BeatCoin: Leaking Private Keys from Air-Gapped Cryptocurrency Wallets

Dr. Mordechai Guri
Ben-Gurion University of the Negev, Israel
Cyber-Security Research Center
gurim@post.bgu.ac.il
demo video (1): https://youtu.be/2WtiHZNeveY
demo video (2): https://youtu.be/ddmHOvT866o

***Abstract*—Cryptocurrency wallets store the wallets private key(s), and hence, are a lucrative target for attackers. With possession of the private key, an attacker virtually owns all of the currency in the compromised wallet. Managing cryptocurrency wallets offline, in isolated ('air-gapped') computers, has been suggested in order to secure the private keys from theft. Such air-gapped wallets are often referred to as 'cold wallets.'**

In this paper we show how private keys can be exfiltrated from air-gapped wallets. In the adversarial attack model, the attacker *infiltrates* the offline wallet, infecting it with malicious code. The malware can be preinstalled or pushed in during the initial installation of the wallet, or it can infect the system when removable media (e.g., USB flash drive) is inserted into the wallet's computer in order to sign a transaction. These attack vectors have repeatedly been proven feasible in the last decade (e.g., [1],[2],[3],[4],[5],[6],[7],[8],[9],[10]). Having obtained a foothold in the wallet, an attacker can utilize various air-gap covert channel techniques (*bridgeware* [11]) to jump the air-gap and exfiltrate the wallets private keys. We evaluate various exfiltration techniques, including physical, electromagnetic, electric, magnetic, acoustic, optical, and thermal techniques. This research shows that although cold wallets provide a high degree of isolation, its not beyond the capability of motivated attackers to compromise such wallets and steal private keys from them. We demonstrate how a 256-bit private key (e.g., bitcoin's private keys) can be exfiltrated from an offline, air-gapped wallet of a fictional character named Satoshi within a matter of seconds[1].

I. Introduction

Cryptocurrencies such as bitcoin [12] and Etherum [13] have emerged as a popular medium of money exchange, with a large associated ecosystem and supporting community. In a nutshell, cryptocurrencies can be considered as a decentralized payment network that is maintained by its users without the need for a single authority. A global log known as 'blockchain' records all of the transactions in the network. Each block in the blockchain represents a number of transactions and includes the transaction data, a timestamp, and a cryptographic hash of the previous block. The distributed nature of the blockchain makes it resistant to adversarial tampering of the information contained in its logs, offering level of protection that is inherently not possible with standard centrally managed databases. The blockchain technology has also been adopted by many other applications such as smart contracts [14], medical records [15] and digital voting [16].

[1]demonstration video: https://cyber.bgu.ac.il/advanced-cyber/airgap

As of the time of this writing (April 2018), more than 3000 different cryptocurrencies are available on the Internet. Most cryptocurrencies share the technology and implementation of the larger cryptocurrencies like bitcoin.

The scope of this paper is relevant to all cryptocurrencies and blockchain applications (e.g., smart contracts), although in this paper we will largely focus on bitcoin, which is the most popular cryptocurrency today.

A. Private & Public Keys

The whitepaper describing bitcoin was published in 2008 by an unknown person (or people) named 'Satoshi Nakamoto.' The paper ("Bitcoin: A Peer-to-Peer Electronic Cash System" [17]) was published on a cryptography mailing list and described the bitcoin network principles. In bitcoin architecture, the payments are performed by issuing *transactions* describing the currency transfers between two *peers* in the network. Every peer in the bitcoin network is referred to by a unique number called a *bitcoin address*. Each bitcoin address is associated with a public key and a private key. The public key is a 65 byte number and the private key is a 32 byte number (256-bit). The public keys are published in the bitcoin network and they are publicly available. Transactions, which are *signed* by a private key can be *verified* by anyone using the corresponding public key. The detailed process of performing transactions in the bitcoin network is provided in the original whitepaper [17].

Although there are various cryptocurrencies with different cryptographic schemes and key sizes, the most popular cryptocurrencies use 256-bit private keys. Table I lists the top-10 cryptocurrencies[2] and the size of their private keys.

B. Cryptocurrency Wallets

A cryptocurrency wallet is a virtual object which refers to the digital credentials of the currency holdings, and it is essentially the public and private keys associated with a peer. A bitcoin wallet contains one or more private keys, which are mathematically related to the bitcoin addresses generated for the wallet. Private keys are the most valuable asset in a wallet as they can be used to transfer all bitcoins in a wallet to

[2]By market capitalization, according to https://coinmarketcap.com/ (April 2018)

TABLE I: The top-10 cryptocurrencies/platforms and the size of their private keys

Symbol	Cryptocurrency	Private key
BTC	Bitcoin	256-bit
ETH	Ethereum	256-bit
XRP	Ripple	256-bit
BCH	Bitcoin cash	256-bit
LTC	Litecoin	256-bit
EOS	EOS	256-bit
ADA	Cardano	256-bit
XLM	Stellar	256-bit
NEO	NEO	256-bit
MIOTA	IOTA	256-bit

another peer. They must be be kept secured and safe to avoid theft and lost.

Some bitcoin wallet applications use a single seed to generate many pairs of public and private keys. This approach is called a hierarchical deterministic (HD) wallet. In one of the common implementations of this type of wallet, the seed value consists of a random 128-bit value represented as a 12 word mnemonic using common English words.

C. Types of Wallets

There are different approaches for managing cryptocurrency wallets. At a technical level, they can be categorized into software wallets, hardware wallets, and paper/brain wallets.

1) Software wallets: A software wallet is the application which stores the public and private keys. It also manages the bitcoin transactions, allowing clients to send bitcoins and view their balance. Most of the software wallets today provide a user-friendly control panel to view the wallet's status and perform online transactions. There are several types of software wallets, and the most important of them are listed below.

- Client-side wallets. Client-side wallets are applications that the user installs on his/her PC, tablet, or smartphone. The public and private keys are stored locally in a wallet file. Many client-side wallet applications support maintaining different types of cryptocurrencies.
- Web-based wallets. Web-based wallets are managed by trusted third parties and can be accessed via online websites. The private keys are stored in the provider's database and are not exposed to the client side.
- Watch-only wallets. Watch-only wallets allow the user to track existing transactions but don't allow them to initiate new ones. Only the public keys are stored in the wallets.
- Cold ('air-gapped') wallets. Cold wallets are managed offline, disconnected from the Internet. Unlike online wallets (hot wallets), cold wallets are not connected to the bitcoin network and hence, can not initiate online transactions. Since cold wallets are managed offline, usually on an air-gapped computer, the private keys are protected from online threats and thought to be safe from cyber theft. Air-gapped wallets will be discussed in Section II and Section III.

