LEARNING MADE EASY

Extreme Networks Special Edition

Wireless Intrusion Prevention Systems (WIPS)

for dummies®
A Wiley Brand

Signature and forensic analysis

Wireless threat detection and mitigation

The future of WIPS security

Compliments of

Extreme networks

ADVANCE WITH US

David Coleman – CWNE #4

About Extreme Networks

Extreme Networks, Inc. (EXTR) creates effortless networking experiences that enable all of us to advance. We push the boundaries of technology leveraging the powers of machine learning, artificial intelligence, analytics, and automation. Over 50,000 customers globally trust our end-to-end, cloud-driven networking solutions and rely on our top-rated services and support to accelerate their digital transformation efforts and deliver progress like never before. For more information, visit www.extremenetworks.com or follow us on Twitter, LinkedIn, and Facebook.

Wireless Intrusion Prevention Systems (WIPS)

Extreme Networks Special Edition

by David Coleman – CWNE #4

for dummies®
A Wiley Brand

Wireless Intrusion Prevention Systems (WIPS) For Dummies®, Extreme Networks Special Edition

Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-119-80882-4 (pbk); ISBN 978-1-119-80883-1 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Development Editor: Ryan Williams
Project Editor: Jennifer Bingham
Acquisitions Editor: Ashley Coffey
Editorial Manager: Rev Mengle
Business Development Representative: Molly Daugherty
Content Refinement specialist: Tamilmani Varadharaj

Introduction

Wi-Fi security had a bad reputation in its early years — and deservedly so. The legacy security mechanisms initially defined by the IEEE did not provide adequate authentication and data privacy that was needed in a mobility environment. To be blunt, they guarded nothing. In 2005, the Wi-Fi Alliance's Wi-Fi Protected Access 2 (WPA2) certification addressed most of these concerns, and slowly Wi-Fi in the enterprise gained acceptance.

Businesses of all sizes deploy wireless networks for mobility and access. Wireless is nothing less than a business necessity these days. When people think of wireless networking, they tend to think only in terms of secure access and not in terms of attacks or intrusions. However, it also became necessary to monitor continuously for many types of wireless attacks because of the potential damage they can cause.

In 2002, the first *wireless intrusion detection system (WIDS)* solutions were introduced to monitor for numerous attacks against Wi-Fi, such as rogue APs, denial-of-service (DoS), hijacking, and more. Wireless intrusion monitoring has evolved since its creation. Today, systems have methods to prevent and mitigate several of the better-known wireless attacks. Therefore, most WLAN vendors instead call their solutions a *wireless intrusion prevention system (WIPS*). In this book, I will use the terminology of wireless intrusion prevention system (WIPS).

As various WLAN architectures evolved over the years, and WIPS solutions became integrated, many vendors provided the bare minimum of WIPS capabilities. Very often, the WLAN vendors' WIPS solution was just enough to check a box in a request-for-proposal (RFP). Sadly, in many cases, WIPS security is now just an afterthought. Furthermore, WIPS has been taken for granted because Wi-Fi security has been enhanced. For example, the WPA2 security certification has recently been upgraded as WPA3 with more robust security mechanisms.

That being said, all the old wireless attacks still exist, and new attacks always debut. Always remember that Wi-Fi and wireless are access technologies for end-users to gain entry into the corporate network. Wi-Fi hackers and other bad guys will try to find

holes in the access layer security. And it's your job to patch the holes before they spring a leak.

As various WLAN architectures have evolved over the years, so has the architecture for WIPS solutions. Although monitoring for Wi-Fi attacks has been the primary focus, other RF technologies *Bluetooth (BT)* and *Bluetooth Low Energy (BLE)* are being used in enterprise networks. As a result, WIPS solutions are evolving to also monitor these RF technologies for threats. Additionally, WIPS solutions have traditionally used a centralized and monolithic server for management and data processing. In recent years, the entire networking industry has been in the middle of a paradigm shift toward cloud services for management and visibility. WIPS solutions are no exception as they transition to the cloud for all the advantages cloud networking offers, such as scalability, machine learning, and an unlimited data horizon.

Although WIPS has been taken for granted in recent years, the emergence of IoT reinforces the need to put WIPS back at the forefront of any enterprise security solution. The vast majority of the 11 million *new* devices introduced to the Internet each day are wireless. All of these devices are potential unauthorized portals into your networks. This book takes a look at all the risks (including rogue access points), the architecture and capabilities of the WIPS solutions, monitoring your networks, and implementing your solution. Hopefully, this information convinces you that WIPS is more essential than ever.

Icons Used in This Book

Throughout this book, I use special icons to call attention to important information. Here's how you should interpret those icons and what to expect.

This icon points out information you should commit to your nonvolatile memory, your gray matter, or your noggin — along with anniversaries and birthdays!

You will not find a map of the human genome here, but if you seek to attain the seventh level of NERD-vana, perk up! This icon explains the jargon beneath the jargon!

TIP

Tips are appreciated, never expected — and I sure hope you will appreciate these tips. This icon points out useful nuggets of information.

WARNING

These alerts point out the stuff your mother warned you about (well, probably not).

Beyond the Book

There is only so much I can cover in 64 short pages, so if you find yourself at the end of this book, thinking "Where can I learn more?" just go to `www.extremenetworks.com`. You can also read the latest edition of David Coleman and David Westcott's book: *CWNA Certified Wireless Network Administrator Study Guide: Exam CWNA-108* (Wiley).

IN THIS CHAPTER

- The dangers of unauthorized Wi-Fi access
- Can someone eavesdrop your Wi-Fi conversation?
- Please don't deny me my Wi-Fi
- Hijacking your Wi-Fi
- IoT is the new security frontier

Chapter 1
Wireless Security Risks

As you probably know, many wireless threats exist. In this short chapter, I give you a brief overview regarding the numerous potential wireless threats that currently exist or may spring up in the future. Any modern-day WIPS may well have hundreds of threat detection signatures. Wi-Fi and other wireless networking technologies have changed our lives, for the better. However, all of these threats need to be taken seriously and an enterprise-class WIPS solution should always be part of your enterprise security strategy.

Unauthorized Access

A WLAN provides a wireless portal into a wired network infrastructure. The big buzz-phrase in Wi-Fi security has always been the *rogue access point*: a potential open and unsecured gateway straight into the entire network that the company wants to protect. Although 802.1X and other authentication solutions should prevent unauthorized access, what prevents an individual from installing their own wireless portal onto the network backbone? A rogue access point is any unauthorized Wi-Fi device that is not under the management of the proper network administrators.

The greatest WLAN security threat is any type of unauthorized rogue Wi-Fi device that is connected to the wired network infrastructure, as depicted in Figure 1-1. The skull and crossbones icon is a common symbol used to represent rogue APs, as well as pirates. Both examples hijack traffic and steal valuables, but pirates tend to stick to the sea and gold doubloons (that's how you can tell the difference). Any consumer-grade Wi-Fi access point or router can be plugged into a live data port. The rogue device easily acts as a portal into the wired network infrastructure. Because the rogue device is likely configured with no authorization and authentication security in place, any intruder could use this open portal to gain access to network resources.

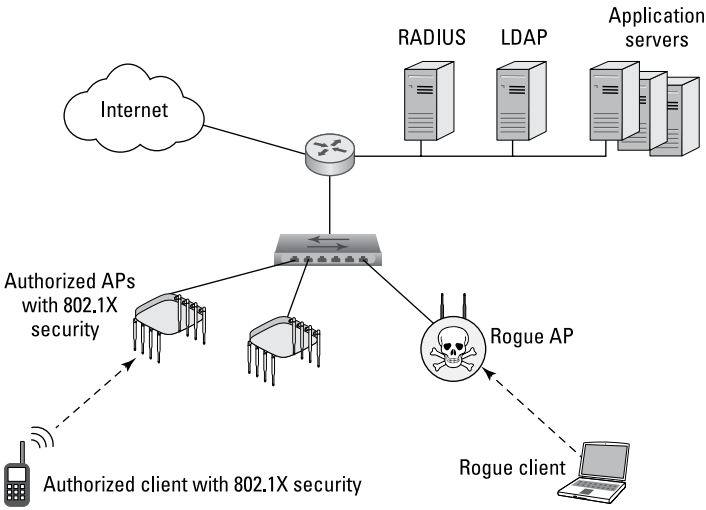

FIGURE 1-1: Here be rogue access points.

Corporate espionage exists in some industries, and government agencies are also key targets for wireless attacks. However, the vast majority of rogue devices are not installed for these malicious purposes. Surprisingly, the individuals most responsible for installing rogue access points are typically not hackers. Instead, these individuals are employees who don't realize the consequences of their actions. Wi-Fi networking has become ingrained in our society, and the average employee has become accustomed to the convenience and mobility that Wi-Fi offers.

As a result, it's not uncommon for employees, contractors, or visitors to install their own wireless devices in the workplace because they believe doing so is easier or more reliable than using the corporate WLAN. Unfortunately, these self-installed access points are often unsecured. Only a single open portal is needed to expose network resources, and many large companies have discovered literally dozens of rogue access points that have been installed by employees.

Because rogue Wi-Fi devices are unauthorized wireless portals, all of your network resources are potentially exposed. If network resources are exposed, you can encounter these risks:

- **Data theft:** Corporate data on database servers can be compromised. Credit card information, corporate trade secrets, personnel information, and medical data can all be stolen if exposed via a rogue device. Any data stored on network servers or desktop workstations is entirely at risk. Data theft is usually the most common risk associated with rogue access.
- **Data destruction:** Destruction of data can also occur. Databases can be erased and drives can be reformatted. Even more common is an attack where your data is encrypted by an attacker who then blackmails your company for ransom money. Ransomware attacks are a global problem.
- **Loss of services:** Network services can also be disabled. Even if no data was stolen, destroyed, or encrypted, imagine the loss of productivity and the potential losses if email services were disabled by an attacker through a rogue AP.
- **Malicious data insertion:** An attacker can use the unauthorized portal to upload viruses and pornography. Remote control applications and keystroke loggers can also be uploaded to network resources and used to gather information at a later date. Attackers have been known to upload illegally copied software and set up illegal servers to distribute the illegal software.

- **Third-party attacks:** Once an attacker has accomplished rogue access, your wired network can be used as a launching pad for third-party attacks against other networks across the Internet. Distributed denial-of-service (DDoS) attacks against other corporate networks can be launched from your network infrastructure. Spammers long ago figured out that they can use a rogue AP as the originating source to send spam. These efforts are part of the botnets often mentioned in connection with DDoS attacks.


TIP

Check out Chapter 3 for a more detailed discussion about the different types of wireless rogue devices. You will also learn about device classification, rogue detection, and rogue mitigation methods.

Did You Hear What They Said?!

Just as human conversations can be overheard by any third party within hearing range of the speakers' voices, Wi-Fi operates in license-free frequency bands, and all data transmissions travel in the open air. Access to wireless transmissions is available to anyone within listening range, and therefore strong encryption is mandatory. Wireless communications can be monitored via two eavesdropping methods: casual eavesdropping and malicious eavesdropping.

Casual eavesdropping, sometimes referred to as *WLAN discovery*, is accomplished by simply monitoring 802.11 frame exchanges between an AP and clients. Software utilities known as WLAN discovery tools exist for the purpose of finding open Wi-Fi networks. In order for a Wi-Fi client to be able to connect to an access point, it must first discover the AP. A client discovers an access point by either listening for an AP (passive scanning) or searching for an AP (active scanning). *In passive scanning*, the client listens for 802.11 beacon management frames, which are continuously sent by the access points.

A casual eavesdropper can simply use any Wi-Fi client radio to listen for 802.11 beacon management frames and to discover layer 2 information about the WLAN. It's just like tuning into a radio station in the car, back when radio was a thing. Some of the information found in beacon frames includes the service set identifier

(SSID), MAC addresses, supported data rates, and other basic service set (BSS) capabilities. All of this layer 2 information is in cleartext and can be seen by any Wi-Fi radio.

In addition to scanning passively for APs, clients can scan actively for them. In *active scanning*, the client transmits management frames known as probe requests. The access point then answers back with a probe response frame, which basically contains all the same layer 2 information found in a beacon frame. A probe request without the SSID information is known as a *null probe request*. If a directed probe request is sent, all APs that support that specific SSID and hear the request should reply by sending a probe response. If a null probe request is heard, all APs, regardless of their SSID, should reply with a probe response.

