Ntiva
Managed IT & Cloud Services

www.ntiva.com

A Field Guide to Secure Wi-Fi

Observations from Your Laptop!

Welcome!

Hi! **My name is Mac** – short for MacBook Pro. My owner and I are about to travel around the world on a business trip to visit clients.

Since I hold so much proprietary information inside of me, I'm always a little uneasy about the **security concerns that come with travel...**

Leaving Home: Man-in-the-Middle Attack

Our first encounter with a potential Wi-Fi security vulnerability happens when my owner opens me up during his flight to London.

He connects to in-flight Wi-Fi, which, by the way, is no different from the public Wi-Fi available at your local coffee shop or mall... Yep, it's a wide open network.

Did you know that a Wi-Fi attack on an open network can take less than 2 seconds? It's SUPER easy for hackers to use a **man-in-the-middle** (MitM) attack to eavesdrop on your data as it travels from point A (your laptop for example) to point B (a website.)

If you must use a public Wi-Fi hotspot, make sure you're at least using a VPN connection!

London, UK: Evil Twin Access Point

We made it to our first stop – London! My owner pops into a coffee shop, and immediately connects me to the coffee shop's wireless network to check his email.

Uh oh, I just noticed the guy next to us typing www.bankofamer... Online banking on an open network? Is he crazy?! There are data thieves everywhere. And I also just noticed that it's not really the coffee shop's access point (AP) that he connected to.

When you connect to an **evil twin access point** that impersonates the real AP's Wi-Fi network name and unique hardware address, it puts users like him at risk of losing private documents that contain highly sensitive information to cyber thieves who intercept data being sent through the network.

Barcelona, Spain: Misconfigured Access Points

We've made it to Barcelona, Spain. My owner is meeting with a client to talk about Wi-Fi security, ensure they have no **misconfigured access points**, and that a wireless intrusion prevention system (WIPS) has been enabled.

The most common misconfiguration is leaving access point configurations set to factory defaults, like usernames, passwords, and even SSID (service set identifier). According to Gartner, the majority of wireless LAN security breaches are caused by poorly configured APs.

Overall, their wireless setup looks good, but they are missing one critical aspect – their WIPS is not yet configured. WIPS is important to the prevention of wireless threats and will detect any misconfigured APs!

Kiev, Ukraine: Rogue Access Points

Eight hours later, we arrive in Kiev, Ukraine to meet with a small business owner about a concern regarding **Rogue Access Points.**

In a business without WIPS security, there is nothing preventing a person from plugging in a foreign access point into your network, inviting unsuspecting people to use their rogue AP vs the one that they meant to connect to.

This happens more often than you think! A hacker can walk into your building with a rogue AP in their laptop backpack, hide it under a desk, and connect it to your network tricking your employees into connecting to the wrong Wi-Fi instead to siphon off sensitive data remotely.

Wireless networks are one of the most overlooked security blind spots within any business. WIPS can scan all the APs in the area and classify them as authorized (known AP that is connected to your network), external (nearby AP that is not connected to your network), or rogue (unknown AP that is connected to your network).

Athens, Greece: Inappropriate & Illegal Content Usage

Opa! Here we are in Athens, Greece, ready for our next meeting with a local secondary school) and educating teachers about the importance of blocking inappropriate and illegal content usage.

According to Nielsen, 45% of children ages 10-12 have smartphones and 68% of parents are concerned about the lack of control over the content their children see online.

In many schools, Wi-Fi security is an afterthought and very few think about **URL content filtering** for adult content and other inappropriate websites.

Secure Wi-Fi solution products not only block inappropriate and illegal content, they can also protect students, faculty, and staff from data theft, password stealing, known malware-compromised websites, and many other harmful attacks.

Sydney, Australia: MAC Address Spoofing

Our next stop is Sydney, Australia – fighting cyber criminals one country at a time!

Today, we are at a local hospital. Hospital wireless networks are a super-easy target for cyber attacks – they're filled with electronic health records. That's a goldmine!

AP **MAC address spoofing** is the Wi-Fi vulnerability we're addressing today. It's a technique where malicious users/hackers change the Media Access Control (MAC) address on their own access point that they brought with them, perhaps in their bag (you'd be surprised how small these devices are nowadays) to match one of the legitimate access point's MAC address.

Basically, AP MAC address spoofing entails changing an access point's identity and stealing important information.

How to keep it from happening to your business? It all comes down to WIPS. There is an "AP MAC Spoofing Prevention" setting in many Wi-Fi Cloud WIPS policies. A secure Wi-Fi Cloud solution can be engineered to provide a safe, protected airspace for both staff and public Wi-Fi environments, while eliminating administrative headaches and greatly reducing costs.

Vancouver, British Columbia: Karma Attack

Our last stop is in Vancouver, British Columbia. After a very long day of flights, we finally land. As we're walking through the airport, my Wi-Fi automatically connects to the free airport Wi-Fi, and my owner didn't even know. Ooops! I must have connected to it in the past and it recognized me.

I'm disabling my Wi-Fi immediately so that I don't experience a **Wi-Fi Karma attack**, otherwise who knows what kind of stranger danger I'll get into having my Wi-Fi automatically connect to network names from my past.

This type of an attack takes advantage of my convenient Wi-Fi features that store wireless network names and passwords so my owner doesn't have to think about them and I always probe out to the world looking to see if these Wi-Fi networks from my past are nearby.

A person running a Karma attack tool can take advantage of my smarts by listening to what Wi-Fi network I'm looking for and offering it to me, which gets me connected to their malicious access point and now my poor owner's data is easily stolen in thin air.

The solution? Once again, it's WIPS – built to cut out Karma attackers as they attempt to gain control.

Summary

Now that we're back home after our journey around the globe, I must say that I saw how vulnerable many Wi-Fi networks are. Hopefully now we have a better understanding of the risks – and the solutions we can use to prevent these risks!

To sum things up, make sure you are correctly and proactively addressing these top 8 vulnerabilities that we have discussed:

1. Man-in-the-Middle Attack (MitM)
2. Evil Twin
3. Misconfigured AP
4. Rogue APs
5. Inappropriate and Illegal Usage
6. AP MAC Address Spoofing
7. Karma Attack

Don't let Wi-Fi be your biggest security gap! Contact your IT professional to make sure you have the Wi-Fi protection you need for your business, whether your employees are in the office, remote workers or on the road!

Interested in learning more about IT security?
Get our free e-book "The Essential Cyber Security Toolkit" which gives you and your staff valuable information on how to keep your business data safe!

Download E-Book Now>