PROTECTING WI-FI NETWORKS

DAVID COLEMAN & NEIL DIENER

From Hidden Layer 1 Security Threats

Executive Summary

As Wi-Fi becomes common in enterprises, the industry has matured to a standard 3-step process of building out Wi-Fi infrastructure. First, conduct a site survey to determine the optimal number and position of access points for a particular site. Second, deploy the access points and other Wi-Fi gear and fine-tune the network for optimal performance. Third, continually monitor the network using a variety of security solutions, such as traditional wireless intrusion detection system (IDS) or intrusion prevention system (IPS).

Many think that doing these things ensures a successful and secure Wi-Fi roll out. But, that belief can lead to insufficient security. What the traditional deployment process and Wi-Fi security products overlook is the physical layer, layer 1 in the OSI stack. In a wired network, layer 1 consists of physical media, such as cables, for carrying traffic. In a Wi-Fi network, layer 1 consists of the spectrum of radio waves. Security solutions such as IPS, and NAC work at layers 2 and above. They ignore layer 1 entirely. But layer 1 is the foundation of the Wi-Fi network. And, because it is the foundation, an attack at the physical layer can be more disruptive than attacks at the higher layers.

There are two main types of attacks unintentional and intentional. Unintentional attacks come from common devices that share the unlicensed spectrum with Wi-Fi, such as cordless phones and Bluetooth devices. Even devices not used for communication, such as microwave ovens, transmit RF in this spectrum, potentially disrupting Wi-Fi communications. This type of RF interference can cause Wi-Fi users to experience degradation of throughput, increased latency, and loss of connectivity.

In an intentional attack, a malicious user disrupts Wi-Fi communications through use of a normal PC and software or a custom jammer. This type of attack can both cause denial of service (DoS), and breaches that provide illicit access to the network.

To correct spectrum problems, network engineers need a solution for detecting and characterizing RF interference and for locating the devices that cause interference. Neither site survey tools nor Wi-Fi gear itself is capable of performing these tasks. The proper solution for this work is a spectrum analyzer. New types of spectrum analyzers are available that can detect the individual, discrete device, and lock onto and locate it, thus making troubleshooting these types of problems possible. In addition, the use of a spectrum analyzer during the site survey portion of an installation helps improve the initial build out of the Wi-Fi network, making it better suited for enterprise use.

Wi-Fi Security Concerns

WLANs have additional security threats to consider that are RF in nature. Protocol-level attacks that attempt to penetrate Wi-Fi data security include rogue access points, authentication attacks, evil twin access points, man-in-the-middle, Wi-Fi phishing, and malicious eavesdropping. Most of these attacks exist at layer 2 of the OSI model. Proper authentication, encryption, and segmentation security solutions can be implemented to mitigate many of these well-known attacks. Layer 2 security monitoring solutions can also be put in place to detect when layer 2 attacks are taking place.

But a major oversight in current wireless intrusion detection systems (WIDS) solutions is that they have been unable to detect layer 1 security threats. WIDS typically use 802.11 radio cards that have limited layer 1 visibility. They are only capable of monitoring high-level layer 1 statistics such as received signal strength and signal-to-noise ratio (SNR) across a channel. These limited capabilities are completely insufficient for full spectrum analysis. For this reason, the 802.11 radio card that resides in a mobile or sensor-based WIDS solution can perform only layer 2 security monitoring and layer 2 performance analysis. With that in mind, it should be understood that the only effective tool for accomplishing proper layer 1 spectrum analysis and layer 1 security monitoring is a true spectrum analyzer.

So what exactly are some of the layer 1 risks that exist as potential security threats? The two major layer 1 security risks include undetectable rogue access points and DoS attacks, both of which are described below.

Undetectable Rogue Access Points

The wireless security risk that receives the most attention is that of a rogue access point. Rogue 802.11 devices are most often connected to an 802.3 Ethernet data port by an employee who does not necessarily realize the consequences of his actions. The issue is that the rogue device is now a “portal” to your 802.3 wired infrastructure. Anyone who can connect to the wireless rogue device now can potentially attack network resources via the wireless portal. WIDS solutions were first developed to detect rogue access points and rogue devices. Not only have WIDS solutions proved to be effective at detecting rogue Wi-Fi devices but the same solutions have been extended to automatically disable the rogue devices using a number of published and unpublished termination methods.