WLAN discovery tools send out null probe requests across all Wi-Fi channels with the hope of receiving probe response frames containing wireless network information, such as SSID, channel, encryption, and so on. Some WLAN discovery tools may also use passive scanning methods. One very popular discovery and troubleshooting tool is WiFi Explorer or WiFi Explorer Pro from `www.intuitibits.com`.

While casual eavesdropping is considered harmless, *malicious eavesdropping*, the unauthorized use of 802.11 protocol analyzers to capture wireless communications, is typically considered illegal. Most countries have some type of wiretapping law that makes it a crime to listen in on someone else's phone conversation. Additionally, most countries have laws making it illegal to listen in on any type of electromagnetic communications, including 802.11 wireless transmissions.

An 802.11 protocol analyzer application allows wireless network administrators to capture 802.11 traffic so they can analyze and troubleshoot their own wireless networks. A protocol analyzer is a passive device that operates in RF monitoring mode to capture any 802.11 frame transmissions within range. Because protocol analyzers capture 802.11 frames passively, a WIPS solution cannot detect malicious eavesdropping. Commercial WLAN protocol analyzers are available, such as Savvius Omnipeek, as well as the popular freeware protocol analyzer Wireshark (`www.wireshark.org`).

A WLAN protocol analyzer is meant to be used as a diagnostic tool. However, an attacker can use a WLAN protocol analyzer as a malicious listening device for unauthorized monitoring of 802.11 frame exchanges. Although all layer 2 information is always available, all layer 3 through layer 7 information can be exposed if WPA2/WPA3 encryption is not in place. Any cleartext communications, such as email, FTP, and web browsing can be captured if no encryption is provided. Furthermore, any unencrypted 802.11 frame transmissions can be reassembled at the upper layers of the OSI model. Email messages can be reassembled and, therefore, read by an eavesdropper. Web pages and instant messages can also be reassembled. VoIP packets can be reassembled and saved as a WAV sound file. Malicious eavesdropping of this nature is highly illegal.


TIP

Because of the passive and undetectable nature of this attack, encryption must always be implemented to provide data privacy. Encryption is the best protection against unauthorized monitoring of the WLAN. WPA2/WPA3 encryption provides data privacy for all layer 3 through layer 7 information. Additionally, some of the better WIPS solutions can also enforce security policies that ensure corporate APs, and client devices are using the mandated authentication and encryption security.


WARNING

The most common targets of malicious eavesdropping attacks are public access hotspots. Most public Wi-Fi hotspots and guest Wi-Fi SSIDs rarely offer security and usually transfer data without encryption, making users prime targets. The good news is that there is a growing trend to offer secure access at public hotspots via Passpoint and other methods. Meanwhile, use a VPN when connected to any open SSID that does not use encryption (think airports or coffee shops).

Sorry, We Can't Serve You

The attack on wireless networks that seems to receive the least amount of attention is the *denial-of-service (DoS)* attack. With the proper tools, any individual with ill intent can temporarily disable a Wi-Fi network by preventing legitimate users from accessing network resources. The good news is that monitoring systems exist that can detect and identify DoS attacks immediately.

The bad news is that usually nothing can be done to prevent DoS attacks other than locating and removing the source of the attack.

DoS attacks can occur at either layer 1 or layer 2 of the OSI model. Layer 1 attacks are known as RF jamming attacks. The two most common types of RF jamming attacks are intentional jamming and unintentional jamming:

- **Intentional jamming:** Intentional jamming attacks occur when an attacker uses some type of signal generator to cause interference in the unlicensed frequency space. Both narrowband and wideband jammers can interfere with 802.11 transmissions, either causing all data to become corrupted or causing the 802.11 radios to continuously defer when performing a clear channel assessment (CCA). Any continuous RF transmitter results in complete layer 1 DoS.
- **Unintentional jamming:** Unintentional jamming is more common than intentional jamming. Unintentional interference from microwave ovens, cordless phones, and other devices can also cause denial of service. Although unintentional jamming is not necessarily an attack, it can cause as much harm as an intentional jamming attack.

The best tool to detect any type of layer 1 interference, whether intentional or unintentional, is a spectrum analyzer. A good example of an affordable standalone spectrum analyzer is the Wi-Spy DBx spectrum analyzer, which is available from `www.metageek.com`. Some of the better WIPS solutions can offer distributed spectrum analysis capabilities to detect non-Wi-Fi activity in both the 2.4 and 5 GHz bands.

The more common types of denial-of-service attacks that originate from hackers are layer 2 DoS attacks. A wide variety of layer 2 DoS attacks exist that are a result of manipulating 802.11 frames. The most common involves spoofing disassociation or deauthentication frames. As shown in Figure, 1-2, the attacker can edit the 802.11 header and spoof the MAC address of an access point or a client in either the transmitter address (TA) field or the receiver address (RA) field. The attacker then retransmits the spoofed deauthentication frame repeatedly. The client that receives the spoofed deauthentication frame thinks the spoofed frame is coming from a legitimate AP and disconnects at layer 2.

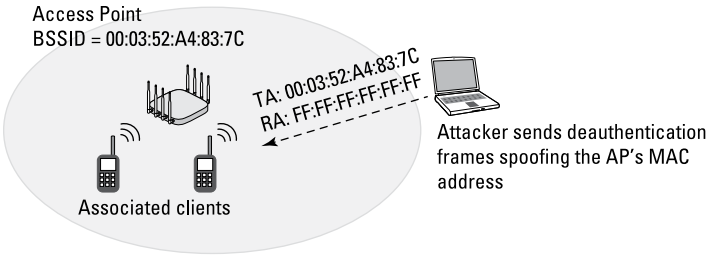

FIGURE 1-2: These APs aren't who they say they are.

Many more types of layer 2 DoS attacks exist, including association floods, authentication floods, PS-Poll floods, and virtual carrier attacks. Luckily, any good wireless intrusion detection system will be able to alert an administrator immediately to a layer 2 DoS attack. The 802.11w-2009 amendment defined *management frame protection (MFP)* mechanisms for the prevention of spoofing certain types of 802.11 management frames. These 802.11w frames are referred to as *robust management frames*.

Unfortunately, not all management frames are considered robust and MFP did not put an end to all layer 2 DoS attacks. Some layer 2 DoS attacks cannot be prevented. In the past, 802.11w MFP mechanisms were not widely supported on the client side because MFP support was optional. However, enterprise WLAN vendors do implement 802.11w mechanisms on access points. Therefore, some of the more common layer 2 DoS attacks can be prevented if the clients support 802.11w. As of 2019, the Wi-Fi Alliance mandates support for management frame protection for all WPA3 certified radios as well as all Wi-Fi 6 (802.11ax) certified radios. The use of MFP protection is still not widespread but is growing.

The best way to prevent any type of denial-of-service attack is physical security. I recommend guard dogs and barbed wire fencing. If that is not an option, then a quality WIPS solution can detect Wi-Fi DoS attacks at both layers 1 and 2 and provide proper alerts. The WIPS solution won't prevent an intruder from getting on the grounds, but it does eat significantly less dog chow.

Hijacking without Wires

An attack that often generates a lot of press is wireless hijacking, also known as the evil twin attack. No goatee or sinister look is required for this method. The attacker configures access point software on a laptop, effectively turning a Wi-Fi client radio into an access point. Other hardware devices often used for penetration testing also can operate as an AP. The access point software on the attacker's laptop is configured with the same SSID that is used by a public-access hotspot. The attacker's access point is now functioning as an evil twin AP with the same SSID, but it is transmitting on a different channel. The attacker then sends spoofed disassociation or deauthentication frames, forcing users associated with the hotspot access point to roam to the evil twin access point. At this point, the attacker has effectively hijacked wireless clients at layer 2 from the original AP. Although deauthentication frames are usually used as one way to start a hijacking attack, an RF jammer can also be used to force any clients to roam to an evil twin AP.

The evil twin is typically configured with a Dynamic Host Configuration Protocol (DHCP) server available to issue IP addresses to the clients. At this point, the attacker can hijack the users at layer 3 using a private wireless network and can perform peer-to-peer attacks on any of the hijacked clients. The user's computer could, during the process of connecting to the evil twin, fall victim to a DHCP attack, an attack that exploits the DHCP process to dump root kits or other malware onto the victim's computer in addition to giving them an IP address as expected.

The attacker may also be using a second wireless NIC with their laptop to execute what is known as a *man-in-the-middle* attack, as shown in Figure 1-3 The second Wi-Fi radio is associated to the original access point as a client. In operating systems, networking interfaces are bridged together to provide routing. The attacker bridged together their second wireless NIC with the Wi-Fi radio that is being used as the evil twin access point. After the attacker hijacks the users from the original AP, the traffic is then routed from the evil twin AP through the second Wi-Fi radio, right back to the original AP from which the users have just been

hijacked. The result is that the users remain hijacked; however, they still have a route back through the gateway to their original network, so they never know they have been hijacked. The attacker can, therefore, sit in the middle and execute peer-to-peer attacks indefinitely while remaining completely unnoticed.

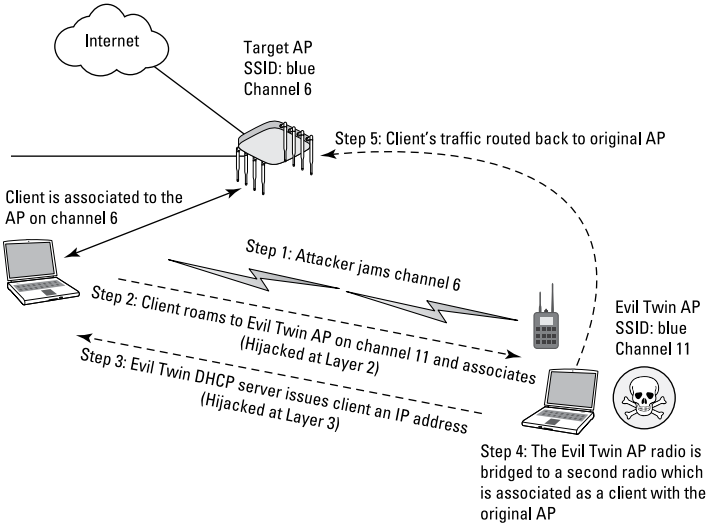

FIGURE 1-3: Avoid the middleman and go straight to the source.

These attacks can take another form in what is known as a *Wi-Fi phishing* attack. The attacker may also have a web server application with captive portal capability. After the users are hijacked to the evil twin access point, they are redirected to a login web page that looks exactly like the hotspot's login page. Then the attacker's fake login page can request a credit card number from the hijacked user. Phishing attacks are common on the Internet and are now appearing at your local hotspot.

The best way to prevent a hijacking, man-in-the-middle, or Wi-Fi phishing attack is to use a strong authentication solution such as 802.1X with validated server certificates. The good news is that a quality WIPS solution also helps you detect the many variations of these types of hijacking attacks.

You Are the Weakest Link

Hackers do not compromise most wired or wireless networks with the use of hacking software or tools. The majority of breaches in computer security occur due to social engineering attacks. *Social engineering* is a technique used to manipulate people into divulging confidential information, such as computer passwords. The best defense against social engineering attacks is strictly enforced policies and employee training to prevent confidential information such as passwords from being shared.

Any information that is static is extremely susceptible to social engineering attacks. For example, WPA2/WPA3-personal security requires the use of a static passphrase.

TIP

This weakness is why many passwords are paired with another verification method, known as multi-factor authentication.

The New Security Frontier

I am fond of saying that the *Internet of Things* (IoT) is the new security frontier. Wi-Fi radios are found in numerous IoT devices, such as manufacturing sensors and patient monitoring equipment. Technology research firm 650 Group estimates that by 2025, the number of wirelessly connected IoT devices will be 59 billion worldwide, far exceeding the expected 28 billion number of PCs, tablets, smartphones, and other connected devices. Traditionally, Wi-Fi IoT devices are often deployed with weaker security despite the fact that they are all possible entry points into your network.

Additionally, wireless IoT threats extend well beyond Wi-Fi. All wireless IoT devices are potential unauthorized entry points into an enterprise network, including Bluetooth (BT) and Bluetooth Low Energy (BLE) IoT devices. In 2018, over 4 billion BLE-enabled devices hit the market.

