Wireless protocols, The evolution of wireless security protocols

So far, you've learned about
a variety of network protocols,
including communication protocols like TCP/IP.
Now we're going to go more in depth
into a class of communication protocols
called the IEEE802.11.
IEEE802.11, commonly known as Wi-Fi,
is a set of standards that define
communications for wireless LANs.
IEEE stands for
the Institute of Electrical and Electronics Engineers,
which is an organization that maintains Wi-Fi standards,
and 802.11 is a suite of
protocols used in wireless communications.
Wi-Fi protocols have adapted
over the years to become more secure and reliable
to provide the same level of
security as a wired connection.
In 2004,
a security protocol called the Wi-Fi Protected Access,
or WPA, was introduced.
WPA is a wireless security protocol
for devices to connect to the internet.
Since then, WPA has evolved
into newer versions, like WPA2 and WPA3,
which include further security improvements,
like more advanced encryption.
As a security analyst,
you might be responsible for making sure that
the wireless connections in your organization are secure.
Let's learn more about security measures.

The evolution of wireless security protocols

In the early days of the internet, all internet communication happened across physical cables. It wasn’t until the mid-1980s that authorities in the United States designated a spectrum of radio wave frequencies that could be used without a license, so there was more opportunity for the internet to expand.

In the late 1990s and early 2000s, technologies were developed to send and receive data over radio. Today, users access wireless internet through laptops, smart phones, tablets, and desktops. Smart devices, like thermostats, door locks, and security cameras, also use wireless internet to communicate with each other and with services on the internet.

Wireless router with antenna connected to WEP, WPA, WPA2, and WPA3 protocols

Introduction to wireless communication protocols

Many people today refer to wireless internet as Wi-Fi. **Wi-Fi** refers to a set of standards that define communication for wireless LANs. Wi-Fi is a marketing term commissioned by the Wireless Ethernet Compatibility Alliance (WECA). WECA has since renamed their organization Wi-Fi Alliance.

Wi-Fi standards and protocols are based on the 802.11 family of internet communication standards determined by the Institute of Electrical and Electronics Engineers (IEEE). So, as a security analyst, you might also see Wi-Fi referred to as IEEE 802.11.

Wi-Fi communications are secured by wireless networking protocols. Wireless security protocols have evolved over the years, helping to identify and resolve vulnerabilities with more advanced wireless technologies.

In this reading, you will learn about the evolution of wireless security protocols from WEP to WPA, WPA2, and WPA3. You’ll also learn how the Wireless Application Protocol was used for mobile internet communications.

Wired Equivalent Privacy

Wired equivalent privacy (WEP) is a wireless security protocol designed to provide users with the same level of privacy on wireless network connections as they have on wired network connections.

WEP was developed in 1999 and is the oldest of the wireless security standards.

WEP is largely out of use today, but security analysts should still understand WEP in case they encounter it. For example, a network router might have used WEP as the default security protocol and the network administrator never changed it. Or, devices on a network might be too old to support newer Wi-Fi security protocols. Nevertheless, a malicious actor could potentially break the WEP encryption, so it’s now considered a high-risk security protocol.

Wi-Fi Protected Access

Wi-Fi Protected Access (WPA) was developed in 2003 to improve upon WEP, address the security issues that it presented, and replace it. WPA was always intended to be a transitional measure so backwards compatibility could be established with older hardware.

The flaws with WEP were in the protocol itself and how the encryption was used. WPA addressed this weakness by using a protocol called Temporal Key Integrity Protocol (TKIP). WPA encryption algorithm uses larger secret keys than WEPs, making it more difficult to guess the key by trial and error.

WPA also includes a message integrity check that includes a message authentication tag with each transmission. If a malicious actor attempts to alter the transmission in any way or resend at another time, WPA’s message integrity check will identify the attack and reject the transmission.

Despite the security improvements of WPA, it still has vulnerabilities. Malicious actors can use a key reinstallation attack (or KRACK attack) to decrypt transmissions using WPA. Attackers can insert themselves in the WPA authentication handshake process and insert a new encryption key instead of the dynamic one assigned by WPA. If they set the new key to all zeros, it is as if the transmission is not encrypted at all.

Because of this significant vulnerability, WPA was replaced with an updated version of the protocol called WPA2.

WPA2 & WPA3

WPA2

The second version of Wi-Fi Protected Access—known as WPA2—was released in 2004. WPA2 improves upon WPA by using the Advanced Encryption Standard (AES). WPA2 also improves upon WPA’s use of TKIP. WPA2 uses the Counter Mode Cipher Block Chain Message Authentication Code Protocol (CCMP), which provides encapsulation and ensures message authentication and integrity. Because of the strength of WPA2, it is considered the security standard for all Wi-Fi transmissions today. WPA2, like its predecessor, is vulnerable to KRACK attacks. This led to the development of WPA3 in 2018.

Personal

WPA2 personal mode is best suited for home networks for a variety of reasons. It is easy to implement, initial setup takes less time for personal than enterprise version. The global passphrase for WPA2 personal version needs to be applied to each individual computer and access point in a network. This makes it ideal for home networks, but unmanageable for organizations.

Enterprise

WPA2 enterprise mode works best for business applications. It provides the necessary security for wireless networks in business settings. The initial setup is more complicated than WPA2 personal mode, but enterprise mode offers individualized and centralized control over the Wi-Fi access to a business network. This means that network administrators can grant or remove user access to a network at any time. Users never have access to encryption keys, this prevents potential attackers from recovering network keys on individual computers.

WPA3

WPA3 is a secure Wi-Fi protocol and is growing in usage as more WPA3 compatible devices are released. These are the key differences between WPA2 and WPA3:

- WPA3 addresses the authentication handshake vulnerability to KRACK attacks, which is present in WPA2.
- WPA3 uses Simultaneous Authentication of Equals (SAE), a password-authenticated, cipher-key-sharing agreement. This prevents attackers from downloading data from wireless network connections to their systems to attempt to decode it.
- WPA3 has increased encryption to make passwords more secure by using 128-bit encryption, with WPA3-Enterprise mode offering optional 192-bit encryption.

Key takeaways

As a security analyst, knowing the history of how Wi-Fi security protocols developed helps you to better understand what to consider when protecting wireless networks. It’s important that you understand the vulnerabilities of each protocol and how important it is that devices on your network use the most up-to-date security technologies.

Revision #1
Created 2023-06-29 05:10:18 UTC by naruzkurai
Updated 2023-07-03 10:29:21 UTC by naruzkurai