

Detecting Rogue Users and APs in a Wireless LAN

Rogues are not just hackers and outside intruders war driving through your parking lot with 802.11 antennae made out of Pringles cans. Most likely, they're your own employees who are unaware of your wireless usage policies. Perhaps they are experimenting with non-enterprise-grade WLAN APs in the office, having grown impatient with IT's pace in deploying wireless tools. Maybe they've connected that AP to the wired network, inadvertently creating a huge security hole. In any case, your corporate information is at risk, unless you take control.

Users love the freedom of mobility. They are not waiting for IT's official approval to bring in WLANs. As with PCs, wireless is a user-driven revolution. It's simple enough for an employee to unplug his laptop from the Ethernet jack, plug in an unsanctioned access point (AP) and reconnect the laptop. The employee has created an ad-hoc WLAN for himself or other employees in his department. They may collaborate in a conference room, link their laptops to their PDAs, or fire up a game of Quake during lunch. The employee has also inadvertently created a security hole through which an intruder can enter. In fact, the Gartner Group estimates that one in five companies has a WLAN that the CIO doesn't even know about. If your company has deployed WLANs, this private rogue may cause interference, open a new security hole, and degrade the sanctioned WLAN's performance.

Or the threat may be an intruder who has set up an AP as a "bug light," luring legitimate WLAN users to connect with the unauthorized AP. Once associated with the rogue AP, the hacker can gain access to a legitimate user's PC. Or the intruder may use an unauthorized private WLAN to mount a man-in-the-middle attack, thereby gaining full network access.

Even if your company has taken a wait-and-see approach to enterprise WLANs, you must be prepared for unexpected rogue invasions. Unsecured WLANs provide open doors to your corporate network and its valuable data. With your wired network, access to the building itself, structured wiring and firewalls prohibit impromptu LAN connectivity. With wireless, physical access no longer provides the most basic line of security.

To detect unsanctioned WLANs, whether it's a department who couldn't wait for the corporate-sponsored rollout of WLANs or whether it's a hacker bent on vandalism, IT needs to have the

Executive Summary

A well-meaning employee may set up an unsanctioned AP to create a convenient workgroup WLAN. Or an intruder may lure legitimate employees to an unauthorized AP as a way to penetrate the corporate network and steal resources. No matter the scenario, rogue users and APs create huge security holes in your network.

This white paper addresses the complexity and importance of identifying and detecting rogue users and APs in your WLAN. Detecting these rogues – and determining their location – is critical to maintaining network security, preventing loss of critical data and intellectual property and reducing potential liability. To date, detecting rogues has been a time-consuming or expensive proposition. However, if the WLAN system vendor integrates the capability to identify and authenticate all users as well as the capability to determine their locations, detecting and locating rogues becomes an inherent system capability.



right tools to detect and locate rogue APs and users. It's not an easy task, but it's essential to maintaining network security and preventing loss of critical data, intellectual property and potential liability. Today these tools are time-consuming, forcing an IT manager to walk around looking for rogues, or expensive, forcing an IT manager to buy an add-on network of rogue AP sensors. Fortunately, the ability to detect and locate rogues is becoming an integral part of enterprise WLAN systems.

Identify the Rogue

The first step in protecting your corporate resources from misuse is to define and identify what constitutes a rogue. While various types of threats may occur from both authorized and unauthorized users, the most common WLAN rogues include:

- An employee connects wirelessly to the wired enterprise network using his or her own unapproved, non-enterprise-grade wireless AP;
- A group of employees set up a standalone AP for their workgroup, which they don't plug into the wired network. Even though they haven't compromised wired security, they are in fact stealing the air of legitimate WLAN users. They may also cause a significant amount of RF interference, which will cause a dramatic slowdown in the entire WLAN, or may open the door to an uninvited guest;
- An unauthorized user, such as an intruder or hacker, uses his own wireless tools and attempts to access your WLAN network from the parking lot, street, or other location physically nearby.

