Wireless security

By Nikolaos Kalivas

Referred to Wikipedia , Wireless security is the prevention of unauthorized access or damage to computers or data using [wireless](https://en.wikipedia.org/wiki/Wireless) networks. The most common types of wireless security are [Wired Equivalent Privacy](https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy) (WEP) and [Wi-Fi Protected Access](https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access) (WPA). WEP is a notoriously weak security standard[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]: the password it uses can often be cracked in a few minutes with a basic laptop computer and widely available software tools. WEP is an old IEEE 802.11 standard from 1997[[1]](https://en.wikipedia.org/wiki/Wireless_security" \l "cite_note-802.11-1997-1), which was superseded in 2003 by WPA, or Wi-Fi Protected Access. WPA was a quick alternative to improve security over WEP. The current standard is WPA2; some hardware cannot support WPA2 without firmware upgrade or replacement. WPA2 uses an encryption device that encrypts the network with a 256-bit key; the longer key length improves security over WEP. Enterprises often enforce security using a [certificate](https://en.wikipedia.org/wiki/Public_key_certificate)-based system to authenticate the connecting device, following the standard 802.1X.

Information Security (InfoSec)

We learn in this course that information security handles risk management. Anything can act as a risk or a threat to the CIA (confidentiality-integrity-availability) triad. Sensitive information must be kept - it cannot be changed, altered or transferred without permission. For example, a message could be modified during transmission by someone intercepting it before it reaches the intended recipient. Good cryptography tools can help mitigate this security threat. Digital signatures can improve information security by enhancing authenticity processes and prompting individuals to prove their identity before they can gain access to computer data. A huge amount of people uses the wireless network by using a laptop or a self-phone and they can be exposed at signal transmission by vulnerabilities such as Hackers. Hackers are trying to find a backdoor in our system or a delayed patched update so they can steal from us personal components.

SECURITY REQUIREMENTS IN WIRELESS NETWORKS

In wireless networks, the information is exchanged among authorized users, but this process is vulnerable to various malicious threats (Hackers) owing to the broadcast nature of the wireless medium. The security requirements of wireless networks are specified for the sake of protecting the wireless transmissions against wireless attacks. Generally speaking secure wireless communications should satisfy the requirements of confidentiality, integrity, availability (CIA triad) and authenticity as I mentioned before:

• Confidentiality: The confidentiality refers to limiting the data access to intended users only, while preventing the disclosure of the information to unauthorized entities.

• Integrity: The integrity of information transmitted in a wireless network should be accurate and reliable during its entire life-cycle representing the source-information without any falsification and modification by unauthorized users.

• Availability: The availability implies that the authorized users are indeed capable of accessing a wireless network anytime and anywhere upon request. The violation of availability, referred to as denial of service, will result in the authorized users to become unable to access the wireless network, which in turn results in unsatisfactory user experience.

• Authenticity: Authenticity refers to confirming the true identity of a network node, to distinguish authorized users from unauthorized users. In wireless networks, a pair of communicating nodes should first perform mutual authentication before establishing a communications link for data transmission

Unauthorized access

A lot of unauthorized access modes can be combined by different ways from hackers and make an attack possible to our system or organization. I will refer to those which are contained to Wikipedia as modes of unauthorized access:

1)Accidental association: truly you need an accident to happened, if you want this mode of attack to works, specific this is when a user turns on their computer and it latches on to a wireless access point from a neighboring company’s overlapping network. The user may not even know that this has occurred and with that way he creates a security breach in which proprietary company information is exposed and now there could exist a link from one company to the other. It can usually happen when a laptop is used to connect to the network and the data could be delivered and seen by the attacker.

2)Malicious association: this mode of attack happens when wireless devices can be actively made by crackers to connect to a company network through a portable device as the middleware of a connection. This device usually runs a software which the attacker can configure the device as an access point and when the victim will connect to it, he/she can easily sniff credentials or initiate an attack.

3)Ad hoc networks: Ad hoc network can be created by a laptop or a device which is connected in the internet, it’s purpose is to create an access point to provide access to other users. And here is where the problem is, the security breach can be found in the exposition of a secure network though unsecured devices(APs).

4)Non-traditional networks: this mode of attack happens to network Bluetooth devices, scanners, handheld pdas or copiers which are not secure and for that reason can be overlooked by IT personnel who have narrowly focus on laptops and access points.

5)Identity theft (MAC spoofing): this mode of attack is about the identity of a network which is referred to MAC address which can be easily found, because it is transmitted in every request of the device through the network. A hacker can combine the MAC address with other software and he can pretend he or his attack statue is happening from another device.