While the bulk of this chapter has focused on many of the well-known Wi-Fi threats and attacks, other RF technologies such as BLE are being used in enterprise networks in addition to Wi-Fi. For example, rogue BLE Beacons and unsanctioned Bluetooth

devices are potential threats. Because of this, best-of-breed WIPS solutions need to also monitor and protect against threats using different RF technologies. For example, Extreme Networks' enterprise-class WIPS solution, AirDefense, provides monitoring for BLE threats as well as Wi-Fi threats, as shown in Figure 1-4.

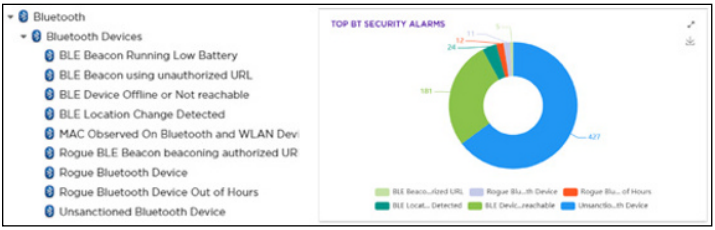

FIGURE 1-4: This war is fought on many fronts.

IN THIS CHAPTER

- Putting the WIPS components together
- Understanding WIPS senor basics and placement strategies
- Should my sensors work full-time or part-time?
- What does the future hold for WIPS?

Chapter 2
WIPS Architecture

Wireless intrusion monitoring has evolved since its creation in 2002. In this chapter, I discuss the necessary components of WIPS architecture, how it has evolved over time, and the future of WIPS security moving forward.

WIPS Components

In today's world, a wireless intrusion prevention system (WIPS) might be necessary even if there is no authorized 802.11 wireless network onsite. Wireless can be an intrusive technology, and if wired data ports at a business are not controlled, any individual (including an employee) can install a rogue access point. Because of this risk, many companies — such as banks, other financial institutions, and hospitals — choose to install a WIPS before deploying a Wi-Fi network for employee access. After a Wi-Fi network is installed for access, it has become almost mandatory to also have a WIPS because of the other numerous attacks against Wi-Fi, such as DoS, hijacking, and so on. The typical WIPS is a client-server model that consists of the following two primary components.

WIPS server

A WIPS server is a software server or hardware server appliance acting as a central point for 24/7 data collection and monitoring of Wi-Fi security threats. Think of it as a really attentive watchdog for your network, that is never distracted by a juicy steak. A WIPS server might also be integrated in a WLAN controller. The server monitoring capabilities can also be unified with a *network management server (NMS)* solution that is used to monitor all aspects of a WLAN. An NMS solution may be deployed in a data center as an on-premises solution or exist in a cloud-based environment. A best-of-breed WIPS server provides enhanced Wi-Fi security visibility from a user interface (UI) that can often be customized.


TIP

A WIPS server uses signature analysis, behavior analysis, protocol analysis, and RF spectrum analysis to detect potential threats. These methods of analysis are discussed in greater detail in Chapter 4.

Sensors

Hardware- or software-based sensors are placed strategically to listen to and capture all Wi-Fi communications. Sensors are the eyes and ears of a WIPS monitoring solution, and are more than reliable than nosy neighbors holding glasses up to walls. Sensors use 802.11 radios to collect information used in securing and analyzing Wi-Fi traffic. Sensors are normally hardware-based and resemble the form-factor of a Wi-Fi access point (AP).

Overlay versus Integrated

The components of a WLAN security monitoring solution are usually deployed within one of the following two major WIPS architectures:

Overlay

The most secure model is an overlay WIPS, which is deployed on top of the existing wireless network. This model uses an independent vendor's WIPS and can be deployed to monitor any existing or planned WLAN. The overlay systems typically offer more extensive features, but they are usually more expensive. That's

always the way, isn't it? The overlay solutions consist of a WIPS server and sensors that are not part of the WLAN solution that provides access to clients.


TIP

Dedicated overlay systems are not as common as they used to be, because many of the WIPS capabilities have been integrated into most enterprise WLAN products.

Integrated

Most WLAN vendors have fully integrated WIPS capabilities. A centralized WLAN controller or a centralized *network management server (NMS)* functions as the WIPS server. WIPS solutions are also moving into cloud-based management. Access points can be configured in a full-time sensor-only mode or can act as part-time sensors when not transmitting as access points. Most APs already use off-channel scanning procedures for adaptive channel and power purposes. These same APs are also effectively part-time sensors for the integrated WIPS server when listening off channel. The integrated solution is a less expensive solution but may not have all the capabilities of an overlay WIPS.


REMEMBER

Of the two WIPS architectures, the integrated WIPS is by far the most widely deployed. The overlay WIPS is usually cost prohibitive for most WLAN customers. The more robust overlay WIPS solutions are usually deployed in defense, finance, and big-box retail vertical markets, where the budget for an overlay solution may be available.

Sensor 101

Sensors are basically radio devices that are in a constant listening mode as passive devices. The sensor devices are usually hardware-based and resemble an access point. The sensors have some intelligence but must communicate with the centralized WIPS server. The centralized server can collect data from literally thousands of sensors from many remote locations and thus meet the scalability needs of large corporations.

As shown in Figure 2-1, an overlay solution uses *standalone sensors* to monitor the preexisting WLAN. Standalone sensors use dedicated radios that function only as sensors and are not used as APs. The standalone sensors, also known as dedicated sensors, require their own cable run and communicate back to the WIPS server.

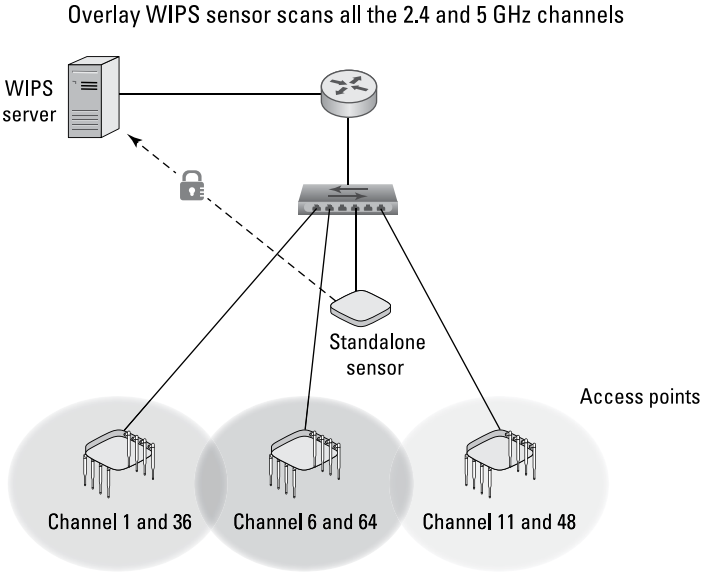

FIGURE 2-1: Sensors standing alone. . .

Standalone sensors do not provide access to Wi-Fi clients, because they are configured in a listen-only mode. To monitor for Wi-Fi security threats, sensors constantly scan across all 14 channels of the 2.4 GHz ISM band as well as all channels of the 5 GHz UNII frequency bands. The channel scanning interval is usually set at a fixed rate between 100 milliseconds to 1 second. However, the channel scanning interval can be adjusted for shorter or longer times. Usually, sensors are set to continuously scan across all Wi-Fi channels. Sensors can also be configured to monitor only a single fixed channel.

Communications from the sensors back to the server can be either a standards-based management protocol such as *Control and Provisioning of Wireless Access Points (CAPWAP)* or a proprietary management protocol. The management protocol is normally protected by an encrypted *Transmit Layer Security (TLS)* tunnel. Typically, a sensor also sends a continuous heartbeat message back to the server to indicate that the sensor is still functional. Sensors are usually centrally managed from the WIPS server but can also be managed individually through SSH or a web browser.

Most WIPS use port 443 for HTTPS communications, which will need to be open outbound on any firewall located between a sensor and the WIPS server. Depending on the vendor, other vendor-specific ports may also need to be open to permit communications between the sensors and the WIPS server. Sensors can also be used for remote packet capturing.

Part-Time versus Full-Time

One of the cost-saving advantages of an integrated architecture is that the existing APs can also function as part-time sensors. In this case, access points use *off-channel scanning* procedures. Although the main purpose of off-channel scanning is to provide adaptive RF capabilities, the off-channel scanning also allows the APs to function as *part-time sensors* for the WIPS server. The off-channel scanning used by the APs effectively provides time slicing between AP and sensor functionality.

For example, an AP that is providing client access on channel six will also monitor other channels where the AP does not transmit. The AP might stay on channel six for 10 seconds. During the 10-second interval, the AP is capable of sending transmissions to an associated client as well as receiving transmissions from an associated client. After the 10-second interval, the AP will listen off-channel on channel seven for 110 milliseconds. The AP will then return to channel six for 10 seconds and then go off-channel to monitor channel eight for 110 milliseconds. This round-robin method of off-channel scanning is used by the APs to listen for the beacon frame transmissions of other access points as well as monitor for any other RF transmissions off-channel. How often an AP spends on-channel and scans off-channel is dependent on the WLAN vendor.

The majority of customers of WLAN vendors opt not to incur the extra expense of deploying APs as full-time sensors and only use the part-time, time-slicing capabilities of the access points. Time slicing between AP and sensor functionality may reduce hardware and deployment expense but offers limited detection and prevention.

WARNING

If you hired a security guard to watch the main entrance to your place of business, would you want the security guard to take a break for 55 minutes every hour and only watch the main gate for 5 minutes of each hour?

An attacker might recognize that a WIPS solution is only using part-time sensors. The attacker could then launch a brief attack during the period that the APs are providing access. The attack occurs when the APs are not performing off-channel scanning and the attack is therefore, not detected.

Another problem with part-time sensors is that they may suspend off-channel scanning if a VoWiFi phone is associated with the access point. Off-channel scanning is notorious for causing choppy audio during an active voice call from a VoWiFi device associated to an AP. Most WLAN vendors now have an option that suspends off-channel scanning based on the detection of QoS priority markings that indicate voice traffic. Effectively off-channel scanning is suspended during an active VoIP call over the WLAN. If the off-channel scanning is suspended due to VoWiFi communications, the WLAN security monitoring is also suspended.

An additional problem with part-time sensor use is wireless rogue containment (which is discussed in Chapter 3). If a time-slicing AP or sensor must go off-channel for an extended period of time to contain a rogue device, the AP is not on its home channel providing access to clients. It should be noted, however, that many WLAN vendors support a configuration setting that prevents a time slicing AP/sensor from performing wireless rogue containment when clients are associated.

As shown in Figure 2-2, APs used in an integrated WIPS architecture also have the capability to be converted to *full-time sensors*. Instead of providing access to clients, the APs scan all channels, continuously listening for attacks, just like a dedicated sensor model. It is also a highly recommended practice to deploy some APs or AP radios as full-time sensors when using an integrated WIPS server solution.

However, this is still usually cost-prohibitive because of the extra hardware required, additional cable drops, and installation costs.

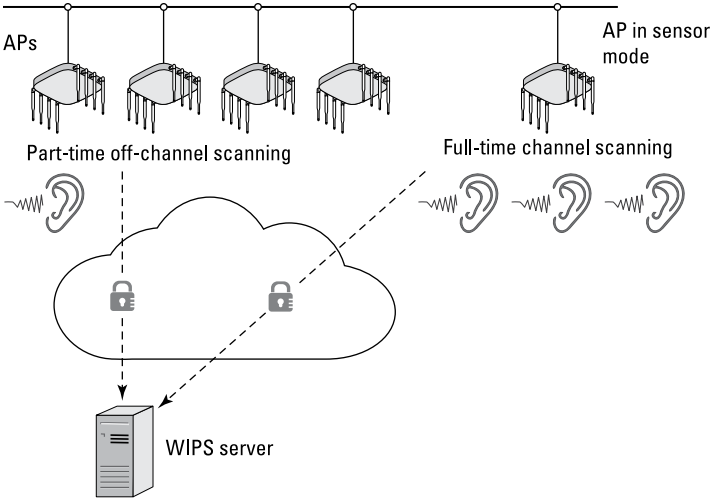

FIGURE 2-2: On the job full-time.

Sensor Evolution

To solve the cost problem, WLAN vendors use various form factors that can provide both full-time client access as well as full-time WIPS monitoring. The form factors of APs that are used for WIPS sensors varies widely depending on the WLAN vendor. However, APs with software selectable radios and/or a third radio can meet your Wi-Fi access needs while at the same time increase security monitoring at a reduced expense.

