Wi-Fi and Wi-Fi Attacks

With the explosive growth in the number of mobile devices over the past decade, wireless (Wi-Fi) networks are now everywhere. Whether you're in an office, hotel, airport, school, or coffee shop, you're likely in range of a Wi-Fi network somewhere.

Of course, as a security professional, your first concern when trying to get connected is "how secure is this Wi-Fi network?" But for the average user, the unfortunate reality is that Wi-Fi connectivity is more about convenience than security.

Thus, the challenge is not only to secure your Wi-Fi networks but also to protect the mobile devices that your organization's employees use to perform work and access potentially sensitive data – no matter where they are or whose network they're on.

Wi-Fi security begins – and ends – with authentication. If you can't control who has access to your wireless network, then you can't protect your network.

Wired Equivalent Privacy

The Wired Equivalent Privacy (WEP) protocol was the wireless industry's first attempt at security. As its name falsely implies, WEP was intended to provide data confidentiality equivalent to the security of a wired network. However, WEP had many well-known and well-publicized weaknesses – such as its weak random value, or initialization vector (IV), and key-generation algorithm – and wasn't effective for establishing a secure wireless network.

Wi-Fi Protected Access (WPA/WPA2/WPA3)

WPA was published as an interim standard in 2003, quickly followed by WPA2 in 2004. WPA/WPA2 contains improvements to protect against the inherent flaws in WEP. These improvements include changes to the encryption to avoid many of the problems that plagued WEP.

WPA2 can be implemented in different ways. WPA2-Enterprise, also known as WPA2-802.1x mode, uses the *Extensible Authentication Protocol* (EAP) and *Remote Authentication Dial-In User Service* (RADIUS) for authentication. Numerous EAP types are also available for use in WPA2-Enterprise.

However, the use of a *pre-shared key* (PSK) is by far the most common, particularly in homes, small businesses, and guest Wi-Fi networks. WPA2-PSK can be implemented with just the AP and the client, requiring neither a third-party 802.1*x* authentication server nor individual user accounts.

WPA2-PSK supports 256-bit keys, which require 64 hexadecimal characters. Because requiring users to enter a 64-hexadecimal character key is impractical, WPA2 includes a function that generates a 256-bit key based on a much shorter passphrase created by the administrator of the Wi-Fi network and the *service set identifier* (SSID) of the AP used as a *salt* for the *one-way hash function*.

Key Terms

The *Extensible Authentication Protocol* (EAP) is a widely used authentication framework that includes about 40 different authentication methods.

Remote Authentication Dial-In User Service (RADIUS) is a client-server protocol and software that enables remote access servers to communicate with a central server to authenticate users and authorize access to a system or service.

A *pre-shared key* (PSK) is a shared secret, used in symmetric key cryptography, that has been exchanged between two parties communicating over an encrypted channel.

In WPA2, the name of the SSID is used for the salt. An easy way to make your Wi-Fi security stronger (and make *rainbow table* attacks impractical) is to change your SSID to something that isn't common or easily guessed.

To execute an attack on a WPA2 passphrase, an attacker needs to be able to test a large number of passphrase candidates. So, although WPA2 remains cryptographically secure (the key isn't recoverable by simple observation of the traffic, as with WEP), methods do exist to test passphrases offline by gathering the handshake packets between the AP and a legitimate user.

To collect the necessary packets to crack a WPA2 passphrase, an attacker could passively gather traffic when a legitimate user joins the network. This method requires time, however, because the attacker does not know when someone will join the network.

For an impatient attacker, the solution is to employ an active attack. As long as a legitimate user is already online, the attacker can force the user's client device to disconnect from the AP with forged de-authentication packets. After getting disconnected, the client device will automatically attempt to reconnect, thus providing the attacker with the handshake packets needed for offline passphrase analysis. Thus, unlike with WEP, attacks on WPA2 can be done without spending a significant amount of time in the proximity of the target network, after the handshake packets have been captured.