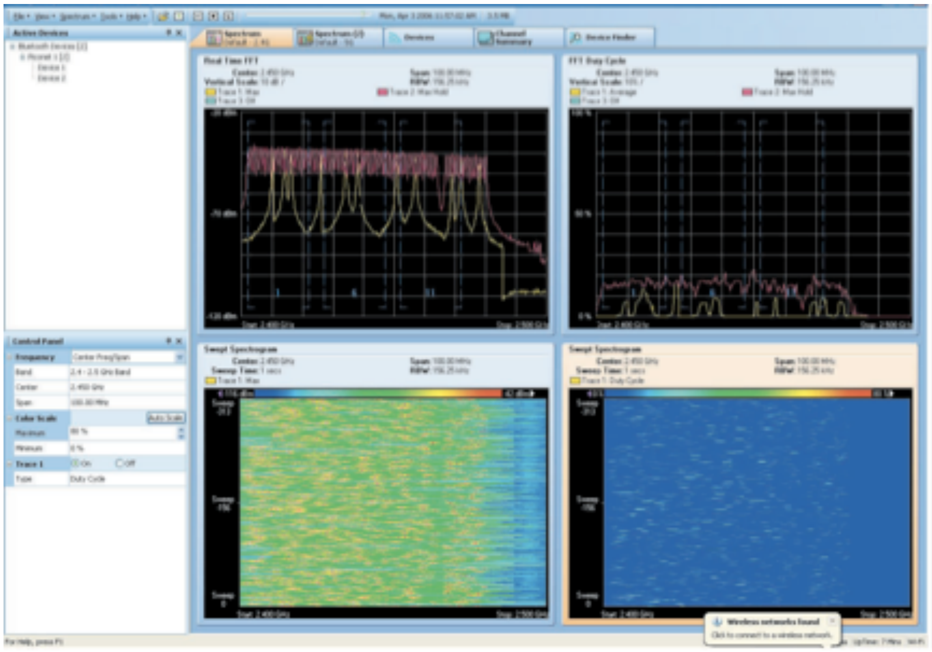
The problem is that certain types of rogue access points currently go undetected because of the layer 1 analysis limitations of the WIDS/WIPS solutions. The 802.11 radio cards that reside inside a WIDS/WIPS solution are designed to understand other Wi-Fi signals. Therefore any rogue device that uses the standard Wi-Fi protocols will be detected fairly instantly. (Although devises that use Wi-Fi in non-standard ways such as operating on a non-standard center frequency may not be easily detected). And devices that use other protocols will also not be detected. Examples of these non-WiFi rogue devices include devices that use frequency hopping spread spectrum (FHSS) radio protocols. Legacy 802.11 access points that were manufactured from 1997-1999 often used a frequency hopping protocol called 802.11 FH. Additionally, a consortium of mobile wireless vendors called the HomeRF

Working Group used to exist. These vendors manufactured non-802.11 access points that also used FHSS transmissions in the 2.4 GHz frequency range. Although 802.11 FH and HomeRF devices are no longer sold, they are widely available at very little cost on eBay and other auction retailers. Bluetooth radios also use FHSS transmissions in the 2.4 GHz frequency range. Because Bluetooth radios are in many devices that also have Ethernet connectivity (such as laptops), Bluetooth radios should also be considered a potential rogue threat.

About David Coleman

David Coleman is a wireless security/networking trainer and consultant. He teaches CWNP classes that are recognized throughout the world as the industry standard for wireless networking certification and he also conducts vendor-specific Wi-Fi training. David has instructed IT professionals from around the globe in wireless networking administration, wireless security, and wireless frame analysis. His company, AirSpy Training, specializes in corporate training and has worked in the past with SpectraLink, Avaya, and Dell Computers. AirSpy Training (www.airspy.com) also specializes in government classes and has trained numerous computer security employees from various law enforcement agencies, the U.S. Marines, the U.S. Army, the U.S. Navy, and other federal and state government agencies.

