Wireless LANs:
Defending the Enterprise Airwaves

Moving Beyond Intrusion Detection to Intrusion Protection

June 2004

Content

NetworkChemistry
The RF Security Company™

Introduction

Consider the Black Swan Theory: the idea that the human mind will go to extreme lengths to explain anomalous and unexplainable events, such as the appearance of a black swan. The mind demands order. Applying this theory in the day-to-day world of wireless security management, it follows that security professionals could expend vast resources attempting to predict and defend against the next black swan, the next wireless attack. Unpredictability, however, is the essence of a black swan – that is what makes them so dangerous. Not only can we be assured there will be some new, anomalous, unpredictable attack, but we run the risk of squandering valuable time, manpower and money attempting to predict and prevent what is unpredictable. Infinite vigilance is not possible.

Faced with this impossibility to predict black swans, network security managers need to plan for, monitor, and recognize *potential* network breaches as well as react quickly when any breach occurs. This is especially true of the new enterprise Achilles heel, the wireless LAN (WLAN). Increasingly enterprises are realizing the benefits of deploying 802.11-based WLANs – increased efficiencies, streamlined workflow, and applications that enable customer satisfaction far beyond what wired networks provide. However, these benefits do not come without risk. Every wireless access point (AP) has the potential to be the open back door to the lifeblood of today's modern business – its information. This document will detail best-of-breed technology and methodology enterprises can implement today to ensure they experience the benefits of WLANs without being hobbled by wireless-specific attacks or the fear of wireless attacks.

Expect the Unexpected – When You Least Expect It

Hackers today are out for dollars, not just to show off their technical expertise. They are stealing financial data, customer credit card numbers and competitive information, and they are doing it wirelessly. Using a well-stocked, readily available tool chest, hackers go after the weakest link, scanning for vulnerable APs or unwittingly open laptops.

The methods used by wireless hackers are entirely different from old wired attacks. To stop them the network security officer must be diligent, resourceful, and in possession of his own well-stocked toolkit. Keeping abreast of the daunting array of wireless attacks is difficult and time consuming; it can seem like new vulnerabilities are discovered every day. But, with systems that can detect wireless attack signatures and the support of a vendor dedicated to wireless security assessment, they can put themselves in a position to thwart hackers before a compromising corporate break-in occurs.

Ease of Wireless Attacks: the Known, Unknown and Unknowable

Attacks like the Melissa virus and Back Orifice have entered mainstream consciousness. Their ability to debilitate is well-known and efforts must be made to protect against them and similar attacks. Wireless LANs have created an entirely new breed of attacks using new techniques and demanding new defenses. Hackers have translated these sophisticated attacks into automated "malware" that greatly reduce the expertise required by the intruder to perform the attack. The list below depicts a sample of wireless attack tools, most of them freely available on the Internet:

- **Scanners**: APScanner, Kismet, NetStumbler, Wavemon, Wellenreiter, Wi-find, Wireless Security Auditor
- **Sniffers**: AiroPeek, AirTraf, Mognet, LinkFerret, NG Wireless Sniffer, SSID Sniff, VPNmonitor
- **Protocol Exploiters**: Anwrap, Asleap, Hotspotter, Pong "GSTsearch", Ittra
- **Denial of Service**: FATAjack, Hunter_Killer, FATAjack, Macfld, Michael, Void11
- **Multi-Use Tools**: AirJack, BSD-Airtools, Ettercap, LSAKnopix, Knopix, THC-RUT, WarLinux
- **WEP Exploiters**: AirSnort, WAP Attack, WEPCrack, WEPWedgie
- **Soft APs**: HostAP, CqureAP, DiskAP, Coyote Linux
- **Other Tools**: Airsnarf, AP Hopper, APTools, Fake AP, WINPCAP

Threats performed by WEPWedgie can penetrate encrypted networks, while attack tools like Airsnarf can dupe users to redirect to a hackers AP. Using other malware, hybrid attacks can be launched, disguising themselves in seemingly legitimate programs and spreading deep within a network before detection. A recent strain of Trojan attacks known as Remote Access Trojans are particularly troublesome as enterprises only discover them after the damage has already been done. The challenges faced by network security managers are immense.