2) Hardware wallets: In hardware wallets the private keys are stored in dedicated trusted hardware modules. They are connected to the host computer via USB interface and commonly contain security features such as PIN codes and embedded screens. In hardware wallets the transactions are signed within a trusted computational environment in the hardware (e.g., the ARM TrustZone), and the private keys are not exposed to the host computer. The signed transactions are delivered to the wallet application via a specific API provided by the vendor of the hardware wallet. Hardware wallets are less vulnerable to online attacks because the private keys can not be accessed by malware in the host computer.Known hardware wallets include TREZOR [18] and Ledger Nano S [19].

3) Paper and brain wallets: In a paper wallet the private keys are kept on a printed piece of paper. They are commonly printed in a form of alphabet string or encoded as a QR code. There are online websites that generate printable wallets (e.g., www.bitaddress.org). Paper wallets are considered the most secure, because they are completely offline and are thus, largely unexposed to cyber threats. Similar to paper wallets, in a brain wallet the private keys are not stored in digital form. Instead, the wallet owner memorizes the wallets mnemonic recovery phrase. If the mnemonic recovery phrase are forgotten, the bitcoins are lost.

D. Wallet Security

The security of a wallet is correlated directly with the level of security of its private keys. Hot wallets are always online and hence, vulnerable to cyber-attacks. Attackers can inject a malicious code into the host computer running the wallet application using wide range of techniques including: compromised web-sites [20], drive-by-download [21], malvertising [22], social engineering [23], malicious documents [24], and so on. A malware in the host can easily access the file that stores the private key(s) and leak them to a remote attacker via the Internet. Several cryptocurrency stealing malware have been found in the wild recently: ComboJack [25], CryptoShuffler [26], and TrickBot [27]. Such online attacks are unavoidable as long as the wallet is connected to the Internet.

Hardware wallets are physically connected to online computers (e.g., when transactions are initiated) and can be considered hot wallets. However, the trusted hardware and secure design provide *logical isolation* of the private keys, preventing malicious code from accessing them. Note that hardware wallets don't provide hermetic security. In recent years bugs and vulnerabilities were found in the implementation of hardware components [28], [29], including in trusted execution environments like the ARM TrustZone [30] [31]. These types of vulnerabilities allow attackers to evade hardware-enforced isolation mechanisms and access protected data.

Air-gapped wallets are thought to provide the highest level of protection of the private keys - since the private keys are kept in an offline computer, they are *physically* isolated from the Internet and hence, cannot be accessed by hackers and leaked out.

Table II presents the four types of wallets along with the level of isolation they provide and the attack surface for each wallet.

In this paper we focus on the vulnerability of air-gapped wallets to cyber-attacks. In particular, we show that despite the level of isolation, private keys can be exfiltrated from such wallets to the Internet. First, we discuss the methods that can be used by attackers to infiltrate the air-gapped wallets. Second, we show that attackers can exfiltrate private keys over the air-gap using special types of covert channels.

II. Wallet Infiltration

In this section we present techniques which can be used by attackers to compromise air-gapped wallets and infect them with malware. We also show that the infiltration of a wallet can be done at a very early stage, before the wallet software installed in the system and before the private keys are generated.

A. Post-Installation

Although air-gapped wallets are kept offline, there are occasions when external media is inserted into the air-gapped host. This media might be a USB flash drive, an optical disk (CD/DVD), or a memory card (SD card). The most common scenario of introducing removable media to air-gapped wallets involves signing and broadcasting transactions. Signing transactions and distributing them online is commonly done through an external USB flash drive. For example, in the Electrum bitcoin client, signing a transaction in a cold wallet is done via a file saved in a removable media device [32]. Once the transaction is signed offline, the transaction file is moved to the online wallet and broadcasted over the bitcoin network. The same work flow is true for other wallet applications as well [33].

The removable media transfers between online and offline wallets can be used by attackers to infiltrate air-gapped wallets and infect them with malware. Using removable media (especially USB flash drives) to spread malware across PCs is known to be effective. Research on this topic released by PandaLabs [1] stated that 25% of all worms in 2010 relied on USB devices to spread to other PCs. Out of 10,000 firms infected with malware, more than 2,500 reported that the attack had originated with an infected USB flash drive. Malware such as Daprosy [3], CryptoLocker [2], Spora, [4] and ZCrypt [34] used removable drives as a primary spread vector. In the arena of advanced threats, many famous APTs used removable media to infiltrate air-gapped systems, including ProjectSauron [35], Fanny [9], Regin [8], Stuxnet [10] and Agent.Btz [36]. HammerDrill 2.0, disclosed in WikiLeaks in 2017, is a cross-platform attacking tool that can use CD/DVD as a covert-channel to compromise air-gapped systems [37]. The Brutal Kangaroo framework, [38] also disclosed in WikiLeaks in the same year, includes components which enable the infection of closed networks via USB devices. In April 2018, researchers exposed a file system vulnerability (CVE-2018-6791) which allows arbitrary command execution on Linux systems via external thumb drives [39].

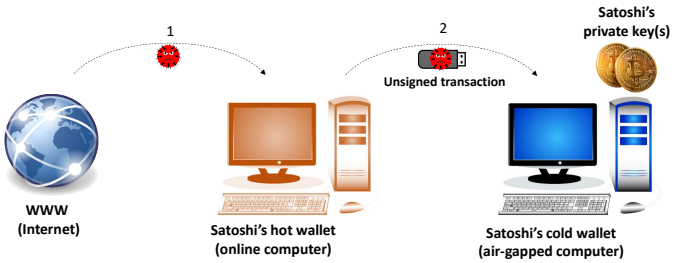

Fig. 1: **Infiltration of an air-gapped wallet during the transaction signing process. When Satoshi plugs the USB flash drive into the air-gapped computer the system is infected.**

The use of such vulnerabilities and tools enables hackers to compromise air-gapped wallets. The infiltration process is illustrated in Figure 1. In the initial stage the Internet-connected computer of the wallet owner is infected with a malware. Once removable media is inserted into the online computer (e.g., to copy the unsigned transaction file), it becomes infected with malware. When the removable media is inserted into the air-gapped computer, it then infects the air-gapped system.