Next, the attacker must recover (or find) the passphrase itself, which requires the following:

A test to check millions of potential passphrases until it finds the correct passphrase. To avoid detection, an attacker can't use the actual target, because the victim would be able to see this attack activity. The alternative is to use an offline method of testing that uses the handshake packets.

A methodology to guess passphrases. The worst-case scenario is to "brute force" the passphrase, trying every possible combination of numbers and characters until a correct value is found. This effort can produce a correct result given enough time and computing power. However, it's much faster to take educated guesses without having to resort to brute force. By using educated guesses on possible passphrase candidates, the attacker can attempt a much shorter list.

Key Terms

A *service set identifier* (SSID) is a case-sensitive, 32-character alphanumeric identifier that uniquely identifies a Wi-Fi network.

In cryptography, a *salt* is randomly generated data that is used as an additional input to a one-way hash function that "hashes" a password or passphrase. The same original text hashed with different salts results in different hash values.

A *one-way hash function* is a mathematical function that creates a unique representation (a hash value) of a larger set of data in a manner that is easy to compute in one direction (input to output) but not in the reverse direction (output to input). The hash function can't recover the original text from the hash value. However, an attacker could attempt to guess what the original text was and see if it produces a matching hash value.

A *rainbow table* is a pre-computed table used to find the original value of a cryptographic hash function.

This basic process for recovering Wi-Fi passphrases is similar to cracking user passwords. In the early days of password cracking, an attacker might have knowledge of a target system's one-way hash function and a list of the system's user password hash values. However, the attacker had no way to decrypt the password, because the original text isn't recoverable from a hash. But by encrypting a list of words with the same one-way hash function (a dictionary attack), an attacker can then compare the resulting hash values with the hash values stored for the various user accounts on the system. So, although the password itself isn't decrypted, a given input that produces a given result – a password match – can be found. With the addition of more computing power, an attacker could try longer word lists and a greater number of variations of each word. The process for attacking WPA2 passphrases is similar.

WPA3 was published in 2018 and introduces security enhancements such as more robust brute-force attack protection, improved hot spot and guest access security, simpler integration with devices that have limited or no user interface (such as IoT devices), and a 192-bit security suite. Newer Wi-Fi routers and client devices will likely support both WPA2 and WPA3 to ensure backward compatibility in mixed environments.

According to the Wi-Fi Alliance, WPA3 features include improved security for IoT devices such as smart bulbs, wireless appliances, smart speakers, and other screen-free gadgets that make everyday tasks easier. The Wi-Fi Alliance hasn't outlined the specific details yet, but WPA3 is expected to support a one-touch setup system that will make devices without screens (such as IoT devices and smart speakers like Google Home and Amazon Echo) easier to connect. It will be similar to the existing Wi-Fi Protected Setup protocol, which involves pushing a button on the router to connect a device.

According to a recent *VentureBeat* article, WPA3 also "supports a much stronger encryption algorithm than WPA2 … intended for industrial, defense, and government applications rather than homes and offices. Specifically, it includes a 192-bit security suite that's aligned with the Commercial National Security Algorithm (CNSA) Suite, a feature requested by the Committee on National Security Systems (CNSS), a part of the U.S. National Security Agency [NSA]."[1]

WPA3 provides protection against brute-force dictionary attacks by implementing "a robust handshake [called the Dragonfly protocol, also referred to as Simultaneous Authentication of Equals] that isn't vulnerable to wireless exploits like KRACK, and it hardens security at the time when the network key is exchanged between a device and the access point."[2] By limiting the number of network password attempts on a per-user basis, WPA3 also reduces the efficacy of common dictionary attacks.

"WPA3 introduces Opportunistic Wireless Encryption (OWE), or individualized data encryption, which encrypts every connection between a device and the router with a unique key. Even if the access point doesn't require a password, your device's data won't be exposed to the wider network."[3]

Instead of breaking into a wireless network, an attacker can trick victims into connecting to a wireless network that the attacker controls. These techniques are part of a larger set of attacks known as man-in-the-middle attacks. With a man-in-the-middle exploit in place on a Wi-Fi network, an attacker can serve up practically any content, for example:

- If a user attempts to download a legitimate file, the attacker can send mobile malware instead.
- When a user attempts to visit a legitimate webpage, the attacker can alter the content to exploit a vulnerability that exists in the device's browser, allowing the attacker to further escalate an attack.
- Email addresses and financial account information can be harvested from the connected endpoint, enabling an attacker to create a very targeted and convincing phishing attack to trick even more users on a network into disclosing sensitive information.

