Protecting your Network from Wireless Attacks

How to Determine the Best Architecture for Mitigating 802.11-based Threats

By Joanie Wexler

TABLE OF CONTENTS

ABOUT THE AUTHOR

Joanie Wexler is an independent analyst, editor, and writer who has spent 15 years covering trends in the computer networking industry. One of her focus areas is enterprise wireless data and voice systems, and she authors the "Wireless in the Enterprise" twice-weekly newsletter published by Network World.

INTRODUCTION: WIRELESS INTRUSION DETECTION AND PREVENTION

Using surveillance scanning capabilities to detect and thwart hacking attempts in wireless networks is called wireless intrusion detection and prevention (WIDP). WIDP is strongly recommended for organizations with highly confidential data to protect—whether or not they have deployed 802.11-based wireless LANs (WLANs) in their own facilities and even if they have a "no-wireless" corporate policy. The reasons will be discussed here.

This guide will also examine architectural options for deploying WIDP. One fundamental decision is whether to integrate this surveillance capability into the WLAN infrastructure you might already use for data communications or to deploy a separate, purpose-built scanning architecture.

Another consideration is where the processing of the data collected by the scanning system should take place: in a central repository containing information gathered throughout the network, in each distributed sensor that collects local security information, or a combination of both. These properties affect the depth of the security incidents that your network can recognize and how fast it can make preventive decisions.

First, though, you might be asking, "Why would my organization need a wireless scanning system for intrusion prevention?"

Why Deploy Wireless Intrusion Prevention?

Enterprises benefit from the use of WLANs both to support task-specific vertical applications and to extend general business applications to increasingly mobile local employees. However, without a scalable security foundation in place, WLANs become a significant vulnerability. Radio signals radiate in three dimensions—permeating walls, ceilings, floors, and windows—and can thus potentially be picked up by outsiders. Different protection measures, then, are required for wireless networks than for cabled networks.

In addition, existing cabled intrusion prevention systems have visibility only into activity at Layer 3 (IP) and above; they are unable to gather information at the radio-frequency (RF) level. Wireless systems are a necessary complement to these systems.

The more far-reaching your WLAN is, the greater the number of vulnerabilities you are likely to have. Today's broad availability of off-the-shelf wireless access points (APs) and laptops guarantees the presence of wireless signals somewhere nearby. Even if you don't use WLANs within your organization, someone could plug an AP into your network and cause mischief if no surveillance system is present to detect the unauthorized device.

Whether your organization has already deployed WLANs, is planning a rollout, or bans their use, you can mitigate their risks. A WIDP system scans the airwaves to quickly detect and prevent airborne attempts by hackers to break into wireless and wired network resources to steal data, divert over-the-air user connections to phony Web sites, and deny service to network users. It also audits the wireless network to check for compliance with your network security policies.

What Are the Greatest Threats?

To make the most of your security budget, focus on threats that pose the greatest risk. A defensive "wireless umbrella" can detect and prevent these top 802.11 threats:

- **Malicious hacking attempts**
- **The presence of unauthorized, or rogue devices, including APs and client devices**
- **Denial-of-service (DoS) attacks**
- **Employees who use mobile devices without appropriate security precautions**

If the wireless network is compromised, all known wired-side attacks become possible, too, jeopardizing the integrity of the entire network infrastructure. With that in mind, let's consider the various options for securing your organization with a WIDP system.

PRIMARY ARCHITECTURAL COMPONENTS AND OPTIONS

WIDP is just one component of the WLAN security foundation. WIDP enforces network security policies that you create by blocking intrusions and alerting you to RF vulnerabilities so that you can remedy them. As such, the WIDP system is complementary to the wireless authentication and encryption capabilities built into the 802.11i security standard.

A WIDP system has two primary components: surveillance sensors distributed throughout the enterprise and a centralized engine (a server or appliance) that runs sophisticated anomaly-detection algorithms. The central engine also implements business policy, generates alerts as necessary, and archives and correlates data. Correlating security events will indicate whether, when taken together, two or more events signal a network intrusion or attack. Alerts and data containing detailed statistics are then usually sent to a client console or third-party management system so the WIDP system can automatically thwart the attack, or IT personnel can take appropriate action.

A third, very useful, component is a mobile, handheld analyzer, for use with the distributed system described above to accelerate incident response. The handheld is used by professionals who walk the wireless environment to fine-tune deployments during initial site surveys and for tracking a device to its exact location. In the most sophisticated WIDP systems, the mobile handheld is database-driven and integrated with the centralized system for accurate location tracking.