B. Pre-Installation

The air-gapped computer might be compromised even before the wallet is installed, via an infected operating system (OS) or compromised image of the wallet software.

1) Modified OS distribution / modified wallet: Attackers can modify OSs and wallets on the download sites. In a famous attack that occurred in 2016, hackers modified the Linux Mint image file (ISO), inserted a backdoor into it, and managed to hack the official website to point to the compromised image [7]. In the same way, instances of wallet software might be distributed with a built-in malware. Such attacks were shown to be feasible in 2017, when an official version of CCleaner was compromised and distributed with a built-in backdoor [40].

2) Post-download infection: A cold wallet is commonly installed in the air-gapped computer using an OS and a wallet application that were downloaded from the Internet. They are then uploaded to removable media (e.g., USB flash drive) and installed on the air-gapped computer. Malware can infect the removable media or the wallet image after the downloads and just before its installation in the air-gapped computer.

Table III lists the attack vectors for air-gapped wallets. Note that there are additional attack vectors such as supply chain attacks and physical access [41] which can be used for infiltration. However, because such attacks are often targeted, and require a significant amount of funding and resources, they require, we consider them less relevant threats for private cryptocurrency wallets.

TABLE II: The level of isolation and attack surface of the private keys

Wallet type	Isolation	Attack surface
Hot wallets	No isolation	Online attacks (e.g., ComboJack [25], CryptoShuffler [26] and TrickBot [27])
Hardware wallets	Logical isoaltion (hardware enforced)	Hardware implementation bugs and vulnerabilities (e.g.,[30] [31])
Air-gapped cold wallets	Physical isolation	Air-gap infiltration and exfiltration (this paper)
Paper wallet, brain wallet	Physical isolation	Physical lost, theft, forgetting they mnemonic phrase, death, etc.

TABLE III: Infiltration vectors

Infiltration vector	Infection method/stage	Examples of past attacks
Removable media	Wallet installation/ Transactions signing	[3],[2],[4],[34],[35],[9],[8]
Modified images	Modified ISO/ Compromised websites/ Post-download infection	[7],[40],[6],[5]

III. Keys Exfiltration

Having a foothold in the air-gapped computer running the wallet, allows an attacker to utilizes air-gap covert channels to leak the private keys out. Air-gap covert channels are special covert channels that enable communication with air-gapped computers - mainly for the purpose of data exfiltration. In 2018, Guri coinded the term *bridgeware* [11] to refer to the class of malware that exploits air-gap covert channels in order to bridge the air-gap between isolated computers/networks and attackers. The air-gap covert channels can be classified into seven main categories which are discussed in the context of the current attack model (air-gapped wallets) in this section: physical, electromagnetic, electric, magnetic, acoustic, optical, and thermal.

In this type of attack vector the wallet keys are transmitted from the offline wallet to a nearby (online) computer, smartphone, webcam, or other type of receiver via these covert channels. The private keys are then sent to the attacker through the Internet. In the next subsections, we discuss these covert channels and examine the security threat they pose to cryptocurrency wallets.

A. Physical (Removable Media)

As discussed in Section II, although cold wallets are physically disconnected from the Internet, a removable media device (e.g., USB flash drive or CD/DVD) may be inserted into the air-gapped host. Attackers can use this as an opportunity for exfiltrating private keys. Note although such occasions might be rare, one is enough for an attacker to leak one or several private keys.

The most common scenario for the use of removable media is for offline transaction signing. After a transaction is signed in the offline computer, it must be broadcasted to the bitcoin network. This can be done by transferring the signed transaction file to the online wallet computer through a USB flash drive [32]. For example, the *bitcore-wallet* manual for air-gapped wallets states that *"Transactions can be pulled from BWS using a proxy device, then downloaded to a pendrive to be moved to the air-gapped device, signed there, and then moved back the proxy device to be sent back to BWS. Note that Private keys are generated off-line in the airgapped device."* [42].

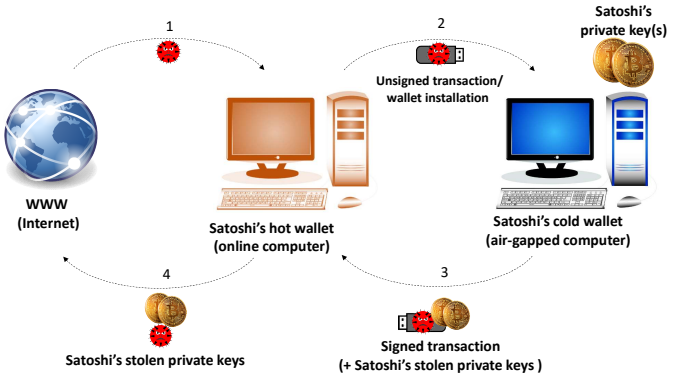

Fig. 2: **Exfiltration of the private keys during the transaction signing process. When Satoshi plugs the USB flash drive into the air-gapped wallet, the private keys are stolen.**

Using removable media to maintain covert channels is a known techniques used by malware and worms [1]. The HammerDrill [37] and Brutal Kangaroo [43] frameworks disclosed in WikiLeaks in 2017 are capable of exchanging data with closed networks via removable media. Similarly, the ProjectSauron APT [35] is capable of exfiltrating data from air-gapped networks via USB sticks. The same mechanism exists in Equation [44], Regin [8] and Fanny APTs [45]. In the case of Fanny, the APT creates a hidden storage area in the USB flash drive, collects the system information, and saves it in the hidden area. When the USB flash drive was inserted into an Internet-connected computer the data was exfiltrated.

This attack vector is illustrated in Figure 2. When a USB flash drive is inserted into the air-gapped computer (e.g., for signing a transaction), the malware stores the private key(s) in a hidden file/partition. Once the USB flash drive is inserted into the hot wallet computer (e.g., for broadcasting the signed transaction), the malware read the private keys and sends it to the attacker over the Internet. Note that the extra I/O operations of writing the private keys to the file-system in the flash drive have a negligible effect in terms of time and are virtually unnoticeable by the user.