Evil Twin

Perhaps the easiest way for an attacker to find a victim to exploit is to set up a wireless access point that serves as a bridge to a real network. An attacker can inevitably bait a few victims with "free Wi-Fi access."

The main problem with this approach is that it requires a potential victim to stumble on the access point and connect. The attacker can't easily target a specific victim, because the attack depends on the victim initiating the connection.

[1] Wiggers, Kyle. "What is WPA3, why does it matter, and when can you expect it?" VentureBeat. May 19, 2018. https://venturebeat.com/2018/05/19/what-is-wpa3-why-does-it-matter-and-when-can-you-expect-it/.

[2] Ibid.

[3] Ibid.

A slight variation on this approach is to use a more specific name that mimics a real access point normally found at a particular location – the Evil Twin. For example, if your local airport provides Wi-Fi service and calls it "Airport Wi-Fi," the attacker might create an access point with the same name using an access point that has two radios. Average users cannot easily discern when they are connected to the real access point or a fake one, so this approach would catch a greater number of users than a method that tries to attract victims at random. Still, the user has to select the network, so a bit of chance is involved in trying to reach a particular target.

The main limitation of the Evil Twin attack is that the attacker can't choose the victim. In a crowded location, the attacker will be able to get a large number of people connecting to the wireless network to unknowingly expose their account names and passwords. However, it's not an effective approach if the goal is to target employees in a specific organization.

Jasager

To understand a more targeted approach than the Evil Twin attack, think about what happens when you bring your wireless device back to a location that you've previously visited. For example, when you bring your laptop home, you don't have to choose which access point to use, because your device remembers the details of wireless networks to which it has previously connected. The same goes for visiting the office or your favorite coffee shop.

Your mobile device detects when it's in proximity to a previously known wireless network by sending a beacon out to see if a preferred network is within range. Under normal conditions, when a wireless device sends out a beacon, the non-matching access points ignore it. The beacon goes unanswered, except when it comes within the proximity of the preferred network.

The Jasager attack takes a more active approach toward beacon requests. Jasager (German for "the yes-man") responds to all beacon requests, thus taking a very permissive approach toward who can connect. The user doesn't have to manually choose the attacker's access point. Instead, the attacker pretends to be whatever access point the user normally connects to (see Figure 1-5). Instead of trying to get victims to connect at random, now the attacker simply needs to be within proximity to the target.