For example, some WLAN vendors offer a *software selectable radio (SSR)* along with a fixed 5 GHz radio within a dual-frequency AP. The radio that has SSR functionality can operate as either a 2.4 GHz or a 5 GHz radio. As a result, a dual-radio AP (one fixed and one SSR) can either offer 2.4 GHz and 5 GHz coverage or offer coverage on two different 5 GHz channels.

Traditionally, in high-density WLAN designs, 60 to 75 percent of the 2.4 GHz radios are disabled to prevent co-channel interference. A popular use case for APs with an SSR is the capability to provide for dual 5 GHz coverage where both radios in the AP are transmitting on different 5 GHz channels. The whole point behind dual 5 GHz coverage is to provide more capacity.

However, because the SSR uses a dual-frequency chipset, the SSR radio can also be converted into a full-time WIPS sensor that can continuously scan both the 2.4 GHz and 5 GHz frequency bands. As shown in Figure 2-3, APs with SSR radios provide a network administrator the capability to offer adequate coverage on both frequencies, additional capacity on 5 GHz, and the capability to deploy full-time sensors for WIPS security monitoring.

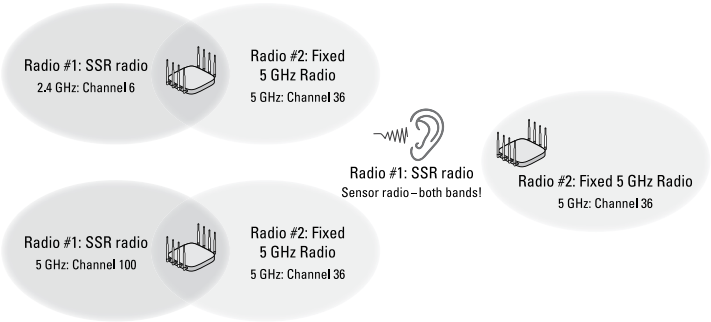

FIGURE 2-3: Covering all the frequencies.

Another recent Wi-Fi vendor trend is to add a third radio to high-end enterprise access points. Three must be better than two, right? One radio is used for 2.4 GHz client access, another radio is used for 5 GHz client access, and a third radio is used strictly as a dedicated WIPS security sensor. Because these are high-end APs, the client access APs are often 4x4:4 MIMO radios while the dedicated sensor radio is a 2x2:2 or 1x1:1 MIMO radio.

Tri-radio APs can also simultaneously use the third radio for other monitoring capabilities behind WIPS. For example, the third radio can also be used for cloud-based location analytics solutions such as ExtremeLocation Essentials.

Place Your Sensor

Sensor placement is an often-discussed topic when deploying a WIPS solution. Most admins ask "How many sensors do I need?" The answer often depends on the budget and the value of what network resources are being protected by WLAN security monitoring.

TIP

The best answer is that you can never have too many sensors. When WLAN security monitoring is deployed, the more ears the better. Bring out all the nosy neighbors!

Every vendor has its own sensor deployment recommendations and guidelines; however, a ratio of one full-time sensor for every three-to-five access points is highly recommended. Full-time sensors are often placed strategically at the intersection points of three AP coverage cells. A common mistake is placing the sensors in a straight line as opposed to a staggered sensor arrangement (which will assure a wider area of monitoring). Another common sensor placement recommendation is to arrange sensors around the perimeter of the building. Perimeter placement increases the effectiveness of triangulation and also helps to detect Wi-Fi devices that might be outside the building. Some of the better WLAN predictive modeling software solutions will also create models for recommended sensor placement.

When WLAN security monitoring is an extremely high priority and cost is not an issue, the more sensor devices the better. WIPS deployments at military bases often follow a ratio of one sensor for every two APs or may even deploy sensors with a 1:1 ratio.

Since most deployments do not use overlay sensors and an integrated WIPS solution is deployed, all access points are deployed as part-time sensors. But as you have learned earlier you still have options to meet security requirements for full-time sensors such as software-selectable radios or APs with a third radio used as a dedicated security sensor.

To The Future of WIPS Architecture!

In early 2020, the FCC voted unanimously to make 1,200 megahertz of spectrum in the 6 GHz band available for unlicensed use in the United States. The first enterprise Wi-Fi APs should be available to operate in this band as early as 2021. To put this in perspective, the new 6 GHz spectrum available for Wi-Fi is more than double the usable channels of the 2.4 GHz and 5 GHz channels combined. With this new spectrum brings new potential threats, especially 6 GHz rogue APs that currently will go undetected by existing WIPS solutions. WIPS sensors will have to be upgraded to include a 6 GHZ radio for monitoring purposes.

Although monitoring for Wi-Fi attacks has been the primary focus for WIPS solutions, other *radio frequency (RF)* technologies *Bluetooth (BT)*, *Bluetooth Low Energy (BLE)*, *and Ultra-wideband (UWB)* are being used in enterprise networks. Many enterprise APs also have an embedded BLE radio. While a best-of-breed WIPS solution may monitor for over 300 Wi-Fi security threats, how will WIPS solutions deal with potential attacks against these other RF technologies? As you learned in Chapter 1, IoT devices often use other RF technologies and are potential security risks. WIPS solutions will need evolve to monitor and protect against threats from multiple RF technologies.

Cloudification refers to the conversion and migration of data and application programs in order to make use of cloud computing. In recent years, the entire networking industry has been in the middle of a paradigm shift toward cloud services for management and visibility. WIPS solutions are no exception as they transition to the cloud. In the past, WIPS servers have been monolithic applications that are available as either a software or hardware appliance that reside in a customer data center. The cloudification of WIPS solutions is already making WIPS more scalable and affordable. A cloud WIPS solution literally offers sensor management and wireless threat monitoring on a global scale. A cloud architecture can also offer storage and access to vast amounts of collected data. The *machine learning (ML)* capabilities that cloud can offer will enhance WIPS anomaly detection and wireless threat assessments.

IN THIS CHAPTER

- Classifying network devices
- Detecting rogue access
- Mitigating network breaches

Chapter 3
The Pirates of Wireless Networking

You probably know that there are many wireless security threats and attacks (for more on this topic, see Chapter 1). In this chapter, I delve deeper into the most worrisome of these threats, unauthorized rogue access. I discuss the subjects of device classification, rogue detection, and rogue mitigation methods.

Skulls and Crossbones?

The same skull and crossbones symbol that is used by Caribbean pirates is often also used as an icon in WIPS solutions to represent a rogue access point (AP). Using a ship to commit acts of robbery and violence against a coastal area or other ships is the definition of piracy. The ships used to commit these acts are pirate ships. Using a wireless rogue device for data theft, data destruction, loss of services, and other attacks are all acts of wireless piracy. A rogue access point is effectively a pirate ship, albeit with fewer parrots and barrels of rum.

WARNING

Any unauthorized wireless device is a potential open and unsecured gateway straight into the corporate network the company wants to protect. A good WIPS solution is therefore, needed to provide a fortress against the wireless pirates.

Looking Through the Spyglass

WARNING

The most worrisome type of unauthorized rogue Wi-Fi device is one that is connected to the wired network infrastructure. WLAN vendors use a variety of wireless and wired detection methods to determine whether a rogue access point is plugged into the wired network. Some rogue detection and classification methods are published, whereas many remain proprietary and trade secrets. Any Wi-Fi device that is not already authorized is automatically classified as an unauthorized device. Rogue device classification methods are more complex. A WIPS characterizes APs and client radios in four or more classifications. Although various WIPS vendors use different terminology, some examples of classifications are discussed in the following sections.

Authorized device

An authorized device refers to any client station or access point that is an authorized member of the company's wireless network. A network administrator can manually label each radio as an authorized device after detection from the WIPS or can import a list of all the company's Wi-Fi radio MAC addresses into the system. Devices may also be authorized in bulk from a comma-delimited file. Integrated WIPS solutions can also offer auto-classification capabilities for corporate-owned AP and clients. Basically, these devices have a badge and are cleared for appropriate access.

Unauthorized device

The unauthorized device classification is assigned automatically to any new Wi-Fi radios that are detected but not classified as rogues. Unknown devices are considered to be unauthorized and are usually investigated further to determine whether they are a neighbor's device or a potential future threat. Unauthorized devices may later be manually classified as a known neighbor device.

Neighbor device

This classification refers to any client station or access point that is detected by the WIPS and whose identity is known. This type of device initially is detected as an unauthorized or unknown device. The neighbor device label is then typically assigned manually by an administrator. Devices manually classified as known are most often Wi-Fi APs or client radio devices of neighboring businesses that are not considered a threat. The WIPS system simply waves over the fence and moves along.

Rogue device

The rogue classification refers to any client station or access point that is considered an interfering device and a potential threat. Most WIPS solutions define rogue APs as devices that are actually plugged into the wired network backbone and are not known or managed by the organization. Most of the WIPS vendors use a variety of methods to determine whether a rogue access point is actually plugged into the wired infrastructure.

Although we typically think of rogues when discussing Wi-Fi APs and their connected clients, the Wi-Fi pirate ships may often disguise themselves in order to gain unauthorized access. For example, most smartphones now have Wi-Fi *hotspot* capabilities, which allows other users to share the cellular uplink bandwidth by connecting to the smartphone's Wi-Fi radio. Not only is this type of access often considered unauthorized within the buildings of some enterprises, but there is also the potential to bridge those hotspot users if the smartphone is also connected to authorized corporate Wi-Fi networks. Wi-Fi clients operating in *ad hoc* mode can also be potentially bridged to the network.

A *mesh AP* is another example of potential wireless pirate ships that are attempting to hide their presence. For example, an authorized AP is connected to the network, however, and unauthorized mesh AP has established a wireless backhaul link to one of the radios of the authorized AP. All of these methods would allow the pirates to sneak into the network undetected. Therefore, classification labels and detection methods for these rogue attacks are also necessary.

WIPS vendors use different terminology when classifying devices. For example, some WIPS classify all unauthorized devices as rogue devices, whereas other WIPS solutions assign the rogue

classification only to APs or WLAN devices that have been detected with a connection to the wired network. Additionally, terminology such as *sanctioned* versus *unsanctioned* devices might be used instead of *authorized* versus *unauthorized* devices.

Many WIPS solutions also have the ability to conduct *auto-classification*. WLAN devices can be automatically added to any classification based on a variety of variables, including authentication method, encryption method, SSID, IP addresses, and other attributes. Auto-classification capabilities should be used carefully to ensure that only proper devices are classified as authorized.

Gotcha, You Rogue!

Most WIPS define rogue APs as devices that are connected to the wired network via an Ethernet cable. Most of the WIPS vendors use a variety of wireless and wired detection methods to determine whether a rogue access point is actually plugged into the wired infrastructure. As previously mentioned, some of the rogue detection and classification methods are published while many remain proprietary and trade secrets.


TIP

One effective approach for classifying rogue APs is to poll access layer switches with *Simple Network Management Protocol* (SNMP) to determine MAC addresses associated with each physical port on the switch. Given that an AP acts as a layer 2 bridge, the WIPS solution builds a MAC table that correlates both the wired-side MAC address and wireless-side MAC address (BSSID) of the access point. This correlated MAC table is then compared to the database of authorized devices. Any unauthorized device that is detected by both a sensor on the wireless side and by SNMP on the wired side will then be classified as a rogue AP.

Another method is shown in Figure 3-1. The WIPS can look at broadcast traffic such as an ARP request from a wired device, for instance, a core router, and then analyze wired and wireless MAC tables. This method helps determine whether a device is hooked up to the wired network.


TECHNICAL STUFF

These steps demonstrate the actions needed for this method of rogue classification:

- A rogue AP with BSSID of 02:02:02:02:02:02 is plugged into the wired network.
- A sensor detects a new BSSID on the air and initially classifies this AP as unauthorized. The new AP has not yet been classified as a rogue AP.
- A default gateway router on the wired network with the MAC address 33:33:33:33:33:33 broadcasts an ARP request packet looking for a host on a particular subnet. Because this ARP packet is a broadcast packet, the rogue AP receives the packet and transmits it out the wireless interface.
- If the sensor and authorized APs are on the same subnet as the rogue AP, the sensor receives the ARP broadcast on its wired interface. This MAC address is stored in the wired-side MAC table and is shared with all other WIPS sensors.
- When the ARP packet is transmitted into the air by the rogue AP, the source address (SA) is the originating router's address of 33:33:33:33:33:33, and the transmitter address (TA) is the BSSID of the rogue 02:02:02:02:02:02.
- The WIPS solution will analyze the wired/wireless MAC tables. Any unauthorized BSSID transmitting an ARP request with the source address of the wired router will now be classified as a rogue AP.