Figure 1 - Sample spectrum analysis view of an active Bluetooth device



Legacy 802.11 FH, HomeRF, and Bluetooth radios can all be used by an attacker as rogue devices and will go undetected by current WIDS/WIPS solutions. In fact, because of this weakness, they make very attractive approaches for someone trying to maliciously install an open port onto your network. The proper tool needed to detect and locate these rogue devices is a spectrum analyzer. Spectrum analyzers can detect all types of non-WiFi radio devices, including frequency hopping radios. In fact, some analyzers can look at the RF signature of the device, and determine exactly what type of non-WiFi radio has been found. Another potential rogue device that can go undetected is an access point that transmits in a frequency range not supported by 802.11 radios. 802.11 radios either transmit in the unlicensed 2.4 GHz ISM frequency band or in the unlicensed 5 GHz UNII frequency bands. Non-802.11 wireless networking equipment exists that operates in the 902-928 MHz unlicensed ISM frequency band. Only a spectrum analyzer that sweeps the 900 MHz frequency range could detect this type of device because 802.11 radios do not listen in 900 MHz frequency range.

A Layer 2 WIDS/WIPS solution is still a recommended solution for detection and prevention of many 802.11 rogue devices. But adding a full-time spectrum analysis solution provides for greater detection of a wider range of rogue devices.

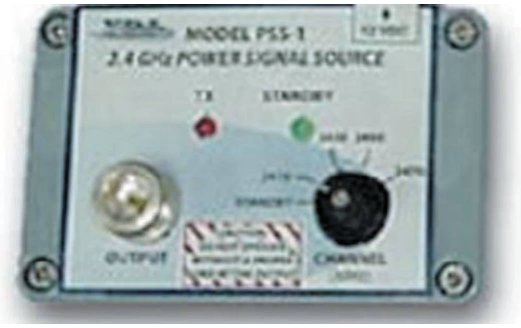
Layer 1 DoS Attacks

A particularly troublesome issue for Wi-Fi security is the denial of service (DoS) attack. In a DoS attack, the goal of the attacker is not to penetrate or steal data from the network it is simply to disable the network. For mission-critical systems, this is a serious security concern. If the WLAN goes down, then any application or network resource being accessed through the WLAN is now no longer available. The wireless VoIP phone conversation comes to an abrupt end, communications with your database server are no longer possible, and wireless access to an Internet gateway has been closed.

Many denial of service attacks exist at layer 2 and occur when an attacker manipulates information in the layer 2 header of an 802.11 management frame and then retransmits the edited frames into a wireless environment with some sort of packet generator. Numerous published layer 2 DoS attacks exist. The most common is achieved by manipulating deauthentication or disassociation management frames. Currently, layer 2 DoS attacks cannot easily be prevented, but can be easily detected. The 802.11w Task Group is addressing methods to also prevent many layer 2 DoS attacks. This method has been driven by Cisco's Management Frame Protection under the Unified Wireless vision.

In the meantime, wireless intrusion detection systems can detect and locate the radio card that is the source of a layer 2 DoS attack. But denial of service attacks to wireless networks can even more easily occur at layer 1 in the RF environment. Layer 1 DoS attacks are a result of radio frequency interference. 802.11 WLAN radio cards use a medium access method called carrier sense multiple access/collision avoidance (CSMA/CA). This medium access method ensures that only one single radio card is transmitting at any given time in the half-duplex radio frequency medium. Part of the CSMA protocol is the clear channel assessment (CCA). The simplest explanation of the clear channel assessment is that 802.11 radio cards listen before they transmit. If an 802.11 radio is about to transmit, it will perform a CCA and listen for current RF transmissions in the same frequency space. If the RF medium is clear, the radio card will transmit. However, if the medium is not clear (based on sensing RF transmissions that exceed pre-defined energy thresholds), the 802.11 radio will defer for a defined amount of time and then perform the CCA once again to listen for a clear medium before transmitting. But if there is a "continuous" RF transmission that is constantly heard during the CCA intervals, 802.11 transmissions will completely cease until the signal is no longer present. If 802.11 transmissions cease due to an interfering RF signal, the result is a denial of service to the WLAN. What can cause layer 1 DoS? Layer 1 DoS can be a result of either intentional or unintentional interference.