The first instance – an internal, unauthorized threat – is the most common misuse of WLANs. For example, an employee who has an 802.11 WLAN at home to connect his laptop, printer and PDA decides to bring his own AP into the office, so he can more easily transfer data to and from his office desktop to his mobile tools. He buys an AP that's suited for home use at the local electronics store. But this AP lacks the security built into an enterprise-grade AP, such as Wi-Fi Protected Access (WPA) or encryption. He may not understand that his WLAN is a threat to corporate network security, so he doesn't seek approval from the IT manager. Nor does he need assistance from the IT helpdesk since wireless networking at this level is plug-and-play, thereby eliminating an opportunity for the IT team to discover this rogue WLAN.

A second type of rogue is a private WLAN user group. They may be using an AP or even a "soft AP" which is software that gives AP functionality to a wireless laptop. Although this WLAN may be isolated from the corporate WLAN, the users are stealing the air from the legitimate WLAN users. The private WLAN can also cause interference with an authorized WLAN in other parts of the company.

An uninvited guest may eavesdrop on the private LAN and can now get into the network through either the employees' LAN connections or by intercepting their user names and passwords on the official wireless LAN. A breach would have occurred and the administrator would never know it.

While security breaches are more likely to come from the inside, external breaches aren't to be ignored. Once the intruder is in, he may launch a man-in-the-middle attack to gain full network access or he may launch a denial-of-service attack that jams the airwaves for all users. An unauthorized use of the network or ISP connection can also create a legal liability for the enterprise.

An external attack is a real threat especially if your WLAN security settings, such as 802.1X authentication and WEP or WPA encryption are not operational or configured to prevent unauthorized intrusions. A knowledgeable intruder with an 802.11 device or other wireless access tool can easily pick off the Service Set Identifiers (SSIDs) and Media Access Control (MAC) addresses and steal the identity of an authorized AP or users.

Such intrusions often occur when the enterprise IT manager doesn't change the AP's default SSID. The defaults are common knowledge and not hard to discover. For instance, Cisco APs use "tsunami," Linksys defaults to "linksys," and Symbol defaults to "101." In this type of intrusion, the rogue can easily log on by posing as a legitimate user or as an AP. The intruder then has complete access to the WLAN and can listen to the airwaves and intercept unencrypted messages. This intrusion can remain undetected to IT, as the WLAN management system will see the intruder as a legitimate user or AP. Intrusion in this manner is not a difficult task for a hacker with even a limited set of wireless intrusion tools and minimal skills.

One of the scariest attacks in wireless networking can be mounted by a man-in-the-middle rogue AP. This type of attack could grant full network access to the rogue in a way that is very hard to detect, even in networks configured to use Transport Layer Security (TLS).

A man-in-the-middle rogue AP makes a PEAP Part 1 connection to a corporate AP, masquerades as a user and trivially authenticates the corporate AP. This first step of this attack results in an encrypted TLS session between the rogue and the authenticator. Next the rogue attracts a legitimate user (called “bug lighting”) and asks for TLS authentication. The rogue tunnels the TLS authentication exchange between the legitimate user and the authentication server. The authenticator thinks it’s completing PEAP-TLS Part 2. Once the legitimate user is authenticated, the rogue can derive the session encryption keys, since they are based on information exchanged in the original PEAP Part 1 phase. The rogue disconnects the legitimate user and turns its bug light off.

The rogue now has complete network access. The authentication server doesn’t think anything went wrong. The legitimate user retries authentication, connects to a corporate AP the next time and gets authenticated, so the user doesn’t realize anything bad has happened other than a slight delay which could have been caused by temporary RF interference.

Risk Factors of Rogues

Once you know how rogue users may be attacking your WLAN, you need to understand the risks that these attacks and usage scenarios may pose. A single rogue can severely compromise your network security in a number of ways. Rogues can:

Create unsecured holes in the network. While your wired network may be a walled fortress guarded by multiple firewalls, your WLAN is much more vulnerable. A single rogue wireless user can gain entry, bypassing the firewalls and opening the floodgates for others to come in and access your corporate data. The AP itself may be suitable for home use, not enterprise use. It may have an IP address and a console port to facilitate remote configuration and management. It may have an embedded DHCP server and be able to dole out IP addresses. APs with console ports and embedded DHCP servers are vulnerable to being reconfigured and maliciously used elsewhere.