B. Electromagnetic

Electromagnetic based covert channels have been studied since the 1990s. Back in 1998, Kuhn et al showed that it is possible to generate electromagnetic emissions from a PC's display cables [46]. They also showed that binary information

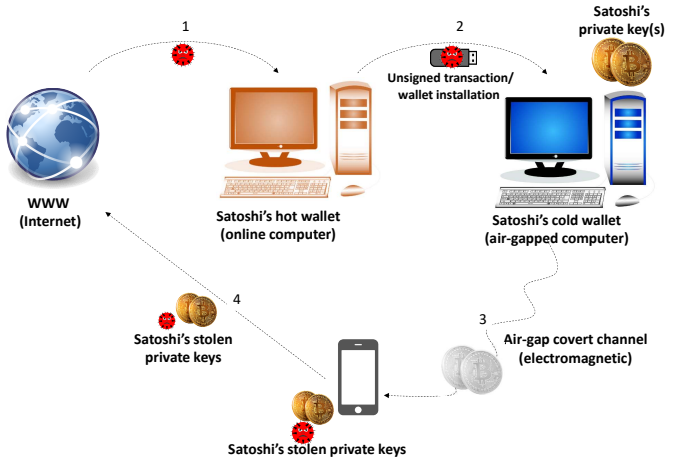

Fig. 3: **Exfiltration of the private keys via electromagnetic covert channels. Satoshi's private keys are transmitted to the nearby smartphone via electromagnetic signals (e.g., AirHopper [48], GSMem [50], RADIoT [51]) and sent to the attacker through the Internet.**

can be modulated on top of the emitted signals. Based on this work, Thiele [47] presented a program which uses the computer monitor to transmit AM radio signals modulated with audio. He demonstrated the method by transmitting the tune Beethoven piece, "Letter to Elise," and showed how it could be heard from a simple radio receiver located nearby. Although the existence of electromagnetic covert channels has long been known, since a radio receiver needs to be located close to the emanating computer, this covert channel was considered less practical for cyber-attacks.

1) AirHopper: More recently, Guri et al demonstrated AirHopper [48], [49], a malware that is capable of exfiltrating data from air-gapped computers to a nearby smartphone via FM signals emitted from the screen cable. The covert transmissions are received by the FM radio receiver which is integrated into many modern smartphones. They also discussed stealth and evasion techniques that help hide the malicious transmission. In a case of an AirHopper attack, the effective distance is a few meters from the air-gapped computer, and the effective bit rate is 100-480 bit/sec. The AirHopper attack can be used to leak the private keys from an air-gapped wallet to the user's smartphone in a few seconds.

2) GSMem: Similar to AirHopper, the GSMem attack [50], enables leaking the data from air-gapped wallets to nearby mobile phones. In this technique malware generates interferences in the cellular bands of the GSM, UMTS, and LTE specification. The signals are generated from the buses which connect the RAM and the CPU on the motherboard. The transmission can be received by a rootkit hidden in the baseband firmware of a nearby mobile phone. In a case of a GSMem attack, the mobile phone must be located close to the air-gapped computer, and the effective bandwidth is 1-2 bit/sec. The GSMem attack can be used to leak the private keys from an air-gapped wallet to the user's smartphone in a few minutes.

3) RADIoT: In the RadIoT attack [51] data can be leaked from air-gapped embedded systems and IoT devices via radio signals. The radio signals - generated from various buses and general-purpose input/output (GPIO) pins of the embedded devices - can be modulated with binary data. In this case, the transmissions can be received by an AM or FM receiver located nearby the device. This attack is relevant to cases where the air-gapped wallet is maintained in embedded and low-power devices, such as a Raspberry PI as suggested in [52][53].In the case of a RADIoT attack, the private keys can be exfiltrated at bit rate of tens to hundreds of bits per second, depending on the type of device used. The RADIoT attack can be used to leak the private keys from an air-gapped wallet to the user's smartphone or RF receiver in a few seconds.

The electromagnetic based covert channels are illustrated in Figure 3. In this case, Satoshi's private keys are transmitted to the nearby smartphone via electromagnetic signals (e.g., AirHopper [48], GSMem [50], RADIoT [51]), and sent to the attacker through the Internet.

C. Electric

In 2018, Guri et al presented PowerHammer [54], an attack which can be used to exfiltrate data from air-gapped computers through power lines. A malware in the air-gapped computer controls the power consumption of the system by changing the CPU workload. It encodes data on top of the changes in current flow, which is propagated through the power lines. In this work, the authors presented a type of attack named phase level power-hammering in which the attacker probes the power lines at the phase level in the main electrical service panel. In the phase level attack, they were able to exfiltrate data at a bit rate of 10 bit/sec. This attack requires the attacker to obtain physical access to the electrical service panel where the air-gapped computer is located. The PowerHammer attack can be used to leak the private keys from an air-gapped wallet in just a few seconds or minutes.

D. Magentic

The private keys can be leaked from air-gapped wallets via magnetic fields.

1) ODINI and MAGNETO: The ODINI [55] and MAGNETO [56] attacks enable the exfiltration of data via magnetic signals generated by the computer processors. Magnetic signals can also be generated from the reading/writing heads of hard disk drives [57]. The receiver may be a magnetic sensor or a smartphone located near the computer. One of the interesting properties of ODINI and MAGNETO attacks is that the low frequency magnetic fields can bypass Faraday shielding. Thus, in the case on an air-gapped wallet, private keys can be exfiltrated even if the wallet or receiver smartphone is enclosed within a Faraday cage. The magnetic covert channels such as ODINI and MAGNETO can be used to leak the private keys from an air-gapped wallet in a matter of minutes.

E. Optical

The private key can be exfiltrated from air-gapped wallets via optical signals. The signals can be received by a nearby cameras, e.g., a webcam, smartphone, or security camera with a line-of-sight with the air-gapped computer. Few optical covert channels which are relevant to our attack model have been proposed over the years.

1) Keyboard LEDs: Loughry introduced the use of PC keyboard LEDs (caps-lock, num-lock, and scroll-lock) to exfiltrate binary data in an optical way [58]. The main drawback of this method is that it is not fully covert. Since keyboard LEDs don't usually blink the user can easily detect the transmission.

2) Hard-disk-drive LEDs: In 2017, Guri et al presented LED-it-GO, a covert channel that uses the hard drive (HDD) indicator LED in order to exfiltrate data from air-gapped computers [59]. The same authors presented a method for data exfiltration from air-gapped networks via router and switch LEDs [60]. In the case of HDDs and routers, the devices blink frequently; hence, transmissions performed via these channels will not raise the user's suspicious. The router LEDs are less relevant in the case of air-gapped wallets, unless the air-gapped wallets are maintained in an internal network with switches or routers.

The optical covert channels described above can be used to leak the private keys from an air-gapped wallet to nearby cameras in a few seconds.