Figure 2 - Signal Generator



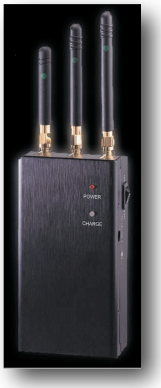
Intentional DoS

Intentional DoS can be described as malicious attack from an individual that possesses some sort of RF signal generator device. Signal generators exist that transmit in both the 2.4 GHz ISM band and the 5 GHz UNII bands. Signal generators often are used for legitimate testing purposes, such as to provide a power source to measure coax loss with a wattmeter.

What is to prevent a villainous individual from transmitting a 1 watt (+30 dBm) signal via an ordinary antenna? The signal generator has now been transformed into a jamming device that will overtake most 802.11 radio cards that transmit at a maximum of 100 mw (+20 dBm). Higher gain antennas can be combined with the signal generator to achieve more radiated power and extend the range of the DoS attack. Unidirectional antennas can be used to focus a layer 1 DoS jamming attack.

Jamming devices and signal generators can be either narrowband or wideband. For example, a 2.4 GHz narrowband generator can cause DoS on specific channels. Figure 4 shows a spectrum capture of a narrowband jamming device.

Figure 3 - Jammer



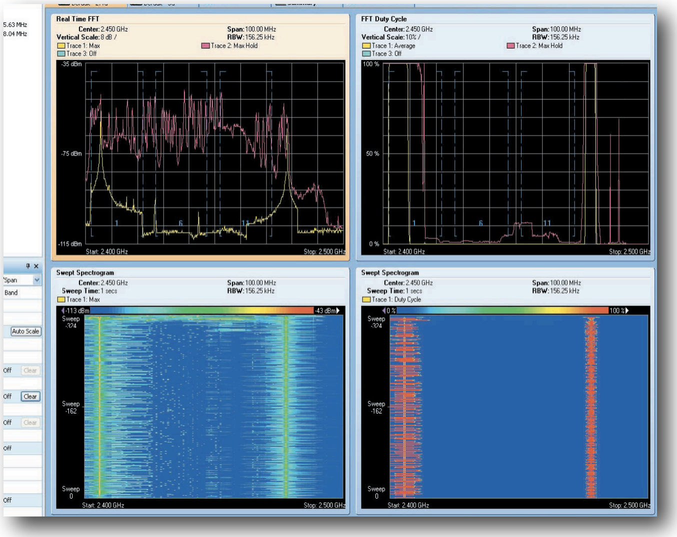
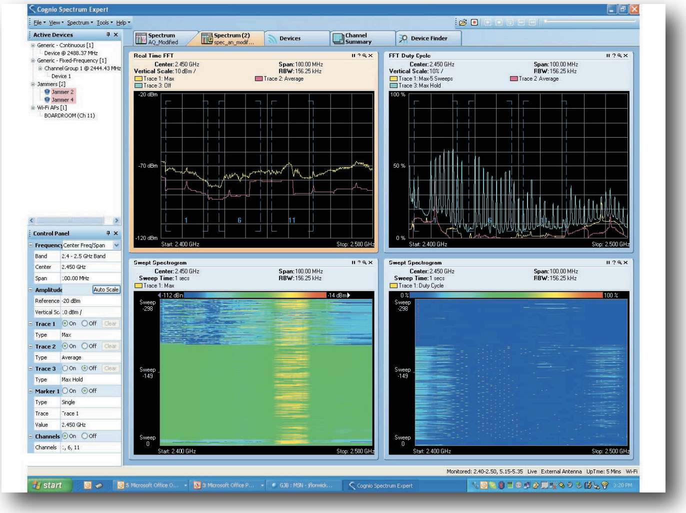


Figure 4 - Sample Spectrum Capture of a Narrowband Jamming Device

A wideband jammer emits a signal that raises the noise floor across several frequencies. Figure 5 depicts a spectrum capture of a 2.4 GHz wideband jammer.

One final device that could be used for an intentional layer 1 DoS is an ordinary 802.11 radio card. What if an 802.11 radio card could be placed in a "continuous transmit" state? In this scenario, the radio card would not actually be sending data or modulating data, but would be sending out a constant RF signal much like a narrowband signal generator. Other 802.11 radios never get to access the medium because whenever they perform a clear channel assessment, the medium is occupied by the continuous transmitter. Researchers at

Figure 5 - Sample Spectrum Capture of a Wideband Jamming Device



Queensland University in Australia discovered this attack is indeed feasible. A major chipset manufacturer of 802.11b radio cards produced a software utility that placed the radios in a continuous transmit state for testing purposes. This utility can also be used for malicious purposes and is often referred to as the Queensland Attack. An 802.11b radio operating in continuous transmit state at 30 mW may not be as large as threat as a 1 watt jammer; however any 802.11b/g cards within range of the malicious radio will be affected.