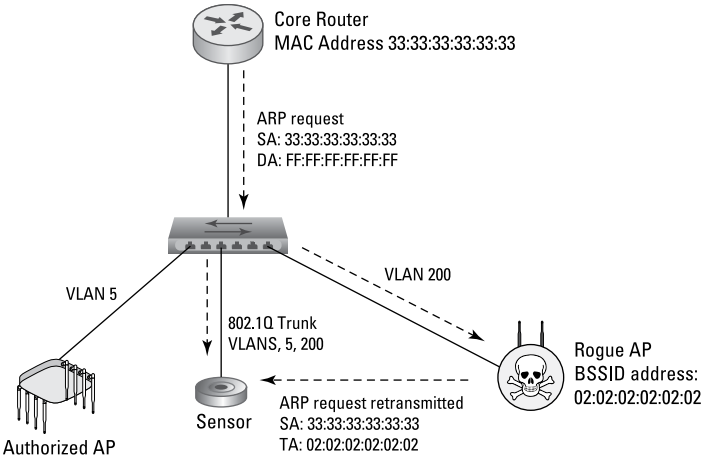

FIGURE 3-1: The traffic report today shows rogues!

This method will only work if the rogue device is plugged into the same broadcast domain as the sensor. Because many networks are designed with a large number of VLANs, a rogue AP could be plugged into a different VLAN than the sensors. As Figure 3-2 depicts, the sensor would need to have an 802.1Q trunk link in order to receive the ARP request from the wired side.

REMEMBER

Any rogue detection method that uses a comparison of MAC tables needs to take into consideration that the wired Ethernet interface of the rogue device does not have the same MAC address as the Wi-Fi radio interface. Luckily, the majority of the WLAN vendors use incremented MAC addresses on the wireless and wired interfaces. As shown in Figure 3-2, the methods of layer 2 rogue detection are augmented by looking for wired MAC addresses within a range of the BSSID detected by a sensor. A simple comparison of wireless and wired MAC is used by the WIPS solution to classify the device as a rogue device.

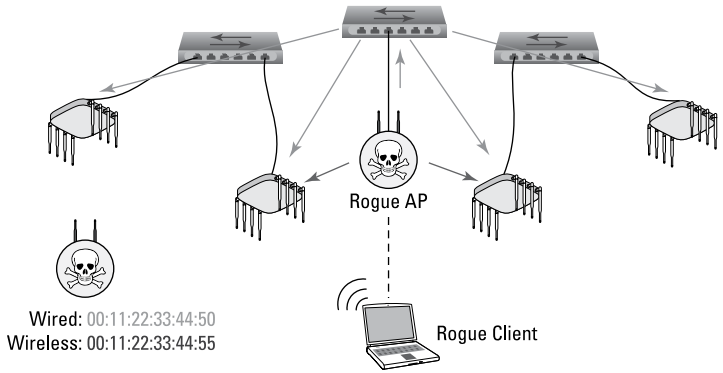

FIGURE 3-2: A side-by-side comparison.

One method of classifying rogue devices is to have a nearby sensor associate as a client station to the unauthorized suspect rogue AP or Wi-Fi router. The sensor then sends traffic, such as a ping, back to the known IP address on the wired network. If the traffic reaches the IP address on the wired side, the suspected rogue AP is confirmed to be on the internal network and then classified as a rogue. A related method might also be that an unauthorized device is not using the networks defined security and the detection of unencrypted 802.11 frames sent by the unauthorized device will trigger a rogue alarm.

The problem with these methods is that very often a rogue AP will have configured security, such as WPA2. A sensor can't associate with the rogue AP and send traffic because the sensor does not know the rogue AP's security settings. And unencrypted 802.11 traffic can't be detected if the unauthorized device is using similar security as corporate Wi-Fi network.

Another method for possibly determining whether there is a potential rogue device connected to the wired network is to examine the time to live (TTL) values of IP packets. Consumer-grade Wi-Fi routers lower the TTL value of a packet when it flows through the device.


REMEMBER

WIPS vendors may also use *secret sauce* methods of rogue detection and classification. These methods are like ordering off-the-menu at your favorite restaurant. Some of these methods are proprietary published and some are not. Very often these methods are also patented. One WIPS vendor might use marker packets, while another WIPS vendor might use a clever analysis of traffic patterns. All of these rogue detection methods might be used independently or used together to eventually classify a device as a rogue threat. For example, Extreme Networks AirDefense solution uses more than twelve methods for detecting rogues.

Although the art of rogue detection and classification has become quite successful, there is always room for improvement. As WIPS solutions become integrated into cloud management solutions, the accuracy and success of rogue detection are enhanced.

Mitigating the Damage

After a client station or AP has been classified as a rogue device, the WIPS can effectively mitigate an attack. WIPS vendors have several ways of accomplishing this. One of the most common methods is wireless *rogue mitigation* using spoofed 802.11 deauthentication frames.


TECHNICAL STUFF

Rogue mitigation (also known as *rogue containment*) is accomplished wirelessly when WIPS' sensors become active and transmit deauthentication frames that spoof the MAC addresses of the rogue APs and rogue clients. The WIPS uses a known layer 2 denial-of-service attack as a countermeasure. The effect is that

communications between the rogue AP and clients are rendered useless. This countermeasure can be used to disable rogue APs, individual client stations, and rogue ad hoc networks.

Any client devices trying to communicate through the rogue AP will be deauthenticated at layer 2 and all upper-layer 3 through layer 7 communications will be disrupted. This method prevents an attacker from accessing network resources through the unauthorized portal of the rogue AP. It also prevents accidental associations of legitimate clients to the rogue AP. Every WIPS vendor has its own marketing name for layer 2 wireless rogue containment, including air termination, rogue blocking, and rogue disabling. Effectively, the rogue AP is shunned from the network.

As shown in Figure 3-3, the sensor transmits deauthentication frames spoofing the rogue AP's MAC address as the *transmitter address (TA)*. The *receiver address (RA)* of the spoofed frames may be a broadcast address to deauthenticate all client stations or may be a unicast address to a single, associated rogue client station. Wi-Fi hackers and pirates have figured out how to tinker with client radio firmware so that client stations ignore deauthentication frames. Therefore, as also shown in Figure 3-3, most WIPS sensors also transmit deauthentication frames spoofing the client station's MAC address as the transmitter address and spoofing the rogue AP MAC address as the receiver address.

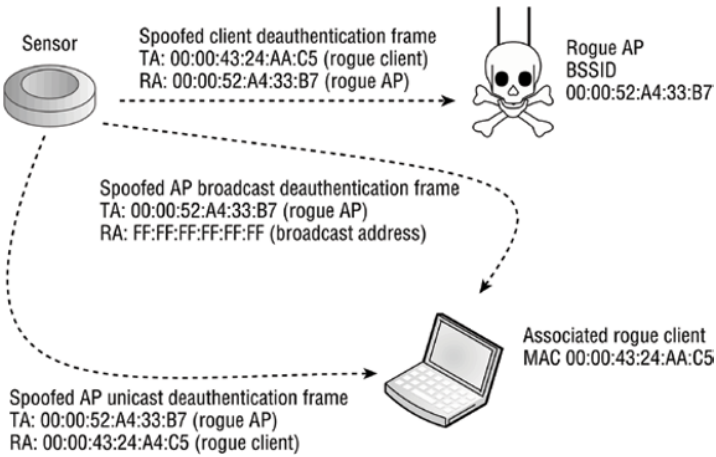

FIGURE 3-3: Left out in the cold.

Wireless rogue termination should be used very carefully. Rogue devices can be manually terminated using wireless rogue containment or a WIPS can be configured to *automatically* terminate any devices that are classified as rogue. An administrator can receive a rogue alarm and then initiate rogue termination manually. Typically, any device that has been classified as rogue is connected to the corporate network and probably should be wirelessly contained. Ultimately, the goal should be to locate the rogue device and disconnect it from the wired network.

WARNING

Many big-box retailers and hospitals trust their WIPS solution automatic rogue termination with confidence and do not rely on manual termination. However, improper use of wireless rogue containment capabilities can create legal problems. What if a WIPS accidently terminated legitimate APs and clients from neighboring businesses? It is up to your organization to choose whether wireless rogue termination is a manual procedure when rogue devices are discovered or if legitimate rogue devices are automatically contained. Often for legal reasons, manual containment might be the wiser choice.

Many WIPS also use a wired-side termination process to effectively mitigate rogue devices. The wired-side termination method of rogue mitigation uses the Simple Network Management Protocol (SNMP) for *port suppression*. Most WIPS can determine that the rogue access point is connected to the wired infrastructure and may be able to use SNMP to disable the managed switch port that is connected to the rogue access point. Port suppression uses an SNMP agent to shut down the physical port on the network switch through which a rogue device is communicating. If the physical port on the switch is disabled, the gateway to a wired network is effectively closed, and an attacker cannot use the rogue AP to access network resources. Port suppression can be an effective method of rogue AP deterrence. Additionally, the use of 802.1X or MACsec authentication for switch port security is becoming more important for rogue AP prevention.

One challenge for wireless rogue termination is if 802.11w *management frame protection (MFP)* mechanisms are enabled. Many of the existing wireless termination methods are rendered ineffective if the APs and clients use MFP. 802.11w provides a level of cryptographic protection for some 802.11 management frames.

MFP is meant to prevent some of the more common layer 2 denial-of-service (DoS) attacks using modified management frames. Currently, the vast majority of legacy Wi-Fi clients do not support 802.11w and, therefore, the capability has rarely been enabled on APs. Eventually, the use of MFP will become more commonplace because it is a requirement for the WPA3 security certification.

REMEMBER

WIPS vendor solutions such as Extreme Networks AirDefense are having to use proprietary methods for disabling MFP-enabled rogue access points and MFP-enabled clients.

Track Them Down!

Once a device has been detected and classified, the internal monitoring capabilities of a WIPS server can be used to locate the device. As shown in Figure 3-4, the location of devices can be shown visually on a graphic image of the building's floor plan that has been imported into the WIPS server. *Location tracking* is often used to pinpoint the location of rogue APs, but location tracking can also be used to establish the vicinity of authorized APs and client stations. Advanced features may also include historical location tracking.

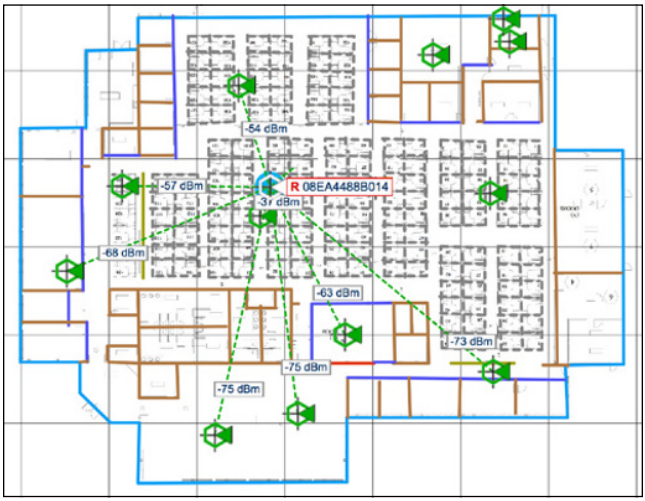

FIGURE 3-4: The chase is on!

The method used to find devices will vary based on vendor implementation and optional configurations. Some methods of location tracking use *received signal strength indicator (RSSI)* values reported from sensors and authorized APs within listening range of the device being tracked. For example, three or more sensors can be used to triangulate the approximate location of a rogue AP. In most cases, an approximation of 10 meters is accurate enough to locate a device physically.


TIP

It is beyond the scope of this book to explain all the methods of *RF triangulation* that can be used for location tracking; however, advanced location technologies are improving accuracy to well under one meter.

IN THIS CHAPTER

- Evaluating signature patterns
- Identifying abnormal network behavior
- Analyzing the protocols and spectrums
- Reviewing the forensic data

Chapter 4
Analyze with WIPS

A distributed WIPS solution can continuously collect information. Because the information gathered from multiple sensors can be extensive, the task of analyzing all the collected data can be overwhelming. Every WIPS solution uses a variety of software modules or software engines to simplify the task of analyzing massive amounts of collected data. In this chapter, I go over the most common methods and what results you can expect.