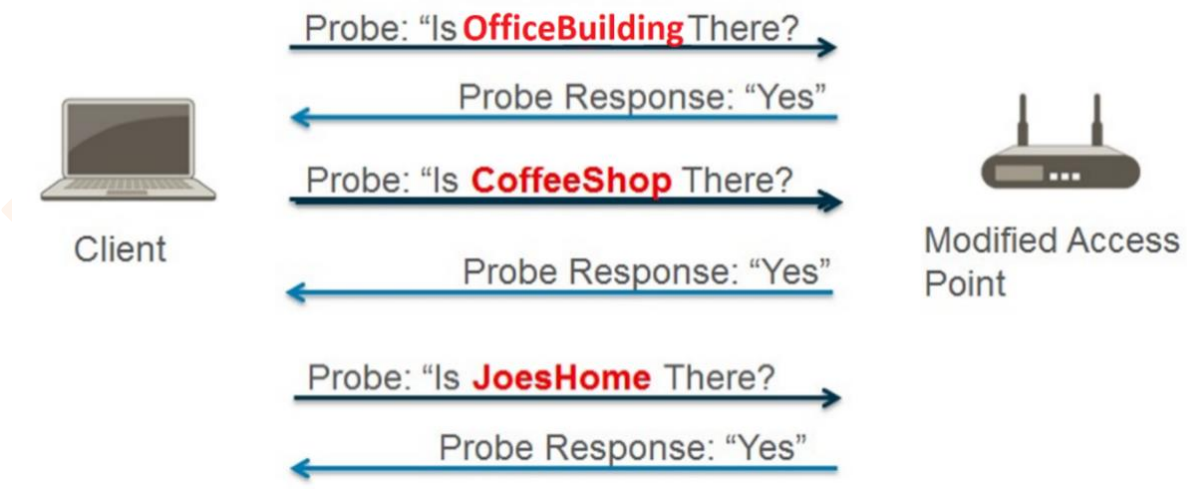

Figure 1-5 *Jasager pretends to be whichever access point is requested by the client's beacon.*

This process intercepts the communication from laptops, mobile phones, and tablets. Many (if not most) 3G/4G/LTE mobile devices automatically switch to Wi-Fi when they recognize that they are near a network that they know.

An attacker can use the same method to capture WPA2 handshake packets to disconnect users from a Wi-Fi network by using forged de-authentication packets. When the users reconnect, they will unwittingly connect to the modified access point. Unlike the Evil Twin attack, the attacker doesn't have to just wait for a victim to connect to the modified access point; with this approach, everyone who's in the vicinity will automatically connect and become a potential victim.

Jasager runs on any number of devices, but perhaps one of the most effective ways to employ it is with the Pineapple access point. The Pineapple is simply an access point with modified firmware that embeds a number of tools for wireless "penetration" testing. It also has a number of accessories, such as support for cellular USB cards to provide network connectivity when it is otherwise unavailable at the target location, and battery packs to operate as a standalone unit. It's also easily concealed because it can be disguised within any number of housings typically found plugged in at the office.

After the attacker has the victim connected to a malicious access point, the man-in-the-middle attack can proceed, and the attacker not only can observe and capture network traffic but also modify it.

SSLstrip

After a user connects to a Wi-Fi network that's been compromised – or to an attacker's Wi-Fi network masquerading as a legitimate network – the attacker can control the content that the victim sees. The attacker simply intercepts the victim's web traffic, redirects the victim's browser to a web server that it controls, and serves up whatever content the attacker desires.

A man-in-the middle attack can be used to steal a victim's online banking or corporate email account credentials. Normally, this type of traffic would be considered safe because the webpage typically uses Secure Sockets Layer (SSL) encryption. Of course, the average user only knows that a padlock somewhere in the address bar means that their browser is secure, correct?

But the padlock appears differently, and in different locations, in different browsers. How does the padlock appear in Internet Explorer? What about Mozilla Firefox, Google Chrome, and Apple Safari? And it appears differently on different smartphones and tablets too. It's no wonder that typical end users – even many security professionals – can be easily tricked.

SSLstrip strips SSL encryption from a "secure" session. When a user connected to a compromised Wi-Fi network attempts to initiate an SSL session, the modified access point intercepts the SSL request (see Figure 1-6). The modified access point then completes the SSL session on behalf of the victim's device. Then the SSL tunnel between the victim's device and the legitimate secure web server is actually terminated – and decrypted – on the modified access point, thus allowing the attacker to see the victim's credentials, and other sensitive information, in cleartext.

