Wireless Security

by Sophia

WHAT'S COVERED

In this lesson, you will learn about how to secure a wireless network.

Specifically, this lesson will cover the following:

BEFORE YOU START

Wireless security was historically nonexistent on access points and clients. The original 802.11 committee just did not imagine that wireless hosts would one day outnumber bounded media hosts, and did not include security standards robust enough to work in a corporate environment.

Today, we have some effective tools and techniques for securing the confidentiality, integrity, and availability of wireless networks.

1. Wireless Threats

There are many threats to the security of wireless networks. We will dive deeper into the processes and procedures designed to mitigate these dangers later in the course, but you will also learn about them here.

1a. Rogue APs

Rogue APs are APs that have been connected to your infrastructure without your knowledge. The rogue may have been placed there by a determined hacker who snuck into the facility and put it in an out-of-the-way location. Or, more innocently, an employee who just wants to connect to a wireless access and does not get just how dangerous doing this is.

One way to keep rogue APs out of the wireless network is to employ a wireless LAN controller to manage your APs. This is a nice mitigation technique because APs and controllers communicate using CAPWAP, and it just so happens that one of the message types they share is called **Radio Resource Management (RRM)**.

Basically, your APs monitor all channels by momentarily switching from their configured channel and by collecting packets to check for rogue activity. If an AP is detected that isn't usually managed by the controller, it is classified as a rogue, and if a wireless control system is in use, that rogue can be plotted on a floor plan and located.

HINT

Another great benefit to this mitigation approach is that it enables your APs to also prevent workstations from associating with the newly exposed rogue.

TERM TO KNOW

Radio Resource Management (RRM)
Ensures efficient use of the available network resources.

1b. Ad Hoc Networks

As you already know, ad hoc networks are created peer to peer or directly between stations and not through an AP. This can be a dangerous configuration because there's no corporate security in place, and since these networks are often created by unsophisticated users who may be wide open to a peer-to-peer attack.

If a laptop happens to connect to the corporate LAN through an Ethernet connection at the same time the ad hoc network is created, the two connections could be bridged by a hacker. This would allow them to gain them unauthorized access to the wired LAN.

Ad hoc networks can be identified over the air by the kind of frames they send, which are different from those belonging to an infrastructure network. When these frames are identified, sophisticated WLAN controllers can prevent harmful intrusions by sending out **deauthentication frames** to keep your stations from associating via ad hoc mode.

TERM TO KNOW

Deauthentication Frames
A type of packet defined in the IEEE 802.11 WiFi standard.

1c. Denial of Service

Not all attacks are aimed at the goal of stealing information. Sometimes the hacker just wants to cause some major network grief, like jamming the frequency the WLAN uses to cause a complete interruption of service until you manage to identify the source of the jamming signal and disable it. This type of assault is known as a **denial of service (DoS) attack**.

If someone is jamming the frequency, there is not much, if anything, you can do. However, many DoS, **on-path-attack (OPA)**, and penetration attacks operate by deauthenticating, or disassociating, stations from their networks. Some DoS attacks take the form of simply flooding the wireless network with probe requests or association frames, which effectively makes the overwhelmed network unavailable for normal transmissions. These types of management frames are sent unauthenticated and unencrypted. Since deauthentication and disassociation frames are classified as management frames, the **Management Frame Protection (MFP)** mechanism can be used to prevent the deluge.

TERMS TO KNOW

Denial of service (DoS)

An attack against data availability.

On-Path-Attack (OPA)

An attack in which an attacker passes on, and potentially alters, messages between two communicating parties without them knowing it.

Management Frame Protection (MFP)

A technique to increase security by providing data confidentiality of management frames, mechanisms that enable data integrity, data origin authenticity, and replay protection.

1d. Passive Attacks

Passive attacks are most often used to gather information to be used in an active attack a hacker is planning to execute later, and they usually involve wireless **sniffing**. During a passive attack, the hacker captures large amounts of raw frames to analyze online with sniffing software that can discover a key and decrypt it in real time. Or the data will be analyzed offline, which simply means the attacker will take the data away and analyze it later.