Potentially cause a loss of private data or intellectual property. Once a rogue has penetrated your network, the door to your corporate network has been opened and the information security line has been breached. For the CIO or IT manager, that means your sensitive system data, such as passwords and policy information, is no longer secure. Applications and data are vulnerable. Confidential corporate information stored anywhere on the network can be accessed or downloaded.

Create a legal liability for the enterprise. Unauthorized use of the network or the Internet connection is a legal liability for the enterprise, not for the rogue user.

Deny service to legitimate users. A rogue who launches a denial-of-service attack can disrupt throughput and performance in the airspace. Jamming the WLAN with data packets forces users to continuously disconnect from and reconnect to legitimate APs, effectively knocking them off the network.

Launch man-in-the-middle attacks. In this attack, a rogue attracts a user at authorization time or it can jam a legitimate AP and force the user to re-associate with the rogue. A man-in-the-middle rogue AP is very difficult to detect and is potentially very damaging because it grants full network access to the rogue.

Degrade wired and/or WLAN performance. Whether a rogue launches a man-in-the-middle or denial-of-service attack or a user inadvertently steals the air from legitimate users, enterprise network performance and throughput can suffer. Once a rogue is on your enterprise network, it can consume even more precious shared resources, such as your Internet connection. The rogue can steal intellectual property, post salaries on the Internet or steal the launch plans for your company’s next new product.

Detecting Rogues in the Wired Enterprise

To understand the challenge of detecting and locating rogues in a WLAN, it's critical to understand how WLANs impact the assumptions upon which network devices and operating systems base their security, and why WLAN system vendors need to address identifying and detecting rogues as an integrated part of their solutions.

A traditional network operating system has no mechanism to detect or locate rogue users, either on the wired or wireless LAN. A network operating system employs user names and passwords to authenticate and authorize users, but it doesn't care where users and devices are physically located once they are authenticated. It cannot detect a rogue hub, router or switch since it is unaware of the underlying network infrastructure, either wired or wireless.

Network devices such as switches and routers base their security model on the existence of a physical connection between the user's device and the switch or router port. Port security is enforced by the device's MAC address or via 802.1X authentication on a switch port. Some switches may be capable of reporting when non-authorized MAC addresses are detected on the LAN. Today, these primitive methods are the only possible means of rogue detection currently available in a wired network.

Once users are mobile, they are no longer connected to a specific port on a switch. Yet, port security is predicated on that physical connection. The network operating system knows who they are but doesn't know where they are. And the switches used to know where the user devices were, but now the devices are moving. Legitimate wireless users move – and so do rogues. The network operating system can't detect the move. Nor can your wired intrusion detection system (IDS) or SNMP management application detect a rogue user or AP since they lack awareness of the air.

Today, to detect a rogue user or AP, the IT manager will have to deploy a separate "wireless defense" network, which is a complex and costly preventative measure. Alternatively, IT managers will be required to perform regular analysis tests on each WLAN, which is a manual and time-consuming process. And it's hardly foolproof.

A better approach is to deploy a WLAN system that is inherently able to detect and locate all APs and users and easily distinguish legitimate users from unauthorized ones. Let's delve into the three approaches for detecting and locating rogues.

Using External Tools for Rogue Detection

To detect rogues, IT managers have two choices. They can do an internal war drive to manually discover the rogues or they can install a network of rogue AP sensors. In an internal war drive, an IT manager physically walks around the building with a wireless laptop or handheld device and wireless analysis software. Several tools are available to capture the 802.11 packets of WLAN transmissions. For example, NetStumbler and AirSnort can scan the airwaves for WLAN signals, list what is available and reveal their descriptors and vital statistics.

