafından değiştirilmiş olsa, özet algoritması e-posta içeriğinden farklı bir özet çıkaracaktır. Bu özet de e-postaya eklenmiş olan şifrelenmiş özetten farklı olacaktır. Böylece hem mesajın değiştirilmediği garanti altına alınmış hem de mesajı gönderenin kimlik bilgisi güvenceye alınmış olmaktadır.

PGP hem veri şifreleme hem de dijital imza algoritmalarını birlikte çalıştırarak tam güvenli e-posta iletişimi sağlamaktadır. Ancak bazı durumlarda e-postayı sadece imzalamak, bazen de sadece metni şifrelemek istenebilmektedir. Bu "tam olmayan güvenlik" şeklinde nitelenebilecek iletişim mekanizmasını PGP kolaylıkla sağlamaktadır. Can, Bora'ya sadece mesajı şifreleyerek gönderebileceği gibi bazen de mesajı başkalarının görmesinin önemi olmadığı, ancak Bora'ya mesajın kendisinden gönderildiğini kanıtlamanın gerekli olduğu durumlarda mesaja dijital imza konulabilmektedir.

Can ve Bora'nın PGP kullanarak e-posta iletişimini gerçekleştirmesi için açık kodlu veya özel programlar İnternet'te kolaylıkla bulunabilmekte ve kullanılabilmektedir. Ancak kullanıcılar alıştıkları e-posta yöntemleriyle de PGP'nin sağladığı güvenlik ortamından yararlanabilmektedirler. Her bir e-posta uygulaması için ek kurulumlar ve programlara eklentiler yardımıyla PGP'nin sağladığı tam güvenlik (şifreleme + dijital imza) veya yarı güvenlik (şifreleme veya sayısal imza) kolaylıkla sağlanabilmektedir.

KİŞİSEL VE KURUMSAL E-POSTA GÜVENLİĞİ

E-posta güvenliği denilince bunun çok katmanlı bir disiplin olduğu ve bu yaklaşımla güvenlik mekanizmalarının ve önlemlerinin tanımlanması gerekliliği ortaya çıkmaktadır. Gerek bireyler, gerek kurumlar, gerekse kurumlar arası iletişim servis sağlayıcılarının kendi güvenlik tanımlarını doğru biçimde yapmadıkları ve yükümlülüklerini yerine getirmedikleri durumlarda büyük güvenlik açıkları ortaya çıkmakta ve tüm e-posta kullanıcıları ve servis sağlayıcıları saldırıların hedefi haline gelmektedir. Ağ güvenlik sistemleri ve ağ güvenlik politikaları, işletmeleri ve kullanıcıları bir bütün halinde korumayı, güvenlik açıklarını zamanında keşfederek proaktif önlemlerle bilgisayar korsanlarının ve veri hırsızlığının önüne geçmeyi hedeflemektedir. Kişisel ve kurumsal anlamda veri güvenliğine yapılacak yatırım her ne kadar belirli bir ilk maliyet gerektirse de, bu maliyet göze alınmadığı takdirde oluşabilecek veri ve iletişim kayıpları ilk maliyetlerin çok üstüne çıkabilmektedir. Günümüzde bunların sayısız örneklerine rastlamak mümkündür. Sahte e-postalara aldanarak piyango kazandığını zanneden ve sonuçta yüklü miktarda para kaybeden kullanıcılar veya yapılan saldırılar sonucu iş göremez hale gelen büyük şirketlerin sunucuları örnek olarak göze çarpmaktadır.

Günümüzde, ağ yapılarında donanım ve yazılımların iyileştirilmesi ve güçlendirilmesi üzerine yapılan akademik çalışmalar kadar bu sistemlerin güvenliği ve sürdürülebilirliği için de oldukça fazla yatırım yapılmaktadır. E-posta ve ağ güvenliği, hem kullanıcıların hem de servis sağlayıcılarının bilincinde oldukları bir kavram olduğu zaman veri ve zaman kayıplarında oldukça büyük düşüş yaşanacağı bir gerçektir. Zira sistemde oluşabilecek en küçük bir açıklık tüm sistemi etkileyebilecek sorunlara neden olmaktadır. Ağ mühendisliğinin günümüzün en geçerli çalışma alanlarından birisi olmasının temel nedeni, ağ güvenliği ve iyileştirme konularının oldukça derin bilgi birikimi ve deneyim gerektirmesinden ve bu konudaki eğitimli personelin perspektifi geniş bir vizyona sahip olmasından kaynaklanmaktadır. Güvenlik konusunda atılan her adımın maddi ve manevi karşılığının değeri, ağların birbirlerini etkilemeleri sonucunda katlanmaktadır.

Son kullanıcıların da hiç şüphesiz almaları gereken önlemler ve bilincinde olmaları gereken noktalar vardır. Bilgisayar korsanlarının bilinçli bir son kullanıcıya zarar verme ihtimali oldukça azdır. Zira temelde bu kullanıcı bilgisayarını virüslere karşı koruyucu programlarla donatmış olup şüpheli tüm e-postaları önce e-posta sunucularının, daha sonra e-posta uygulayıcılarının ve en sonunda kendi mantığının süzgecinden geçirmekte ve e-postalar aracılığıyla bulaşması muhtemel zararlı içerikten korunmaktadır. Temelde bilinçli kullanıcı, şüpheleri olan bir kullanıcıdır. Her kaynağın güvenilmezlik unsuru barındırdığını bilen şüpheli kullanıcı kendi özel hayatını korsanlara karşı koruduğu gibi farkında olmadan sistemin ve ağ trafiğinin düzgün ve verimli çalışmasına da katkıda bulunmaktadır.

Özet

AMAÇ 1 *E-posta güvenliği kavramını ve ihtiyacını açıklamak*

Günümüzde iletişimin ve haberleşmenin temel altyapısını oluşturan e-posta, yaygınlığı ve sağladığı kullanım kolaylığı ölçüsünde bilgisayar virüslerinin yayılması, veri hırsızlığı ve ücretsiz reklam ve pazarlama dünyası için de çok çekici bir platform haline gelmiştir. Her e-posta kullanıcısı, gerek kişisel gerek kurumsal boyutta sayısız oltalama, kandırmaca, zararlı kodların yerleşmesine olanak sağlayan saldırının kurbanı olma sıkıntısını yaşamakta, bunun gerçekleşmesi durumunda maddi ve manevi zarar görmektedir. E-posta güvenliği artık bir gereklilik ötesinde iletişimin olmazsa olmazı konumuna gelmiş ve hem e-posta kullanıcıları hem de e-posta sağlayıcıları boyutunda zararlı iletişimin önünü kesecek önlemlerin alınmasını sağlayacak yöntemleri beraberinde getirmiştir. E-posta hizmet sağlayıcıları, sunucu boyutunda gerek yazılım gerek donanımsal koruma profilleri geliştirmekte ve bunları hizmete sokmaktadırlar. Ayrıca ortak savunma mekanizmaları araştırılmakta ve spam ile zararlı kod içerikli e-postaların kullanıcılara ulaşmadan engellenebilmesi için çalışmalar yapılmakta, yöntemler ortaya konulmaktadır. Son kullanıcılara ulaşan istenmeyen e-postalar, yasal e-postalardan, son kullanıcı hizmeti veren programlar sayesinde filtrelenmeye çalışılmaktadır. Tüm bu çabanın en temel çıkış noktası, oluşabilecek hasarın sadece kullanıcı boyutuyla kalmayıp tüm ağ trafiğinde sorun yaratmasıdır. Zira günümüz trafiğini etkileyen ve büyük maddi kayıplara neden olan büyük ölçekli saldırıların çoğunlukla zararlı e-postalarla yayılmış kodlar tarafından yapıldığı gözlenmektedir.

AMAÇ 2 *Sunucu tarafından spam e-posta yollanmasına neden olan güvenlik açıklarını betimlemek*

Spam istenmeyen e-postalar için geliştirilmiş bir terimdir. SMTP protokolüne uygun her mesaj başlangıçta, istenen sunucu kullanılarak gönderilebilmekteydi. Bu sayede spam e-postalar hem sunucuların hem de kullanıcıların başını ağrıtan önemli bir sorun haline gelmiştir. Spam yanında zararlı kod içeren e-postaların da yaygınlaşması sonucu sunucularda alınacak temel önlemler, spam dağıtımının engellenmesine yönelik olmuştur. SMTP geçişi çoğu spam üreticisinin kullandığı bir tekniktir. Bu teknikle herhangi bir e-posta sunucusundan istenen kimse adına e-posta göndermek olasıdır. İşte bu açığın fark edilmesiyle sunucular SMTP geçişi engelle-diklerinde oldukça büyük çaplı bir spam trafiğinin de önünü kesmiş olmaktadırlar. Temelde bu engelleme, ilgili SMTP sunucuda tanımlanmamış e-posta göndericilerinin gönderdikleri e-postaları çöpe atmak yoluyla olmaktadır. Ayrıca bunun bir adım ötesinde SMTP sunucuların bağlı olduğu alan sunucularında da aynı mantıkta kontrollerin yapılması, spam e-posta üreticilerinin ve göndericilerinin işini zorlaştırmaktadır. Sonuçta e-posta göndermeden önce gönderenin belirlediği çıkış ve dönüş noktaları bir güvenlik testinden geçirilmekte ve bu testi geçemeyen e-postaların ömürleri İnternet ortamına çıkmadan sonlandırılmaktadır.

AMAÇ 3 *Spam filtrelerin temel çalışma prensiplerini açıklamak*

İstenmeyen e-postaların her zaman sunucularda önünün kesilmesi olanak dâhilinde olmadığından, oluşacak spam trafiğinin sonuçta alıcıların SMTP sunucularına hatta alıcının e-posta ortamına ulaşması kaçınılmazdır. İşte bu noktada da spam güvenliğinin sağlanması için gelen e-postaları belirli ölçütlere göre test eden programlar geliştirilmekte, spam postaları ile kullanıcının buluşması engellenmek istenmektedir. Spam üreticileri de bu ölçütlerin neler olduğunu bildiklerinden sürekli değişik yöntemler denemekte, oluşturdukları spam e-postanın kullanıcının eline geçmesini ve kullanıcının bu e-postayı açıp okumasını, içerdiği kodları çalıştırmasını istemektedir. İşte böylesi karşılıklı atakların süregittiği bir ortamda statik yöntemli programlarla spam ile başa çıkılmasının olanaksızlığı karşısında sürekli öğrenen ve sisteme kendini adapte eden spam filtre algoritmaları denenmekte ve geliştirilmektedir. Ayrıca dünya çapında spam trafiğiyle başa çıkabilmek için spam ürettiği düşünülen noktalar kara listelere alınmakta ve buralardan gelen e-postalar spam olarak nitelendirilmektedir.

AMAÇ 4 *PGP e-posta aşamalarını açıklamak*

E-posta güvenliği denilince sadece zararlı ve istenmeyen e-postaların sonucunda oluşacak maddi manevi zararların engellenmesi yanında, yasal e-postanın gönderici ile alıcı arasındaki hareketi boyunca da e-postanın güvenliğinin sağlanması ilkesi de göz önünde bulundurulmalıdır. İletişim güvenliği temelde dört ana güvenlik servisini sağlamalıdır. Bunlar,

- Mesaj gizliliği
- Kimlik doğrulama
- Mesaj bütünlüğü
- İnkâr edilememe

olarak tanımlanmaktadırlar. PGP tüm bu güvenlik koşullarını bir bütün halde sağlayan ya da istenilen güvenlik koşulunu diğerleri olmadan gerçekleştiren bir yöntemdir. Burada PGP'nin e-posta gönderme gibi bir amacı olmadığını, sadece SMTP üzerinden gönderilen e-postanın güvenliğini sağlayan bir mekanizma olduğunu hatırlamakta fayda vardır. E-posta gönderilirken gizlilik, simetrik şifreleme algoritmaları ve ilgili e-postaya özgü üretilmiş bir anahtarla sağlanmaktadır. Kimlik doğrulama ise PGP'nin yapısal mekanizması içerisinde e-postaya eklenen sayısal imza ile sağlanmaktadır. Bu sayısal imza ise asimetrik şifreleme mekanizmasını kullanır. Kullanıcıların gizli ve açık anahtarları, anahtar sağlayıcı servis sunucuları vasıtasıyla dağıtılmakta ve böylece tam güvenlik sağlanabilmektedir. Mesaj bütünlüğü ve inkâr edilememe de yine dijital imzanın getirdiği güvenlik mekanizmalarıyla sağlanmaktadır. PGP ile mesaj yollanırken istenirse sadece dijital imza kullanılabileceği gibi istendiğinde sadece mesaj da şifrelenebilmektedir.

AMAÇ 5

Temel e-posta güvenlik gereksinimlerini listelemek

E-posta trafiğinin temelde iki türlü güvenlik sorunu vardır. Birincisi istenmeyen e-posta trafiği yüzünden oluşan sistemsel güvenlik açıkları, ikincisi de alıcı ile e-posta göndericisi arasında e-postanın tüm hareketi boyunca bu e-postanın alıcıya ve göndericiye zararı dokunacak aşamalardan korunmasıdır. Spam e-posta trafiği gerek uç noktalarda gerekse ağ içerisinde sunucularda alınabilecek önlemlerle azaltılabilmektedir. Ancak bu trafik ile başa çıkabilmek için çok yetkin, iyi düzeyde protokol bilgisine sahip ağ mühendislerine ihtiyaç vardır. Spam filtreleme ise başlı başına değişik araştırma konularının bir araya geldiği bir çalışma ortamıdır.

E-posta güvenliğinin başka bir temel ilkesi de uçtan uca güvenliğin sağlanmasıdır. Özel hayatın gizliliği temelde e-posta trafiğinin de olmazsa olmaz ilkesidir ve bu gizliliğin sağlanması için PGP gibi yöntemlere ihtiyaç duyulmaktadır. Tüm güvenlik ilkelerinin gerçekleştiğine ikna olan kullanıcılar e-postayı yaşamının bir parçası haline getirebilmektedirler.

Kendimizi Sınayalım

1. E-posta iletişiminin ilk zamanlarında SMTP portu olarak aşağıdakilerden hangisi kullanılmaktaydı?

a. 20
b. 25
c. 45
d. 80
e. 625

2. Günümüzde Türkiye'de SMTP geçişin engellenmesi için aşağıdaki port numaralarından hangisi kullanıma sokulmuştur?

a. 25
b. 125
c. 225
d. 587
e. 1024

3. Bir MX sorgusu sonrası SPF kayıtları aşağıdaki gibi olan bir etki alanı için:

```
v=spf1 include:spf-a.outlook.com include:spf-b.outlook.com ip4:157.55.9.128/25 include: spf.protection.outlook.com include:spf-a.hotmail.com include:_spf-ssg-b.microsoft.com include:_spf-ssg-c.microsoft.com ~all
```

FROM kısmında kimse@alo.com şeklinde bir e-posta yollanmaya kalkılırsa sonuç aşağıdakilerden hangisinde en doğru biçimde tanımlanmıştır?

a. E-posta gönderilmez.
b. E-posta çöpe atılır.
c. E-posta SPAM olarak işaretlenir ve gönderilir.
d. E-posta SPAM olarak işaretlenir ve çöpe atılır.
e. E-posta Hotmail.com sunucusuna yönlendirilir.