Compound the known and unknown with the certainty of yet-to-be-discovered future attacks, and the only way to be as prepared as possible is to think like a hacker, develop a counter-measures plan, and blanket-monitor the airwaves for vulnerabilities, rogues, signs of "knob rattling," and active attacks.

Deficiencies in Current Defenses

At a minimum, enterprises must encrypt and authenticate communications on the WLAN, but that's just step one. Even with a VPN in use, WLANs are vulnerable to many advanced attacks that prey on the inherent loopholes in these security implementations. Robust network security is based on a layered approach that includes continuous monitoring for vulnerabilities, suspicious activities, and active attacks.

At first blush, traditional approaches for detecting network vulnerabilities and attacks seem viable for the WLAN domain. But with further examination, it becomes clear each is severely flawed for protecting the WLAN from intrusions.

- **Wired Network IDS:** Unfortunately, techniques used in securing wired networks do not translate to the wireless world. For instance, a wired network intrusion detection system (IDS) operates at Layer 3 (IP packet) and above;

wireless-specific attacks occur at Layer 1 and Layer 2. This lower layer information is stripped by the AP before it hits the wired IDS, making wireless intrusions invisible on the wired side. The only way to detect wireless-specific attacks is to deploy a wireless IDS with RF-monitoring surveillance sensors.

- **Wired Network Vulnerability Assessment:** As with a wired side IDS, a wired side vulnerability assessment system (or scanner) is unable to see most wireless-specific vulnerabilities. Even in the case of the most common and pernicious wireless vulnerability – the rogue wireless device – a wired side scanner is severely flawed. Wired side scanners can detect some types of rogue APs connected to the network. But there are many types that they won't detect, such as rogues that are not connected to the network (i.e. a hacker's honeypot AP in the parking lot), a rogue based on a consumer-grade AP (i.e. one without SNMP support), and a rogue based on software that turns a PC into an AP (i.e. a PC running "softAP" will be detected as a PC). Other rogues such as rogue wireless clients and bridges will also be transparent to the wired side scanner. The only way to completely detect wireless-specific vulnerabilities is with an approach based on RF-based surveillance sensors.

- **Walk-Around Wireless Scanning:** Portable wireless test equipment provides a role in on-site wireless site surveys and installation troubleshooting. There are many popular freeware tools available along with expensive commercial wireless network analyzers. The main problem with walk-around wireless scanning is that it's labor-intensive and infrequent. Offering a snapshot of the network state at a given time, walk-around scanning is reactive, missing more than it will find. Instead, a proactive approach is needed, one that economically enables distributed, 24x7 monitoring and logging of wireless security anomalies across the enterprise geography.

- **Security Monitoring by the Wireless APs:** An AP simply can't be both an AP and an intrusion monitor simultaneously. A wireless IDS requires the continuous scanning of all 802.11 channels while an AP must stick to a single channel. Nevertheless, some APs can, every hour or so, stop being an AP and scan the other channels for rogue APs and potentially a few other wireless anomalies. The problem with this approach is twofold. First, AP vendors aren't IDS vendors; they can't deliver the specialized support that best-of-breed companies dedicated to wireless monitoring can. Second, depending on the network transmission equipment to also perform the intrusion monitoring is a flawed defensive strategy, since it's this same equipment that hackers can probe, highjack, and disable.

Network Chemistry – Beyond Intrusion Detection to Wireless Intrusion Protection

Network Chemistry has pioneered a superior approach for managing wireless security anomalies, going beyond just intrusion detection to intrusion protection. Its fully integrated offering, the RFprotect™ Wireless Intrusion Protection System, performs real-time, distributed, and continuous security monitoring using RF-based surveillance sensors. Supporting all 802.11 vendors, protocols, and devices, RFprotect provides intrusion protection, one of four requirements of a complete security plan for enterprise WLANs.

Wireless intrusion protection goes beyond intrusion detection, encompassing all functions of wireless security monitoring as a single cohesive offering. Wireless

intrusion protection adds the proactive pieces around the core function of intrusion detection. Intrusion detection is a critical, but reactive function, identifying attacks already in progress. Intrusion protection augments this on the front-end with the proactive functions of rogue detection and vulnerability assessment. This allows security professionals to identify and plug wireless security holes before hackers exploit them, reducing the threat of compromising attacks and breaches. On the back-end, wireless intrusion protection adds usage auditing and forensic analysis. Since intruders are innovative and unpredictable, security professionals need to assess the impact of breaches and learn to prevent them from happening again.