6)Man in the middle attacks (MITM): this mode of attack can be happened usually in public areas. The attacker tempts the victims to connect to a softer Access point and then when the victims fall for,it he can steal transmissions data that the victims exchange with the others. Then the attacker uses the victim as shield, and he connects to the real access point as he still uses the victims to protect his position on the real network.

7)Denial of service (DoS) : this mode of attack it happens usually when we have a big amount of attacks such as failure messages ,or network with premature successful connection messages and the attacker tries to crash our network ,so he can observe the recovery of the wireless network and steal precious components which we want to recover from our crash.

8)Network injection: this mode of attack happens when a hacker can make use of access points that are exposed to non-filtered network traffic and his main purpose is to execute commands to re-configure the network itself.

9)Caffe Latte attack: this mode of attack happens when a hacker tries to defeat the WEP wireless security protocol and he can do it by targeting the windows wireless stack. By sending a lot of ARP(MAC address or ipv4 address.) request the attacker takes advantage of the shared key authentication and he can obtain our WEP key within some minutes.

Wireless security protocols

As I referred on the start after the unauthorized access in Wikipedia it is mentioned the wireless security protocols as the biggest part of “Wireless security”. I am going to describe them, how they were implemented by the passage of time. So, Wi-Fi security algorithms have been through many changes and upgrades since the 1990s to become more secure and effective. Different types of wireless security protocols were developed for home wireless networks protection. The wireless security protocols are WEP, WPA, and WPA2, serving the same purpose but being different at the same time. Their main goal is to protects as from attackers to connect our wireless network, but also encrypt our private data sent over the airwaves. No matter how protected and encrypted, wireless networks cannot keep up in safety with same as wired networks. Because wireless networks broadcast it within their range in every direction to every connected device that happens to be listening and this were the unauthorized access comes to attack with different ways. Bellow is the description of each protocol:

WEP. Wired Equivalent Privacy

**WEP** was developed for wireless networks and approved as a Wi-Fi security standard in September 1999. WEP was supposed to offer the same security level as wired networks, however there are a lot of well-known security issues in WEP, which is also easy to break and hard to configure. Analytical WEP is an IEEE 802.11 wireless protocol which provides security algorithms for data confidentiality during wireless transmissions. WEP uses 24-bit initialization vector (IV) to form stream cipher RC4 for confidentiality and the CRC-32 checksum for integrity of wireless transmission. A 64-bit WEP uses 40-bit key size,128-bit WEP uses 104-bit key size,256-bit WEP uses 232-bit key size. WEP was developed without academic, public nor cryptologists review and it has significant vulnerabilities and design flaws.

Despite all the work that has been done to improve the WEP system it still is a highly vulnerable solution. Systems that rely on this protocol should be either upgraded or replaced in case security upgrade is not possible. WEP was officially abandoned by the Wi-Fi Alliance in 2004.

WPA. Wi-Fi Protected Access

For the time the 802.11i wireless security standard was in development, WPA was used as a temporary security enhancement for WEP. One year before WEP was officially abandoned, WPA was formally adopted. Most modern WPA applications use a pre-shared key (PSK), most often referred to as WPA Personal, and the Temporal Key Integrity Protocol or TKIP for encryption. WPA Enterprise uses an authentication server for keys and certificates generation.

WPA2. Wi-Fi Protected Access version 2

The 802.11i wireless security standard based protocol was introduced in 2004. The most important improvement of WPA2 over WPA was the usage of the Advanced Encryption Standard (AES). AES is approved by the U.S. government for encrypting the information classified as top secret, so it must be good enough to protect home networks. At this time the main vulnerability to the system, is when the attacker already has access to a secured Wi-Fi network and can gain access to certain keys to perform an attack on other devices on the network. As it referred to Wikipedia the vulnerability uses the WPA2 Group Temporal Key (GTK), which is a shared key among all users of the same [BSSID](https://en.wikipedia.org/wiki/BSSID), to launch attacks on other users of the same [BSSID](https://en.wikipedia.org/wiki/BSSID)(BSSID meaning referred to Wikipedia again :[In IEEE 802.11 wireless local area networking standards, a service set is a group of wireless network devices that are operating with the same networking parameters.)](https://en.wikipedia.org/wiki/Service_set_(802.11_network))

WPA3. Wi-Fi Protected Access version 3(Next generation protocol)

Protecting Wi-Fi from hackers is one of the most important tasks in cybersecurity. Which is why the arrival of next-generation wireless security protocol WPA3 deserves your attention: Not only is it going to keep Wi-Fi connections safer, but also it will help save you from your own security short comings. WPA3 will take advantage of WPA2 accomplishments and will bring new features. It will simplify the security configuration, and this will help devices with limited or without display to easily connect to a network. Secondly, it will use 192-bit encryption, this is a mandatory for securing Wi-Fi, because of the strength of the encryption.