4. SPF TEXT kayıtları nerede tutulur?

a. SMTP sunucusunun bağlı olduğu etki alanı sunucularında tutulur.
b. SMTP sunucusunda tutulur.
c. SPF sunucusunda tutulur. Bu sunucu SMTP hizmeti de sağlar.
d. SMTP hizmeti sağlayan MX sunucusunda tutulur.
e. SPF.MX sunucusunda tutulur.

5. PGP için aşağıda verilen seçeneklerden hangisi **söylenemez?**

a. PGP e-posta yollamak için kullanılabilir.
b. PGP ile mesaj güvenliği sağlanabilir.
c. PGP ile kimlik doğrulama sağlanabilir.
d. PGP ile inkâr edilememe sağlanabilir.
e. PGP ile mesaj bütünlüğü sağlanabilir.

6. Bir bilgisayar, 1 bit ile şifrelenmiş mesajı kaba kuvvet yöntemiyle en çok 1 saniyede çözebiliyorsa aynı bilgisayar 4 bit ile şifrelenmiş bir mesajı en çok kaç saniyede çözebilir?

a. 2 Saniye
b. 4 Saniye
c. 8 Saniye
d. 16 Saniye
e. 32 Saniye

7. Bilgisayarlarda bulunan sertifikaların kullanım amacı aşağıdakilerden hangisinde açıklanmıştır?

a. Bilgisayarın kime ait olduğunu kanıtlamak için kullanılır.
b. İşletim sisteminin çalıntı olup olmadığını anlamak için kullanılır
c. İstenmeyen kullanıcıların e-posta yollamasını engellemek için kullanılır.
d. İstenmeyen e-postaları filtrelemek için kullanılır.
e. Kullanıcıya atanan anahtarları tutmak için kullanılır.

8. Bir özet fonksiyonu programı 8 bitlik özetler üretiyorsa, bu program en fazla kaç değişik veriyi özetleme kabiliyetine sahiptir?

a. 4
b. 8
c. 16
d. 256
e. 1000

9. Bir özet fonksiyonu aşağıdaki amaçlardan hangisi için kullanılır?

a. E-postaya sayısal imza yaratmak için kullanılır.
b. E-postayı şifrelemek için kullanılır.
c. E postayı doğru alıcıya ulaştırmak için kullanılır.
d. E-postanın doğru alıcıya ulaşıp ulaşmadığını kontrol etmek için kullanılır.
e. E-postanın spam olmadığını kanıtlamak için kullanılır.

10. PGP ile tam kimlik doğrulaması yapılmış bir e-posta alıcıya ulaştığında ve alıcı tarafta kimlik doğrulama süreci çalışırken aşağıda tanımlanan işlemlerden hangisi bu süreç içerisinde **yer almaz?**

a. E-postanın özeti çıkartılır.
b. Göndericinin gizli anahtarı karşı taraftan alınır.
c. E-postada gelen şifrelenmiş özet verisinin şifresi çözülür.
d. Göndericinin genel anahtarına ulaşılır.
e. Karşılaştırma yapılır.

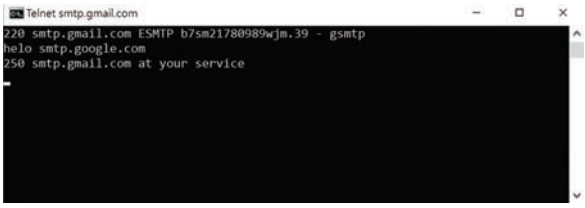
Kendimizi Sınayalım Yanıt Anahtarı

1. b	Yanıtınız yanlış ise "E-posta Temelleri" konusunu yeniden gözden geçiriniz.
2. d	Yanıtınız yanlış ise "Bir Güvenlik Açığı: SMTP Geçiş (SMTP Relaying)" konusunu yeniden gözden geçiriniz.
3. c	Yanıtınız yanlış ise "Gönderen Teyit Politikası (SPF)" konusunu yeniden gözden geçiriniz.
4. a	Yanıtınız yanlış ise "Gönderen Teyit Politikası (SPF)" konusunu yeniden gözden geçiriniz.
5. a	Yanıtınız yanlış ise "PGP (Pretty Good Privacy) ile E-posta Güvenliği" konusunu yeniden gözden geçiriniz.
6. c	Yanıtınız yanlış ise "E-posta şifreleme:" konusunu yeniden gözden geçiriniz.
7. e	Yanıtınız yanlış ise "Kimlik Doğrulama ve Sayısal İmza" konusunu yeniden gözden geçiriniz.
8. d	Yanıtınız yanlış ise "Kimlik Doğrulama ve Sayısal İmza" konusunu yeniden gözden geçiriniz.
9. a	Yanıtınız yanlış ise "Kimlik Doğrulama ve Sayısal İmza" konusunu yeniden gözden geçiriniz.
10. b	Yanıtınız yanlış ise "Kimlik Doğrulama ve Sayısal İmza" konusunu yeniden gözden geçiriniz.

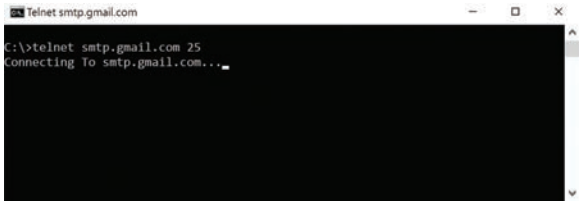
Sıra Sizde Yanıt Anahtarı

Sıra Sizde 1

Windows komut satırı çalıştırıldığında Telnet komutu ile adres ve port tanımlanır ve bu adres ile yazılan port üzerinden iletişime geçilir. Google tarafından sunulan SMTP sunucusu smtp.google.com adresindedir. Bu adrese TCP 25 numaralı port üzerinden bağlanılmaya çalışıldığında muhtemelen port kapalı olacağından yanıt alınamayacaktır. Ancak TCP 587 numaralı port üzerinden bağlantı isteğine karşılık güvenli bağlantı ile iletişim yapabileceğinize dair bir cevap alabileceksiniz. Aşağıdaki şekillerde bu denemeler görülmektedir. Sonuç olarak smtp.google.com servis yöneticileri SMTP geçişine izin vermemektedirler.



587 Numaralı port iletişime açık



25 Numaralı port iletişime kapalı

Sıra Sizde 2

Eğer 64 bit şifre kullanılırsa toplamda en fazla 2^{64} = 18446744073709551616 deneme yapılması gerekmektedir. 1 saniyede 1000000000 şifre denemesi yapan bir bilgisayar programının şifreyi çözmesi için yaklaşık 18446744073 saniyeye ihtiyacı olmaktadır. 1 yıl = 365 * 24 * 3600 = 31536000 saniyedir. Böylece bu şifre en kötü ihtimalle yaklaşık 584 yılda çözülebilir.

Sıra Sizde 3

Her işletim sisteminin kendine göre sertifika görüntüleme yöntemi bulunmaktadır. Windows işletim sistemine ait bir bilgisayarda Chrome İnternet tarayıcı varsa burada ⋮ menüsünden ayarlar tıklanmalıdır. Gelişmiş ayarları göster tıklandığında açılacak HTTPS/SSL paragrafı altında Sertifikaları Yönet butonu, bilgisayara yüklenmiş sertifikaların görüntülenmesini sağlar.

Sıra Sizde 4

Eğer SHA1 algoritması 128 bitlik özet çıkarabiliyorsa bu algoritma en fazla $2^{128} = \sim 3.4 * 10^{34}$ değişik metnin farklı özetini çıkarabilmektedir.

Sıra Sizde 5

Asimetrik şifrelerde anahtar uzunluğu 1.024 bit veya 2.048 bit boyutlarına çıkmaktadır. Bu uzunluktaki anahtarlarla uzun metinlerin blok şifrelenmesi ve şifrelerinin çözümü ancak çok güçlü işlemcilere sahip bilgisayarlarla gerçekleşebilir. Kişisel bilgisayarlarda bu işlemler çok uzun zaman alacaktır ve işlem gücü yeterli olmayacaktır.

Yararlanılan ve Başvurulabilecek Kaynaklar

Kurose James F. ve Ross Keith F., (2013). ***"Computer Networking A Top Down Approach",*** Pearson 6'th Ed.

Chandramouli R., Garfinkel S., Nigthingale S., Rose S. (2016). ***"Trustworthy Email",*** NIST Special Publication 800-177, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-177.pdf

http://www.openspf.org/

AĞ YÖNETİMİ VE BİLGİ GÜVENLİĞİ

8

Amaçlarımız

Bu üniteyi tamamladıktan sonra;

- Sistem güvenliği ile ilgili temel kavramları açıklayabilecek,
- Sistem güvenliği için olası tehditleri analiz edebilecek,
- Güvenlik hedeflerini açıklayabilecek,
- Bilgi güvenliği yaşam döngüsü içindeki temel adımları tanımlayabilecek,
- Yazılım ve donanım güvenliğindeki temel tehditler için alınacak önlemleri açıklayabilecek,
- Güvenli bir sisteme ulaşmak için gerekli kriterler ve ilgili standartları kullanabilecek,
- Sistemi güvenli halde tutmak için yapılması gereken önemli ipuçlarını açıklayabilecek

bilgi ve becerilere sahip olacaksınız.

Anahtar Kavramlar

- Sistem Güvenliği
- Güvenlik Tehditleri
- Bilgi Güvenliği Politikası
- Bilgi Güvenliği Yaşam Döngüsü
- ISO 27001
- Virüsler
- Truva Atı
- Varsayım ve Güven
- Risk
- Güvenlik Açığı

İçindekiler

Ağ Yönetimi ve Bilgi Güvenliği → Sistem Güvenliği

Sistem Güvenliği

GİRİŞ

Büyük ölçekli kuruluşlardan küçük ölçekli şirketlere, hatta son kullanıcının ihtiyaç duyduğu kişisel kullanım cihazları bile çok hızlı dijitalleşirken, bilgisayarlar, cep telefonları, tabletler ve daha birçok dijital cihaz, iş hayatı ve ticaret için birer zorunluluk haline gelmiştir. Elektronik cihazlar aracılığıyla oluşturulan bu sistemlerde gizli tutulması gereken hassas kuruluş verileri ve kullanıcı bilgileri, sistem üzerindeki uygulamaların değeri ve sistemde zarar oluşturmak gibi nedenler ile giderek artan bir şekilde saldırıların öncelikli hedefi haline gelmektedir.

Bir şirketin veya bir şahsın bilişim sistemlerindeki bilgi işlem cihazlarını güvenli bir şekilde kullanabilmesi ve sistem üzerindeki bilgilerin güvenliğini sağlayabilmesi için öncelikle cihazların herhangi bir tehdit altında olmadığından emin olunması gerekmektedir. Eğer sisteme karşı bir tehdit varlığı söz konusu ise bu tehdide karşı gereken güvenlik önlemleri alınmalıdır.

Üniteye başlarken kuruluşların veya bilişim sistemlerini kullanan son kullanıcıların nasıl güvende kalabileceğine odaklanan bir genel bakış vereceğiz.

Günümüzde elektronik cihazlar ve sistemler her yerde karşımıza çıkar ve iletişim, gizlilik, finans, bilim, sanat ve konuşma özgürlüğü gibi modern yaşamın önemli yönlerini etkiler. Elektronik sistemlerin ve altyapının güvenliği ve güvenilirliği her zaman yüksek seviyede endişe kaynağı olmuştur. Bu güvenliği sağlamak son derece zordur. Çünkü sisteme sızmak isteyen bir saldırganın kötü niyetli işlemlerini gerçekleştirmek için tek bir zayıflık bulması yeterliyken, sistemi savunan yapılar sistem güvenliğini sağlamak için sistemi sonsuz sayıda olası güvenlik açıklıklarına karşı korumak için çaba gösterirler. Saldırgan ve sistemi savunan mekanizma arasındaki bu ilişki düşünülürse, güvenlik mekanizmasının hedefi belirli bir tehdit modeli göz önüne alındığında bir güvenlik açığı sınıfının tespit edilmesi ve önlenmesidir. Tüm tehdit modelleri ve güvenlik açıklarını belirleme ve çözme görevi hiçbir zaman tamamen bitirilebilecek bir iş değildir. Bu yüzden her yeni çıkan ve çıkabilecek tehdit için sistem güvenlik politikası sürekli geliştirilmeli ve sistemin güvenlik boşlukları kapatılmalıdır. Ancak böylece saldırganın sisteme erişimi engellenebilir.

Bu bağlamda, sistem güvenliği için aşağıdaki tanımlamayı vermek doğru olur.

Sistem güvenliği, bilgi sistemi kaynaklarının bütünlüğünü, erişilebilirliğini ve gizliliğini korumak amacıyla uygulanacak tedbirler bütünüdür.

Sistem güvenliği tanımında verilen üç temel güvenlik kavramını kısaca tekrar hatırlayalım.

Gizlilik: Bilginin yetkisiz kişilere ifşasının önlenmesi.

Bütünlük: Bilginin yetkisiz kişiler tarafından değiştirilmesinin önlenmesi.

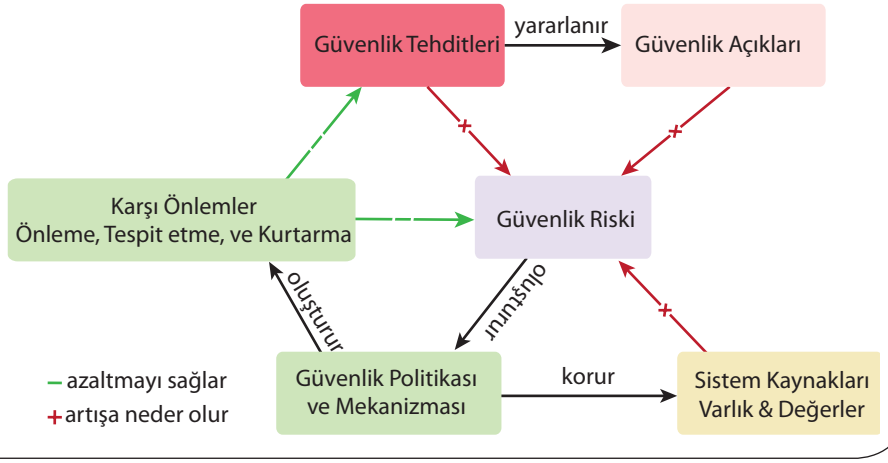
Hazır Bulunma (Erişilebilirlik): Bilgi veya kaynakların yetkisiz bir şekilde alıkonulmasının önlenmesi.

Sistem güvenliğinde gizlilik, bütünlük ve erişilebilirlik olarak sıralanan bu üç unsur büyük önem arz etmektedir. Bilginin yalnızca erişim hakkı tanınmış kişiler tarafından ulaşılabilir olması, bilginin bütünlüğünün ve doğruluğunun temin edilmesi ve yetkili kullanıcıların ihtiyaç duydukları bilgiye her an erişebilmelerinin garanti altına alınması bilgi güvenliğinin temelini oluşturur. Sistem güvenliği uygulamalar, politikalar, yöntemler, yazılım ve donanım fonksiyonları ve organizasyon ile ilgili yapılar gibi birbiri ile ilişkili uygun denetim sağlama araçları ile temin edilebilir.