RFprotect leverages intelligent radio frequency (RF) sensors distributed throughout a physical environment, coupled with a high-performance, centralized server and management console. RFprotect automatically detects device vulnerabilities, wireless rogue devices, intrusion attacks, plus the logging of detailed user and traffic activities. This distributed and scalable system monitors all WLAN activity 24x7 across 802.11a, b, and g bands. Second-by-second real-time updates enable immediate response. Wireless traffic capture capability with deep decoding analysis allows detailed forensics of complex problems. RFprotect's plug-and-play architecture facilitates installation and operation in a matter of minutes. Plus, the solution comes ready for integration with any existing security management system.

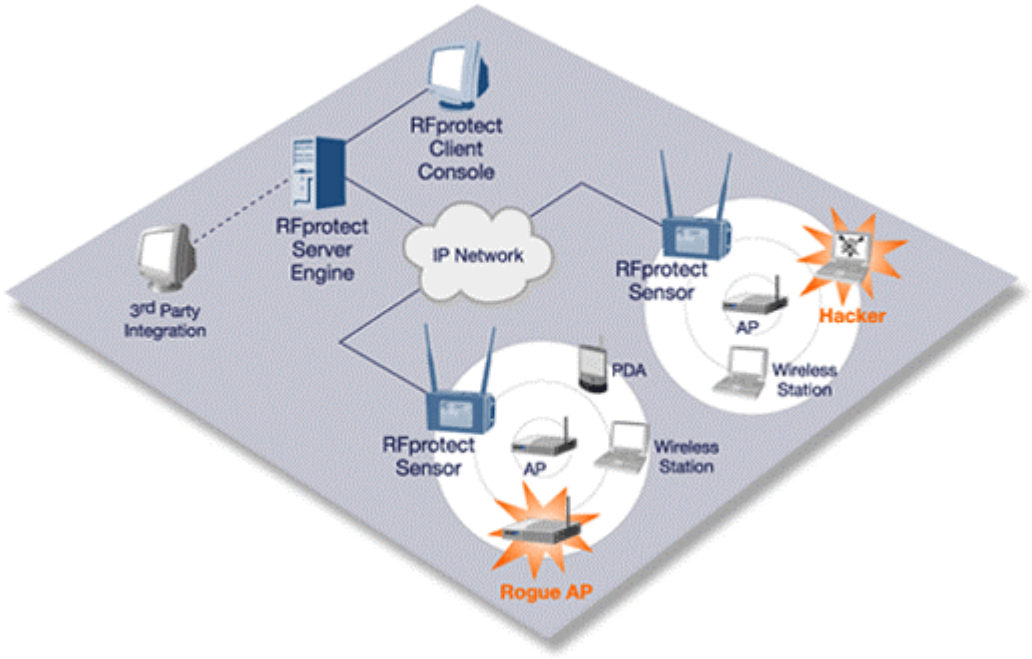

Figure 1 With its highly scalable three-tier architecture – composed of distributed RF-based Sensors, 24x7 Server Engine and real-time Client Console – RFprotect is the first to provide Wireless Intrusion Protection in a single cohesive solution.

Network Chemistry's RFprotect has implemented innovations drawn directly from the feedback of enterprise security professionals. This feedback led to a very accurate and adaptable system that is also highly scalable and fully open for integration into other enterprise security platforms. Of utmost importance are the architectural cost reductions that make it economically feasible to blanket the complete enterprise geography with wireless intrusion protection.

Scalability to Grow With You

802.11 network traffic is highly redundant and hence voluminous, making deep distributed analysis difficult. While some wireless monitoring vendors have chosen to analyze all the traffic on the remote sensors, others have chosen to perform this function on a central server. The problem with “sensor-centric analysis” is the lack of data correlation between sensors, which can cause, among other inaccuracies, alert duplication. For even a medium sized WLAN, the lack of alert correlation bogs down the system and the operator. Sensor-centric analysis is also prone to performance degradation due to limitations in processing power and memory. On the other hand, server-centric analysis consumes precious network bandwidth and proves costly for remote branch office monitoring. Both methods fail to deliver the scalability required for wireless intrusion protection and hence limit the functionality that can be offered.