3) Invisible image (VisiSploit) / QR stenography: In some air-gapped wallets (e.g., BitKey [33]) the signed transaction can be scanned from the screen rather than copied to removable media. The signed transaction is shown in a form of QR code on the computer display and can be scanned with a standard smartphone. Guri et al showed that data can be leaked optically through fast blinking images or low contrast invisible QR code projected on the LCD screen [61]. The QR code is invisible to humans but can be reconstructed by a snapshot taken by the smartphone camera. In our case, the private keys are covertly projected on the screen along with the QR code of the signed transaction. When the user scans the visible QR code, the invisible private keys are also scanned.

Another option is to hide the private key data within QR codes to establish a *stenography* based covert channel [62]. Using this method, the private key (or part of it) is covertly embedded within the legitimate QR code of the signed transaction. After the signed transaction is scanned by the smartphone, the private keys are extracted and sent to the attacker. This covert channel is illustrated in Figure 4.

F. Acoustic

In acoustic covert channels the private keys are exfiltrated via inaudible sound waves. Hanspach [63] show how to maintain an ultrasonic covert channel between air-gapped laptops equipped with speakers and microphones. He established communication between two computers located 19 meters apart and achieved a bit rate of 20 bit/sec. Using the same method, Deshotels [64] showed that data can be transferred from computer to smartphone via ultrasonic waves. All of the

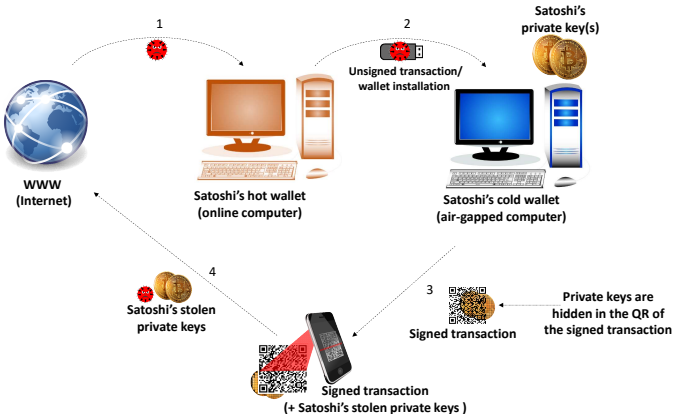

Fig. 4: **Exfiltration of an the private keys during the transaction signing process. Satoshi's private keys are hidden in the signed transaction QR code. When Satoshi scans the QR code, the private keys are extracted and sent to the attacker through the Internet**

aforementioned ultrasonic attacks are relevant to environments in which the computers are equipped with both speakers and microphones. The ultrasonic communication can be used to leak the private keys from an air-gapped wallet to nearby PC or smartphone in a few seconds.

1) Ultrasonic (speaker-to-speaker communication): In many IT environments desktop computers are not equipped with microphones. To overcome this limitation, Guri et al presented MOSQUITO [65] a malware that covertly turns headphones, earphones, or simple earbuds connected to a PC into a pair of microphones, even when a standard microphone is not present. Using this technique they established so-called speaker-to-speaker ultrasonic communication between two or more computers in the same room. This attack is useful when the air-gapped computer is located in the same room with a microphone-less Internet-connected computer that is equipped with passive loudspeakers or headphones. It can be used to leak the private keys in a few seconds.

2) Fansmitter: Computer fan noise: In 2016, Guri et al introduced Fansmitter, a malware which facilitates the exfiltration of data from an air-gapped computer via noise generated from the computer fans [66]. In this method, the air-gapped computer does not need to be equipped with loudspeakers, and the data could be leaked through acoustic signals generated from the computer fan.

3) Diskfiltration: hard-disk-drive noise: Guri et al also presented a method dubbed DiskFiltration that uses the acoustic signals emitted from the hard disk drive (HDD) to exfiltrate data from air-gapped computers [67]. Similar to the previous attack, the air-gapped computer does not need to be equipped with loudspeakers, and the data could be leaked through acoustic noise generated by the HDD.

The Fansmitter and Diskfiltration methods can be used to leak the private keys from an air-gapped wallet in a few minutes.

TABLE IV: The air-gap covert channels relevant for private keys exfiltration

Type	Method	Recevier	256-bit key
Physical	Removable and external media (E.g., USB flash drives)	Computer	<0.01 sec
Electromagentic	AirHopper (FM signals emitted from the video cable [49], [48])	Mobile phone	<1 sec
Electromagnetic	GSMem (cellular interferences emitted from the CPU-RAM bus) [50]	Mobile phone	∼300 sec
Electromagnetic	RADIoT (radio signals generated by embedded and IoT devices) [51]	Mobile phone/ Dedicated receiver	∼1-50 sec
Electric	PowerHammer (data exfiltrated thorough the power lines) [54]	Dedicated receiver	∼ 30-300 sec
Magnetic	MAGNETO (magnetic signals generated by the CPU to smartphone) [56] ODINI (magnetic signals generated by the CPU) [55] HDD (Magnetic signals emitted from the HDD) - laptops [57]	Mobile phone	∼70-1000 sec
Acoustic	Ultrasonic (generated by loudspeakers) [63]	Computer/ Mobile phone	∼1-20 sec
Acoustic	MOSQUITO (speaker-to-speaker ultrasonic communication) [65]	Computer	∼2-20 sec
Acoustic	Fansmitter (acoustic signals generated by the CPU/chassis fans) [66]	Computer/ Mobile phone	∼1000-2000 sec
Acoustic	Diskfiltraition (acoustic signals generated by the HDD actuator arm) [67]	Computer/ Mobile phone	∼100-200 sec
Optical	Keyboard LEDs [58]	Local camera (e.g., webcam)	∼50-100 sec
Optical	Hard disk drive LEDs (LED-it-GO) (optical signals by HDD indicator LED) [59]	Local camera (e.g., webcam)	∼10-100 sec
Optical	Invisible images on screen [61]	Mobile phone	A snapshot
Optical	QR code steganography [62]	Mobile phone	A snapshot

G. Thermal

In 2015, Guri et al presented BitWhisper [68], a thermal covert channel allowing an attacker to establish bidirectional communication between two adjacent air-gapped computers via temperature changes. The heat is generated by the CPU/GPU of a standard computer and received by temperature sensors that are integrated into the motherboard of the nearby computer. Due to the low bit rate we consider this method as a less relevant alternative for private key exfiltration.