Sisteme nüfuz etmeye çalışan bir saldırgan, sistemde istismar edebileceği mevcut herhangi bir açığı kullanarak sistemin içine izinsiz girebilir. Bundan korunmak için sistemin gizlilik, bütünlük ve hazır bulunma özelliklerinin korunması sağlanmalıdır. Sistemde bu özelliklere sahip olabilmek için erişimin kontrolü, denetimi ve hata kurtarma gibi birtakım teknik güvenlik önlemleri uygulanması gerekmektedir. Bunlara ek olarak sistem, gerçekliği (kimliği) ve hesap verebilirliği (mesuliyet) açısından da desteklenirse bütüncül güvenlik sağlanmış olur. Sistem, yazılım ve donanım bileşenleri ile birlikte bir bütün olarak düşünülmelidir.

Şekil 8.1

Sistem Güvenliği ile ilgili Birimlerin İlişkileri.



SIRA SİZDE 1

Şekil 8.1. incelendiğinde sistemde güvenlik riskini arttıran bileşenler nelerdir?

Sistem güvenliği ile ilgili temel unsurları ve bu unsurların birbirleriyle olan bağlantılarını Şekil 8.1'den takip edebilirsiniz. Güvenlik açıklarından doğan güvenlik tehditleri, sistem üzerinde güvenlik riski oluşturur. Sistemin kaynakları, yani sistemin toplam değerinin büyüklüğü de güvenlik riskini arttıran bir etmendir. Bu riski minimum düzeye indirmek ve hatta ortadan kaldırmak için güvenlik politikası ile birtakım mekanizmalar geliştirilir. Güvenlik politikası sistemde ortaya çıkan tehditleri azaltan ve hatta bu tehditler karşısında sistemi kurtaran birtakım karşı önlemler alır. Temel anlamda *sistem güvenliği*, sistemde oluşan riskleri en düşük seviyeye indirmek için alınması gereken güvenlik politikası ve mekanizmaların bütünü olarak açıklanabilir.

Bu girişten sonra ünitede, bilgi sistemleri güvenliği ile ilgili temel kavramlar gözden geçirilecek, sistem üzerindeki olası güvenlik tehditleri açıklanacaktır. Belli başlı güvenlik tehditlerini ortadan kaldırmak veya hafifletmek için uygulanabilecek önlemler üzerin-

de durulacaktır. Sistem güvenliğini sağlamak için öncelikle kabul edilen varsayımların doğruluk düzeyi güvenlik seviyesini arttırır. Bunu bir örnek üzerinden göstereceğiz. Bu varsayımlar ve garanti edilen güven üzerine, sisteme yapılan saldırılara karşı oluşturulan korunma mekanizmasının mantığı üzerinde durulacak ve alınacak önlemlerden bahsedilecektir. Böylece sistemin güvenli kalabilmesi için gerekli güvenlik politikasının nasıl oluşturulması gerektiği hakkında fikir sahibi olacaksınız. Oluşan tehditler, kabul edilen varsayımlar, güvenlik politikası ve mekanizmasının tasarımı ve bunların uygulanması sonucu tekrar yeni tehditler ortaya çıkar. Bunlar güvenlik politikasının güncellenmesini ve ilgili tüm adımların tekrar yapılmasını gerektirir. Sistem güvenliğini sağlamak için uygulanan bu adımlar bilgi güvenliği yaşam döngüsünü oluşturur. Bu döngünün sürekliliğinin sağlanması konusundaki gereklilikler açıklanacaktır. Bundan sonra sistem, yazılım ve donanım olarak iki ana kısma ayrılacak ve bu kısımların güvenliği ayrı ayrı derinlemesine incelenecektir. Bütün bunlar ışığında bilgi güvenliği yönetim sistemi gereksinimlerini tanımlayan ISO 27001 standardının kapsamı üzerinde durulacaktır. Ünite, sistem güvenliğini yüksek seviyede tutmak için gerekli altın kurallar ile sonlanacaktır.

SİSTEM GÜVENLİĞİ İLE İLGİLİ TEMEL TERİMLER

Bu ünite kapsamında sistem güvenliği ile ilgili bilinmesi gereken temel terimler aşağıda kısaca tanımlanmıştır.

Güvenlik Açığı: Sistemin güvenlik politikasını ihlal etmek için kullanılabilecek, sistemin tasarımında veya gerçeklemesinde ortaya çıkan, tasarımcı tarafından düşünülmemiş zayıflıklar olarak tanımlanır.

Tehdit: Bir güvenlik açığından yararlanabilecek olası bir tehlike, tehdit kavramını ifade eder. Güvenliği ihlal etme potansiyeli olarak da ifade edilir.

Risk: Bilgi veya kaynak kaybı olasılığı, sistem güvenliğinde risk olarak tanımlanır. Belirli bir tehdidin sistemde bulunan bir güvenlik açığından yararlanarak sistemi zarara uğratma olasılığını ifade eder.

Saldırgan: Sisteme saldıran kişi ya da kuruluş olarak tanımlanır.

Saldırı: Sistem ve bilgi güvenliği önlemlerini aşmak için bir güvenlik açığından yararlanıp sisteme akıllı bir şekilde izinsiz girmeye denir. Sistemdeki güvenlik servislerini aşan ve güvenlik politikalarını ihlal eden kasıtlı bir girişimdir.

Karşı Önlem: Sistem üzerindeki tehdidi, saldırıya açıklığı veya saldırının neden olabileceği zararları öngörüp bunları azaltarak ortadan kaldırmaya ya da engellemeye yönelik bir eylemdir. Bu amaca yönelik uygulanan araç, yöntem veya teknikler karşı önlem olarak adlandırılır.

Sistem Kaynakları: Sistemin kendisi, sistem yetenekleri, sistem hizmetleri, donanım bileşenleri, iletişim hatları vb. varlıklar sistem kaynağı olarak kabul edilir.

Güvenlik Politikası: Gizli kalması gereken verileri ve kritik sistem kaynaklarını korumak için sistemin güvenlik hizmetlerini nasıl sağladığını belirten birtakım kural ve uygulamalardan oluşan prensipler bütünüdür.

SİSTEM GÜVENLİĞİ İÇİN TEHDİTLER

Güvenlik tehdidi aslında potansiyel bir güvenlik ihlalidir. Sistem güvenliğinde *tehdit,* bir güvenlik açığını kullanarak güvenlik politikasında belirtilmiş güvenlik kurallarını ihlal edebilecek ve bunun sonucunda zararlara yol açabilecek olası tehlike olarak tanımlanır. Aslında ihlalin sadece bir güvenlik tehdidi olması gerekmez. İhlalin gerçekleşebileceği gerçeği, bunun gerçekleşmesine neden olan eylemlere karşı korunma veya bunlara hazır olunmasını gerektirir. Bu eylemlere *saldırı* denir. Bu eylemleri gerçekleştiren veya gerçekleşmesine neden olan kişiler ise *saldırgan* olarak tanımlanır.

Bir tehdit ya kasıtlı olarak yapılan bir eylemden ya da bir sistem arızasından kaynaklanabilecek bir hatadan meydana gelebilir. Uluslararası Standartlar Teşkilatının yayınladığı bilgi güvenliğinde risk yönetimi ile ilgili olan standartları içeren ISO 27005 standardında tehdit, sistemden oluşabilecek olası bir olay, sistemin ve/veya organizasyonun zarar görmesine neden olması olarak tanımlanmıştır. Gizlilik, bütünlük ve erişilebilirlik olarak bilinen üç önemli güvenlik servisi, bir sistemin güvenliğine yönelik tehditler karşısında koruma mekanizması olarak görev alır. Shirey (1994) tehditleri dört ana sınıfta incelemiştir. Bunlar şöyle sıralanabilir:

1. ***Ele geçirme:*** Gözetleme, ifşa etme veya yetkisiz bilgiye erişim,
2. ***Uydurma/Üretme:*** Aldatma veya sahte verilerin kabul edilmesi,
3. ***Kesinti:*** Bozulma, kesinti veya doğru çalışmayı engelleme,
4. ***Değişiklik:*** Zorla el koyma veya bir sistemin bir bölümünün yetkisiz kontrolü; sadece yetkisiz erişim elde etmekle kalmaz, aynı zamanda bilgiyi değiştirir.

SIRA SİZDE 2

Yetkisiz bir kullanıcının bir sistemi çökertmek amacıyla sisteme giriş yapmaya çalıştığını varsayalım. Amacı sadece sistemin çalışmasını engellemektir. Bu saldırı hangi sınıfta incelenebilir?

Yukarıda listelenen bu dört sınıf pratikte birçok sistem üzerinde görülen ortak tehditleri kapsamaktadır. Sistemlerde oluşabilecek tehditler, sistemin birçok yerinde karşımıza çıkabileceğinden dolayı belli başlı tehdit unsurları hakkında giriş niteliğinde bir açıklama ile sistem güvenliğinin daha iyi anlaşılabilmesi sağlanacaktır.

Araya girme (snooping) tehdidi sistem üzerindeki gizlilik hizmeti ile engellenir.

Araya girme (Snooping), bilginin izinsiz bir şekilde ele geçirilmesidir ve bir gözetleme biçimi olarak değerlendirilir. Pasif bir tehdit biçimidir; tehdit eden varlığın sistemin bilgisini ve dosyalarını taraması veya iletişimini dinlemesi örnek olarak verilebilir. Pasif olarak "hatta girme", hattı dinleyerek bir ağın izlendiği gözetleme biçimidir. Ağı oluşturan fiziksel kablo hatları nedeniyle "hatta girme" ya da "Telekulak" olarak adlandırılır. Ancak herhangi bir fiziksel kablolama söz konusu olmadığında bile bu terim kullanılır. Gizlilik hizmeti bu tehdide karşı koruma mekanizması olarak görev yapar. Böyle bir tehdidin oluşması durumunda gizlilik hizmeti tarafından sunulan bilgi güvenliği mekanizmaları ile hat dinlense bile içindeki veriye ulaşmak mümkün olmayacaktır.

Değişikliğe uğratma veya modifikasyon, yetkisiz olarak bilginin değiştirilmesidir. Yukarıda bahsedilen tehdit sınıflarından üçünü birden kapsar. Modifikasyon ile asıl hedeflenen, aldatma tehdidi oluşturmaktır. Çünkü bazı sistemler sistemdeki veriler üzerinde değişiklik yaparak hangi eylemi yapacağını belirler. Bu değişikliğe uğratılan veriler tehdit eden varlıklar tarafından değiştirilerek yapılacak eylemin kendi amaçlarına hizmet eden başka bir eylem olması sağlanır veya yanlış bir bilgiyi doğru olarak kabul ettirme durumunu oluştururlar. Eğer bu değiştirilen bilgi, sistemin çalışmasını kontrol ediyorsa bozulma veya zorla el koyma tehditleri de ortaya çıkar. Gözetleme tehdidinin aksine modifikasyon aktif bir tehdit biçimidir. Bir varlığın bilgiyi değiştirmesinden kaynaklanır. Ağ üzerinde iletilen verinin değiştirilerek alıcı tarafa ulaşması, aktif olarak hattı dinleme ve hattaki bilgiyi değiştirme olduğundan modifikasyon tehdidi sınıfına girer. Buradaki "aktif" kelimesi, bu tehdidin gözetleme tehdidinden ayrılmasını sağlar. Bir saldırganın gönderenden gelen iletileri okuması ve bu iletileri değiştirerek, alıcı ve gönderici farkında olmadan alıcıya ulaşmasını sağlaması modifikasyon tehdididir. Saldırgan, gözetleme tehdidinde pasif modda verileri sadece dinlerken, modifikasyon tehdidinde ise aktif bir biçimde verileri değiştirerek sisteme saldırı gerçekleştirmektedir. Bu örnekteki saldırganın yaptığı saldırı "aradaki adam" saldırısıdır. Mesaj bütünlüğü servisi bu tehdide karşı bir savunma mekanizması sunar. Eğer gönderen, gönderdiği verinin bütünlüğünü mesaj bütünlüğü sağlayan

yöntemler ile desteklemişse, alıcı gelen verinin değiştirilmediğinden emin olacaktır. Bu yöntem, sistemde modifikasyon tehditlerine karşı koruma mekanizmasının önemli bir kısmını teşkil eder.

Sahtecilik veya olduğundan başkası gibi görünmek, bir varlığın başkasının kimliğine bürünerek sistemde yetkisi olmayan servislerden faydalanması ya da sisteme erişerek sistemin doğru çalışmasını engellemek istemesidir. Aldatma ve zorla el koyma tehdit sınıfları içinde değerlendirilen bir tehdit çeşididir. Burada saldırıya maruz kalan sistemin iletişim kurduğu varlığın farklı bir varlık olduğuna inanması sağlanmıştır. Örneğin; bir kullanıcı İnternet üzerinden bir bilgisayara giriş yapmaya çalışırken, gerçekte girmek istediği bilgisayar yerine giriş yapılmak istenen bilgisayar olduğunu iddia eden başka bir bilgisayara erişmesi için yönlendirilebilir. Bu durum kullanıcının nihayetinde dolandırılmasına yol açacak bir tehdit ile karşı karşıya kalmasına sebep olacaktır. Benzer şekilde, bir kullanıcı bir dosyayı okumak istediğinde, saldırganın bu dosya yerine kullanıcıya başka bir dosyayı açmasını sağlaması da başka bir sahtecilik saldırısı örneğidir. Sahtecilik pasif bir saldırı olarak da karşımıza çıkabilirken genellikle aktif bir saldırı yöntemidir. Sahtecilik yapan saldırgan kullanıcıya kendi kimliği hakkında yanıltıcı yanıtlar göndererek aktif bir saldırı gerçekleştirmesine yol açabilir. Öncelikle aldatma tehdidi olarak düşünülmesine rağmen, saldırganın yetkili bir yönetici veya denetleyiciyi taklit etmesi yoluyla sistemin kontrolünü gasp etmesiyle sistemin tüm kontrolünü alacak bir tehdide dönüşmesi durumu sıklıkla karşımıza çıkar. Mesaj bütünlüğü ve kimlik doğrulama metotları bu tehdidin engellenmesinde önemli rol oynar.

Bu tip tehdit ve saldırılara daha birçok örnek verebiliriz. Fakat anlaşılması gereken bu tip tehditlerin dört ana sınıf içinde değerlendirebileceğidir. Sistemde oluşabilecek tehditleri engelleyecek mekanizmaları barındıran bir güvenlik politikasının tüm yönleriyle güçlü bir şekilde oluşturulması sistem güvenliği açısından büyük önem arz etmektedir.

Tehditler, sistemde var olan güvenlik açıkları üzerinden gerçekleşirler. Güvenlik açıkları donanım, yazılım ve veri olmak üzere üç ana kısımda incelenebilir. Sistemin donanım bileşenlerinden kaynaklanan açıklara örnek olarak kasıtlı veya kasıtlı olmayan bir fiziksel hasar verilebilir. Sistemin kendisinde, kaynaklarında veya sistem ile ilgili ekipmanda hasar oluşma olasılığı, donanım güvenlik açığı olarak düşünülür. Ulaşılabilirlik özelliğine karşı en önemli tehditler, bu tip açıklar aracılığıyla oluşturulur. Gelişen teknoloji ile **entegre devre içinde** ve tespit edilmesi oldukça zor olan daha farklı donanım güvenlik açıkları oluşturma riski ortaya çıkmaktadır.