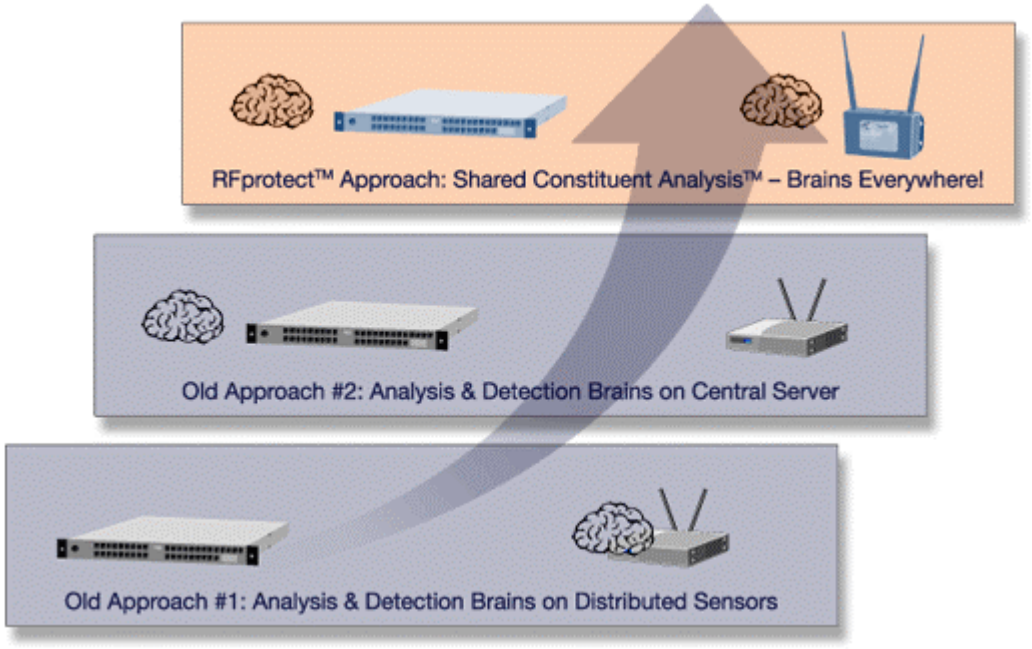

Figure 2 System Architecture Evolution: A highly scalable Intrusion Protection System needs both central servers and sensors that are highly intelligent and can share the analysis function. It is the only way to maintain real-time network state while still keeping back-haul overhead at a minimum.

The ideal solution is a hybrid approach to enable scalable functionality and performance, intelligently splitting traffic analyses between the remote sensors and the centralized server. Using Network Chemistry’s patent-pending Shared Constituent Analysis™ technology, the RFprotect Sensors analyze wireless traffic into "key indicators" that signify security anomalies. The pre-processed data is forwarded to and further analyzed by the RFprotect Server Engine, consuming very little back-haul bandwidth.

The RFprotect Server Engine archives the data and builds a knowledge base that maintains the real-time network state. This knowledge base is the foundation for the system's "aggregated analysis," the basis for deep and accurate detection algorithms.

