wifi wall

Wireless Security Report

No.2 ▣ May 19, 2019

Is this is the end of WiFi security saga?

Is this is the end of WiFi security saga?

Over the years, the IEEE 802.11 group introduced many WiFi Network security improvements. Starting in 1997 with the WEP protocol, continue with a big step forward of WPA and later WPA2.

Every generation of WiFi security algorithm promised a new era of WiFi security; however, soon after the WiFi attackers demonstrated further attacks proving that the fundamental of WiFi network security did not change.

A year and a half ago, post the KRACK attack demonstration (breaking WPA2 in less than a minute), IEEE 802.11 group introduced the new WPA3 protocol including many improvements over the later. **Will WPA3 end the saga, and declare WiFi networks are safe?**

Widely adaptation of new WiFi security protocol takes many years. Whenever new hardware and software of Access Point and Station is released, it mandates everything (computers, phones, WiFi cameras, IoT devices, etc.) to be replaced (due to hardware changes and profound software changes).

We are twenty years after the release of the WEP protocol, and sixteen years after the release of WPA and yet, about 6% of the worldwide WiFi networks are based on WEP or WPA security. Think about the effort required to replace every Access Point in every airport, restaurant, hotel, offices, homes, etc.

WPA3 protocol was introduced in 2018. We now start to see a few vendors' products available to purchase. A good friend and top Wireless security specialist that is running "red team"s' 'catch the flag' games, recently introduced a new break a WAP3 WiFi Network competition. The mission of the white hat attackers was to obtain a data resource located on a specific machine within a WPA3 based WiFi network. Except for one mention (https://hackercombat.com/serious-vulnerabilities-detected-in-the-wpa3-protocol/) we do not know of any WPA3 vulnerability, yet, almost all the attackers, caught the flag quickly.

How did they do it?

Very simple, every WPA3 network, supports WPA2 protocol. This is mandatory for backward compatibility and allowing newly introduced devices to connect to existing WPA2 WiFi networks. We expect that WPA3 WiFi networks will be the most popular networks only within 8 - 10 years. Users of new WiFi devices must be able to communicate with WPA2 networks or otherwise be offline.

All the attackers forced the WPA3 equipment to downgrade to WPA2 (requesting WPA 2 support), and here, penetration was a question of seconds.

Is WiFi security issue is like the OS vulnerability? Can we fix the weaknesses?

Modern Operating Systems security is relatively stable. It's true that Attackers still finds vulnerabilities, and with a significant number, however, the fundamental of the OS security is stable. There will always be weaknesses and vulnerabilities, at least as long as humans will develop the software.
This is not the case with WiFi security. WiFi security suffers from design and structural problems that create major weaknesses on top of the "normal" human errors that create vulnerabilities. The fundamental and basics of WiFi security are wrongly implemented. Since WiFi networks broadcast openly in the air, they are much more vulnerable than any wired network.

Explanation please:

The WiFi Access Point manages the communication with other Stations and AP using 802.11 frames. The most critical frames are the management and control frames. These frames body is never encrypted. Even when using WiFi encryption protocol and a VPN server, they are still not encrypted (only the encapsulated data in the data frame is

encrypted). As a result, every Attacker can use widely available equipment (sniffer) to see that content.

More, the communication between the AP and the Station does not include any identity verification allowing the Attacker to control and manage a Station that is assigned to any other AP. We call it Rogue AP or Evil Twin AP.

Combining these two factors makes any WiFi entity an easy target.

These architectural flaws are on top of the "standard" vulnerabilities in other systems.

How can we fix it?

A dramatic change in protocol is required. A few years ago, there was a protocol that encrypts WiFi management frames: MFP - Management Frame Protection. It was published and released, but yet, seldom found in reality.

WPA3 is a big step in the right direction, but as mentioned earlier, the transition will be over many years.

Therefore, I believe that the only remedy that can ill the problem today and continues to bring substantial value when WPA3 is widely deployed is a 3rd entity that is overseeing the flow of WiFi management frame.

There is a lot of similarity between the current WiFi situation and the early days of the WWW and TCP/IP. Then, every server that connects to the WWW could access any other connected server. The concept of the Firewall was born.

This is why we called our WiFi security product WifiWall.

It is an independent entity, that monitors all WiFi traffic, searching for Attacks that are based on the architectural flaw in WiFi network and adding restrictions and governance. It also searches for vulnerabilities and exploits.

WifiWall, look for 802.11 frames that should not be transmitted, representing WiFi attack such as man in the middle, hijack a connection, Rogue AP and Rogue Station, etc.
They police the WiFi networks similar to a Firewall job over TCP/IP.

Why is the Firewall not doing the work of WifiWall?

Firewall do TCP/IP communication control. Based on a defined policy, the Firewall allows or denies TCP/IP communication between IP addresses and ports.
WifiWall police the 802.11 communication. 802.11 communication is layer 2 and 3, while TCP/IP communication is layer 4.

The equivalent to IP addresses in layer four is the MAC addresses. The Firewall doesn't see the 802.11 frames, but TCP/IP packets and therefore cannot control 802.11 communication.