H. Other Techniques

There are other air-gap covert channels that have been suggested over the years which requires a hardware receivers or transmitters as a part of the attack. We consider these covert channels as less feasible for the attack model described in this paper. For example, in 2016, Guri et al presented USBee, a malware that uses the USB data buses to generate electromagnetic signals from a desktop computer [69]. Similarly, researchers also proposed using GPIO ports of printers to generate covert radio signals for the purpose of data exfiltration [70]. Both attacks require a dedicated RF receiver in the area. Lopes presented a covert channel based on a malicious hardware component with implanted IR LEDs [71]. However, in this method the attacker must find a way to attach the compromised hardware to the target computer. In 2017, Guri et al presented aIR-Jumper, a malware that uses security cameras and their IR LEDs to covertly communicate with air-gapped networks from a distance of hundreds of meters [72]. This method is relevant only to corporate networks where surveillance cameras are installed.

Table IV. summarizes the relevant air-gap covert channels along with the estimation of time it takes to leak a 256-bit private key in each covert channel.

IV. Countermeasures

Many of the countermeasures for air-gap covert channels are adapted from standards and regulations for governmental and military organizations. Although some of the regulations are restrictive for personal users, they can be employed to some extent for the maintenance of air-gapped wallets.

A. Infiltration

Anti-virus programs (AVs), host-based intrusion detection systems (HIDs) and host-based intrusion prevention systems (HIPs) may be used to prevent the initial infection of the air-gapped wallet with malicious code. Modern AVs may employ static scanning and runtime analysis to every file stored on the removable media device. However, malware authors have repeatedly proven that they can successfully bypass AVs, HIDs and HIPs by using zero-day vulnerabilities and employing stealth and evasion techniques [1],[2],[3],[4],[5],[6],[7],[8],[9],[10].

B. Exfiltration

It is possible to detect and block some covert channels presented in this paper using behavioral analysis. For example, hooking system resources and tracing the use of suspicious

APIs [50], [68], [65] have been suggested for identifying intentional electromagnetic, acoustic, thermal, or optical transmissions. In this approach behavioral analysis, machine learning, and anomaly detection techniques may be used to detect the presence of covert channels and raise alerts. As noted in previous work on this topic, such forms of behavioral detection inherently suffer from high false positive rates [50], [68], [65].

1) Policy-based countermeasures: At the policy level it is possible to define a radius around the air-gapped wallet in which computers, smartphones, cameras, and other receivers are not allowed to cross. This approach is also known as red/black isolation, and refers to a physical separation between systems that may carry information with different levels of classification [11]. However, such measures might not be practical for private users. In addition, some air-gapped wallets intentionally utilize smartphones for the transfer of transactions between cold and hot wallets [33].

2) Hardware-based countermeasures: A basic hardware-based countermeasure scheme involves shielding computers with metallic materials to prevent electromagnetic radiation from leaking from the shielded equipment. Shielding can limit the effective range of many electromagnetic-based attacks. However, it is less suitable for private users due to the maintenance required and cost. When a highly valuable wallet is involved, a signal jamming approach might be taken. In this approach, a specialized hardware transmitter continuously generates random noises that interfere with potential transmissions from the wallet. Jamming is primarily used to block of electromagentic and acoustic signals [73].

V. Conclusion

The threat of data exfiltration from air-gapped computers is often discussed in the context of sophisticated cyber-attacks. However, with the emergence of cryptocurrencies (e.g., bitcoin) and the accompanying need to secure private keys from online threats, it has been suggested that private users manage their cryptocurrency wallets offline in isolated, air-gapped computers.

We show that despite the high degree of isolation of cold wallets, motivated attackers can steal the private keys out of the air-gapped wallets. With the private keys in hand, an attacker virtually owns all of the currency in the wallet. In the attack model presented, the attacker infiltrates the offline wallet, infecting it with malicious code. Then, by using air gap covert channels, attackers can jump the air-gap and leak the private keys to nearby online computers, smartphones, or cameras. We evaluate the exfiltration techniques, including physical, electromagnetic, electric, magnetic, acoustic, optical, and thermal. We present a chain of attack that allows an attacker to compromise an air-gapped wallet and exfiltrate the private keys from it. We demonstrate how bitcoins private keys are exfiltrated from an offline, air-gapped wallet in a matter of a few seconds, using electromagnetic and acoustic covert channels[3].

[3]https://cyber.bgu.ac.il/advanced-cyber/airgap

References

[1] "25% of new worms in 2010 are designed specifically to spread through usb devices - panda security mediacenter," https://www.pandasecurity.com/mediacenter/press-releases/25-of-new-worms-in-2010-are-designed-specifically-to-spread-through-usb-devices/, (Accessed on 04/05/2018).

[2] "New cryptolocker spreads via removable drives - trendlabs security intelligence blog," https://blog.trendmicro.com/trendlabs-security-intelligence/new-cryptolocker-spreads-via-removable-drives/, (Accessed on 04/05/2018).

[3] "W32.daprosy — symantec," https://www.symantec.com/security_response/writeup.jsp?docid=2009-071521-4358-99, (Accessed on 04/05/2018).

[4] "Spora - the shortcut worm that is also a ransomware," https://www.gdatasoftware.com/blog/2017/01/29442-spora-worm-and-ransomware, (Accessed on 04/05/2018).

[5] "Cisco's talos intelligence group blog: The medoc connection," http://blog.talosintelligence.com/2017/07/the-medoc-connection.html, (Accessed on 04/08/2018).

[6] "Shadowpad: How attackers hide backdoor in software used by hundreds of large companies around the world — kaspersky lab," https://www.kaspersky.com/about/press-releases/2017_shadowpad-how-attackers-hide-backdoor-in-software-used-by-hundreds-of-large-companies-around-the-world, (Accessed on 04/08/2018).

[7] "Beware of hacked isos if you downloaded linux mint on february 20th! the linux mint blog," https://blog.linuxmint.com/?p=2994, (Accessed on 04/08/2018).

[8] "Kaspersky_lab_whitepaper_regin_platform_eng.pdf," https://securelist.com/files/2014/11/Kaspersky_Lab_whitepaper_Regin_platform_eng.pdf, (Accessed on 04/05/2018).

[9] "A fanny equation: "i am your father, stuxnet" - securelist," https://securelist.com/a-fanny-equation-i-am-your-father-stuxnet/68787/, (Accessed on 04/05/2018).

[10] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security & Privacy*, vol. 9, no. 3, pp. 49–51, 2011.