WLAN analyzers are another choice. Usually selling in the \$3,000 to \$4,000 range, products such as AirMagnet, WildPackets' AiroPeek, and Sniffer Wireless are able to capture 802.11 packets and analyze the Layer 1 and Layer 2 information. They report transmission data such as signal strength, channel and data rates. Some require expert WLAN network and security analysts to understand the data and locate the threats detected. These types of products usually come in both laptop and handheld formats. These tools usually can't pick up signals from microwaves or portable phones operating in the same spectrum that can also cause interference. So if you're looking to resolve channel conflicts between 2.4 GHz cordless phones and your WLAN, you will need a spectrum analyzer.

Most importantly, this manual approach to rogue detection requires the IT manager to walk around the building performing WLAN packet sniffing on an ongoing and regular basis. Walking around the office looking for rogues is an unreasonable and time-consuming burden for IT. Surely the IT staff has more important tasks to do than to police the building, manually looking for rogue users on a daily basis.

Additionally this approach is not particularly accurate. While it may allow IT to discover some vulnerabilities in the network, the odds of locating a rogue who is on the WLAN at the exact moment when the IT manager is sniffing are slim. These tests provide only a random sample of the airwaves, and a rogue could log on only seconds after a sweep and therefore go undetected. In addition, rogue users can typically see the IT managers performing a sweep and can simply turn off and hide the rogue device for a short time.

Continuous monitoring of the airwaves requires even more expensive wireless intrusion detection tools, such as AirDefense. Similar to an IDS for a wired network, wireless IDS requires a network of sensors. So in essence you will have to set up a second set of sensor APs to monitor the production WLAN for rogues. These sensor APs cannot carry enterprise network traffic. Once a rogue is detected, these tools use triangulation techniques to locate the rogue. Without intimate knowledge of the facility layout and the enterprise WLAN's architecture, it can be difficult to zero in on a rogue AP or user. Wireless intrusion detection tools typically start at \$25,000 for a minimum installation, so 24x7 rogue detection quickly becomes a costly add-on if your WLAN system vendor doesn't integrate support for rogue detection and location.

802.1X Authentication is Your Best Security Offense

While expensive sniffing and monitoring tools can help with rogue user and AP detection, the best defense is a good offense. Adding 802.1X authentication combined with 802.11i encryption or even pre-standard 802.11i techniques like Wi-Fi Protected Access (WPA) will deliver a strong offense. If only authenticated users can communicate on the network and all communication is encrypted, the chances are small that a rogue will be able to penetrate and do damage. By using 802.1X authentication with AAA, the IT manager can severely limit if not completely eliminate rogue attacks in the enterprise.

Access control must address the unique circumstances of mobile users. First, because mobile users are not always associated with the same AP, access control must be based on the user's identity. Second, it must be a mutual authentication process, whereby the network authenticates to the user and the user authenticates to the network. Mutual authentication is important so that the user doesn't accidentally join a rogue AP.

Once you set up 802.1X authentication by user or group for your company, you have severely limited the ways in which a rogue user can penetrate your network. The 802.1X authenticated users comprise a "legal users" list, along with all of the authorized APs on the WLAN. Once you have the legal users list, you can determine whether a user or AP that is not on the list should be considered a rogue or a new, legitimate user.

An intruder cannot use an unsecured AP to gain access to your corporate network, because all users must be authenticated before gaining access to corporate resources. A rogue AP will have a much harder time attracting and authenticating clients since the client will demand strong authentication from the rogue AP as well. Using 802.1X authentication completely integrates the detection of rogue APs and users into the network system, rather than overlaying an expensive and complex system specifically to identify rogues.

Implementing 802.1X authentication is best done in conjunction with a RADIUS server. You may implement a RADIUS server separately or as a part of NT Domain or Active Directory. The payoff for centralized authentication is significant, as it is one of the best ways to effectively manage WLAN usage and prevent rogues. While 802.1X is typically deployed with a WLAN, deploying 802.1X across both your wireless and wired network will bring stronger authentication to your entire enterprise. With 802.1X authentication, your defense against rogues becomes an integral part of your WLAN system, not a complex after-market bolt-on.

