wifi wall

Wireless Security Report

No.5 ▣ August 2, 2019

Bad WiFi configuration calls for the attacker

What's more annoying than having a great WiFi connection, but slow internet speeds? - Security flaws!

When our service provider or we deploy WiFi in the Office, Airports, Hotel, Coffee shops, etc. we optimize for performance. The planning phase will spend most of the attention on assuring high-speed connection everywhere. Use of many Access Points will keep our devices roaming transparently maximizing performance and reducing switching time to a near-zero figure.

On the other hand, many times, fewer resources and panning will be spent on security. The designers may not review all the embedded security risk in the current design. For example, how easy is it for an attacker to launch a Rogue Access Point or Evil Twin that will smoothly become part of the public network. Or, how easy it is for the Attacker to steal personal information when connecting to the "Free" WiFi network.

An example of such a flaw:

Last month, I was traveling to London. Upon arrival, and while being in the terminal, I did what thousands of people do in the airport every hour: connecting to the Heathrow Free WiFi network.

Using WifiWall at Heathrow Airport shows: "open" WiFi network

I immediately noticed that it is an "open" WiFi, meaning, there is no communication encryption. When selecting the Heathrow Free WiFi, I was getting a connection form to complete. Almost every Public WiFi will require you to fill such form before providing an internet connection. It is kenned as "Splash Screen."

So, upon connection, my Phone was diverted to the Heathrow WiFi Splash Screen. The screen requires me to fill a form with personal information. Specifically, the Heathrow WiFi requires to add my name, last name, birthday (I can fake that) email and phone number. If I specify a wrong eMail address or wrong Phone number, I will not get an access code to connect to the internet, so at least that data must be real.

What is the problem?

All needed is a simple "sniffing" application to get the personal data of everyone on this WiFi network. Most of the users of this WiFi network will complete all the required data. This constitutes a severe private data leak.

There are even more devastating design flaws that we encounter in Public WiFi networks:

1. The RSN Diversity (also known as "Crypto Drop" attack):
WiFi network encryption must be the same across all Access Points. This means that all Access Points should have an equal "RSN" value. However, WiFi networks change over time. An Access Point may stop working, and a technician may replace it with a new Access Point with different RSN. Or, when adding WiFi coverage to a new area, the implementation may have a different RSN. We may think that this never happens and all Access Points of a specific WiFi network share the same encryption level. However, in reality, we may find a "Free Paris WIFI" with no password to connect near one that requires a password to connect. This mal configuration makes the life of WiFi attacker very easy. The Attacker adds his Rogue Access Point with different RSN (or none), and no one can see the difference between the Rogue AP and the other APs with different RSN reading.

2. Multiple WiFi networks (multiple SSID) within the same range:
When attackers find many SSIDs belonging to the same WiFi network owner, it is straightforward for him to add Rogue Access Point. For example, image a WiFi network called "Costa Free WiFi" and on the same location, we may find "Costa Management WiFi" and "Costa Suppliers" SSID. The motivation for Costa Company is to "isolate" the different WiFi network. However, the Attacker may add a Rogue Access Point called "Costa Finance." This SSID will confuse and lure some Company employees into connecting. Some of the most popular Access Point vendors, such as Meraki, supports many SSID on the same Access Point.

3. Use of "open" WiFi combined with Splash Screen: I already talked about the Heathrow Airport example and how easy it is to still personal information of travelers. This time, I will explain that Splash Screen, in general, creates considerable risk. The Attacker can easily set a Rogue Access Point, hosting the same HTML page of the Splash Screen (they are all HTML pages). When connecting to the Rogue Access Point, the user will see no difference from the original Access Point Splash Screen. However, the Attacker may include Malware, Spyware, Trojan Horse, or any other malicious content in the same Splash Screen. The user cannot "see" the malicious content which is transferred to the user device. From that point, the malware is traveling with the user and is active even when the VPN is loaded. The Attacker gets full control over the content and device of the user. This attack is so bad that I recommend not using at all Splash Screen in any WiFi network.

4. Same SSID name for 2.4GHz and 5.0GHz networks:
Everyone is assigning same SSID name for their 2.4GHz and 5.0GHz networks. This makes the user life easier. The differences between the 2.4GHz network and 5.0 GHz network are a wide bandwidth in the 5.0GHz network but about 2-3 times the range with the 2.4GHz network. The Attacker wants to be as far as he can from the victim.

However, the victim mostly will be connecting to the 5.0GHz network. Therefore, the Attacker will get close to the victim, connect to the 5.0GHz network, and will send an 802.11 control frame, instructing the victim device to switch to the 2.4GHz network. Now, the Attacker can be far away, and carry the attack using long-range on the 2.4GHz network. The user will get no indication this is happening. If we keep different SSIDs for each network, the Attacker can not use this method. The "cost" is forcing the user to select a 2.4GHz when they are far from the Acces Point.

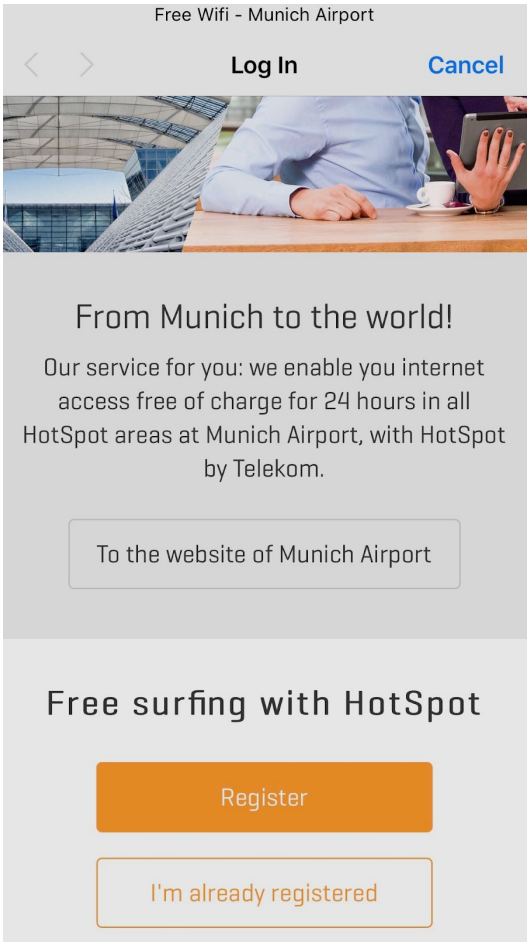
5. Losing track of all Access Points in the network: Many public WiFi owners will invest in improving the connectivity of their WiFi network. This, by itself, is very positive. It also means that from time to time, they may add new Access Points to improve coverage. If they do not manage a White List of all their Access Points, (including all details such as BSSID - MAC Address of the Access Point), they may run into problems. Having a White List is vital, so if there is a new SSID/BSSID combination that is showing in their network, it must be a Rogue Access Point.

Without a special tool to detect Rogue Access Point, the owner of Public WiFi must maintain and manage AP White List.

6. Limit the number of supported channels across Access Points: Some Public WiFi owners define multiple and different channels to every Access Points. In such a rich Channel configuration, it may be common for an Access Point, to instruct user devices to switch the channel. The Attacker is also using the technique of channel switching frames to divert user device to its Rogue Access Point. It is harder to detect such attack, in a WiFi network that is saturated with Channel Switching events.

Summary:

When we design a WiFi network, we must allocate the necessary resources and attention to security. From my experience, the more simple is the design, the fewer components we add to the design, it is usually safer.



Munich Airport "open" WiFi network