Gelişen teknoloji ile **entegre devre içindeki** donanım, güvenlik açıklarını kullanarak sisteme saldırılar gerçekleşebilir.

Yazılım güvenlik açıkları yazılım silme, yazılım değiştirme, yazılım hırsızlığı olmak üzere kendi içinde üç ayrı kısımda incelenebilir. Yazılım değiştirmeye örnek olarak Truva atı, virüs ve arka kapı uygulamaları verilebilir. Yazılım, herhangi bir aşamada kötü bir amaçla ya da kasıtsız bir şekilde değiştirilebilir, silinebilir veya yok edilebilir. Bu saldırı, yazılımdaki güvenlik açığı üzerinden yapılır. Kötü amaçlı bir yazılım aslında kendisinden bekleneni ve yapması gereken işleri yapmaya devam eder ancak aynı zamanda sistem arka planında fazladan kötü amaçlı işlemler yapar. Örneğin, kullanıcının istediği işlemleri yaparken aynı zamanda kötü amaçlı olarak kullanıcının özel bilgilerini üçüncü şahıslara sunabilir.

Veri üzerinden ortaya çıkan güvenlik açıklarını engellemek için veri üzerinde güvenlik, bütünlük ve ulaşılabilirlik sağlanmalıdır. Buradaki temel ilke, bilgisayar üzerindeki bilgi değerini kaybedene kadar güçlü bir şekilde korunmasıdır.

VARSAYIMLAR VE GÜVEN

Bir sistemin güvenliğini sağlayabilmek için gerekli güvenlik seviyesini, türünü ve ilgili mekanizmaları doğru bir şekilde tanımlamak sistem güvenliğinde ilk olarak çözülmesi

gereken sorulardan bir tanesidir. Buradan hareketle güvenlik, gerekli güvenlik türüne ve çalıştırılacağı ortama özgü *varsayımlara* dayanmaktadır.

Kaba kuvvet saldırısı, bilgi güvenliği konusundaki en basit saldırı yöntemidir. Bir işin çok zeki olmayan ama güce dayalı çözümüdür ve her zaman en uzun çözüm yoludur. Olası bütün parola ihtimallerinin denenmesi ile doğru parolanın bulunmasına dayanır. Burada kaba kuvvetten kasıt, saldırı yapan varlığın elinde bulundurduğu kaynakları tanımlar. Eğer saldırı yapan varlık sahip olduğu bütün imkân ve kaynaklar ile makul bir zamanda bütün ihtimalleri deneyerek parolayı bulabiliyorsa, kaba kuvvet saldırısı başarılı olmuştur denir.

Örnek olarak, bir sisteme giriş yapabilmek için sistemin kullanıcıdan bir parola girmesini istediğini düşünelim. Buradaki en temel varsayım, sistem giriş parolasının **kaba kuvvet saldırısı**na dayanıklı olacak şekilde karmaşıklığa sahip olmasıdır. Bu varsayım bir aksiyom olarak ele alınır ve parola ile sistem erişim kontrolü en temel erişim kontrollerinden bir tanesi olarak değerlendirilir. Eğer saldırıyı gerçekleştirecek varlık parola sisteminin bütün olası ihtimallerini makul zamanda deneyecek yeterli güçte kaynaklara sahip ise bir kullanıcının sisteme giriş için kullandığı parolasını çözebilir. Dolayısıyla, böyle yetenekli ve güvenilmez bir varlığın bulunduğu bir ortamda kabul edilen varsayım yanlıştır.

Varsayımlar ile ilgili bir başka örnek şöyle olabilir: Sistem erişim kontrolü için kullanılan parolaların sistem içinde saklanıp, kullanıcılar sisteme giriş yaparken kontrol edildiği ve bu giriş kontrol mekanizmasının bir yönetim birimi tarafından kontrol edildiğini düşünelim. Bu durumda varsayım, parola yönetim biriminin güvenilir olmasına dayanır. Eğer bu birim güvenilir ise varsayım doğrudur. Güvenilirlik terimi ise sisteme giriş yapmak isteyen kullanıcının, sistem kendisinden parolasını istemediği sürece kullanıcın parolasını kullanmaması, güvenli bir şekilde saklaması ve herhangi başka üçüncü bir şahıs ile paylaşmaması anlamına gelir. Burada üzerinde durulan güven ilişkisi, güven rolü ile ilgili bir diğer örnektir. Sistemin güvenlik kuralları içinde tanımlanmış bir istisna, sisteme girişte güvenlik mekanizmalarının atlanabildiği bir arka kapı sağlar. Buradaki güven ise güvenlik politikası içinde tanımlanmış olan bu istisnanın bir arka kapı olarak kullanılmayacağı varsayımı üzerine dayanır. Eğer bu kapı kullanılırsa, güven yanlış yerleştirilmiş demektir ve güvenlik mekanizması hiçbir güvenlik sağlamayacaktır.

Parola örneğinde olduğu gibi bir güvenlik politikası, bu politikayı oluşturan sistem tasarımcılarının uygulayabileceği düşünülen birtakım aksiyomlardan oluşur. Sistem tasarımcıları temel olarak daima iki varsayımda bulunurlar. Birincisi, politika doğru ve kesin olarak olası bütün sistem durumları kümesini "güvenli" ve "güvenli olmayan" olmak üzere bölmelere ayırır. İkincisi ise, güvenlik mekanizmaları sistemin "güvenli olmayan" bir duruma girmesini engeller (Bishop, 2015). Eğer varsayım hatalıysa, sistem güvensiz olacaktır.

Burada verilen ikinci varsayım, güvenlik politikasının güvenlik mekanizmaları tarafından uygulanabileceğini söyler. Bu mekanizmalar güvenli, hassas ya da geniş kapsamlıdır. Olası tüm durumların kümesi olarak P kümesini tanımlayalım. Q ise güvenlik politikası tarafından belirtilen, sistemdeki güven olarak nitelenen durumları tanımlayan küme olsun. Güvenlik mekanizmalarının sistemi R kümesi içinde tanımlanan birtakım durumları sınırlar. Bu tanımdan hareketle, $R \subseteq P$ denir. Buradaki kümelerin matematiksel gösterimlerini kullanarak aşağıdaki tanımı verebiliriz:

Eğer $R \subseteq Q$ ise sistem güvenlik mekanizması güvenlidir; Eğer $R = Q$ ise sistem güvenliği hassas ve kesindir. Eğer sistemde $r \in R$ ve $r \notin Q$ gibi sistem durumları mevcutsa ilgili sistemin geniş kapsamlı olduğu anlamına gelir.

İdeal olarak sistemin güvenlik mekanizmasının hassas ve kesin olması gerekir ($R = Q$). Bütün sistem güvenlik mekanizmalarının bileşenleri, güvenli olmayan durumları engellemek için aktif bir şekilde çalışmalıdır. Hâlihazırda güvenli olan sistem durumları için güvenlik mekanizmasının işlem yaparak sistem kaynaklarını boşa kullanması istenmeyen bir durumdur. Gerçekte ise güvenlik mekanizmaları geniş kapsamlıdır ve sistemin güvenli olmayan durumlara girmesine sebep olabilir.

Sistem güvenliğinde güven için yapılan varsayımlar çok açık değildir ve sistemler değiştiğinde mutlaka başarısız olurlar. Örneğin; İnternette küresel ölçekte sistemler kullanıldığında, İnternet üstünde alınan varsayımlar üstü örtülü olduğu için sistem güvenliği başarısız olur.

Güvenlik gereksinimlerinin analizinde son zamanlarda yapılan bir değişiklik, güvenli yazılım mühendisliğinde güven varsayımlarına yöneliktir. Viega ve ark. (2001) güven ve güvenilirliğin, güvenliğin ve güven ilişkilerinin temelini oluşturduğunu savunur. Aynı zamanda, güven oluşumunu herhangi bir sistemin altında yatan güvenliği önemli ölçüde etkileyebileceğini de savunurlar. Güven varsayımlarının yanıltıcı olduğunu iddia ederler.

Sistemlerde ortaya çıkan birçok **güvenlik açığı**, pratikte bir karşılığı bulunmayan veya yanlış değerlendirilen varsayımların sonucunda meydana gelir. Bu bağlamda düşünüldüğünde bir sömürme (exploit), kullanılan varsayımın yanlış olduğunu ispatlamanın bir yoludur.

Sistemlerde ortaya çıkan birçok **güvenlik açığı**, yanlış bir şekilde değerlendirilen varsayımların sonucunda meydana gelir.

Exploit kelimesinin Türkçe anlamı kendi çıkarı için kullanmak, istismar etmek ve faydalanmaktır. Bilişim dünyasında ise "exploit" yani sömürme, bir sistem üzerinde var olan sistem açıklarından, kod hatalarından veya hatalı varsayımlardan faydalanarak istenmeyen veya planlanmamış hatalar oluşturmak için tasarlanmış küçük kod veya programlardır. Bir sisteme yetkisiz bir şekilde erişmeye çalışma, yetkili sahte kullanıcı kimliği oluşturma ve sistemi devre dışı bırakma amacıyla yazılmış programları örnek olarak verebiliriz. Sistemin bilgi güvenliği politikası ve mekanizmaları, sistem üzerinde herhangi bir açık, hata veya yanlış varsayım barındırmadan, bu tip sömürü programlarına geçit vermeyecek şekilde bir bütün olarak ele alınmalıdır.

BİLGİ GÜVENLİĞİ POLİTİKASI VE MEKANİZMASI

Bilgi güvenliğinde en önemli etmenler, güvenlik politikasının bir bütün olarak oluşturulması ve kurgulanan mekanizma ile arasındaki ayrımın net bir şekilde yapılmasıdır. Bu noktada güvenlik politikası ve mekanizmasının Bishop tarafından verilen tanımlarına göz atalım (Bishop, 2015):

Güvenlik politikası, nelere izin verilip verilmeyeceğini belirleyen kurallar bütünüdür.

Güvenlik mekanizması, bir güvenlik ilkesinin uygulanması için kullanılan yöntem, araç veya izlektir.

Konuyu daha derinlemesine anlamak için birkaç örnek üzerinden bu kavramları inceleyeceğiz. Mekanizmalar, şifre değiştirmeden önce kimlik belgesi istemek gibi teknik olmayan şekillerde de olabilir. Aslında politikalar, teknolojinin uygulayamayacağı bazı mekanizmaları da gerektirebilir. Sistemde bilgi güvenliğini sağlayan güvenlik politikasını örnekler üzerinden açıklamaya çalışalım. Bir üniversitenin bilgisayar laboratuvarında herhangi bir öğrencinin başka bir öğrencinin hazırlamış olduğu laboratuvar sonuçlarını kopyalamasını yasaklayan bir politikası olduğunu varsayalım. Bu tip bir güvenlik politikasını oluşturabilmek için, bilgisayar sistemi her kullanıcı için diğer kullanıcıların ilgili dosyalara erişimini engelleyecek mekanizmalar sunar. Mesela, Can sistem tarafından sunulan bu mekanizmaları laboratuvar ile ilgili oluşturmuş olduğu dosyalarını korumak için kullanmaz ve Bora onlara erişir ve kopyalar. Bu durumda Bora güvenlik politikasını ihlal ederek bir güvenlik ihlali meydana gelmesine yol açar. Can'ın laboratuvar süresince sadece kendinde kalması ve başka öğrencilerin erişmemesi gereken dosyaları korumasındaki başarısızlığı, Bora'nın bu dosyaları kopyalamasına olanak tanır. Bu örnekte, Can sistem tarafından sunulan imkânlar ile kendi dosyalarını çok kolay bir şekilde koruyabilecekken, başka sistemlerde böyle bir koruma kolay olmayabilir. Buna örnek olarak İnternet ortamını düşünebiliriz. Çünkü İnternet yalnızca en temel güvenlik mekanizmalarını sağlar. Bu temel mekanizmalar ağlar üzerinden gönderilen bilgileri korumak için yeterli değildir. Bununla beraber, web sitelerindeki hesaplara ulaşmak için kullanılan şifrelerin ve diğer kişisel hassas bilgilerin, işlemlerin vb. verilerin kayıt altına alınması, birçok sitenin öne sürdüğü güvenlik politikasını ihlal etmektedir. Dikkat edilmesi gereken husus ise bu verilerin bir kullanıcının gizli varlığı olduğu ve kimsenin bu bilgileri kaydedemeyeceğidir.

Güvenlik politikaları, "izin verilen" yani güvenli ve "izin verilmeyen" yani güvenli olmayan durumların bir listesi olarak matematiksel olarak tanımlanabilir. Biz burada, herhangi bir politikanın içerdiği matematiksel olarak ifade edilmiş bu güvenli (izin verilen) ve güvenli olmayan (izin verilmeyen) durumların açık bir şekilde verildiğini varsayacağız. Aslında gerçekte politikalar nadiren çok açık bir şekilde ifade edilmiştir. Bu politikalar normalde kullanıcıların ve personelin ne yapmalarına izin verildiğini açıklayan tanımlamalardan oluşmaktadır ve bu tanımlamaların bazı belirsizlikler barındırması söz konusudur. Tanımlanan bu açıklamalar içinde bulunan belirsizlikler, "izin verilen" veya "izin verilmeyen" olarak sınıflandırılmayan durumların oluşmasına yol açmaktadır. Örnek olarak yukarıda tartışılan laboratuvar dersi politikasını ele alalım. Bir kullanıcının başka bir kullanıcının laboratuvar dosyalarını kopyalamadan, sadece onun dizinine göz atması acaba bir güvenlik ihlali midir? Bu sorunun cevabı birçok parametreye bağlıdır. Bunlar bu ünitede işlediğimiz konuların dışındaki konuları kapsamaktadır ve zamanla değişebilecek olan gelenekler, kurallar, yönetmelikler ve yasalar üzerinden değerlendirilir.

İki farklı sistem veya kuruluş birbirleriyle iletişim kurduğunda veya işbirliği yaptığında, bu kuruluşlar birbirleriyle yapacakları iletişimi tanımlayan ve iki tarafın güvenlik politikalarına dayanan bir güvenlik politikası tanımlarlar. Eğer bu politikalar tutarsızsa, taraflardan biri kendi başına veya ikisi birlikte bu ortak güvenlik politikasının ne olması gerektiğine karar vermelidir. Tutarsızlık genellikle güvenlik ihlali olarak kendini gösterir. Örneğin, bir şirket fikri mülkiyet belgelerini bir üniversiteye verirse, şirketin gizlilik politikası çoğu üniversitenin açık politikaları ile uyuşmayacaktır. Üniversite ve şirket, tutarlı bir politika üretmek için ihtiyaçlarına cevap veren karşılıklı bir güvenlik politikası geliştirmelidir. Aksi halde bir güvenlik ihlali olasılığı doğacaktır. Ayrıca, bu iki kuruluşun, bir İnternet servis sağlayıcısı gibi bağımsız bir üçüncü taraf aracılığıyla iletişim kurması söz konusu olduğunda, durumun karmaşıklığının hızla büyüyeceği de göz önünde bulundurulmalıdır.