[11] M. Guri and Y. Elovici, "Bridgeware: The air-gap malware," *Commun. ACM*, vol. 61, no. 4, pp. 74–82, Mar. 2018. [Online]. Available: http://doi.acm.org/10.1145/3177230

[12] "Bitcoin - open source p2p money," https://bitcoin.org/en/, (Accessed on 04/10/2018).

[13] "Ethereum project," https://www.ethereum.org/, (Accessed on 04/10/2018).

[14] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *Security and Privacy (SP), 2016 IEEE Symposium on*. IEEE, 2016, pp. 839–858.

[15] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in *Open and Big Data (OBD), International Conference on*. IEEE, 2016, pp. 25–30.

[16] M. Pilkington, "11 blockchain technology: principles and applications," *Research handbook on digital transformations*, p. 225, 2016.

[17] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[18] "Trezor bitcoin wallet (official) — the most secure hardware wallet." https://trezor.io/, (Accessed on 04/10/2018).

[19] "Ledger wallet - ledger nano s - cryptocurrency hardware wallet," https://www.ledgerwallet.com/products/ledger-nano-s, (Accessed on 04/10/2018).

[20] N. Provos, D. McNamee, P. Mavrommatis, K. Wang, N. Modadugu *et al.*, "The ghost in the browser: Analysis of web-based malware." *HotBots*, vol. 7, pp. 4–4, 2007.

[21] M. Cova, C. Kruegel, and G. Vigna, "Detection and analysis of drive-by-download attacks and malicious javascript code," in *Proceedings of the 19th international conference on World wide web*. ACM, 2010, pp. 281–290.

[22] A. K. Sood and R. J. Enbody, "Malvertising–exploiting web advertising," *Computer Fraud & Security*, vol. 2011, no. 4, pp. 11–16, 2011.

[23] T. R. Peltier, "Social engineering: Concepts and solutions," *Information Systems Security*, vol. 15, no. 5, pp. 13–21, 2006.

[24] C. Smutz and A. Stavrou, "Malicious pdf detection using metadata and structural features," in *Proceedings of the 28th annual computer security applications conference*. ACM, 2012, pp. 239–248.

[25] "Sure, ill take that! new combojack malware alters clipboards to steal cryptocurrency," https://researchcenter.paloaltonetworks.com/2018/03/unit42-sure-ill-take-new-combojack-malware-alters-clipboards-steal-cryptocurrency/, (Accessed on 04/11/2018).

[26] "Cryptoshuffler trojan has quietly stolen $140,000 worth of bitcoin kaspersky lab official blog," https://www.kaspersky.com/blog/cryptoshuffler-bitcoin-stealer/19976/, (Accessed on 04/11/2018).

[27] "Trickbot's cryptocurrency hunger: Targeting exchange users to steal coins," https://securityintelligence.com/trickbots-cryptocurrency-hunger-tricking-the-bitcoin-out-of-wallets/, (Accessed on 04/11/2018).

[28] P. Kocher, D. Genkin, D. Gruss, W. Haas, M. Hamburg, M. Lipp, S. Mangard, T. Prescher, M. Schwarz, and Y. Yarom, "Spectre attacks: Exploiting speculative execution," *arXiv preprint arXiv:1801.01203*, 2018.

[29] M. Lipp, M. Schwarz, D. Gruss, T. Prescher, W. Haas, S. Mangard, P. Kocher, D. Genkin, Y. Yarom, and M. Hamburg, "Meltdown," *arXiv preprint arXiv:1801.01207*, 2018.

[30] "us-15-shen-attack-your-trusted-core," https://www.blackhat.com/docs/us-15/materials/us-15-Shen-Attacking-Your-Trusted-Core-Exploiting-Trustzone-On-Android.pdf, (Accessed on 04/11/2018).

[31] "Project zero: Trust issues: Exploiting trustzone tees," https://googleprojectzero.blogspot.co.il/2017/07/trust-issues-exploiting-trustzone-tees.html, (Accessed on 04/11/2018).

[32] "Cold storage electrum 3.1 documentation," http://docs.electrum.org/en/latest/coldstorage.html, (Accessed on 04/04/2018).

[33] "Bitkey - secure bitcoin swiss army knife," https://bitkey.io/, (Accessed on 04/05/2018).

[34] "Bitdefender stops zcrypt worm-like ransomware bitdefender labs," https://labs.bitdefender.com/2016/06/bitdefender-stops-zcrypt-worm-like-ransomware/, (Accessed on 04/05/2018).

[35] "The-projectsauron-apt_research_kl.pdf," https://securelist.com/files/2016/07/The-ProjectSauron-APT_research_KL.pdf, (Accessed on 04/05/2018).

[36] R. Grant, "The cyber menace," *Air Force Magazine*, vol. 92, no. 3, 2009.

[37] "Hammerdrill v2.0," https://wikileaks.org/ciav7p1/cms/page_17072172.html, (Accessed on 04/05/2018).

[38] "Wikileaks - vault 7: Projects," https://wikileaks.org/vault7/?#Brutal%20Kangaroo, (Accessed on 04/05/2018).

[39] "https://www.kde.org/info/security/advisory-20180208-2.txt," https://www.kde.org/info/security/advisory-20180208-2.txt, (Accessed on 04/05/2018).

[40] "Ccleaner.com - security notification for ccleaner v5.33.6162 and ccleaner cloud v1.07.3191 for 32-bit windows users," https://www.ccleaner.com/news/release-announcements/2017/9/18/security-notification-for-ccleaner-v5336162-and-ccleaner-cloud-v1073191-for-32-bit-windows-users, (Accessed on 04/08/2018).

[41] F. E. McFadden and R. D. Arnold, "Supply chain risk mitigation for it electronics," in *Technologies for Homeland Security (HST), 2010 IEEE International Conference on*. IEEE, 2010, pp. 49–55.

[42] "Github - bitpay/bitcore-wallet: A command line interface multisig hd wallet, based on 'bitcore-wallet-service'." https://github.com/bitpay/bitcore-wallet, (Accessed on 04/04/2018).

[43] "Wikileaks: Cia uses 'brutal kangaroo' toolkit to hack air-gapped networks," https://www.theinquirer.net/inquirer/news/3012499/-wikileaks-cia-uses-brutal-kangaroo-toolkit-to-hack-air-gapped-networks, 2017, (Accessed on 12/03/2017).

[44] "Equation_group_questions_and_answers.pdf," https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf, (Accessed on 04/04/2018).