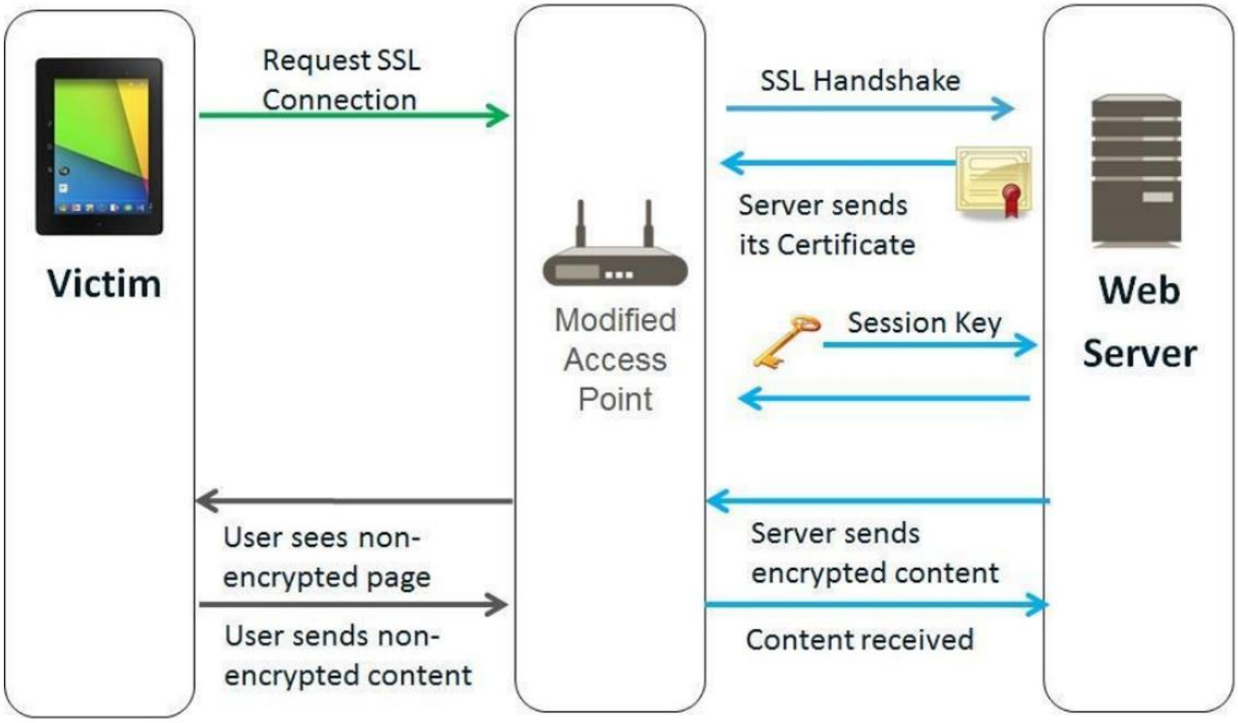

Figure 1-6 *Man-in-the-middle with SSLstrip*

With SSLstrip, the modified access point displays a fake padlock in the victim's web browser. Webpages can display a small icon called a *favicon* next to a website address in the browser's address bar. SSLstrip replaces the favicon with a padlock that looks like SSL to an unsuspecting user.

Emotet

Emotet is a Trojan, first identified in 2014, that has long been used in spam botnets and ransomware attacks. Recently, it was discovered that a new Emotet variant is using a Wi-Fi spreader module to scan Wi-Fi networks looking for vulnerable devices to infect.[4] The Wi-Fi spreader module scans nearby Wi-Fi networks on an infected device and then attempts to connect to vulnerable Wi-Fi networks via a brute-force attack. After successfully connecting to a Wi-Fi network, Emotet then scans for non-hidden shares and attempts another brute-force attack to guess usernames and passwords on other devices connected to the network. It then installs its malware payload and establishes C2 communications on newly infected devices.

Key Terms

A *favicon* ("favorite icon") is a small file containing one or more small icons associated with a particular website or webpage.

[4] Quinn, James. "Emotet Evolves With New Wi-Fi Spreader." Binary Defense. February 7, 2020. https://www.binarydefense.com/emotet-evolves-with-new-wi-fi-spreader/.

Doppelganger

Doppelganger is an insider attack that targets WPA3-Personal protected Wi-Fi networks. The attacker spoofs the source MAC address of a device that is already connected to the Wi-Fi network and attempts to associate with the same wireless access point.

Cookie guzzler

Muted peer and hasty peer are variants of the cookie guzzler attack which exploits the Anti-Clogging Mechanism (ACM) of the Simultaneous Authentication of Equals (SAE) key exchange in WPA3-Personal.