Güvenliğin Hedefleri

Bir güvenlik politikasının "güvenli" ve "güvenli olmayan" eylemlerinin tanımları göz önüne alındığında, bu güvenlik mekanizmaları sisteme karşı oluşabilecek saldırıyı önleyebilir, bu saldırıyı tespit edebilir veya saldırıdan kurtarabilir (Bishop, 2015). Güvenlik politikası içindeki stratejiler birlikte veya ayrı olarak kullanılabilir. Burada saldırıya karşı oluşturulan güvenlik politikasının hedeflerini ayrıntılı bir şekilde örnekler üzerinden inceleyeceğiz.

Saldırıları Önleme

Saldırıları önleme bir saldırının başarısız olma durumu anlamına gelir (Bishop, 2015). Örneğin, bir kişi İnternet üzerinden sistem içindeki bir ana bilgisayara girmeye çalışırsa ve bu ana bilgisayar İnternete bağlı değilse, bu saldırı engellenmiştir. Saldırı önleme, doğru ve değiştirilemez bir şekilde uygulanmalıdır. Güvenilir olan ve kullanıcıların geçersiz kılamadığı mekanizmaların uygulanmasını içerir ve böylece saldırgan mekanizmayı değiştirerek yenemez. Koruyucu mekanizmalar genellikle hantaldır ve sistemin normal kullanımını engelleyen bir noktaya gelinceye kadar sistemin kullanımına müdahale eder. Bunun tersine, yetkisiz kullanıcıların sisteme erişmesini önlemeyi amaçlayan parolalar gibi bazı basit önleme mekanizmaları yaygın şekilde kabul görmüştür. Gerçekte farklı çeşitlerde önleme mekanizmaları var olmaktadır. Bunlar herhangi bir sistem parçasının ele geçirilmesini önler. Bu mekanizmalar tarafından korunan değerin veya kaynağın, en azından teorik olarak güvenlik sorunları için ayrıca izlenmesi gerekmez.

Saldırıları Tespit Etme

Saldırı tespiti, bir saldırının önlenemediği durumlarda en kullanışlı seçenektir. Ayrıca önleyici tedbirlerin etkinliğini de gösterebilir (Bishop, 2015). Sisteme karşı yapılan saldırıların tespit edilmesi söz konusudur. Tespit mekanizmaları bir saldırının gerçekleştiğini kabul eder. Buradaki amaç ise bir saldırının devam ettiğini veya oluştuğunu belirlemek ve rapor etmektir. Bununla birlikte tespit, saldırının doğası, şiddeti ve sonuçları hakkında veri sağlamak için izlenebilir. Yaygın olarak görülen tespit mekanizmaları, bir saldırıyı belirten eylemleri veya bilgileri arayacak şekilde sistemin çeşitli yönlerini devamlı izler. Böyle bir mekanizmaya örnek olarak, bir kullanıcı sisteme giriş yaparken üç kez yanlış şifre girmesi durumunda uyarı veren bir mekanizmayı verebiliriz. Oturum açma devam edebilir, ancak sistem günlüğünde yanlış yazılan çok sayıda parola, bir hata iletisi olarak kullanıcıya bildirilir. Eğer bu durum kullanıcının bilgisi dâhilinde değilse başka birinin sisteme giriş yaptığı tespit edilir. Tespit mekanizması tarafından korunan kaynak veya değer, güvenlik sorunları için sürekli veya periyodik olarak izlenir.

Saldırılardan Kurtarma

Saldırılardan kurtulma iki biçimde ortaya çıkabilir. İlki, yapılan saldırıyı durdurmak ve bu saldırının yol açtığı hasarları değerlendirip onarmaktır. Örneğin, bir saldırı sistem üzerinde saklanan bir dosyayı hedef alıp sildiyse, bu saldırının kurtarma mekanizması, o dosyanın yedekleme yapılan hafızadan tekrar geri yüklemesi şeklinde olabilir. Her saldırı kendine özgü yöntemler izleyerek sistem üzerindeki farklı açıklıklardan yararlanıp birbirine benzemeyen özellikler barındırdığı için her bir saldırı özelinde uygulamada kurtarma mekanizması oluşturmak çok karmaşık bir mekanizma gerektirir. Bu yüzden saldırı sonucunda ortaya çıkan hasarın kapsamını tamamen tanımlayabilmek oldukça zor bir işlemdir. Bunun bir adım ötesi, saldırganın geri dönmesi ve aynı sistem açığını kullanarak sisteme saldırıyı tekrarlamasıdır. Bunu önleyebilmek için saldırgan tarafından kullanılan güvenlik açıkları tanımlanmalı ve kapatılmalıdır. Bazı durumlarda, saldırganı durdurmak için onun sistemine saldırı yapmak da kurtarma işleminin bir parçası olarak düşünülebilir. Burada anlatılan durumlarda sistemin doğru bir şekilde çalışması engellenir. Kurtarma işleminin asıl tanımı, sistemin yeniden doğru çalışma noktasına geri dönmesini sağlamaktır.

İkinci bir kurtarma biçimi ise sistem saldırı altındayken, **sistemin çalışmasına devam etmesi**dir. Fakat bu tür bir kurtarma mekanizması sistemlerin karmaşıklığını düşününce oldukça zor bir hedeftir. Böyle bir mekanizma hataya dayanıklılık ve güvenlik tekniklerinin birleşmesi neticesinde mümkün olabilir. Kritik görev barındıran sistemler için ise bu tip kurtarma mekanizmaları mutlaka sağlanmalıdır. Bu kurtarma yöntemi, ilk kurtarma yönteminden oldukça farklıdır. Çünkü sistem saldırı altındayken hiçbir noktada hata yapmaz. Fakat bazı önemli olmayan bileşenlerini devre dışı bırakabilir. Sistem, kurtarma mekanizması olarak hatayı tespit ettikten sonra hatayı düzeltme işlemlerini devreye alabilir.

Sistem saldırı altındayken **sistemin çalışmasına devam etmesi**, hataya dayanıklılık ve güvenlik tekniklerinin birleşmesi neticesinde mümkün olur.

Güvenilir Sistem Değerlendirme Kriterleri

Ünitenin bu kısmında bir sistemin içinde yer alan güvenlik kontrollerinin etkinliğinin değerlendirilmesi açısından temel teşkil edecek bazı kriterler verilecektir. Sistemin güvenliğinin değerlendirilmesi birçok fayda sağlamaktadır. Güvenlik değerlendirmeleri, objektif ve iyi tanımlanmış değerlendirme kriterleri ve yöntemleri gerektirir. Bu ölçüt ve yöntemlerin uluslararası olarak kabul edilen birkaç versiyonu vardır.

Güvenlik Politikası Doğrulaması: Bir sistemin güvenliği açısından çok güçlü bir takım standartlar ve protokoller kullanılsa bile, sistemin bu mekanizmaları taşıyıp taşımadığı hakkında bir doğrulama mekanizması yoksa bir üst düzey güvenlik boyutuna geçilemez.

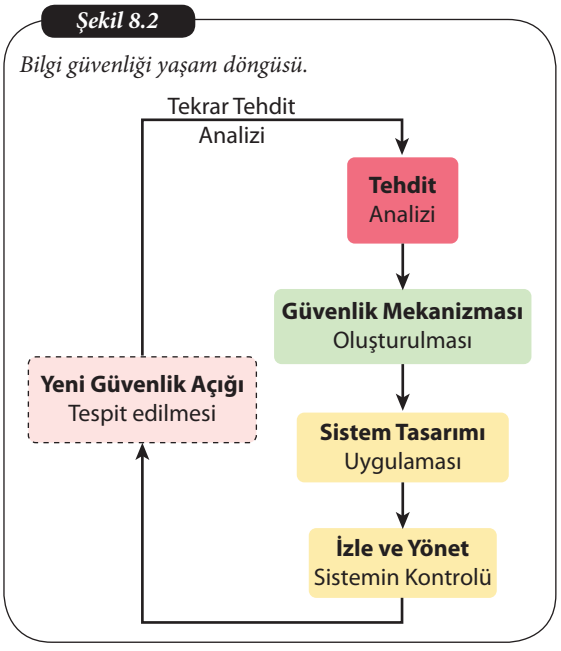
Birçok üretici, sisteminin güvenlik açısından açık barındırmadığını iddia edebilir. İddia edilen güvenlik servislerinin sistemde bulunduğunun bağımsız başka bir araç vasıtasıyla doğrulanması, sistemin güvenliğini bir üst düzeye çıkartacaktır. Bu yüzden güvenlik doğrulama sistemin güvenliği açısından oldukça büyük öneme sahiptir.

BİLGİ GÜVENLİĞİ YAŞAM DÖNGÜSÜ

Sistem kaynakları yani sistemin sahip olduğu varlıklar, kötü niyetli kişi ve kuruluşlar tarafından değerli görüldüğü sürece kötü amaçlı tarafların saldırısı altında kalabilecekleri için bir güvenlik tehdidi oluşturacaklardır. Bu oluşan tehditlerin sistem içinde karşı önlemlerinin alınması ve güvenlik politikası içinde eksiksiz bir şekilde uygulanması Şekil 8.2'de verilen bilgi güvenliği yaşam döngüsü ile sağlanır.

Şekil 8.2

Bilgi güvenliği yaşam döngüsü.



Her sistem için öncelikli olarak yapılması gereken sistem varlıklarının ve kaynaklarının değerinin tespit edilmesi işlemidir. Sistemde oluşabilecek olası tehditler sistemin toplam değeri ölçeğinde analiz edilip sistemdeki güvenlik riski belirlenir. Sistem için belirlenen güvenlik tehditlerini ortadan kaldırmak veya hafifletmek için uygulanabilecek önlemler belirlenip bir güvenlik politikası oluşturulur. Sistemin güvenliğini sağlamak için öncelikle kabul edilen varsayımların doğruluğunu yüksek tutarak güvenlik seviyesini de yükseltiriz. Bu varsayımlar ve garanti edilen güven üzerine, sisteme yapılan saldırılara karşı oluşturulan güvenlik politikasını işletecek korunma mekanizması geliştirilir. Bundan sonraki aşama bu belirlenen mekanizmanın sistem içinde tasarlanıp uygulanması aşamasıdır. Sistem güvenliği belirlenen hedefler kapsamında sürekli izlenmeli ve takip edilmelidir. Özellikle güvenlik mekanizmasının tasarımı aşamasında oluşan bazı hatalar, tehdit eden varlığın gücü ile orantılı yeni oluşan tehditler veya tehdit eden varlığın sistem üzerinde güvenlik politikasının kapsamadığı yeni bir güvenlik açığı bulması durumunda bilgi güvenliği yaşam döngüsü (Şekil 8.2) tekrar takip edilmelidir. Meydana çıkan yeni tehditler karşısında sistem güvenlik politikası ve mekanizması bu yaşam döngüsü takip edilerek güncellenmelidir. Burada üstünde durulması gereken en önemli unsur sistemin olası tehditlere karşı sürekli takip edilmesi gereğidir. Oluşan tehditler karşısında kabul edilen varsayımlar üzerine güvenlik politikası ve mekanizmasının tasarımı ve bunların uygulanması sonucu sistem güvenli hale gelse bile, yeni tehditlerin ortaya çıkma durumu her zaman düşünülmelidir. Bunlar güvenlik politikasının güncellenmesini ve ilgili tüm adımların tekrar yapılmasını gerektirir. Sistem güvenliğini sağlamak için uygulanan bu adımlar bilgi güvenliği yaşam döngüsünü oluşturur ve bu döngünün sürekliliğinin sağlanması gerekir.

SIRA SİZDE 3

Bilgi güvenliği yaşam döngüsü içerisinde ortaya çıkan yeni güvenlik açıkları nasıl tespit edilir. Buna bir örnek verir misiniz?

YAZILIM VE DONANIM GÜVENLİĞİ

Bilgisayar tabanlı bir sistem, yazılım ve donanım olmak üzere iki ana bölümden oluşur. Bu iki unsur birbirini tamamlar ve herhangi biri olmadan diğeri bir anlam ifade etmez. Donanım, bilgisayarın fiziksel ve elektronik alt yapısını oluşturan ana ve çevre birimlerinin

tümüne verilen isimdir, örneğin; ana kart, Ethernet kartı, monitör vb. Yazılım ise bu donanım birimlerinin üzerinde koşan ve donanım ünitelerinin nasıl çalışacağını belirleyen algoritmaların barındığı komutlar kümesidir.

Ünitenin bu kısmında sistem üzerinde yer alan bu iki temel bileşen için var olan tehditleri göz önüne alarak, yazılım ve donanım güvenliği üzerinde duracağız.

Yazılım Güvenliği

Bir bilgisayar sisteminde sistem güvenliğini tehdit eden zararlı programlar aşağıdaki gibi bir sınıflandırma içinde birbirinden ayrılır.

Virüsler, bilgisayarlar ilk çıktığı zamanlardan beri var olan, kendini diğer dosyalar içinde gizleyerek kullanıcının izni ya da bilgisi dışında bilgisayarın planlanan çalışma şeklini bozan bir tür bilgisayar programıdır (Bayoğlu, 2016). İlk zamanlarda disketler ve CD gibi araçlar yoluyla bulaşan virüsler, İnternetin yaygınlaşmasıyla bilgisayarları daha fazla etkilemeye başlamıştır. Virüslerin en tehlikeli ve yayılması nispeten daha kolay olan türleri olan **solucanlar** daha yaygın bir etkiye sahiptir. Mesela, bir solucan, bir elektronik posta içine yerleştirilerek birçok bilgisayara gönderilmekte, kurban olarak adlandırılan bilgisayarların adres rehberinde bulunan diğer elektronik posta adreslerine otomatik olarak kendi kendini göndermekte ve bunun yanında ağları ve kurbanın bilgisayarını kullanılamaz duruma getirmektedirler. Solucanlar, kendilerini bir bilgisayardan diğerine otomatik olarak kopyalamak için tasarlanan, yerel sürücüde ya da ağda bant genişliğini tüketerek bilgisayar hızını etkileyip bilgisayarın çökmesine kadar etkilere yol açabilen zararlı yazılımlardır. Virüslere karşı en iyi korunma yöntemi bir anti virüs yazılımı kullanmak ve güncellemelerini zamanında edinmektir. Ayrıca, kimden geldiği bilinmeyen veya şüpheli e-postaları açmadan silerek muhtemel virüs bulaşması durumlarını önleyebilirsiniz.

Solucanlar, kendilerini bir bilgisayardan diğerine otomatik olarak kopyalamak için tasarlanan, yerel sürücüde ya da ağda bant genişliğini tüketerek bilgisayar hızını etkileyip bilgisayarın çökmesine kadar etkilere yol açabilen zararlı yazılımlardır.

