Guide

Wi-Fi Cards and Chipsets

Greetings aspiring hackers.
I have observed an increasing number of questions, both here on Null-Byte and on other forums, regarding the decision of which USB wireless network adapter to pick from when performing Wi-Fi hacks. So in today's guide I will be tackling this dilemma. First I will explain the ideal requirements, then I will cover chipsets, and lastly I will talk about examples of wireless cards and my personal recommendations. Without further ado, let's cut to the chase.

Ideal Requirements

When you are dealing with hacking, you have got to be equipped with all of the features on offer. In this particular instance involving wireless hacking, there are a few requirements that need to be met in order to achieve the full potential of whatever it is you are performing. Make sure your network card:

1. Supports Monitor mode and Promiscuous mode
2. Supports Master mode
3. Has a fairly good signal reach
4. Supports simultaneous packet injection and capturing
5. Supports as many IEEE PHY modes as possible
6. Supports signal strength management
7. Supports both 2.4GHz and 5GHz frequencies

Let's go step by step.

The chipset you are using should have support for Monitor mode and Promiscuous mode. "Huh, there's a difference?" you ask. Yes, there is.

Neatly put by an answer on StackExchange:
"""
Monitor mode: Sniffing the packets in the air without connecting (associating) with any access point.
Think of it like listening to people's conversations while you walk down the street.

Promiscuous mode: Sniffing the packets after connecting to an access point. This is possible because the wireless-enabled devices send the data in the air but only "mark" them to be processed by the intended receiver. They cannot send the packets and make sure they only reach a specific device, unlike with switched LANs.

Think of it like joining a group of people in a conversation, but at the same time being able to hear when someone says "Hey, Mike, I have a new laptop". Even though you're not Mike, and that sentence was intended to be heard by Mike, but you're still able to hear it.
"""
(Yes, that's Python commenting. And there's nothing wrong with it ;) right?)

One reason to supports these two modes is specifically, as stated above, for packet sniffing. Packet sniffing is essential for most techniques practiced in the sphere of Wi-Fi hacking. One notable example would be using Promiscuous mode with Ettercap and Driftnet to capture browser images.

Another reason could be for deauthing. Deauthing, or formally deauthenticating, means sending a deauthentication frame to an access point (AP) to inform it that the sending client is disconnected. This will disassociate the client from the active connections of the AP. However, a deauth attack involves sending an excessive amount of deauthentication frames that inform the AP of every client being disconnected from it, thus fooling it into disassociating all connected clients. This can also put strain on the AP to eventually cause it to crash, resulting in an additional Denial of Service (DoS) attack being performed unintentionally (and sometimes intentionally). To perform such attacks, Monitor mode is implemented.

2

Having support for Master mode is a more-than-useful feature to have in a network card. A lot of network cards support Master mode, but there are some that do not.

Master mode grants the ability for the chipset to act as an AP. This is useful for creating evil-twin APs and using Karma attack vectors, nothing more to explain here really.

Pretty straightforward so far.

3

Having a fairly good signal reach is self explanatory. You want to be able to sniff data, perform remote injection and capture packets, all the while being a good 80 feet (25 metres, the length of most swimming pools) away from your victim's AP. Wouldn't that be great? This means having a decent (or should I say amazing) antenna that can do all of that.

But this isn't just about the antenna — it is also about the processing done to the data before it can be used properly. Some chipsets are able to work with data collected from very low signals and produce surprisingly accurate and precise calculations. This technology feat is a remarkable advantage to have in wireless hacking, all thanks to the wonders of well-manufactured chipsets. Don't worry about chipsets for the moment, we'll get to that in the next section.

4

Your chipset, whatever it may be and whatever it may hold, should importantly, if not most importantly, possess the ability of packet injection. What is packet injection anyway?

Packet injection means interfering with an already established network connection and sending packets into the stream of data, trying to make those packets seem as if they are part of the normal communication.

I should also note that being able to capture and inject packets simultaneously is essential. This is something well known to be used in WEP password cracking, as it requires that while packets are injected into the victimised AP (usually using aireplay-ng and Monitor mode), an ongoing capture of Initialisation Vectors (IVs) takes place under the hood

This is just one example, and a very important and widely used one, among many other uses for simultaneous packet capturing and injection.

5

IEEE 802.11 are specifications for Wi-Fi communication, and those include Media Access Control (MAC) and Physical Layer (PHY). Currently the talk is about the PHY specification. There are many 802.11 protocol modes that exist but for wireless hacking there are the essentials. Your chipset must support 802.11ac/a/b/g/n (the *ac* isn't a must, but is favourable).