Unintentional DoS

Can RF interference still cause a denial of service even though there is no malicious attack? Absolutely! All sorts of devices transmit in the very crowded 2.4 GHz ISM band. RF video cameras, baby monitors, cordless phones, and microwave ovens are all potential sources of interference. The whole point of the original site survey is to eliminate these sources of interference. But what if an employee forgets about corporate policy and employs a leaky microwave oven or a 2.4 GHz cordless phone after the original site survey was performed? Microwave ovens typically operate at 800 to 1,000 watts. Although microwave ovens are shielded, they can become leaky over time. A received signal of -40 dBm is about 1/10,000 of 1 milliwatt and is considered a very strong signal for 802.11 communications. If a 1,000 watt microwave oven is even .0000001 percent leaky, the oven will interfere with the 802.11 radio. Figure 6 shows a spectrum view of a microwave oven. Note how the signal sweeps across a wide band of the spectrum and operates at about 50% duty cycle (as the magnetron turns on and off with the 60 Hz cycles of the electrical system.) Figure 7 also shows a spectrum view of an analog video camera. Note how the signal operates at a single frequency and transmits with 100% duty cycle. Not nearly as many as interfering devices transmit in the 5 GHz UNII frequencies; however that will change with time. 5 GHz spectrum analysis should also be considered mandatory.

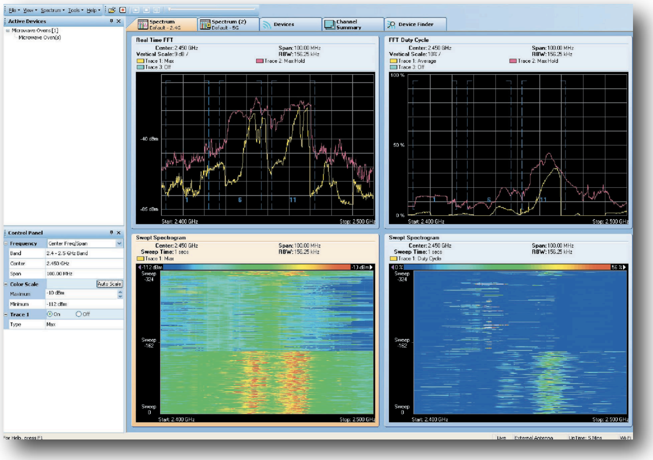


Figure 6 - Sample Spectrum Capture of Microwave

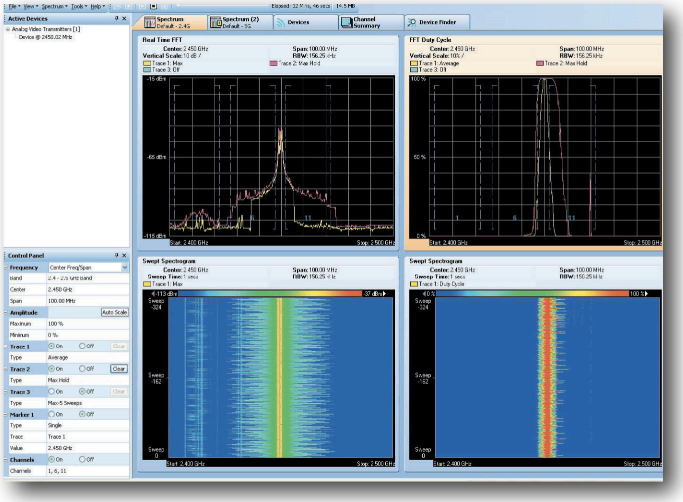


Figure 7 - Sample Spectrum Capture of Analog Security Camera

Unintentional interference may cause continuous DoS, however, the disruption of service is often sporadic. This disruption of service will upset the performance of Wi-Fi networks used for data applications but can completely disrupt VoIP communications within a Wi-Fi network. At the very least, unintentional interference will result in retransmissions. The site survey eliminated these sources of interference initially; however, full-time or part-time spectrum monitoring may be necessary in case these interfering devices reappear.