Casus Yazılım, kullanıcılara ait önemli kişisel bilgileri ve kullanıcının bilgisayar üzerinde yaptığı işlemleri, kullanıcının bilgisi dışında kötü niyetli kişilere gönderen kötü amaçlı yazılımlardır. Casus yazılımları virüs ve solucanlardan ayıran en önemli fark hedef sisteme bir kez bulaştıktan sonra daha fazla yayılmaya ihtiyaç duymamalarıdır. Asıl amacı kurban olarak seçilen sistem üzerinde gizli bir şekilde istenen bilgileri toplayarak bunları kötü amaçlı kullanmasıdır. Kişisel gizliliğe karşı yapılmış en önemli saldırıların aracı olarak kullanılır. Bilgisayar sistemlerini yama ve güncellemelerle sürekli güncel tutmak bu tür yazılımlara karşı sistemi korumada önem arz eder. Ayrıca, İnternet üzerinde bilinmeyen programlardan uzak durulması bunların sistem üzerinde çalıştırılmaması gibi önlemler de karşı koruma da etkin rol oynar.

Virüsler yayılabilmek için bir kullanıcının ilgili virüsü diğer kullanıcılara isteyerek ya da istemeyerek göndermesini beklerler, fakat solucanlar böyle bir dış etki beklemeden kendisini çoğaltmaya ve yeni sistemlerin kullanıcılarına erişmeye çalışırlar.

DİKKAT

Truva Atları, bir tür casus yazılımı olarak düşünülebilirler (Bayoğlu, 2016). Truva atlarının bilgisayara bulaşma yöntemi virüslerin bulaşma metoduna benzer. Elektronik posta ile gelen zararlı bir eklentiyi açmak ya da İnternetten kaynağının güvenliğinden emin olunmayan bir dosyayı indirip çalıştırmak bir Truva atını bilgisayar sistemine bulaştırabilir. Fakat virüslerin aksine Truva atlarının sistem üzerinde görünür bir zararı olmayabilir. Truva atlarının bilgisayarda yaptığı en belirgin iş, bir TCP ya da UDP portu açarak, bu portlar aracılığıyla kötü amaçlı başka bir varlığın sisteme ulaşmasını sağlamaktır. Truva atlarının sunucu ve istemci olarak isimlendirilen iki bileşeni vardır. Sunucu, Truva atının bilgisayara bulaşan ve o bilgisayar üzerinde bir port açan parçasıdır. İstemci ise, saldırganın sunucu ile iletişime girdiği ve saldırgan bilgisayarın üzerinde bulunduğu parçasıdır.

Truva atının hedefi sistem üzerinde belli kanallar açarak programcısına, bulaştığı kullanıcının sistemini izlemesini veya kontrol etmesini sağlayan bir ortam yaratmaktır.

Saldırgan, Truva atlarının istemci bileşeninden yararlanarak sunucu ile iletişime geçer ve sunucunun bulaşmış olduğu bilgisayarın birçok kaynağına erişebilir. Truva atları kullanılarak bilgisayarın ekran görüntülerinin alınması, sabit diskinin formatlanması, bilgisayar üzerindeki gizli dosyalara erişim gibi kötü niyetli işlemler gerçekleştirmek mümkündür. Bu tip kötü amaçlı programlardan korunma yöntemi, bir anti virüs yazılımı kullanmak ve güncellemelerini vakit geçirmeden sisteme yüklemektir. Yine, elektronik posta olarak gelen ve nereden geldiği bilinmeyen veya şüphelenilen eklentilerin hiç açılmadan silinmesi gerekir.

Virüsler, solucanlar, casus yazılım veya Truva atı kategorisine girmeyen daha başka kötü amaçlı yazılımlar da bulunmaktadır (Bayoğlu, 2016). Bu yazılımlar işlemciye çok fazla yük bindirerek bilgisayarı işlevsiz bırakabilir ya da hafızayı anlamsız bilgiler ile doldurup bilgisayarı kullanılamaz duruma getirebilirler. Bu tip programlar ve kaynak kodları İnternette birçok sitede bulunabilir. Bu tip programları bir anti virüs programı aracılığıyla tespit etmek ve yapacağı kötü niyetli işlemleri engellemek mümkün olmayabilir. Bu tip zararlı programlar genelde büyük bir tehdit unsuru olarak değerlendirilmezler çünkü diğer bahsi geçen kötü amaçlı programlar gibi yayılma özellikleri yoktur. Fakat bir bilgisayar sisteminin kullanılmaz hale gelmesi de başlı başına büyük bir problemdir. Bu tip zararlı programlardan korunmak için önlem olarak yine sistemde güncel bir anti virüs programının bulunması, kaynağına güvenilmeyen herhangi bir e-postanın açılmaması ve İnternet üzerinden çalıştırılabilir dosyalar indirilirken dikkatli olunması gerekir.

Antivirüs programı olarak adlandırılan güvenlik yazılımları ise yukarıda açıklanan zararlı programlardan korunmak için yazılmış programlara denir. İnternette yaygın olarak görülen birçok kötü amaçlı yazılım için korunma imkânları sunarken, sistemi her türlü saldırılardan tamamen koruması beklenmemelidir.

Kötü niyetli yazılımlar İnternette yayıldıkça antivirüs programları üreten yazılım firmaları bu tür programlara karşı geliştirdikleri korunma metotlarını yazılım güncelleme yöntemleri ile bilgisayarlarda kurulu anti virüs programına aktarırlar. Bu yüzden anti virüs programlarının güncel tutulması olası saldırılara karşı korunma seviyesini en üst düzeyde tutacaktır. Ancak en önemli korunma yöntemi kullanıcıların İnterneti bilinçli ve güvenli bir şekilde kullanmasıdır. Çoğu zararlı yazılım, kaynağı kesin olarak doğrulanamayan e-postalar, çalıştırılabilir dosyalar vb. yollarla sistemlere bulaşıp zarar vermektedirler.

Güvenlik duvarı yazılımı daha önceden tanımlanmış kurallar ışığında ağa gelen ve giden trafiği izleyen ve ağdan gelebilecek olası tehditleri durduran bir ağ güvenliği sistemidir. Ağa gelen giden paketlerin IP adreslerini filtreleme, port filtreleme, Web filtreleme ve içerik filtreleme ağ duvarı içindeki ağ izleme çeşitlerinden birkaçıdır.

Yedekleme programları, sistem üzerinde oluşacak bir saldırı ya da bir güç kaybı neticesinde olası veri kayıplarının önüne geçmek için kullanılan yazılımlardır. Sistem üzerindeki verilerin güvenli başka bir ortamda yedeklenmesi, saldırı sonucunda oluşacak hasarları en aza indirgemeyi amaçlar. Bu programlar, olası başarılı bir saldırı sonrasında sistem üzerindeki verilerin kurtarılması görevini üstlenir. Bu nedenle sistem güvenliğini ve güvenilirliğini en üst düzeye çıkarabilmek için sistemde bulunan verilerin yedeklenmesi oldukça önemlidir.

Donanım Güvenliği

Günümüzde, elektronik cihazlar ve sistemler bilişim teknolojilerindeki her sistemde karşımıza çıkmaktadır. Elektronik sistemlerin ve altyapının güvenliği ve güvenilirliği konusundaki endişeler her zaman çok büyük bir öneme sahiptir. Sistemler çok karmaşık donanım tanımlamalarına sahip olduğu için sistem güvenliğini sağlamak son derece zordur. Bunun sebebi, bir saldırganın kötü niyetli işlemleri yapmak için tek bir zayıflık bulmasının

yeterli olmasıdır. Saldırgan için bu zayıflıktan yararlanıp sisteme giriş yapmak yeterliyken, sistemi savunan yapılar sistem güvenliğini sağlamak için sonsuz sayıda olası güvenlik açıklarına karşı korumak üzere çaba gösterirler.

Entegre devre tasarımı sırasında entegre devre yongasının içine yerleştirilen ve amacı devrenin yerine getirmesi gereken işlevselliğinin dışında zararlı işlemler yapmak olan donanım değişikliklerine "donanımsal Truva atı" denir. Donanım Truva atı, yazılımsal Truva atı gibi programcısına sisteme erişebilme imkânı sunar.

Donanım Truva atları, yonga tasarım ekosisteminin karmaşıklığı nedeniyle, hem yarı iletken devre tasarımı yapan firmalar hem de devletler için büyük bir endişe kaynağıdır (Adee, 2008; Mitra ve ark., 2015). Ekonomik faktörler, silikon tabanlı çiplerin tasarımı, imalatı, testi ve kurulumunun farklı ve genellikle çelişkili amaç ve menfaatleri olan birçok şirket ve ülkede yaygınlaşmasına neden olur. Donanım Truva atları, bilgisayar güvenliğinde sistem hizmet ve olanaklarının kullanılamaz duruma düşürülmesi ile sonuçlanan saldırılar, sistemde keşfedilmemiş ayrıcalıklı erişim elde etmeye çalışan saldırılar (Fern ve ark., 2016), entegre devrenin hızlı bir şekilde ömrünü azaltan saldırılar ve yonga üzerindeki sistem veri yolu kilitlenmesine neden olan saldırılar gibi daha birçok saldırı türüne neden olabilir.

Bu tip saldırılar sistem güvenliğinde çok yüksek seviyede tehdit oluşturur. Entegre devre üzerinde böyle bir donanım Truva atının var olup olmadığını doğrulamak, sistem güvenliğinde önemli araştırma alanlarından biridir.

Donanım seviyesindeki zararlı donanım bileşenlerinden korunmak için sistem için gerekli donanım elemanlarını, güvenilirliği kanıtlanmış tasarım şirketlerinden temin etmek önerilir.

ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

ISO 27000 Bilgi Güvenliği Yönetim Sistemi bilgi güvenliği ile ilgili birtakım standartları tanımlar ve kuruluşların kendi bilgi, değer ve varlıklarını güvence altına almalarına yardımcı olan mekanizmaları ve bunun yönetilmesinin tanımlayan kurallar ve politikaları içerir. Bu standartlar ailesini kullanmak, kuruluşun finansal bilgiler, fikri mülkiyet hakları, personel bilgileri veya üçüncü partilerin kuruluşa emanet ettiği bilgiler gibi birtakım değer ve varlıkların güvenliğini yönetmesine yardımcı olacaktır.

ISO 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS), bilgi güvenliği ile ilgili gereksinimleri tanımlayan ISO 27000 standartlar ailesinin en iyi bilinen standardıdır. Bir kuruluşun hassas bilgilerini yönetmek için sistematik bir yaklaşım sunarak bilginin güvenli kalmasını sağlayan kuralları içerir. Bir risk yönetimi süreci uygulayarak kişi, süreç ve sistemleri de içererek herhangi bir sektördeki küçük, orta ve büyük ölçekli işletmelerin bilgi varlıklarını güvende tutmasına yardımcı olur.

ISO 27001 standardı ticari işletmeler, devlet kurumları, kâr amacı gütmeyen kuruluşlar gibi her türlü organizasyonu kapsar. İlgili kuruluşun genel ticari riskleri bağlamında belgelenmiş bir bilgi güvenliği yönetim sisteminin oluşturulması, uygulanması, işletilmesi, izlenmesi, gözden geçirilmesi, sürdürülmesi ve sürekli iyileştirilmesi için gerekli şartları tanımlar. Aynı zamanda, organizasyonun ihtiyaçlarına göre hazırlanmış bilgi güvenliği risklerinin değerlendirilmesi ve uygulanması ile ilgili gereklilikleri de içerir. Organizasyon içinde yer alan bilgi varlıklarını koruyan ve ilgili taraflara güven veren yeterli ve orantılı güvenlik denetimlerinin belirlenmesini sağlamak üzere tasarlanmıştır. Bu standart genel gereklilikleri belirtir. Tüm organizasyonlara tip, boyut ve koşullara bakılmaksızın uygulanabilir kuralları ve tanımlamaları içerir. ISO 27001 BGYS aşağıdakileri de içeren birçok farklı kullanım türü için uygundur:

- Kuruluşların güvenlik gereksinimlerini ve hedeflerini formüle etmek,
- Kuruluşlar içinde güvenlik risklerinin maliyet etkin bir şekilde yönetilmesini sağlamak,
- Kuruluşların yasa ve yönetmeliklere uyumunu sağlamak,
- Bir organizasyonun kendine özgü güvenlik hedeflerinin yerine getirildiğinden emin olmak,
- Kurumların iç ve dış denetçilerince bir organizasyon tarafından benimsenen politikalara, direktiflere ve standartlara uyum derecesini belirlemek,
- Kuruluşlar tarafından ticari ortaklıklar veya ticari nedenlerden dolayı etkileşimde bulunduğu diğer kuruluşlara, bilgi güvenliği politikaları, direktifleri, standartları ve prosedürleri hakkında gerekli bilgileri sağlamak,
- İş ortamında bilgi güvenliğinin uygulanmasını sağlamak ve
- Kuruluşlar tarafından müşterilere bilgi güvenliği ile ilgili bilgi sağlamak için kullanılır.

Diğer ISO yönetim sistemi standartlarında olduğu gibi, ISO 27001'e uygunluk belgesi veya sertifikası edinmek de mümkündür ancak zorunlu değildir. Bazı kuruluşlar, içerdiği uygulamalardan en iyi biçimde yararlanmak için standart uygulamayı tercih ederken diğerleri, müşterilerine standart içinde tanımlanan tavsiyelerin yerine getirildiği güvencesini verebilmek amacıyla sertifika sahibi olmak isterler.

Uluslararası Standartlar Kuruluşu (International Standards Organization–ISO) sertifika vermez. ISO 27001 BGYS sertifikası almak isteyen kuruluşlar standardın gerektirdiği tüm adaptasyonları sağlamalarının ardından bağımsız bir belgelendirme kuruluşuna başvurur ve denetlenirler. Denetlemenin başarılı olmasının ardından sertifikasyon belgesi almaya hak kazanırlar. Bu belge ile kuruluş, sahip olduğu değer ve varlıkların farkında olduğunu ve bu değer ve varlıkları korumak için gelişmiş yöntemler uyguladığını gösterir. Ayrıca, sahip olduğu bilgi varlıklarını korumak üzere belirlediği hedef ve politikalarını gerçekleştirmek için ISO 27001 BGYS kapsamında belirtilen gereksinimleri yerine getirdiğini taahhüt eder.

ISO 27001 BGYS en güncel sürümü, 2005 yılında yayınlanan sürümü revize edilerek geliştirilen ve 2013 yılında yayınlanan sürümüdür. Bütün olarak standardın yeni sürümüne bakıldığında yapılan değişiklikler şöyle sıralanabilir: (1) ISO 27000 standartlar ailesindeki diğer standartlar ile uyumlu olması, (2) BGYS gereksinimlerinin daha açık bir şekilde yapılandırılması, (3) eski sürümde yer alan hataların düzeltilmesi, eksiklerin giderilmesi ve (4) BGYS tarafından teknik olarak ihtiyaç duyulan gereksinimlerin revize edilmesi olarak sıralanabilir.

Yeni sürümde görülen en önemli fark, bilgi güvenliği hedeflerinin özelliklerinin ayrıntılı olarak verilmesidir. Bu özellikler:

- Bilgi güvenliği politikasına uyumlu olması,
- Kurum içinde yaygınlaştırılmış olması,
- Hedeflerin ölçülebilir olması,
- Bilgi güvenliği gereksinimlerini dikkate alması,
- Risk değerlendirme sonuçlarını göz önünde bulundurması ve
- Uygun aralıklarla revize edilerek güncellenmesi olarak sayılabilir.