There are three primary options for purchasing and deploying a WIDP system:

- **Purchase WIDP sensor features built into the APs you get from a WLAN systems provider. These are referred to below as dual-mode AP/sensors.**
- **Use APs that a WLAN systems vendor has converted to dedicated sensors.**
- **Deploy a separate, purpose-built overlay WIDP system (dedicated sensors and corresponding, purpose-built central engine) from a third-party wireless expert.**

Let's examine each option.

Dual-Mode AP/Sensors

If and when you purchase a WLAN data communications system, you can often purchase RF surveillance capabilities as part of the package. This is convenient and affords flexibility in the nature of the devices you purchase. You also have just one vendor and one set of wireless devices to manage.

The drawback is that in most implementations, the AP time-slices its dual role as security sensor and transmission device. As such, it provides only part-time security. And it can scan only the channels that local regulation allows for data transmission, short-changing you on your surveillance. Because it isn't scanning all the time and only monitors a subset of channels when it is scanning, this approach is prone to generating a large number of "false negatives"—reports indicating no suspicious activity—when there might indeed be some that the system (and you) can't see.

This situation is analogous to leaving all the outside doors and windows of your company open and having a security guard passing by the front door, then the back door, every half hour looking for intruders. You are playing a form of Russian roulette, gambling that the time you are checking for bad behavior will, indeed, be the time that the bad behavior is occurring. It also assumes that the front and back door (not the side doors and windows) are the only "channels" that an interloper will use to gain access.

Another downside from a security standpoint is that if hackers learn how to break into the APas a transmission device, they have also penetrated the RF security foundation. The dual-mode option is best considered by organizations that do not have critical data to protect and do not have to comply with industry-based regulatory mandates.

APs as Full-Time Sensors Using WLAN Vendor Software

This option allows you to use APs as full-time security sensors and, as such, is a stronger alternative than dual-mode AP/sensors. However, a primary drawback associated with using WLAN-embedded WIDP functions also applies here: A single or dual radio in an AP, which is constructed as a transmission device, can scan just the regional channels that it has been configured to cover—in other words, it can scan just one set of channels at a time, not all channels simultaneously. If a user visiting a North American facility from Asia brings along his own AP and plugs it into an Ethernet jack, for example, the scanning system will not detect it, because the scanning system is configured to monitor only North American channels, not Asian channels. As a result, the unauthorized device could go unnoticed as a threat.

A second issue is that if the system provides some correlation functionality, the compute resources to handle the analysis are shared with the central engine's processing power to manage the communications traffic. The potential tradeoffs are the same as those with any appliance-versus-multifunction device decision (such as whether to purchase a standalone firewall or a router with firewall software embedded in it): Performance and scalability based on the size of the existing deployment, as well as its future anticipated size, must be considered.

In addition, location-tracking features of AP-based scanners are often less accurate than those of specialized systems. It is advisable to benchmark these capabilities for comparison before purchasing a system.

Purpose-Built WIDP Overlays

A dedicated WIDP system provides a surveillance sensor network with a corresponding central server or appliance that offers dedicated 24x7 scanning of all 802.11 channels. Because it is not tied to a single wireless AP vendor, the system can be deployed independently of whether or not you have a WLAN system installed.

It also offers centralized, enterprise-wide correlation of security events and the ability to instruct the sensors to take automated containment action against rogue devices. Usually designed by companies that specialize in wireless security, these systems automatically classify the devices they discover using policy enforcement engines to reduce false negatives and the "running around" resulting from continually being alerted of legitimate devices.

The most sophisticated overlay systems use multiple containment methods and generate highly actionable reports (as opposed to reams of logged security events with little context). Most also support compliance reporting, checking your wireless configuration against the wireless requirements of legislative mandates that might apply to your organization, such as the Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley Act, Gramm-Leach Bliley Act, and Department of Defense Directive (DoDD) 8100.2 initiatives.

The reports will display the specific clauses that pertain to wireless in your industry, what percentage of your wireless installation is in compliance, and the specific devices that are not. Then the report will delineate what you need to do to bring your WLAN completely into compliance.

Purpose-built systems do introduce an additional vendor and equipment into your infrastructure, which must be managed.

There is another option that is complementary to the purpose-built system: a hybrid approach that combines the dedicated system described above with your WLAN vendor's APs. Like the dedicated overlay alternative, this option has the merits of the sophisticated, 24x7, full-channel scanning and centralized event correlation. However, it also allows you to take advantage of the AP hardware in which you may have already invested for data transmission as your sensor network.

COST CONSIDERATIONS

From a cost perspective, the integrated AP/sensor approach can save money because a shared management console can be used, and another full set of sensors does not need to be purchased. However, companies with heterogeneous APs (from multiple vendors) can't always take advantage of an integrated, single-management solution.

Perhaps most important, though, are the security goals of the deployment. For enterprises that desire a separate monitoring channel and wish to gain features available in a dedicated overlay system that they can't get in the integrated AP/sensor, the cost tradeoff may be a matter of paying for what is required. In these cases, the requirement for tighter security will trump the product-to-product price comparison.