About Neil Diener

Neil Diener is the technical leader for the Chief Technology Officer at Cisco systems. Neil has over 20 years of experience in the architecture and design of reliable communication systems. Prior to Cisco, Neil was CTO and cofounder of Cognio, a leader in spectrum analysis. Before joining Cisco, he held a series of director-level positions at companies including Motorola, Sun Microsystems, and Xerox. Neil holds a BS Electrical Engineering from MIT and an MS in Computer Engineering from USC. He has

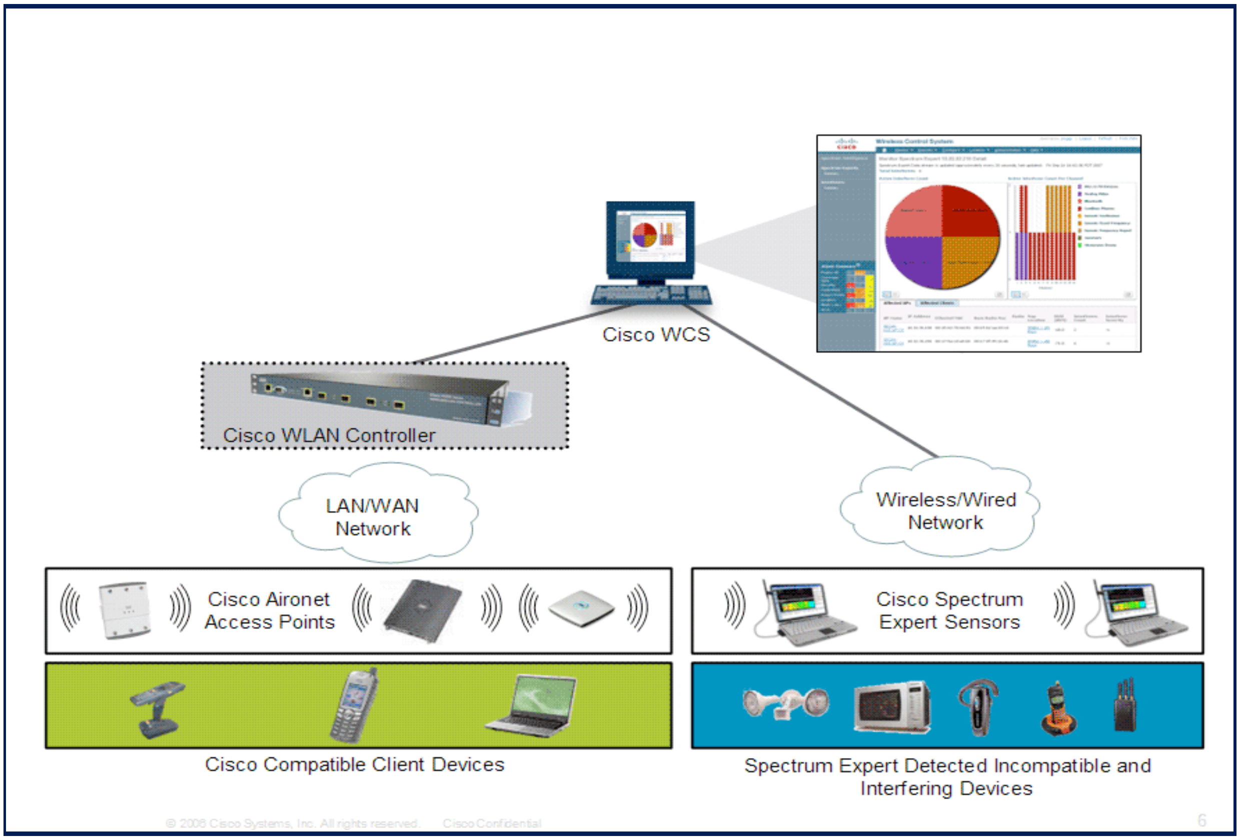
Mobile spectrum analysis versus distributed spectrum security

Traditional spectrum analyzer hardware can cost upward of $40,000 (in U.S. dollars), thereby making it cost prohibitive for many smaller and medium-size businesses. However, the introduction of affordable and easy-to-use spectrum intelligence products Cisco® Systems have enabled most site survey professionals to now consider spectrum analysis as a mandatory part of an 802.11 site survey. These products are affordable software-based spectrum analysis solutions that work with proprietary PC card hardware. The product will usually pay for itself after the first site survey, reducing ongoing support costs for the network by eliminating interference problems from the start. Additionally, WLAN professionals are now implementing these spectrum analysis solutions as preventative measures against layer 1 security risks.