To Catch a Rogue: Location, Location, Location

Simply detecting a rogue is not enough. You have to be able to locate it to stop it. While some vendors recommend complex approaches like triangulating a rogue's location using GPS, which doesn't work reliably indoors where your office WLAN is undoubtedly located, the best solution is far simpler. The best solution lies in knowing where all APs and wireless users are located as well as being able to distinguish the authorized users from the unauthorized ones.

Locating rogues means the WLAN system must have an accurate and thorough map of the RF topology. The WLAN system tools must understand the facility's physical attributes, such as the locations of the walls and floors. The WLAN system must be able to detect where all of its APs are located – and map them to the floor plans.

The WLAN system software should perform regular RF sweeps of the WLAN domain. During a sweep, each AP listens across every channel to determine who's connected. It's critical to listen across all channels, not just on the channels actively transmitting since a rogue could be quietly hiding on another channel. Some rogue detection methods rely on listening only to beacons. Smart hackers turn off beaconing when trying to penetrate a network.

An RF sweep arms the IT manager with a complete view of all 802.11 APs and devices, whether legitimate or not. From there, the WLAN system can determine which APs and users are rogues and which are approved and authenticated. If a rogue is detected, then the WLAN system can triangulate the known physical location of the APs to determine where the rogue is. The WLAN system can accurately use RF signal strength to help the IT manager identify the device in question.

Once the IT manager has confirmed the presence of a rogue, it's time to do a little police work. He may choose to narrow the scope of the RF sweep and perform it again. Or he may arm himself with a wireless LAN analyzer to look for the illegal device.

IT managers should be wary of rogue-detection tools that offer automatic control or shutdown. For starters, it's practically impossible for a rogue-detection tool to exercise any control over the rogue. Breaking the encryption keys is virtually impossible – you can thank the improvements to WLAN security for this additional barrier. Being able to identify the brand of rogue AP and its operational commands is quite difficult if you're not the vendor of that AP. Detecting rogues is an inexact science, and it's important not to knock off a legitimate but unrecognized user, such as a guest that didn't properly log into the network, in the name of fast-acting police work. Ask questions first, shoot later.

In Summary

Go on the offensive to build a good defense against rogues:

- Know what constitutes a rogue in your network and how to identify rogue usage on your WLAN.
- Make sure everyone in your company's IT department is aware of the risk factors associated with rogue users and APs.
- Understand and know how to fully implement authentication and encryption tools, including 802.1X, WPA and 802.11i.
- Make user authentication the cornerstone to WLAN access control, both in wired and wireless networks. By using 802.1X authentication with AAA, the IT manager can severely limit if not completely eliminate rogue attacks in the enterprise.
- Demand from the vendors that rogue detection tools be part of the WLAN system. Determining a rogue's actual location within an enterprise WLAN can be difficult and can involve expensive tools, such as an overlay of specialized APs or triangulation techniques. In lieu of having all of those disparate tools, the detection and location of rogues should be built into the WLAN system itself, providing a more complete, integrated solution that meets the needs of an enterprise.

Recommended Reading

To learn more about building enterprise-quality wireless LANs, please read the following white papers from Trapeze Networks:

- Planning and Managing Wireless LANs
- Fat, Thin, or Fit – AP Architecture
- The Effects of AP Architecture on WLAN Integration



5753 W. Las Positas Blvd., Pleasanton, CA 94588 Phone 925.474.2200 Fax 925.251.0642

Trapeze Networks, the Trapeze Networks logo, the Trapeze Networks flyer icon, Mobility System, Mobility Exchange, MX, Mobility Point, MP, Mobility System Software, MSS and RingMaster, Trapeze Access Point Access Protocol and TAPA are trademarks of Trapeze Networks, Inc. All other products and services are trademarks, registered trademarks, service marks or registered service marks of their respective owners. © 2003 Trapeze Networks, Inc. All rights reserved.

WP-DRU-304