SİSTEM GÜVENLİĞİ İÇİN İPUÇLARI

Bilgisayar tabanlı bir sistemin zararlı yazılımlardan korunması amacıyla aşağıda sıralanan önlemlerin alınması gerekir.

- Sistem üzerinde kurulu uygulamaları düzenli aralıklarla denetleyin, artık kullanılmayan programları sistem üzerinden kaldırın.
- Sistem üzerindeki programların son güncellemelerini yükleyin.
- Sisteme giriş yapan kullanıcıların girişlerini denetleyin ve parola politikanızı güçlü parola kullanımını zorunlu kılacak şekilde değiştirin.
- Sistemdeki trafiği izleyip müdahale edin ve izinsiz sistem girişlerini engelleyin.
- Sisteme yapılan uzaktan erişimi denetleyin ve güçlü bir erişim altyapısı kullanın.
- Bilgisayarınıza çok yönlü ve güvenlik duvarı içeren güçlü bir güvenlik yazılımı yükleyin.
- Özellikle işletim sisteminizi ve İnternet tarayıcılarınızı güncel tutun.
- Kimden geldiğini bilmediğiniz e-postaları açmayın.
- Kaynağını bilmediğiniz programları bilgisayarınıza yüklemeyin, çalıştırmayın.
- Ücretsiz yazılımlara dikkat edin, güvenlik açıkları barındırabilirler.
- Lisanslı yazılım kullanmaya özen gösterin.
- Önemli verilerinizin başka bir bellekte yedeklemesini mutlaka yapın.

Sistem güvenliğini en üst düzeye çıkarmak için burada verilen ipuçlarını uygulamanın yanı sıra sistemi sürekli takip ve kontrol etmek gereklidir. Sistemi olası yeni tehditlere karşı güvende tutmanın en önemli kuralı sistem üzerindeki güvenlik açıklarının doğru bir şekilde değerlendirilmesi ve bunlara karşı tam ve kusursuz önlemlerin alındığından emin olunmasıdır.

"İşletim sistemleri güvenliği", Ulusal Bilgi Güvenliği Kapısı, TÜBİTAK-BİLGEM, https://www.bilgiguvenligi.gov.tr/son-kullanici-kategorisi/isletim-sistemleri-guvenligi.html İNTERNET

Matt Bishop, (2015), "Computer Security: Art and Science", Addison-Wesley Professional. KİTAP

Özet

AMAÇ 1 *Sistem güvenliği ile ilgili temel kavramları açıklamak*

Bir kuruluşun bilişim sistemlerini güvenli hale getirebilmek ve sistem üzerindeki bilgilerin güvenliğini sağlayabilmek için sistem cihazlarının herhangi bir tehdit altında olup olmadığı ile ilgili tehdit analizinin yapılması gerekmektedir. Eğer sisteme karşı bir tehdit varlığı söz konusu ise bu tehdide karşı gereken güvenlik önlemleri alınmalıdır.

Bilişim sistemlerinin ve altyapısının güvenliği ve güvenilirliği sisteme karşı yönelen risklerden dolayı tehdit altındadır. Güvenliği sağlamak son derece zordur. Çünkü sisteme sızmak isteyen bir saldırganın kötü niyetli işlemlerini gerçekleştirmek için tek bir zayıflık bulması yeterliyken, sistemi savunan birimlerin ise sistem güvenliğini sağlamak için sonsuz sayıda olası güvenlik açıklıklarına karşı önlemler alması gerekir.

Sistem güvenliğinde gizlilik, bütünlük ve erişilebilirlik olarak sıralanan temel üç unsur büyük önem arz etmektedir. Bilginin yalnızca erişim hakkı tanınmış kişiler tarafından ulaşılabilir olması, bilginin bütünlüğünün ve doğruluğunun temin edilmesi ve yetkili kullanıcıların ihtiyaç duydukları bilgiye her an erişebilmelerinin garanti altına alınması bilgi güvenliğinin temelini oluşturur.

Kötü niyetli saldırganlar tarafından güvenlik açıklarından yararlanarak oluşturulan güvenlik tehditleri sistem üzerinde güvenlik riski oluşturur. Bu riski minimum düzeye indirmek ve hatta ortadan kaldırmak için güvenlik politikası oluşturularak birtakım mekanizmalar geliştirilir. Güvenlik politikası, sistemde ortaya çıkan tehditleri azaltan ve bu tehditler karşısında sistemin zarar görmesini engelleyici karşı önlemler alır.

AMAÇ 2 *Sistem güvenliği için olası tehditleri analiz etmek*

Ele geçirme, uydurma, kesinti ve değişiklik olarak bilinen dört tehdit sınıflandırması birçok sistem üzerinde görülen ortak tehditleri kapsamaktadır. Araya girme (snooping), bilginin izinsiz bir şekilde ele geçirilmesidir ve bir gözetleme biçimi olarak değerlendirilir. Pasif bir tehdit biçimidir; tehdit eden varlığın sistemin bilgisini ve dosyalarını taraması veya iletişimini dinlemesi örnek olarak verilir. Değişikliğe uğratma veya modifikasyon, yetkisiz olarak bir bilginin değiştirilmesidir. Gözetleme tehdidinin aksine modifikasyon aktif bir tehdit biçimidir. Bir varlığın bilgiyi değiştirmesinden kaynaklanır. Ağ üzerinde iletilen verinin, değiştirilerek alıcı tarafa ulaşması aktif olarak hattı dinleme ve hattaki bilgiyi değiştirme olduğundan modifikasyon tehdidi sınıfına girer. Sahtecilik veya olduğundan başkası gibi görünmek, bir varlığın başkasının kimliğine bürünerek sistemde yetkisi olmayan servislerden faydalanması ya da sisteme erişerek sistemin doğru çalışmasını engellemek istemesi, aldatma ve zorla el koyma tehdit sınıfları içinde değerlendirilen bir tehdit çeşididir.

İdeal olarak sistemin güvenlik mekanizmasının hassas ve kesin olması gerekir. Bütün sistem güvenlik mekanizmalarının bileşenleri güvenli olmayan durumları engellemek için aktif bir şekilde çalışmalıdır. Hâlihazırda güvenli olan sistem durumları için güvenlik mekanizmasının herhangi bir işlem yaparak sistemin kaynaklarını boşa kullanması istenmeyen bir durumdur.

AMAÇ 3 *Güvenlik hedeflerini açıklamak*

Güvenlik politikası, izin verilen ve verilmeyen işlevler ile ilgili kurallar bütünü iken, güvenlik mekanizması ise bir güvenlik ilkesinin uygulanması için izlenen yöntem, araç veya prosedür olarak tanımlanır. Bir güvenlik politikasının "güvenli" ve "güvenli olmayan" eylemlerinin tanımları göz önüne alındığında, güvenlik mekanizmaları sisteme karşı oluşabilecek saldırıyı önleyebilir, bu saldırıyı tespit edebilir veya sistemi saldırıdan kurtarabilir. Saldırıları önleme, tespit etme ve saldırılardan kurtarma sistem güvenliği için oluşturulan politika için güvenlik hedeflerini sınıflandırır. Burada en üst düzey güvenlik hedefi, sistemi gerçekleştirilen saldırıdan kurtarmaktır.

AMAÇ 4 *Bilgi güvenliği yaşam döngüsü içindeki temel adımları tanımlamak*

Belirlenen sistem güvenlik politikası ve mekanizmasının sistem içinde tasarlanıp uygulanması gerekir. Sistem güvenliği belirlenen hedefler kapsamında sürekli izlenmeli ve takip edilmelidir. Güvenlik mekanizmasının tasarımı aşamasında oluşan istenmeyen hatalar, tehdit eden varlıklar tarafından oluşturulan yeni tehditler veya tehdit eden varlığın sistem üzerinde güvenlik politikasının kapsamadığı yeni bir güvenlik açığı bulması durumunda bilgi güvenliği yaşam döngüsü tekrar takip edilmeli, bilgi güvenliği politikası ve mekanizması yeni tehditlere karşı savunma amacıyla güncellenmelidir.

AMAÇ 5 *Yazılım ve Donanım güvenliğindeki temel tehditler için alınacak önlemleri açıklamak*

Sistem, yazılım ve donanım bileşenleri ile birlikte bütün bir şekilde düşünülmelidir. Bir bilgisayar sisteminde sistem güvenliğini tehdit eden zararlı programlar virüsler, solucanlar, casus yazılım, Truva atı vb. olarak yaygınca günlük hayatta karşımıza çıkmaktadır. Virüsler yayılabilmek için bir kullanıcının virüsü diğer kullanıcılara isteyerek ya da istemeyerek göndermesini beklerler, fakat solucanlar ise böyle bir dış etki beklemeden kendisini çoğaltmaya ve yeni sistemlerin kullanıcılarına erişmeye çalışırlar. Truva atının hedefi sistem üzerinde belli kanallar açarak programcısına, bulaştığı sistemi izlemesini veya kontrol etmesini sağlayan bir ortam yaratır. Güvenlik duvarı yazılımı daha önceden tanımlanmış kurallar ışığında ağa gelen ve giden trafiği izleyen ve ağdan gelebilecek olası tehditleri durduran bir ağ güvenliği sistemidir. Yedekleme programları, sistem üzerinde oluşacak bir saldırı ya da bir güç kaybı neticesinde olası veri kayıplarının önüne geçmek için kullanılan yazılımlardır.

Entegre devre tasarımı sırasında entegre devre yongasının içine istemeden bir hata sonucunda ya da entegre devre tasarımcısı tarafından kasıtlı olarak yerleştirilen, devrenin yerine getirmesi gereken işlevlerin dışında zararlı işlevler yapan donanım değişikliklerine "donanımsal Truva atı" denir. Kullanıcının bu zararlı donanım değişikliklerini tespit etmesi oldukça zor bir iştir. Donanım Truva atı, yazılımda karşımıza çıkan Truva atı yazılımları gibi programcısına kullanıcının sistemine erişebilme imkânı sunar.

AMAÇ 6 *Güvenli bir sisteme ulaşmak için gerekli kriterler ve ilgili standartları kullanmak*

ISO 27001 Bilgi Güvenlik Yönetim Sistemi (BGYS), bir bilgi sisteminin güvenli biçimde çalışması için gerekli yönetimsel gereksinimleri açıklayan ISO 27000 standartlar ailesinin en iyi bilinen standardıdır. Bu standart kısaca ISO 27001 BGYS olarak bilinir. Bir kuruluşun hassas, gizli kalması gereken bilgilerini (ticari bilgi, kullanıcı bilgisi vb.) yönetmek için sistematik bir yaklaşım sunarak bilginin güvenli, bilgi sisteminin güvenilir kalmasını sağlayan kuralları içerir. Risk yönetimi süreci uygulayarak kişi, süreç ve sistemleri kapsayan politikalar geliştirilmesini motive eden ve küçük, orta ya da büyük ölçekli işletmelerin bilgi varlıklarını güvende tutmasına yardımcı olan önerilerde bulunur.

AMAÇ 7 *Sistemi güvenli halde tutmak için yapılması gereken önemli ipuçlarını açıklamak*

Bilgisayar tabanlı bir sistemin zararlı yazılımlardan korunması amacıyla aşağıda sıralanan önlemlerin alınması gerekir.

- Sistem üzerinde kurulu uygulamaları düzenli aralıklarla denetleyin, artık kullanılmayan programları sistem üzerinden kaldırın.
- Sistem üzerindeki programların son güncellemelerini yükleyin.
- Sisteme giriş yapan kullanıcıların girişlerini denetleyin ve parola politikanızı güçlü parola kullanımını zorunlu kılacak şekilde değiştirin.
- Sistemdeki trafiği izleyip müdahale edin ve izinsiz sistem girişlerini engelleyin.
- Sisteme yapılan uzaktan erişimi denetleyin ve güçlü bir erişim altyapısı kullanın.
- Bilgisayarınıza çok yönlü ve güvenlik duvarı içeren güçlü bir güvenlik yazılımı yükleyin.
- Özellikle işletim sisteminizi ve İnternet tarayıcılarınızı güncel tutun.
- Kimden geldiğini bilmediğiniz e-postaları açmayın.
- Kaynağını bilmediğiniz programları bilgisayarınıza yüklemeyin, çalıştırmayın.
- Ücretsiz yazılımlara dikkat edin, güvenlik açıkları barındırabilirler.
- Lisanslı yazılım kullanmaya özen gösterin.
- Önemli verilerinizin başka bir bellekte yedeklemesini mutlaka yapın.

Kendimizi Sınayalım

1. Araya girme (snooping) tehdidi aşağıda verilen hangi güvenlik kavramı ile engellenir?

a. Bütünlük
b. Gizlilik
c. Hazır bulunma
d. Anti virüs
e. Erişilebilirlik

2. Aşağıdakilerden hangisi virüs bulaşma yöntemlerinden biri olarak **değerlendirilmez?**

a. USB bellek
b. E-posta
c. Ağ paylaşımı
d. Kaynağı güvenilir program yüklemek
e. CD

3. Bilişim sistemini zararlı yazılımlardan korumak için aşağıdakilerden hangisi **önerilmez?**

a. Çok yönlü ve güvenlik duvarı içeren güvenlik programı kullanmak
b. İşletim sistemini ve İnternet tarayıcılarını güncel tutmak
c. Tüm hesaplar için tek bir şifre oluşturmak
d. Önemli verilerin başka bir bellekte yedeklemesini yapmak
e. Sisteme yapılan uzaktan erişimi denetlemek ve güçlü bir erişim altyapısı kullanmak

4. Kendisini bir bilgisayardan diğerine kopyalamak için tasarlanan ve bunu otomatik bir şekilde gerçekleştiren, işlem gücü ya da bant genişliğini tüketerek bilgisayarın çalışma hızını etkileyip çökmesine kadar etkilere yol açabilen yazılımlara verilen ad aşağıdakilerden hangisidir?

a. Truva Atları
b. Solucanlar
c. Casus yazılımları
d. Antivirüs
e. Yedekleme programı

5. Bilgisayar sistemlerini ve üzerinde saklanan verileri zararlı yazılımlardan korumak için aşağıdakilerden hangisinin yapılması uygun **değildir?**

a. Bilgisayar çalışma performansı etkilememesi için anti virüs programı kurmamak
b. Kimden geldiği bilinmeyen e-postaları açmamak
c. İşletim sistemine ait güncellemeleri yapmak
d. Anti virüs programlarını güncel tutmak
e. Karmaşık düzeyde, tahmin edilmesi zor ve uzun bir parola seçmek

6. Aşağıdakilerden hangisi bilgi güvenliği yaşam döngüsü içinde **yer almaz?**

a. Tehditlerin analizi
b. Sistem fonksiyonlarının iyileştirilmesi
c. Güvenlik mekanizmasının oluşturulması
d. Sistemin tasarlanması ve uygulanması
e. Sistemin sürekli izlenip kontrol edilmesi

7. Bir üniversitenin, laboratuvar ortamında herhangi bir öğrencinin başka bir öğrencinin hazırlamış olduğu laboratuvar sonuçlarını kopyalamasını yasaklayan bir politikası olduğunu varsayalım. Dersi alan bir öğrencinin sistem tarafından sunulan bu mekanizmaları, laboratuvar ile ilgili oluşturmuş olduğu dosyalarını korumak için kullanmadığını ve başka bir öğrencinin bu dosyaları gördüğünü düşünelim. Bu koşullar altında aşağıdakilerden hangisi **yanlıştır?**

a. Bir güvenlik ihlali oluşmamıştır çünkü güvenlik politikası başka bir öğrencinin dosyaları kopyalamasını yasaklamıştır.
b. Bir güvenlik ihlali söz konusudur ve güvenlik politikası doğru bir şekilde tanımlanmıştır.
c. Güvenlik politikası, laboratuvar sonuçlarını kopyalamasını ve görüntülemesini yasaklayacak şekilde değiştirilmelidir.
d. Dersi alan öğrencilerin yapabileceği olası güvenlik ihlallerinin hepsi güvenlik politikasında tanımlanmalıdır.
e. Güvenlik politikası, olası tüm ihlalleri tamamen engelleyecek şekilde de tanımlanabilir.