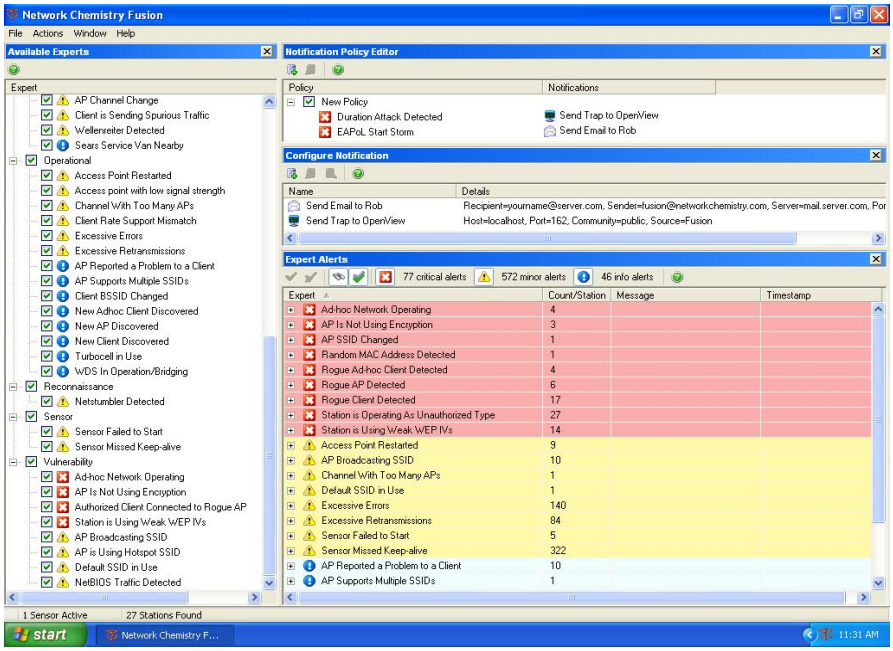

Figure 3 Network Chemistry's Shared Constituent Analysis™ enables a highly scalable solution for intrusion protection in even the largest WLAN deployments, providing accurate and instantly actionable alerts of wireless security anomalies.

Real-Time Accuracy Without a Blindspot

Another challenge in monitoring WLANs is watching all the channels used in 802.11 communications. 802.11b communications, for example, occur on 1 of 14 channels; 802.11a has even more channels. If you consider the channels in the 802.11 range and the amount of time required to scan each, you are faced with two problems. First, a security sensor must scan through all the channels. Second, it must scan quickly and intelligently identify breaches. Some vendor's scan rate is one minute per channel. On 802.11b alone, a channel could go unscanned for 13 minutes, giving a hacker plenty of time to install malware while a sensor watches other channels. Yet, wireless intrusion detection solutions purport real-time notification. How do they define real-time? Is it an hour, a minute, a second? How big is the blind-spot for hackers to get in unnoticed?

RFprotect's Channel RapidScan™ technology shrinks real-time from minutes to milliseconds, closing the hacker's window of opportunity to a fraction of a second and making unnoticed penetration virtually impossible. Fast vulnerability, rogue, and intrusion detection gives security professionals immediate information about the health of their wireless network and enables them to quickly address problems before they escalate.

The Five Components of Wireless Intrusion Protection

1. Rogue Detection

- RF-based monitoring to accurately detect all types of rogue wireless devices - rogue APs, AP software for laptops, rogue clients, rogue bridges, ad-hoc networks - on all 802.11 frequencies
- Real-time notification when rogue wireless devices appear in your air space
- Auto-discovery that distinguishes between authorized, unauthorized, and "friendly" stations

2. Vulnerability Assessment

- Scanning for mis-configurations and weak implementations that open the network to attack
- Scanning for mis-configurations on wireless clients, such as Laptops, PDAs, and Scanners
- Customize detection signatures to enforce security policies specific to an enterprise

3. Intrusion Detection

- Real-time detection and notification of probing and network discovery activities (i.e. from war drivers) that are often the first steps of a wireless attack
- Real-time detection and notification of specific wireless attacks - such as probing and network discovery, denial of service, surveillance, impersonation, client intrusion, and network intrusion
- Real-time dashboard of current wireless activity so you can accurately gauge threats and take appropriate action

4. Usage Auditing

- Automatic discovery of all wireless AP and client stations, with real-time display of which clients are associating with which APs, and how usage activity changes over time
- Real-time detection and notification of accidental or malicious associations, i.e. an employee's laptop accidentally associating with the neighboring tenant's AP or vice versa.

5. Forensic Analysis

- Activity logging and reporting of connection status, activity patterns, and activity transitions to monitor for acceptable use and/or analyze the "footprints" of a wireless hacker
- Real-time traffic capture and comprehensive decode analysis to analyze unauthorized and malicious network activity

Customize and Adapt to You

A wireless security policy is another key element of a complete security plan for enterprise WLANs. Implementing best practices in wireless security should be the foundation of this policy. Since no two network environments or sets of business requirements are the same, there is no "cookie-cutter" wireless security policy that fits all enterprises.

Because every enterprise environment is different, RFprotect provides CustomProtect™, giving the operator the ability to define customer detection signatures to monitor policies that are unique to the enterprise. CustomProtect provides a simple GUI and rule syntax for creating alerts when policy violations are detected.