HINT

In addition to the tools already described, you can use an intrusion detection system (IDS) or an intrusion protection system (IPS) to guard against passive attacks.

EXAMPLE An **intrusion detection system (IDS)** is used to detect several types of malicious behaviors that can compromise the security and trust of your system. These malicious behaviors include network attacks against vulnerable services; data-driven attacks on applications; host-based attacks like privilege escalation; unauthorized logins; access to sensitive files; and malware like viruses, Trojan horses, and worms.

EXAMPLE An **intrusion prevention system (IPS)** is a computer security device that monitors network and/or system activities for malicious or unwanted behavior and can react, in real time, to block or prevent those activities. For example, a network-based IPS will operate inline to monitor all network traffic for malicious code or attacks. When either is detected, it can drop the offending packets while still allowing all other traffic to pass.

TERMS TO KNOW

Sniffing

The interception of data by capturing the network traffic.

Intrusion detection system (IDS)

A device or software application that monitors a network or systems for malicious activity or policy violations.

Intrusion prevention system (IPS)

An IDS with the ability to respond to detected intrusions.

2. Securing Wireless Networks

When it comes to securing wireless networks, the approach you will opt to go with depends on the size of your wireless network and how tight your security needs to be.

KEY CONCEPT

The goal of a security mechanism is to provide three features:

- Confidentiality of the data
- Integrity of the data
- Availability of the data

This is commonly referred to as the “CIA triad.”

KEY CONCEPT

And when faced with decisions about security, you need to consider these three things:

- The safety of the authentication process
- The strength of the encryption mechanism
- Its ability to protect the integrity of the data

Let’s discuss some ways to defend the confidentiality, integrity, and availability of data transmitted on a wireless network.

2a. Geofencing

Geofencing is the process of defining the area in which an operation can be performed by using global positioning (GPS) or radio frequency identification (RFID) to define a geographic boundary. An example of usage involves a location-aware device of a location-based service (LBS) user entering or exiting a geo-fence. This activity could trigger an alert to the device’s user as well as messaging to the geo-fence operator.

TERM TO KNOW

Geofencing

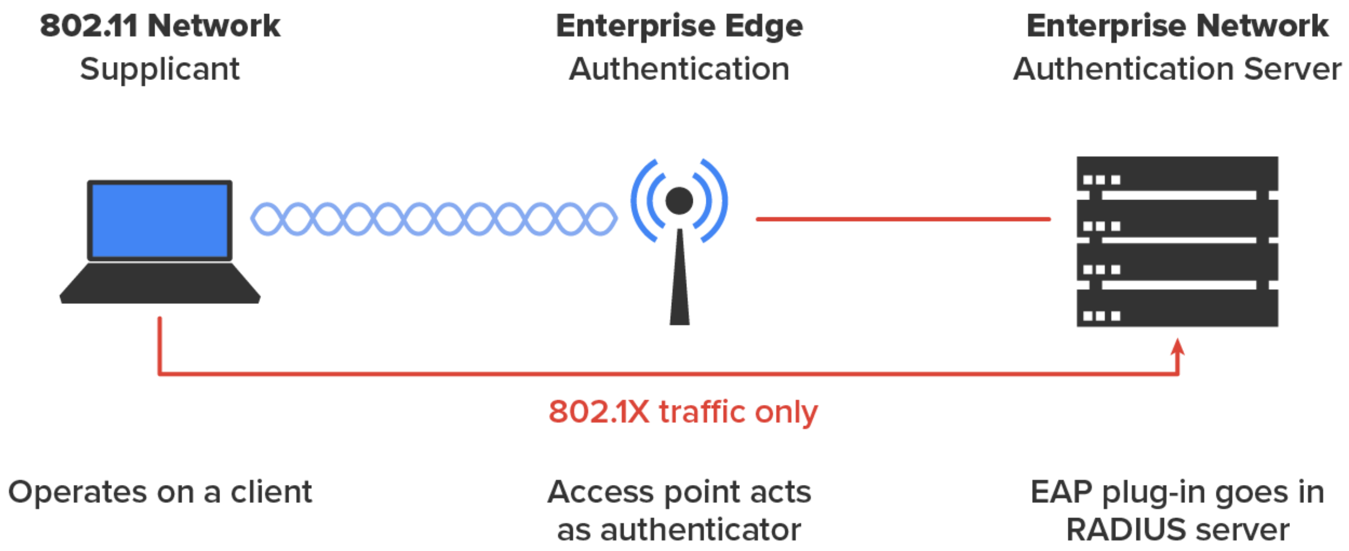
A method of limiting certain wireless network activity to within a certain geographic area.