Moving on…

6

The support for signal strength management isn't a gem among sand grains, but it is something good to have as a feature of your chipset. This includes things like setting the *Tx-Power* on your network card, which controls the dBm signal on it. Usually cards have it at 20dBm (100mW) for normal network usage. You can see how being able to change this can aid in wireless hacking, but increasing the strength beyond a certain level can damage the chip in your network card, possibly making it unusable.

Apparently increasing the *Tx-Power* of network cards is illegal in some countries, but I personally don't pay any attention to this, as it cannot be observed by any outsiders.

7

As goes for 802.11ac, being able to work at a 5GHz frequency is not a must, but it is favourable. Most (if not all) network cards these days support 2.4GHz, so there's no need to look for those.

Now that is us, done with the ideal requirements. I will tell you now that there are no perfect cards out there, but if there were any to be built, they would all need to meet the above requirements to be marked as *ideal for wireless penetration testing.*

Chipsets

Throughout the last few sections and paragraphs I've been mentioning these things called chipsets, but what does that actually mean?

Well, a chipset is basically a mini-computer within a motherboard that works by managing the data flowing between the processor, memory and other I/O (input/output) peripherals.

Let's break it down. We have the motherboard, which is the flat material that holds all of the components together. Then there is a processor (also called CPU - Central Processing Unit) that carries out the instructions of a system's functions by performing mathematical calculations based on I/O operations. Then we have the memory, which, unlike storage, holds data for immediate use and gets erased when the system is turned off. Finally we have the peripherals, which are I/O components and allow a system to function through user interaction. Now what a chipset does is it manages/

control/distributes (whatever the word is) the information between all these electrical components.

Get the image? Yes? Now you know what a chipset is.

Recommendations

Lastly, I would like to tell you all about the different examples there are of chipsets used in wireless cards that are pretty close to being ideal.

1. **Atheros AR9271**

This is probably the best, most compatible, plug and play out of the box, fully featured and ready-for-hacking wireless chipset available on the market currently. I believe this is so, as this checks most of the requirements that I listed above (only doesn't check 7, and a bit of 5 as it lacks 802.11ac support), and very few chipsets are up on that level. In fact, none other well-known ones are.

There are two network cards that implement this chipset that I know of:'

AWUS036NHA by Alfa Network

And TL-WN722N by TP-LINK

I have both and to tell you the truth, there is a difference when deciding between the two. The main noticeable difference is the form factor, which is obviously an advantage for the TL-WN722N but don't get too excited to buy it. I would have to pick the AWUS036NHA when performing penetration tests at home or the lab, since it has an immensely surprising advantage of being able to catch and work with such low signals, ones that another card with a (slightly) stronger antenna couldn't even detect.

Now I don't know if that is an actual advantage or if it's the result of my amazing chipset tweaking skills (they aren't that amazing), either way I like both cards equally. I only take the TP-LINK into the real world with me, and that is mainly because it is more portable and less questionable to put on show in front of strangers gazing eyes.

2. **Realtek RTL8187/L**

I find that the RTL8187 and RTL8187L chipsets work very similarly, so similarly that I will just classify them as one. Regardless, they both have great compatibility and work well out of the box in all of the manufactured cards they are used in. They aren't as well refined and their data processing isn't quite as effective on low signals as the AR9271, but they do their job very well. Network cards manufactured with the RTL8187/L embedded include the AWUS036H and AWUS036EW by Alfa Network.

3. **Ralink RT3070**

This chipset is not perfect, it has a few flaws and it doesn't tick the requirements checklist all the way (has minor problems from 3-7), but it is better than many others on the market. Once again Alfa takes the lead by manufacturing the AWUS036NEH and AWUS036NH with the RT3070. Alfa's network game is really on fleek.

Epilogue

So there you have it folks, we've just covered the Wi-Fi hacking grounds from a to z (no we didn't). We discussed the requirements that needs to be met to fit the description of an ideal chipset. We talked about what a chipset actually is, although it would have been more useful if I'd put that section at the start (but I didn't for the fun of it :P). We even covered ground on existing chipsets on the market and which card manufacturers implement those chipsets in their network cards. I mean, what else is there to cover?

I hope you learned something new today and I hope that most of your questions have been answered after reading this guide, which I also hope was somewhat useful.

That's it for today's guide. As always, leave any suggestions for future posts down in the comments below. I will soon be posting a tutorial (yay, not a guide) so stay tuned for that.

As always have a great day, peace.
TRT