A Closer Look at Signatures

WIPS solutions use *signature analysis* to analyze frame patterns or "signatures" of known wireless intrusions and WLAN attacks. A best-of-breed WIPS uses a database of hundreds of threat signatures for various WLAN attacks. As shown in Figure 4-1, threat signatures can include man-in-the-middle attacks, DoS attacks, flood attacks, and many more. Because Wi-Fi operates at layers 1 and 2 of the OSI model, signatures are based on layer 1 and layer 2 attacks. Every WIPS utilizes some sort of signature analysis engine that processes 802.11 frames and RF data. Most WIPS solutions use signature detection, which is comparable to most virus protection systems where the signature database is updated automatically as new signatures are discovered. WIPS vendors are constantly updating their signature databases as new attacks emerge.

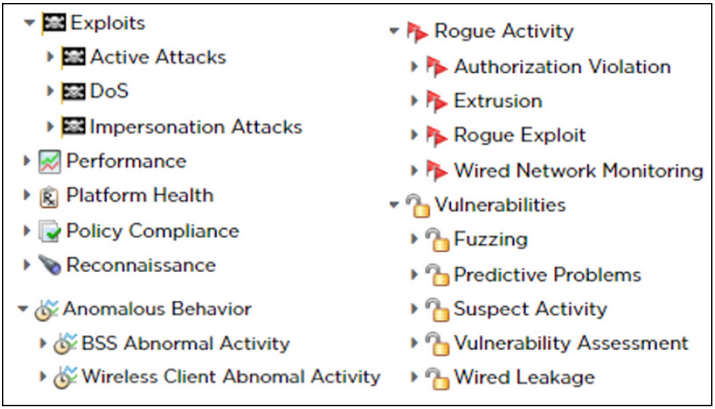

FIGURE 4-1: Let's have a look at your signature.

REMEMBER

You should understand that not all WIPS solutions possess the same caliber of signature analysis. Some vendors may offer a WIPS solution with 20 to 30 threat signatures, while others have hundreds. The top-of-the line WIPS solutions also have the capability of creating custom signatures. This is useful for WLAN administrators who want to monitor for a behavior or attack that could be specific to their WLAN environment.

Oh, Behave. . .

A good WIPS solution can utilize *behavioral analysis* to recognize any patterns that deviate from normal Wi-Fi activity. Behavioral analysis identifies abnormal network behavior based on historical metrics. Because historical normal WLAN behavior is the baseline, anomalies can be detected that would not necessarily be discovered by other intrusion detection techniques.

REMEMBER

Whereas the signature analysis identifies known threats, anomalous behavior analysis recognizes unknown attacks or threats that have no signature.

Detection of anomalies can be based on various thresholds of 802.11 management, control and data frames, fragmentation thresholds, and many other variables. Behavior analysis helps detect *protocol fuzzing*, where an attacker sends malformed input to look for bugs and programming flaws in AP code or client-station firmware. Attackers transmit malformed data by tampering with bits

and fields of data in 802.11 frames. Protocol fuzzing attacks often identify driver vulnerabilities and find weaknesses that result in a buffer overflow attack. After all, it just makes sense to attack the weak points.

Known attacks can be easily identified by signature analysis. However, the greatest threat to WLAN security is a new attack that is not known and cannot be detected. It's much easier to fight when you know your opponent, and that's not the case here. An unknown threat used to exploit computer networks is known as a *zero-day attack*. Very often, a zero-day attack will create some sort of anomaly in 802.11 behavior that can be detected. As shown in Figure 4-2, behavior thresholds can be configured on the WIPS to trigger an alarm.

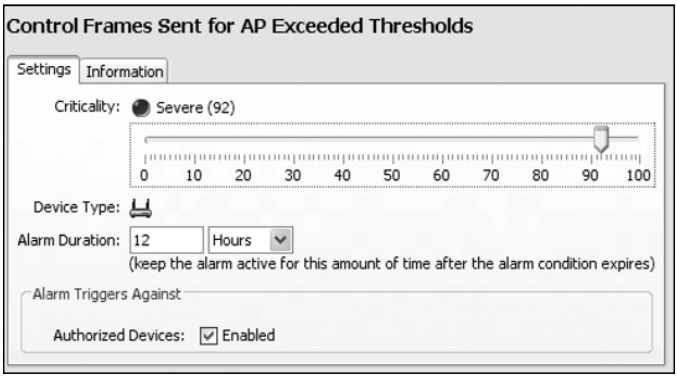

FIGURE 4-2: Where are the attacks coming from?

TIP

Setting thresholds can often be difficult and time-consuming to achieve a balance in detecting possible zero-day attacks versus triggering false positive alarms. However, the machine learning capabilities of the cloud is making anomaly detection faster and more accurate.

What's the Protocol Here?

Protocol analyzers provide network visibility into exactly what traffic is traversing a network. Think of this tool as a traffic report from high up in a helicopter. Protocol analyzers capture and store network packets, providing you with a protocol decode for each

packet captured, which is a readable display showing the individual fields and values for each packet. The power of a protocol analyzer allows you to see conversations between various networking devices at many layers of the OSI model. Protocol analysis is often the only way to troubleshoot a difficult networking problem. Protocol analysis can also be used for WIPS monitoring purposes.

All WIPS vendors use *protocol analysis* to dissect the MAC layer information from 802.11 frames. Protocol analysis may also be used to analyze layer 3 through layer 7 information of 802.11 data frames that are not encrypted.

An enterprise WIPS solution provides for distributed protocol analysis, with each hardware sensor acting as a listening device. Wi-Fi radios communicate via 802.11 frame exchanges at the MAC sublayer. Distributed protocol analysis is mainly used to monitor all the 802.11 frame exchanges that occur at layer 2. Attacks can be detected at layer 2 by reading the headers and trailers of all of the frames captured with WIPS sensors that can effectively function on a distributed protocol analyzer.

TECHNICAL STUFF

An in-depth discussion of 802.11 protocol analysis is beyond the scope of this book (and maybe two or three more). However, here's a quick look at the 802.11 frame format: The technical name for an 802.11 data frame is a *MAC Protocol Data Unit (MPDU)*. An 802.11 frame contains a layer 2 MAC header, a frame body, and a trailer, which is a 32-bit CRC known as the *frame check sequence (FCS)*. The layer 2 header contains MAC addresses and the duration value. The frame body contains the *MAC Service Data Unit (MSDU)*, which is the layer 3 through layer 7 payload.

Unlike many wired network standards, such as IEEE 802.3, which uses a single data frame type, the IEEE 802.11-2020 standard defines three major frame types:

- **Management** frames are used by wireless stations to join and leave a basic service set (BSS). Management frames do not carry any upper-layer information. The payload carries only layer 2 information fields and information elements. Information fields are fixed-length mandatory fields in the body of a management frame. Information elements are variable in length and are optional. Examples of management frames include beacons, probe requests, and association request frames.

- **Control** frames clear the channel, acquire the channel, and provide unicast frame acknowledgments. They contain only header information. Control frames do not have a frame body. Examples of control frames are acknowledgments, request-to-send, and clear-to-send frames.
- **Data** frames carry the actual data that is passed down from the higher-layer protocols. The layer 3 through layer 7 MSDU payload is normally encrypted for data privacy reasons.

REMEMBER

The IEEE 802.11-2020 standard defines three major frame types that are used by Wi-Fi radios. These 802.11 frame types are further subdivided into multiple subtypes.

Most WIPSs have the capability to monitor 802.11 frame exchanges in real time just like a standalone WLAN protocol analyzer. Enterprise WIPSs also usually have the ability to use sensors and AP radios for *remote packet capture*. An individual sensor can be configured to capture on a single channel or multiple channels. In some cases, captured 802.11 traffic can be redirected to a remote IP address for real-time frame analysis. Remotely captured traffic information can also be stored and viewed at a later time. Although there are many commercial WLAN protocol analyzers, Wireshark (`www.wireshark.org`) is open source and the tool of choice for many WLAN professionals.

Protocol analysis can also provide insight to some layer 1 and RF statistical information. *Radiotap* headers provide additional link-layer information that is added to each 802.11 frame when they are captured. The drivers of an 802.11 radio supply additional information via the Radiotap header. Please understand that the Radiotap header is not part of the 802.11 frame format. However, the capability to see additional information, such as signal strength associated to each 802.11 frame heard by a sensor radio, is quite useful.

Taking in the Entire Spectrum

Spectrum analyzers are frequency domain measurement tools that can measure the amplitude and frequency space of electromagnetic signals. Standalone spectrum analyzers are normally used for RF site survey purposes to find potential sources of unintentional RF interference in the 2.4 and 5 GHz unlicensed frequency

bands. One of the most important capabilities of a spectrum analyzer is the ability not only to detect RF energy but also to classify the sources of the interference. The better spectrum analyzers use RF signature analysis to identify and classify interfering RF transmitters, such as Bluetooth, microwave ovens, wireless cameras, and so on.

REMEMBER

Wi-Fi devices operate at both layers 1 and 2. The layer 1 physical medium is the uncontrolled, unlicensed, and unbounded RF spectrum.

Traditionally, WIPS solutions have mostly been used strictly to monitor layer 2 communications and have mostly ignored layer 1 for security monitoring. DoS attacks can occur at layer 1 (for more on this, see Chapter 1). Any continuous transmitter will cause a DoS. RF jamming devices can be used by an attacker to cause an intentional layer 1 DoS attack. As shown in Figure 4-3, to detect these jamming attacks, you need a spectrum analyzer.

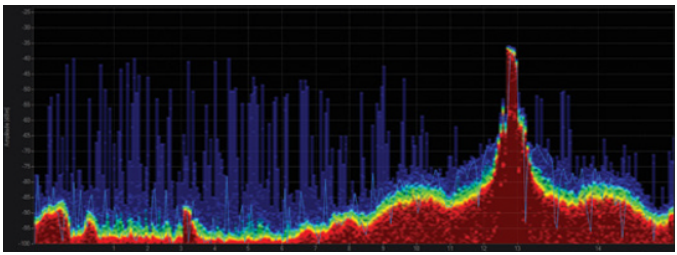

FIGURE 4-3: Pure energy.

WIPSs have begun to operate as *distributed spectrum analysis systems (DSAS)*. The advantage of any distributed solution is that they run 24/7 and can be administered remotely. You can spend more time looking from wherever you need to be and still get the necessary information. Most DSAS solutions use APs for the distributed spectrum analysis. Some vendor APs use an integrated spectrum analyzer that operates independently from the 802.11 radio. Other vendor APs use the 802.11 radio to accomplish a lower grade of spectrum analysis. A good DSAS is capable of RF signature analysis and can also physically pinpoint sources of RF interference using location tracking capabilities.

Review the Transcripts

Enterprise WIPS solutions may also provide *forensic analysis* that allows an administrator to retrace the actions of any single WLAN device down to the minute.

With forensic analysis, investigating an event takes minutes instead of potentially hours. Administrators can rewind and review minute-by-minute records of connectivity and communication within a WLAN. This data may not be as exciting as the minutes from a juicy court case, but you need this data. As shown in Figure 4-4, the WIPS records and stores hundreds of data points per WLAN device, per connection, per minute. This allows an organization to view months of historical data on any suspicious device as well as all authorized devices. Forensic analysis can scale significantly with a cloud-based WIPS that has access to potentially unlimited collected data.

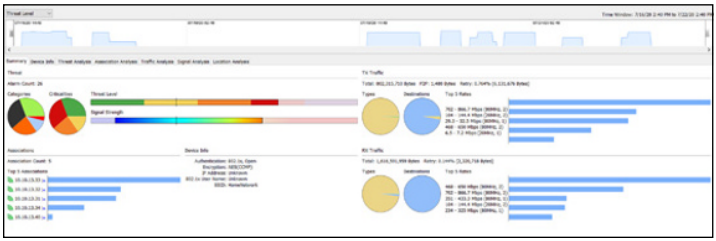

FIGURE 4-4: Can you read the testimony back to me?

TIP

Information such as channel activity, signal characteristics, device activity, and traffic flow and attacks can all be viewed historically.

IN THIS CHAPTER

- Enforcing your policies
- Evaluating alarms and notifications
- Weeding out false positives
- Creating reports and audits

Chapter 5
Monitor Your WIPS

An enterprise WIPS solution collects a lot of data from sensors about potential wireless security threats – way more than you can evaluate on your own (even though you're pretty smart). In this chapter, you will learn how to best decipher all the security alerts and make use of auditing and reporting features with some incredibly effective tools.