Two forms of spectrum analysis systems are available: mobile and distributed. An example of a mobile spectrum analysis device is the Cisco Spectrum Expert which consists of a CardBus card and software, and works with an IT professional's laptop to create a portable measurement system. An example of a distributed spectrum analysis system is the Cisco Wireless Control System (WCS) with Cisco Spectrum Cardbus Sensors. This distributed spectrum intelligence consists of a set of static or mobile deployed Power-over-Ethernet (PoE) sensors that constantly take spectrum measurements and send the data to a server where it is archived, analyzed, and then presented to the user. Both mobile and distributed systems have their own strengths and usefulness, as described below.

Mobile systems are very useful before any infrastructure has been deployed, as in the case of a site survey. In addition, a mobile system can be used to investigate all the nooks and crannies of a floor space, to see if there is interference in these extreme reaches possibly coming from outside the building. When an interference source has been detected, a mobile system is also very useful for tracking down the location of the interference device. By putting the system into tracking mode, it can be used as a "Geiger counter" to find the interference device using a hot-potato, cold-potato approach. This location ability can be further enhanced with the use of a directional antenna. From a security standpoint, a mobile tool can be used as part of a periodic sweep of the floor space, looking for rogue devices, jammers, etc. This essentially is more of a "spot check" than a true security monitoring solution-but for many companies without highly secure data, this may be considered sufficient.

Figure 3 - Cisco Spectrum Intelligence Diagram


Cisco WCS
Cisco WLAN Controller
LAN/WAN Network
Wireless/Wired Network
Cisco Aironet Access Points
Cisco Spectrum Expert Sensors
Cisco Compatible Client Devices
Spectrum Expert Detected Incompatible and Interfering Devices
© 2006 Cisco Systems, Inc. All rights reserved. Cisco Confidential
6

Distributed spectrum analysis systems offer some additional features, but do cost a bit more due to the infrastructure cost of the sensors. The key advantages of a distributed system are that they run 24x7 and can be administered remotely (important for large organizations with many buildings). By running in a 24x7 fashion, the system is guaranteed to find any layer 1 security issues that occur, even if they are very intermittent in nature. Companies that deploy mission-critical applications and/or sensitive data should consider a distributed system.

An additional application of a distributed system is to implement a "No Wireless Zone." This is a secure area of a building where wireless devices are not allowed because of a need to keep information secure. An example would be a segmented compartmented information facility (SCIF) within a government installation. WLAN IDS systems are currently used in some of these installations, but a true layer 1 analysis system is needed to enforce non-usage of other wireless devices such as Bluetooth, cordless phones, etc. In addition, other bands can be monitored to guarantee that no wide area network (WAN) devices such as pagers, cellular phones, and WiMax radios are in use. The distributed system can be used to automatically generate reports required as part of a security audit.

For many deployments, it makes sense to have both mobile and distributed spectrum analysis tools at the ready. The mobile tool is used for the initial site survey and for periodic sweeps of hard to reach places. The distributed tool is used for 24x7 monitoring and archiving of spectrum usage. When the distributed tool detects the presence of interference, the mobile tool can also be used to exactly locate the device in the rough area identified by the distributed system. The mobile and distributed spectrum analysis solutions work together to form a complete enterprise spectrum security solution.

Conclusion

Topics such as capacity, coverage, and quality of service will always remain top priorities when deploying 802.11 wireless networks. Yet security always seems to be the number one subject whenever an 802.11 WLAN deployment is considered and/or planned. Layer 2 wireless security monitoring solutions will remain valuable tools to protect the WLAN and wired infrastructure. In today's enterprise environment, however, an IT professional should also be concerned with layer 1 wireless security. The best method available for proper protection against potential layer 1 RF threats is spectrum intelligence.

AirSpy training

CISCO