DESIGN CONSIDERATIONS

The overlay and hybrid WIDP systems, in general, offer the highest levels of wireless intrusion security because of their location-tracking accuracy and ability to scan all channels all the time.

If you decide to deploy one of these systems, there are some product design points to consider that can affect your levels of security, system performance, and total cost of ownership (TCO). There are currently three basic WIDP system designs, which differ in where security event processing takes place:

- **At the "edge" of the network in the distributed sensors**
- **In the centralized engine**
- **Partially in the sensors and partially in the central engine, in a two-tiered manner**

Let's take a brief look at each.

Edge Analysis

Systems with this design analyze every wireless packet, device, and session locally in each distributed sensor. Additional sensors can simply be added as requirements grow until the centralized engine maxes out on the number of sensors it can support.

Generally, only results are forwarded back to the central engine for storage. However, when these systems do detect an issue, they generally shift into a "debug all" mode in which sensors capture and transmit all information to the central engine for analysis. Debug mode, then, consumes large volumes of network bandwidth.

Edge systems also can have trouble identifying distributed attacks. Because analysis is performed locally, it is unlikely that correlations between events occurring in more than one location simultaneously will be made. So the system could easily overlook a security problem. In addition, updating the sensor infrastructure can involve transmitting updates as large as 30MB to 40MB if the entire software image must be updated to reflect just one (or a few) newly discovered malicious signatures.

Centralized Analysis

In this scenario, sensors function simply as capture devices, forwarding wireless packets to the central engine over LAN and WAN links. The greatest benefit to this architecture is that the central engine can apply multi-sensor correlation within its detection algorithms, providing more advanced and accurate alerts. In addition, as new alerts are discovered, only the centralized server/appliances need updating, not all the distributed sensors.

A drawback of this approach is that the more event data the sensors collect, the more bandwidth is required to shuttle it all to the centralized engine. This can be slow and consume bandwidth that's needed for other critical applications. Enterprises are likely to suffer WAN performance degradation or be forced to make additional investments in WAN bandwidth (or both).

Two-Tiered Analysis

This architecture blends the benefits of the two approaches described above. "Lightweight" sensors process event data and send a distilled version to the centralized server/appliance to conserve bandwidth. From there, the centralized server performs data correlation for a comprehensive, enterprise-wide view.

This approach doesn't require the expense and continual updating of fully smart sensors as new alerts are developed; updates can be made once to the central engine instead. In addition, this design does not consume significant volumes of bandwidth between sensors and the WIDP engine.

KEY FEATURES AND TCO

The primary architectural considerations that go into selecting the right WIDPsystem for your environment have been discussed. Because there are a number of key security capabilities, ease of operations issues, and cost of ownership drivers that contribute to overall deployment success, a summary table of these considerations is included below for your quick reference.

Capability	Description/Considerations
Complete surveillance scanning	Continual and concurrent scanning of all 221 802.11 U.S. and international channels on all frequencies so as to not overlook any intrusion attempts
Policy enforcement	Automatic action taken based specifically on what your organization deems acceptable and unacceptable conditions and behavior
Device location tracking	Ability to distinguish legitimate devices from rogues and identify where they are located, whether they are inside or outside your facility. Speed of systems should be compared.
Automated rogue containment	Automatic disassociation of rogues from the wireless network or shutdown of direct-connected rogues at the Ethernet port level. Alternatively, association of rogue or infected devices to a "sticky tarpit" – one or more "virtual machines" dedicated to answering suspicious connection attempts.
Integration with mobile handheld component	Enables greater location-tracking efficiencies
Scheduled compliance reporting	Keeps your organization in compliance with the wireless requirements of legislative mandates that pertain to your industry

SUMMARY AND CONCLUSION

Because low-cost consumer products are widely available and users want mobile capabilities, it has become a wireless world—whether or not 802.11 networking is sanctioned in your enterprise. As a result, enterprises with confidential data to protect require WLAN monitoring to quickly detect and prevent wireless intrusions that could result in data theft or denial of service to network users.

There are several architectural options from which to choose for surveillance scanning and data analysis. If seeking optimum security, few organizations will choose the part-time security embedded in APs built initially for data transmission. Generally, an overlay or hybrid WIDP system offers the highest security. The sensors can handle all of the data analysis, none of it, or some of it. There are pros and cons to each approach; however, having lightweight sensors filter key event data and transmit it to a centralized engine for correlation works especially well, because it scales from both a sensor-resource and WAN bandwidth perspective.

This paper is brought to you by Network Chemistry, the wireless security experts. For more information, visit www.networkchemistry.com or call 1-888-952-6477.