It's Standard Policy

Enterprise WIPS solutions allow administrators to define, monitor, and enforce wireless LAN policies for security, performance, usage, and vendor types. Organizations can minimize vulnerability by ensuring that WLAN devices are using the proper security protocols. Improper configuration of WLAN devices is one of the most common causes for wireless security breaches. And these breaches are more than a little embarrassing, really.

For example, you can define a *security policy* that requires all client stations to use an 802.1X/PEAP solution for authentication and CCMP/AES for encryption. If an end-user configures a client station that is not using PEAP and CCMP, the WIPS generates a policy-based alarm (something along the lines of "That don't look right!"). Defining security policies ensures that all

devices are properly configured with the mandated level of protection. A WIPS solution's auto-classification capabilities can mandate security configuration for wireless client devices (for more on this, see Chapter 3).

Security policies are needed for both access point (AP) and client station configuration thresholds. You can define policies for authorized APs and their respective configuration parameters, such as Vendor ID, authentication modes, and allowed encryption modes. You can also define allowed transmit channels and normal activity hours of operation for each AP. You can even define RF thresholds for minimum signal strength from a client station associating with an AP to identify potential attacks from outside the building.

The defined security policies form the baseline for how the WLAN should operate. The thresholds and configuration parameters should be adjusted over time to tighten or loosen the security baseline to meet real-world requirements. For example, you can scale back regular activity hours for an AP due to working hour changes.

REMEMBER

No single security policy fits all environments or situations. There are always trade-offs between security and usability.

A WIPS can also be used for *policy enforcement*. If an end-user configures a client station that is not using the defined security, the WIPS generates a policy-based alarm. However, the security policy can also be set to trigger an automatic response in addition to the alarm. For example, the WIPS can use spoofed deauthentication frames against the misconfigured client, similar to rogue containment measures. Two can play at that game!

This ensures that authorized devices are protected with the required authentication or encryption methods. A policy is only as good as its ability to be enforced uniformly. An alarm will alert you to an unsecured environment or device but does not take steps to enforce the policy. A WIPS offers the additional protection of preventing devices from communicating outside of policy by terminating noncompliant device connections. This approach has the potential to disrupt business and should be appropriately weighed against potential security problems when deciding to terminate noncompliant connections. Many users of WIPS in

larger enterprise deployments with 24/7 staffing prefer to receive notifications of noncompliant device communications and manually remediate the problem to avoid business interruption.


TIP

Before implementing actions to enforce policy, any written organizational security policy must be consulted, followed, updated, and required. Policy violation reporting and policy enforcement may also be dictated by outside organizations based on industry and governmental regulations. It's your job to stay on top of things – your tools are only as smart as you make them.

Alarms and Notifications

In a congested WLAN environment or an area with very little traffic, any 802.11-based transmitter can be heard by the WIPS sensors. The WIPS will detect all Wi-Fi transmissions and then, if necessary, generate the appropriate alarms. Depending on the configured threshold, the alarms can be triggered by signature analysis, spectrum analysis, behavioral analysis, or protocol analysis. Alarms can also be policy-based (see the previous section). These practical questions arise after the alarms are triggered:

- What do I do with all of this information?
- What do these alarms mean?
- Do I need to be informed about every device detected?
- Who is going to respond to the alarms?
- Is my network being attacked?
- Is this normal or acceptable behavior?
- Do any or all of these detected devices belong to my network?
- Are my Wi-Fi devices secured properly and is my network safe?

As shown in Figure 5-1, the triggered alarms often have a detailed description of the attack or performance problem. The WIPS alarm may also have suggested mitigation actions. How helpful! The detailed description and recommended actions often help you answer the questions you just reviewed.

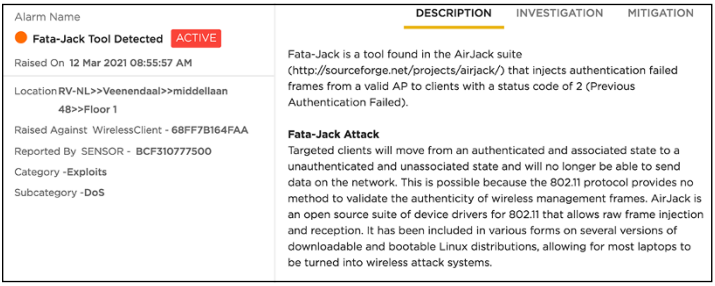

FIGURE 5-1: Another day, another (incredibly helpful) alarm.

WIPS solutions can discover, classify, and then conduct behavioral analysis event alarms that indicate the system has detected a rogue device or particular behavior. Different behaviors will trigger various warnings. If a user turns on a new client device within the hearing range of a sensor, the solution triggers an unauthorized device alarm. If that user then connects to an authorized AP without their new client device first being authorized, a rogue client alarm is triggered. What happens beyond that depends on the vendor of the WIPS and the customization done to the system. For example, a WIPS can proactively begin to protect the network using rogue client containment. WIPS can't deploy a physical cage, but the rogue client is trapped, nonetheless.

You can classify alerts or alarms, just like devices. Events that trigger alarms are not always indications of security threats or vulnerabilities. Some events are normal behavior. Depending on the WIPS solution, the alarms can be grouped into several categories:

- Rogue activity
- Exploits
- Behavioral
- Vulnerabilities
- Policy compliance
- Reconnaissance
- Performance

All alerts have a default threat-criticality level the WIPS vendor has determined to be optimal. Basically, the vendor establishes

how serious the threat has to become before WIPS notices. However, you may wish to adjust the alarm thresholds or even disable some alarms. Within the categories, alarms or alerts can be given custom threat levels from "everything is fine" to "we are under attack." These levels include the following:

- **Safe:** No immediate threat.
- **Minor:** Potential problem alarms that may worsen if ignored.
- **Major:** Potentially serious alarms that require priority attention.
- **Critical:** Serious alarms that require immediate attention.
- **Severe:** Serious alarms that may have catastrophic effects.

Tuning the alerts or alarms to threat levels is an important and possibly time-consuming task when deploying a WIPS. However, spending the time up front to calibrate alarm thresholds properly will make the alerts more meaningful.


TIP

Keeping a record of everything that is detected is a sound practice for forensic or even legal reasons. However, you may not want to receive a notification about everything the system detects. Most likely, you will only designate severe or critical alarms to trigger automatic notifications. Notifications can be sent from the WIPS to a network admin via an email, SMS message, or sent to a Syslog server.

It SEEMED Real. . .

The physical radio frequency (RF) medium used for Wi-Fi communications is both harsh and unpredictable. RF behaviors, such as reflections and multipath, often create a hostile environment that results in corrupted 802.11 frames and layer 2 retransmissions. Because the RF environment is at worst unstable and at best fluctuating (like your average playgroup of 3-year-olds), not every WIPS alarm is perfectly accurate. In other words, you should expect some false-positive alarms. A *false positive*, also known as a false detection or false alarm, is a result that is erroneously positive when the situation is actually normal. A false positive is simply another way of saying "mistake." All intrusion detection

systems, both wired and wireless, will have some occurrence of false positives. A false positive WIPS alarm indicates that a WLAN attack occurs when the threat does not exist. False positive alarms can be time-consuming for you to verify or invalidate. Even worse, false positives are often ignored due to their volume, increasing the possibility that an actual attack alarm is ignored.

Corrupted frames are the leading cause of false-positives. However, improper configuration of the WIPS or misinterpretation of alarms by administrators can also lead to false-positive alarms. Proper classification of all devices as either authorized devices or neighbor devices is essential to prevent unnecessary alerts. Some inaccurate reporting of events, seen as false positives, are unavoidable. However, fine-tuning alarm thresholds can significantly reduce the number of false positives. A reduction in false positives will save time and improve the security of the WLAN.

A WIPS solution integrated within a cloud architecture can offer storage and access to vast amounts of collected data, much more so than monolithic WIPS server solutions. The *machine learning (ML)* capabilities in the cloud can analyze these large data sets, which will result in better WIPS anomaly detection and a reduction in false positives.

Let Me See That Report!

The diligent practice of wireless security auditing is a crucial component of a well-rounded network security strategy. However, wireless security auditing is often overlooked due to budgetary and time constraints. Additionally, WIPS solutions are often considered a luxury or an undesired expense until a breach costs an organization a lot of time and money. Furthermore, if a wireless security breach becomes public news, the organization faces embarrassment, potential loss of stock values, and possible legal liabilities. Simply put—it's better to keep the cows in the barn than try to shove a stampede back.

The good news is that a premiere WIPS solution may have auditing report capabilities built into the system. As shown in Figure 5-2, an integrated wireless security audit report can validate WLAN security compliance for all of your APs and client devices. In other words, if the mandated security required the use of *Protected Extensible Authentication Protocol (PEAP)* authentication

and CCMP/AES encryption, all authorized devices can be evaluated to verify the proper security configuration. Any authorized devices that have not been properly configured will be flagged.

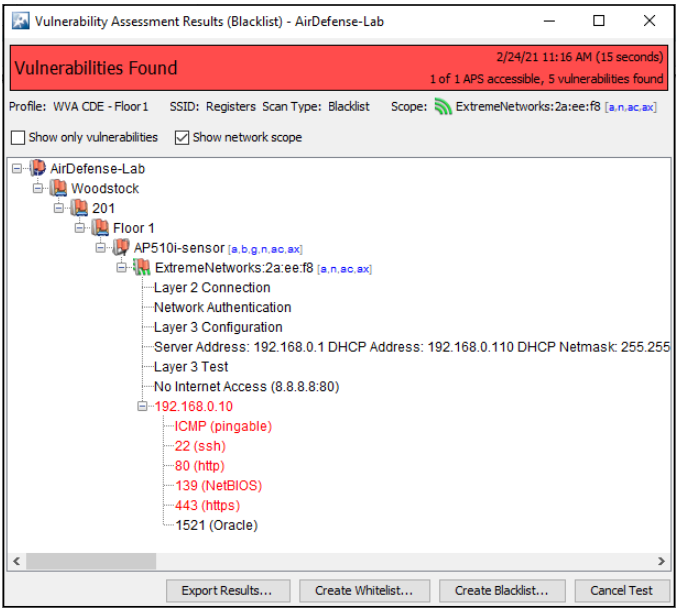

FIGURE 5-2: An audit report.

WIPS auditing reports might also be industry-specific. For example, a healthcare company can require a HIPAA compliance report, while reports for *Payment Card Industry (PCI)* compliance are critical for any business that uses credit cards for financial transactions.

Enterprise WIPS solutions usually offer extensive report-generation capabilities. Reports can be created manually or scheduled for automatic creation and delivery. Viewing and saving these reports is part of maintaining a secure wireless environment. When properly compiled, reports are useful tools in security analysis and resolution. Reports can also justify expenditure issues with upper management concerning network security requirements.

TIP

In other words, reports pay for themselves and maybe even your salary as well.

IN THIS CHAPTER

- Defending the airwaves
- Incarcerating the Wi-Fi pirates
- Finding your wireless network vulnerabilities
- Monitoring for Bluetooth and IoT threats
- Aiming for the clouds

Chapter 6
In Praise of Extreme AirDefense

Extreme Networks' AirDefense has been one of the premiere *wireless intrusion prevention system (WIPS)* in the Wi-Fi industry for over 18 years. It simplifies the protection, monitoring, and security of your wireless LAN networks. It safeguards the network from external threats and provides additional visibility into potential threats. It also enables compliance with regulations such as PCI-DSS, Sarbanes-Oxley, HIPAA, and GLBA.

Defending the Airwaves

AirDefense continues to lead the industry with a library of over 325 threat detection signatures. AirDefense is also a leader in *behavioral analysis*, helping to recognize any patterns that deviate from regular WLAN activity. Behavioral analysis identifies abnormal network behavior based on historical metrics. Basically, anything that seems a little off draws the attention of AirDefense. Anomalies are found, even though other intrusion detection techniques would not necessarily discover them. Recently, Extreme added support for Wi-Fi 6 (802.11ax) and WPA3 related security signatures.

Wi-Fi Pirates in Jail

AirDefense supports both dedicated and part-time sensor modes of operation to monitor for all kinds of rogue devices and wireless attacks. Extreme APs with software selectable radios or a dedicated third radio sensor can meet your Wi-Fi access needs while increasing security monitoring at a reduced expense.