[45] "A fanny equation: "i am your father, stuxnet" - securelist," https://securelist.com/a-fanny-equation-i-am-your-father-stuxnet/68787/, (Accessed on 12/03/2017).

[46] M. G. Kuhn and R. J. Anderson, "Soft tempest: Hidden data transmission using electromagnetic emanations." in *Information hiding*, vol. 1525. Springer, 1998, pp. 124–142.

[47] "Tempest for eliza," http://www.erikyyy.de/tempest/, (Accessed on 12/03/2017).

[48] M. Guri, G. Kedma, A. Kachlon, and Y. Elovici, "Airhopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies," in *Malicious and Unwanted Software: The Americas (MALWARE), 2014 9th International Conference on*. IEEE, 2014, pp. 58–67.

[49] M. Guri, M. Monitz, and Y. Elovici, "Bridging the air gap between isolated networks and mobile phones in a practical cyber-attack," *ACM Transactions on Intelligent Systems and Technology (TIST)*, vol. 8, no. 4, p. 50, 2017.

[50] M. Guri, A. Kachlon, O. Hasson, G. Kedma, Y. Mirsky, and Y. Elovici, "Gsmem: Data exfiltration from air-gapped computers over gsm frequencies." in *USENIX Security Symposium*, 2015, pp. 849–864.

[51] M. Guri, "Radiot: Exfiltration of data from air-gapped internet-of-things (iot) and embedded devices via radio signals," 2018.

[52] "Secure your bitcoins! how to build a hackproof bitcoin wallet cryptohq," https://cryptohq.org/secure-your-bitcoins-how-to-build-a-hackproof-bitcoin-wallet/, (Accessed on 04/14/2018).

[53] "Offline bitcoin wallet creation on raspberry pi steemit," https://steemit.com/bitcoin/@deaddy/offline-bitcoin-wallet-creation-on-raspberry-pi, (Accessed on 04/14/2018).

[54] M. Guri, B. Zadov, D. Bykhovsky, and Y. Elovici, "PowerHammer: Exfiltrating Data from Air-Gapped Computers through Power Lines," *ArXiv e-prints*, Apr. 2018.

[55] M. Guri, B. Zadov, A. Daidakulov, and Y. Elovici, "Odini: Escaping sensitive data from faraday-caged, air-gapped computers via magnetic fields," *arXiv preprint arXiv:1802.02700*, 2018.

[56] M. Guri, A. Daidakulov, and Y. Elovici, "Magneto: Covert channel between air-gapped systems and nearby smartphones via cpu-generated magnetic fields," *arXiv preprint arXiv:1802.02317*, 2018.

[57] N. Matyunin, J. Szefer, S. Biedermann, and S. Katzenbeisser, "Covert channels using mobile device's magnetic field sensors," in *Design Automation Conference (ASP-DAC), 2016 21st Asia and South Pacific*. IEEE, 2016, pp. 525–532.

[58] J. Loughry and D. A. Umphress, "Information leakage from optical emanations," *ACM Transactions on Information and System Security (TISSEC)*, vol. 5, no. 3, pp. 262–289, 2002.

[59] M. Guri, B. Zadov, and Y. Elovici, *LED-it-GO: Leaking (A Lot of) Data from Air-Gapped Computers via the (Small) Hard Drive LED*. Cham: Springer International Publishing, 2017, pp. 161–184. [Online]. Available: https://doi.org/10.1007/978-3-319-60876-1_8

[60] M. Guri, B. Zadov, A. Daidakulov, and Y. Elovici, "xled: Covert data exfiltration from air-gapped networks via router leds," *arXiv preprint arXiv:1706.01140*, 2017.

[61] M. Guri, O. Hasson, G. Kedma, and Y. Elovici, "An optical covert-channel to leak data through an air-gap," in *Privacy, Security and Trust (PST), 2016 14th Annual Conference on*. IEEE, 2016, pp. 642–649.

[62] J. Cucurull, S. Guasch, A. Escala, G. Navarro-Arribas, and V. Acín, "Qr steganography: A threat to new generation electronic voting systems," in *Security and Cryptography (SECRYPT), 2014 11th International Conference on*. IEEE, 2014, pp. 1–8.

[63] M. Hanspach and M. Goetz, "On covert acoustical mesh networks in air," *arXiv preprint arXiv:1406.1213*, 2014.

[64] L. Deshotels, "Inaudible sound as a covert channel in mobile devices." in *WOOT*, 2014.

[65] M. Guri, Y. Solwicz, A. Daidakulov, and Y. Elovici, "Mosquito: Covert ultrasonic transmissions between two air-gapped computers using speaker-to-speaker communication," *arXiv preprint arXiv:1803.03422*, 2018.

[66] M. Guri, Y. Solewicz, A. Daidakulov, and Y. Elovici, "Fansmitter: Acoustic data exfiltration from (speakerless) air-gapped computers," *arXiv preprint arXiv:1606.05915*, 2016.

[67] ——, "Acoustic data exfiltration from speakerless air-gapped computers via covert hard-drive noise (diskfiltration)," in *European Symposium on Research in Computer Security*. Springer, 2017, pp. 98–115.

[68] M. Guri, M. Monitz, Y. Mirski, and Y. Elovici, "Bitwhisper: Covert signaling channel between air-gapped computers using thermal manipulations," in *Computer Security Foundations Symposium (CSF), 2015 IEEE 28th*. IEEE, 2015, pp. 276–289.

[69] M. Guri, M. Monitz, and Y. Elovici, "Usbee: Air-gap covert-channel via electromagnetic emission from usb," in *Privacy, Security and Trust (PST), 2016 14th Annual Conference on*. IEEE, 2016, pp. 264–268.

[70] "funtenna github," https://github.com/funtenna, 2015, (Accessed on 12/03/2017).

[71] A. C. Lopes and D. F. Aranha, "Platform-agnostic low-intrusion optical data exfiltration." in *ICISSP*, 2017, pp. 474–480.

[72] M. Guri, D. Bykhovsky, and Y. Elovici, "air-jumper: Covert air-gap exfiltration/infiltration via security cameras & infrared (ir)," *arXiv preprint arXiv:1709.05742*, 2017.

[73] O. Puñal, A. Aguiar, and J. Gross, "In vanets we trust?: characterizing rf jamming in vehicular networks," in *Proceedings of the ninth ACM*

international workshop on Vehicular inter-networking, systems, and applications. ACM, 2012, pp. 83–92.