8. ISO 27001 BGYS aşağıdakilerden hangisi **kapsamaz?**

a. Kuruluşların güvenlik gereksinimlerini belirler.
b. Kuruluşlar içinde güvenlik risklerinin yönetilmesini sağlar.
c. Kuruluşların yasa ve yönetmeliklere uyumunu sağlar.
d. Kuruluşlara öz kaynak sağlar.
e. İş ortamında bilgi güvenliğinin uygulanmasını sağlar.

9. Bir sisteme giriş için sadece nümerik karakterlerden oluşan 4 basamaklı bir PIN numarası kullanılsın. Saldırgan bir program aracılığıyla bütün olası PIN numara kombinasyonlarını deneyerek bu erişim kontrol mekanizmasını kırar. Bu saldırı çeşidinin ismi aşağıdakilerden hangisi ile ifade edilir?

a. Aradaki adam saldırısı
b. Kaba kuvvet saldırısı
c. Araya girme (snooping)
d. Telekulak
e. Sahtecilik

10. Saldırganlar sisteme aşağıdakilerden hangisinden faydalanarak kötü niyetli saldırı düzenlerler?

a. Karşı önlem
b. Güvenlik mekanizmaları
c. Güvenlik açığı
d. Tehdit
e. Güvenlik politikası

Yaşamın İçinden

Siber saldırılara karşı Türkiye'de bir ilk

STM'nin Ankara'da kuracağı ve dünyada sadece birkaç ülkede bulunan Siber Füzyon Merkezi ile Türkiye, henüz ortaya çıkmamış siber saldırı tehditlerini önceden tespit edebilecek. Savunma Teknolojileri ve Mühendislik AŞ'nin (STM), Ankara'da kuracağı ve dünyada sadece birkaç ülkede bulunan Siber Füzyon Merkezi ile Türkiye, henüz ortaya çıkmamış siber saldırı tehditlerini önceden tespit edebilecek.

Son dönemde siber güvenlik alanındaki çalışmalarıyla dikkati çeken STM, bu alanda bir ilke imza atmaya hazırlanıyor. STM, bu kapsamda, Ankara'da dünyada sadece birkaç ülkede bulunan ve yeni nesil siber güvenlik merkezi olarak nitelenen Siber Füzyon Merkezi kuracak. STM'nin gelecek ay faaliyete geçireceği merkez sayesinde, artık sadece bilinen siber tehditler değil, henüz ortaya çıkartılmamış, gelişmiş karmaşık metotlar kullanan yeni tehditler de saldırıdan önce tespit edilebilecek ve önlem alınabilecek.

Merkezde, zafiyet yönetimi, siber tehdit istihbaratı, tehdit savunma operasyonu, siber harekat merkezi ve olay müdahale yönetimi yetenekleri, özellikle üst seviye yöneticilerin siber olayların yönetiminde inisiyatif almasına imkan sağlayacak yenilikçi harp oyunları yöntemleriyle birleştirilerek modern bir siber güvenlik yaklaşımının uygulanmasına imkan sağlanacak.

Siber Füzyon Merkezi'nde sadece siber güvenlik uzmanları değil, büyük veri, veri bilimi, istatistik, matematik, doğal dil işleme, görüntü ve ses işleme gibi farklı disiplinlerden uzmanlar da görev alacak. Her yönüyle ilk olacak bu merkez, siber saldırılara karşı Türkiye'nin önemli bir gücü olacak.

Kaynak: Göksel Yıldırım, Anadolu Ajansı, 1 Mart 2016, NTV Teknoloji Haberleri, https://goo.gl/Qnjixh

Okuma Parçası

Giyilebilir Teknolojilerin Siber Güvenliği

Akıllı sensörlerle donatılmış ve nesnelerin interneti sayesinde çevredeki diğer akıllı ürünlerle de etkileşim içinde olabilen giyilebilir teknolojiler yakın zamanda hepimizin hayatının bir parçası haline gelecek. Eğer yeterli siber güvenlik önlemleri alınmazsa kıyafetlerimizin bir bilgisayar korsanı tarafından kontrol edilmesi ise hiç de şaşırılacak bir durum değil.

"Nesnelerin İnterneti"nin kullanımının geniş bir alana yayılması sonucu akıllı sensörlerin ve uygulamaların giyilebilir ürünlerde de kullanımıyla kıyafet ve aksesuarlarımız da dijitalleşmeye başlamıştır. Akıllı ürünler dediğimiz bir yazılım ve donanım entegrasyonuyla çevreyle iç içe olan her ürün gibi giyilebilir teknolojiler de siber saldırılara uğrayacak ve güvenlik önlemleri alınması gerekecektir. Yapılan araştırmalar bir kullanıcının PIN ve parolaları kırmak için giyilebilir teknolojilerde bulunan gömülü sensörlerin kullanılabileceğini göstermiştir. Binghamton Üniversitesi ve New York'taki Stevens Institute of Technology arasındaki işbirliğiyle yapılan bir araştırma sonucunda özellikle akıllı sporcu aksesuarları ve saatlerin güvenlik ihlallerine karşı savunmasız oldukları kanıtlanmıştır.

Şifre Tuşlama Tabanlı Sistemlere Yapılan Saldırı Çeşitleri

ATM gibi tuş tabanlı sistemler için en büyük güvenlik tehdidi, banka kartlarının manyetik şeritlerinden veri çalmak amacıyla ATM'lere takılan sıyırıcı dediğimiz özel cihazlar ya da kullanıcıların şifrelerini okumak için kullanılan gizli kameralar olmuştur. Sıyırıcılar ATM'lerde kart yuvalarına yerleştirilir ve onlarım özel şifrelerini içeren hassas verileri kopyalamak ve ele geçirmek için kullanılır. Sıyırıcıları bir kullanıcının fark etmesi oldukça zor olmakla birlikte çoğu banka bu cihazların ATM'lere yerleştirilmesini engellemek amacıyla çeşitli güvenlik önlemleri almıştır.

Bir başka yöntem de klavye ile yazılan anahtarı bulmak için dilsel modelleri kullanarak ses kaydı yapmaktır. Yine veri korsanları tarafından klavyede basılan tuşları bulmak için ses sinyallerinin çok yollu sönümlenmesi de kullanılabilir. Ayrıca makine öğrenmesi bazlı kullanılan yöntemler de vardır. Veri korsanlarının geliştirdikleri tüm bu teknikler anahtar tabanlı sistemlerde kullanıcı PIN ve parolalarını ele geçirmeye yöneliktir. Kısaca kullanıcılar veri korsanları için bir araçtır. Direkt olarak üzerinde gömülü sensörler bulunan tüm dijital cihazlarla etkileşim içinde bulunan bir kullanıcı ise veri korsanları için çok kolay bir lokma haline gelebilir.

Giyilebilir Teknolojiler ve Gömülü Sensörler

Giyilebilir Teknoloji terimi sporcular için izleme, epileptik nöbetler tespiti, kullanıcı kimlik doğrulaması gibi geniş bir uygulama alanını hatta daha fazlasını içerir. Bu uygulamalar geniş bir yelpazeye sahip olduğundan, çeşitli sensörlerin kıyafetler ve aksesuarlara dâhil edilmesi gerekir. Bu yüzden akıllı aksesuar ve kıyafetlerin, amacına uygun ve başarılı bir şekilde kullanılması için çevreden büyük miktarda veri toplaması ve bu verileri değerlendirmesi gerekmektedir. Akselerometreler, jiroskop ve manyetometreler giyilebilir cihazlarda yaygın olarak kullanılan sensörlerden sadece bazılarıdır. Bu sensörler aracılığıyla bir kişinin hareketlerinin tüm takip edebilirsiniz. Bu yazının amacı ise bizim tüm bu teknolojinin bilgilerimizi kaydedip değerlendirmesine hazır olup olamayacağımızdır.

Peki ya biz bankamatikten para çekerken kıyafet ve aksesuarlarımızın kaydettiği hareketlerimiz bir veri korsanının eline geçerse? Belki de en önemli soru: Bir giyilebilir cihaz PIN Numarası veya şifreler gibi hassas bilgilerimizi ifşa edebilir mi?

Yeni Şifre Kırma Yöntemi: Veri Sıyırma

Yeni bir araştırma gerekli verileri ayıklamak için giyilebilir cihazdaki düşük kalitede sensörleri kullanan bir algoritma sunar. Gömülü sensörlerin şifrelenmemiş çıkış verileri, Bluetooth aracılığıyla veri süzme yöntemi veya bir malware uygulaması yükleyerek elde edilebilir.

Giyilebilir cihazlar önceki sürümlerle karşılaştırdığımızda daha az güvenli olan Bluetooth Low Energy (BLE) kullanırlar. BLE'nin Bluetooth'tan en büyük farkı isminden de anlaşılacağı üzere daha az enerji harcamasıdır. Fakat BLE ve Bluetooth için düşük enerji düşük güvenliktir demek yanlış olmaz. BLE'de korsanlar için veri süzmek çok daha basittir. Veri süzmenin dışında giyilebilir cihaza Malware yazılımı yüklemek de bir başka veri çalma yöntemidir. Malware karşı taraftan veri çalmak için yazılan kötü amaçlı yazılımlara verilen genel bir isimdir. Malware aracılığıyla çalınan sensör verileri, korsana uzak bağlantı aracılığıyla gönderilebilir. Özellikle akıllı kıyafet ve aksesuarları kullanan kişilerin klavyeye parmak vuruş hareketlerinin çıkartılıp yorumlanması PIN ve parola hırsızları için önemli verilerdir.

Kaynak: Hakan Kahraman, Elektrik Elektronik Mühendisi, 6 Kasım, Allaboutcircuits ve Pgicyber web sitelerinden de yararlanılmıştır. https://goo.gl/gpCq7V

Kendimizi Sınayalım Yanıt Anahtarı

1. a	Yanıtınız yanlış ise "Yazılım Güvenliği" konusunu yeniden gözden geçiriniz.
2. d	Yanıtınız yanlış ise "Yazılım ve Donanım Güvenliği" konusunu yeniden gözden geçiriniz.
3. c	Yanıtınız yanlış ise "Sistem Güvenliği İçin İpuçları" konusunu yeniden gözden geçiriniz.
4. b	Yanıtınız yanlış ise "Yazılım Güvenliği" konusunu yeniden gözden geçiriniz.
5. a	Yanıtınız yanlış ise "Sistem Güvenliği İçin İpuçları" konusunu yeniden gözden geçiriniz.
6. b	Yanıtınız yanlış ise "Bilgi Güvenliği Yaşam Döngüsü" konusunu yeniden gözden geçiriniz.
7. b	Yanıtınız yanlış ise "Bilgi Güvenliği Politikası ve Mekanizması" konusunu yeniden gözden geçiriniz.
8. d	Yanıtınız yanlış ise "ISO 27001 Bilgi Güvenliği Yönetim Sistemi" konusunu yeniden gözden geçiriniz.
9. b	Yanıtınız yanlış ise "Varsayımlar ve Güven" konusunu yeniden gözden geçiriniz.
10. c	Yanıtınız yanlış ise "Sistem Güvenliği ile İlgili Temel Terimler" konusunu yeniden gözden geçiriniz.

Sıra Sizde Yanıt Anahtarı

Sıra Sizde 1

Güvenlik tehditleri, güvenlik açıkları ve sistem kaynakları güvenlik riskini arttırır. Güvenlik politikası gereği uygulanan karşı önlemler sistemdeki bu riski azaltmaya çalışır.

Sıra Sizde 2

Saldırganın amacı sadece sistemin doğru çalışmasını engellemeye yöneliktir. Soruda değiştirme veya sahtecilik gibi başka bir kasıt verilmediği için bu saldırı Kesinti saldırısı sınıfında incelenebilir.

Sıra Sizde 3

Sistem güvenlik politikası mevcut tehditleri engellemeye yönelik karşı önlemler alır. Bilgi güvenliği yaşam döngüsünün bu adımından sonra sistem üzerinde yapılan bütün veri iletişimi, yapılan bütün işlemler ve sistem kaynaklarının kullanım istatistikleri incelenip olağan görülmeyen sistem aktiviteleri kaydedilerek bir saldırı olarak kabul edilir. Bu normal olmayan aktivitenin sistem üzerinde kötü sonuçlara yol açtığı tespit edildiği durumda, buna yol açan sistem bileşeninin ilgili kısmı yeni bir güvenlik açığı olarak değerlendirilir. Bu yeni açığı kullanarak tekrar istenmeyen bir durumun oluşmasını engelleyecek yeni karşı önlemler almak bilgi güvenliği yaşam döngüsünün gereğidir ve sistemi güvenli tutmak için bu döngü sürekli olarak takip edilmelidir.

Yararlanılan ve Başvurulabilecek Kaynaklar

Adee, S. (2008), "The hunt for the kill switch", ***IEEE Spectrum***, 45 (5): 34–39.

Bayoğlu, B. ***"İşletim sistemleri güvenliği"***, Ulusal Bilgi Güvenliği Kapısı, TÜBİTAK-BİLGEM, Erişim tarihi: 15 Aralık 2016, https://www.bilgiguvenligi.gov.tr/son-kullanici-kategorisi/isletim-sistemleri-guvenligi.html

Bishop, M. (2015). ***"Computer Security: Art and Science"***, Addison-Wesley Professional.

Fern, N., San, I., Koc, C.K. ve Cheng, K.T.T. (2016). "Hiding Hardware Trojan Communication Channels in Partially Specified SoC Bus Functionality," in ***IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems***, vol.PP, no.99, pp.1-1, doi: 10.1109/TCAD.2016.2638439.

ISO/IEC 27001. (2005, 2013). ***Information technology — Security techniques — Information security management systems — Requirements.***

Mitra, H. S., Wong, S.P. ve Wong, S. (2015), ***"Stopping hardware trojans in their tracks"***, IEEE Spectrum.

Viega, J., Kohno, T. ve Potter, B. (2001), "Trust (and mistrust) in secure applications", ***Communications of the ACM***, 44 (2): 31-36.

Shirey, Robert W. (1994***). "Security Architecture for Internet Protocols. A Guide for Protocol Designs and Standards"***, Internet Draft.

Bu Ünitede Kullanılan Resimler Anadolu Üniversitesi Açıköğretim Fakültesi Görsel Arşivinden Alınan Resimlerdir.