2b. Remote Authentication Dial-In User Service

Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that offers several security benefits: authorization, centralized access, and accounting supervision regarding the users and/or computers that connect to and access our networks' services.

Once RADIUS has authenticated the user, it allows us to specify the type of rights a user or workstation has, plus control what it, or they, can do within the network. It also creates a record of all access attempts and actions. The provision of authentication, authorization, and accounting is called **AAA**, which is pronounced 'triple A', and is part of the **IEEE 802.1X** security standard.

The illustration below shows how the AP becomes an authenticator when you choose the RADIUS authentication method.



TERMS TO KNOW

Remote Authentication Dial-In User Service (RADIUS)

A networking protocol that provides centralized authentication, authorization, and accounting (AAA) management for users who connect and use a network service.

AAA

Authentication, authorization, and accounting, three security factors described in IEEE 802.1X.

IEEE 802.1X

A standard for port-based network access control, describing how devices can connect to a LAN or WLAN.

3. Encryption

Wi-Fi Protected Access (WPA), which was discussed earlier in the course, is a standard developed by the Wi-Fi Alliance. WPA provides a standard for authentication and encryption of WLANs that is intended to solve known security problems. The standard takes into account common man-in-the-middle WLAN attacks.

BIG IDEA

Encryption is the last line of defense for data in transit across wireless networks.

We use **WPA3** to help us with today's security issues. WPA3 is the most recent standard for providing robust encryption to secure wireless networks. It improves the level of security compared to the widely popular WPA2 standard, yet maintains backward compatibility.

The mechanics of how WPA3 works are quite complex and beyond the scope of this course, but there is lots of documentation online if you are interested in learning the technical details.

TERM TO KNOW

WPA3

A wireless encryption standard that provides 192-bit cryptographic strength.

SUMMARY

In this lesson, you learned about how to secure a **wireless network**. We started by exploring specific wireless threats, including rogue APs, unauthorized ad hoc connections, denial of service attacks, and passive attacks. We addressed mitigation techniques to **secure wireless network traffic**, including intrusion detection systems, intrusion prevention systems, geofencing, and **encryption**.

Source: This content and supplemental material has been adapted from CompTIA Network+ Study Guide: Exam N10-007, 4th Edition. Source **Lammle: CompTIA Network+ Study Guide: Exam N10-007, 4th Edition - Instructor Companion Site (wiley.com)**

TERMS TO KNOW

AAA

Authentication, authorization, and accounting, three security factors described in IEEE 802.1X.

Deauthentication Frames

A type of packet defined in the IEEE 802.11 WiFi standard.

Denial of service (DoS)

An attack against data availability.

Geofencing

A method of limiting certain wireless network activity to within a certain geographic area.

IEEE 802.1X

A standard for port-based network access control, describing how devices can connect to a LAN or WLAN.

Intrusion detection system (IDS)

A device or software application that monitors a network or systems for malicious activity or policy violations.

Intrusion prevention system (IPS)

An IDS with the ability to respond to detected intrusions.

Management Frame Protection (MFP)

A technique to increase security by providing data confidentiality of management frames, mechanisms that enable data integrity, data origin authenticity, and replay protection.

On-Path-Attack (OPA)

An attack in which an attacker passes on, and potentially alters, messages between two communicating parties without them knowing it.

Radio Resource Management (RRM)

Ensures efficient use of the available network resources.

Remote Authentication Dial-In User Service (RADIUS)

A networking protocol that provides centralized authentication, authorization, and accounting (AAA) management for users who connect and use a network service.

Sniffing

The interception of data by capturing the network traffic.

WPA3

A wireless encryption standard that provides 192-bit cryptographic strength.