AirDefense uses a combination of over a dozen methods to detect rogue devices, including rogue APs, rogue mesh APs, rogue clients, unauthorized hotspots, and many more. Once detected, sensors can perform either automatic or manual rogue termination for rogue containment based on predefined business rules. AirDefense can even contain 802.11w-capable rogue clients that are using management frame protection (MFP). Of course, you can pinpoint the location of rogue access points and clients on a floor plan to disconnect them from the network quickly. Think of these features as the bodyguards for your network, keeping everything safe and secure so you can get backstage for the show.

Forensic Detectives

AirDefense *forensic analysis* provides administrators with the capability to rewind and review detailed records of wireless activity that can assist in forensic investigations or network performance troubleshooting. Administrators can view a suspect device's activity for many months in minute-by-minute detail if needed. The number of device statistics stored for each wireless device is over 300 data points per connection per device per minute. Automated forensic analysis of these data points provides visibility into devices and a more accurate assessment of wireless threats, including anomalies and day-zero attacks. The only thing missing is the cool crime drama sound effect or snappy one-liner.

REMEMBER

Forensic analysis provides instant access to historical data required by many regulations such as HIPAA, GLBA, Sarbanes-Oxley (SOX), Payment Card Industry (PCI), and other industry security standards. Your organization's compliance—and proof of compliance becomes automatic and routine.

Vulnerability Assessment

A wall is only as strong as the weakest point of the structure. AirDefense wireless *vulnerability assessment* capabilities use patented technology to test wireless security remotely (which is definitely easier than walking to every possible access point). An administrator can use one or both wireless radios of an AirDefense sensor to mimic a wireless client. The admin can then check for vulnerabilities from a wireless hacker's perspective and validate end-to-end network testing. Sensors conduct wireless penetration testing, proactively identifying vulnerabilities before they are exploited, so you can better manage threats and keep your systems secure. An admin configures the vulnerability scans to run either automatically or on-demand. All assessments can be performed remotely and scheduled to run, eliminating the costs associated with on-site visits and manual testing.

Bluetooth Monitoring

RF technologies such as BLE operate in enterprise networks in addition to Wi-Fi. For example, rogue BLE beacons and unsanctioned Bluetooth devices are potential threats. AirDefense provides monitoring for BLE threats as well as Wi-Fi threats. AirDefense offers multiple BLE classification signatures to view, identify, act, and immediately locate unsanctioned and rogue Bluetooth devices that may pose a threat. Unauthorized access and phishing attacks can be prevented by monitoring advertisements in Google Eddystone and Apple iBeacon-enabled tags using the BLE 4.0 protocol.

A View from the Cloud

The entire networking industry has been in the middle of a paradigm shift toward cloud services for network management and visibility. *ExtremeCloud IQ* is the enterprise cloud-driven networking management solution from Extreme Networks that helps you navigate and secure that transition.

ExtremeCloud IQ delivers unified, full-stack management of wireless access points, switches, and routers and enables onboarding, configuration, monitoring, troubleshooting, reporting, and more. Using innovative machine learning and artificial

intelligence technologies, ExtremeCloud IQ analyzes and interprets millions of network and user data points from the network edge to the data center. These data points power actionable business and IT insights to deliver new levels of network automation and intelligence.

WIPS solutions have also begun their transition to the cloud. So please allow me to introduce you to *ExtremeAirDefense Essentials*, the first best-of-breed WIPS solution via the cloud. As shown by the dashboard and tools from Figure 6-1, Extreme Networks believes that WIPS is an *essential* aspect of your daily network security monitoring, which is why ExtremeAirDefense Essentials is now part of the ExtremeCloud IQ management platform.

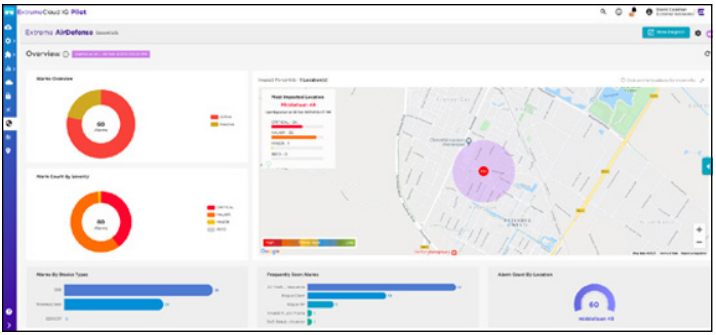

FIGURE 6-1: ExtremeAirDefense Essentials – WIPS in the cloud.

ExtremeAirDefense Essentials can simplify the protection, monitoring, and compliance of your wireless networks. This cloud-based WIPS solution notifies IT staff when attacks occur, enabling an immediate response. A shortlist of the features include:

- Cloud-based security monitoring well beyond basic rogue detection
- Global sensor management
- Historical timeline review of threats and alarms
- *Machine learning (ML)* capabilities that enhance anomaly detection

AirDefense has been one of the premiere WIPS solutions of the wireless networking industry for over 18 years. And now, ExtremeAirDefense Essentials continues that proud legacy with the power of the cloud.

Chapter 7
Top Ten WIPS Facts

Want a quick refresher on important points from this book? Need to reinforce some learning from other chapters? Did you just skip to the back of the book to see how it all ended? In all these cases, I have you covered. Keep these ten things in mind when researching for a WIPS solution.

Sensors Are the Eyes and Ears

Because WLAN security monitoring is critical, the more sensors the better. Experts recommend a ratio of one full-time sensor for every three to five *access points (APs)*. However, the CAPEX cost of dedicated sensors is decreasing because WLAN vendors offer APs with *software selectable radios (SSRs)* that can function as full-time sensors. High-end enterprise APs also come equipped with a third radio used strictly as a dedicated WIPS security sensor.

Rogue APs Are the Biggest Threat

The big buzz-phrase in Wi-Fi security has always been the *rogue AP*. This opening isn't a vent on a certain large orbiting space station, but a potential open and unsecured gateway straight

into the wired infrastructure that the company wants to protect. A wireless rogue device can be used for data theft, data destruction, loss of services, and other attacks; all are acts of wireless piracy. The individuals most responsible for installing rogue APs are typically not hackers. Instead, these individuals are employees who don't realize the consequences of their actions.

Rogue Devices Have Many Faces

When discussing rogue access, you might think at first of an unauthorized AP connected to your wired network. However, hackers use many types of rogue devices in order to gain unauthorized access. Mesh APs, virtual APs, Wi-Fi hotspot devices, and wireless IoT devices are all potential unsecured entry points into your network. Wi-Fi clients operating in ad hoc mode can also be potentially bridged to the network for unauthorized access. A quality WIPS solution uses a variety of wireless and wired detection methods to determine which type of rogue device is posing a threat to your network. WIPS has the tools and the talent to deal with this situation.

Contain the Rogues

All WIPS solutions use wireless rogue termination. Wireless containment is accomplished using a known layer 2 denial-of-service attack as a countermeasure. This countermeasure can be used to disable rogue APs, individual client stations, and rogue ad hoc networks. Your organization chooses whether wireless rogue termination is a manual procedure when rogue devices are discovered or if legitimate rogue devices are automatically contained. Moving forward, WIPS solutions will also have to be able to mitigate rogue clients that support management frame protection (MFP).

TIP

Ultimately, the goal should be to locate the rogue device and disconnect it from the wired network.

Not All Attacks Are Rogues

Although rogue APs get the most press when discussing WIPS, many other attacks are also potentially harmful. An enterprise WIPS solution uses a database of hundreds of threat signatures, including man-in-the-middle attacks, wireless hijacking, DoS attacks, flood attacks, and many more. You've gotta know what you're facing to properly address it.

WIPS Use a Variety of Analytics

A best-of-breed WIPS solution uses a variety of methods for analyzing all the collected data from sometimes thousands of sensors. WIPS uses *signature analysis* to analyze known wireless threats. *Behavioral analysis* identifies abnormal network behavior based on historical metrics. WIPS uses *protocol analysis* to dissect the MAC layer information from 802.11 frames. *Spectrum analysis* identifies sources of RF interference. And a best-of-breed WIPS solution can provide *forensic analysis* for historical purposes (and not just prime-time procedural shows).

False Positives Are a Problem

Security threats and vulnerabilities trigger alarms and alerts with various levels of threat-criticality. All intrusion detection systems generate some occurrence of false positives. A false positive WIPS alarm indicates that a WLAN attack occurs when the threat does not exist. False positive alarms can be time-consuming for you to verify or invalidate. Even worse, false positives are often ignored due to their volume, increasing the possibility that an actual attack alarm is ignored. To keep your WIPS alarm from crying "WOLF!", fine-tune alarm thresholds to significantly reduce the number of false positives. Additionally, cloud-based WIPS solutions can use machine learning to reduce the number of false positives.

WIPS Is Not Just about Wi-Fi

WIPS solutions are primarily focused on monitoring for 802.11-based wireless attacks and threats. In other words, WIPS is all about Wi-Fi security monitoring and protection. However, other RF technologies, such as *Bluetooth Low Energy* (BLE) are used in enterprise networks in addition to Wi-Fi. For example, rogue BLE beacons and unsanctioned Bluetooth devices are potential threats. Because of this, best-of-breed WIPS solutions need to also monitor and protect against threats using different RF technologies.

IoT Is a WIPS Concern

Wi-Fi radios are found in numerous IoT devices, such as manufacturing sensors and patient monitoring equipment. Traditionally, Wi-Fi IoT devices are often deployed with weaker security, despite the fact that they are all possible entry points into your network. Additionally, wireless IoT threats extend well beyond Wi-Fi. All wireless IoT devices are potential unauthorized entry points into an enterprise network, including Bluetooth and BLE IoT devices.

Cloud Is the Future for WIPS

REMEMBER

Like all of networking, WIPS solutions are in the middle of a paradigm shift toward cloud services for management and visibility. The cloudification of WIPS solutions is already making WIPS more scalable and affordable. A cloud WIPS solution offers sensor management and wireless threat monitoring on a global scale. A cloud architecture can also offer storage and access to vast amounts of collected data. The machine learning capabilities that cloud can offer will enhance WIPS anomaly detection and wireless threat assessments.

CLOUD APPLICATIONS FOR ESSENTIAL NETWORK OPERATIONS

ExtremeCloud™ IQ provides management from the edge to the datacenter and helps organizations automate network operations, gain insights from analytics, and optimize the end-user and application experience. Included at no extra cost with the standard ExtremeCloud IQ Pilot license are four applications which are essential for network management.

ExtremeAirDefense™ Essentials simplifies the protection, monitoring, and compliance of your Wireless LAN networks. This cloud-managed wireless intrusion prevention system (WIPS) continuously safeguards the network from external threats 24x7x365 and notifies IT staff when attacks occur, enabling an immediate response.

ExtremeGuest™ Essentials provides secure guest onboarding and analytics for distributed organization, as well as enterprise campus deployments. Guest Wi-Fi access is crucial to improving guest, visitor, and shopper experiences in retail, hospitality, and at large event venues.

ExtremeLocation™ Essentials is a resilient and scalable cloud-driven solution, that provides enterprises powerful multitier location services that can scale to thousands of sites. Supporting Wi-Fi and/or BLE technologies, enterprises can monitor workflows and assets, in real-time or historically, to improve their overall operations and efficiency.

ExtremeIOT™ Essentials is a simple IoT security solution that is designed to protect high risk, wired IoT devices. Through the application of security profiles, it controls IoT device attachment and access to the network. It locks down IoT communications to only what's authorized, blocking everything else.

LEARN MORE
https://www.extremenetworks.com/extremecloud-iq

The evolution of wireless security prevention systems

Despite Wi-Fi security such as WPA3, a WIPS remains critical to prevent bad guys from finding holes in your network. While monitoring for Wi-Fi attacks has been the primary focus, other RF technologies such as BLE are used in the enterprise, and new threats emerge. The growth of IoT reinforces the need for WIPS as part of any enterprise security solution.

Inside...

- Learn the evolution of WIPS architecture
- Identify all wireless security threats
- Defend against rogue APs and devices
- Using signature and forensic analysis
- Understand WIPS alarms and reports
- Best-of-breed WIPS security with Extreme AirDefense

David Coleman works at the Office of the CTO for Extreme Networks and is a technology evangelist, public speaker, and proficient author. He has written of numerous books, blogs, and white papers about Wi-Fi and wireless security. He is also the 2020 recipient of the Wi-Fi Lifetime Achievement Award.

ISBN: 978-1-119-80882-4
Not For Resale

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.