These unique policies – along with best practice policies – must be monitored to be enforced. For example, an enterprise may allow WLAN use during business hours but prohibit WLAN use during the evening and weekend hours. Another enterprise may have standardized on a particular vendor's Wi-Fi network adaptor and prohibit the use of other vendor's cards. The best wireless network security system should be able to adapt to meet these various needs.

Open to Integrate With You

Network Chemistry's RFprotect was designed with an open architecture that facilitates easy integration with third party security and network operations systems, including those used for network intrusion detection, IP security, and security event, performance, and enterprise network management. RFprotect Sensors and the RFprotect Server Engine have been designed to easily integrate with existing systems.

Economical Breakthrough

Perhaps most importantly, RFprotect has made use of the latest technology to deliver wholesale cost reductions in its system architecture. The software based central server and very low cost RF sensors make it economically feasible to deploy wireless intrusion protection across the entire enterprise geography. Costing a fraction of competing solutions, RFprotect can be deployed for overlapping blanket coverage around the enterprise, and not just in "the most vulnerable areas."

Because the RFprotect sensors are purpose-built security appliances, they are designed for extended range, simplified installation, and superior performance that equates to lower overall cost, compared to systems that use re-purposed APs as its sensors. Finally, RFprotect's plug-n-play setup and operations minimize the chances of improper deployment and reduce the training time to get security operations fluent with the system.

The Four Rules to Securing Enterprise WLANs

There are risks involved in any new project and deploying a wireless LAN is no different. Mitigating risk involves having good intelligence, a sound plan, and the right tools for the job. Working with leading wireless security experts, Network Chemistry has developed the four essential rules for robustly securing enterprise WLANs. Failure to implement any of these rules opens the possibility of serious security risks, perhaps wiping out the many benefits and expected return on investment of WLANs.

Rule 1: Know and Plan

Start with knowing what the vulnerabilities of WLANs are and how a hacker can exploit them. Think like a hacker and how they might want to break into your WLAN. What might they want to do once they get in? Get to know the readily available hacker tools and how they might be used in your environment. Knowing what a hacker can do is the first step to knowing how to defend against them.

Just like wired networks, 802.11 networks require policies that can be implemented and enforced to reduce exposure to the inherent security flaws in WLANs. Once you know the wireless vulnerabilities, plan for effective security policies that start with defining

and documenting them. Management must then buy-into the documented policies. The policies should then be communicated to all employees, contractors, on-site vendors, and anyone else expected to comply with the policy. Later, the WLAN must be monitored to audit for policy compliance. To deal with devices and individuals found violating the policy, enterprises should have an established procedure to take corrective actions for those in non-compliance. Finally, the process to revise and fine-tune the policy should be in place to handle evolving security standards, user behavior, and changes to the network.

Rule 2: Protect Communications

Since a WLAN is an uncontrolled medium, encrypting and authenticating the communications are an essential step to robust wireless security. Protect data in transit over the wireless network using strong encryption, or else anyone with a sniffer can look over your virtual shoulder at your mail, passwords, and your work. Security professionals can deploy standard encryption available on APs like WEP/WPA or use a more proprietary implementation from wireless VPN appliances based on IPsec or similar standards.

In addition, it is essential to ensure that only authorized users can connect to the WLAN. Control access using a robust wireless authentication method using standards-based features on enterprise class APs or more sophisticated capabilities from wireless VPN appliances that include policy-based access control. This means you can specify different authentication methods for different groups of users to limit access by entering a user name and password, or with more secure two-factor authentication mechanisms.

Rule 3: Protect Wireless Devices

Because they are mobile and often distributed outside the enterprise, wireless devices must be protected, both the AP infrastructure and the client end devices, such as Laptops, Scanners, and PDAs.

Locking down APs is an essential step in WLAN security. Configuration access to APs and gateways must be hardened to eliminate the possibility of hackers disabling the network or modifying the configuration to open a backdoor to the network. Many AP vulnerabilities are preventable: a recent survey showed roughly 75% of APs are mis-configured due to complexity and misunderstanding, not unlike firewalls in their early deployments.

As for the end devices, start with disabling insecure settings. Laptops running Windows XP are particularly vulnerable since by default they will scan the airwaves in search of WLANs and connect to the AP with the strongest signal. The laptop is at risk of accidentally associating with a neighboring network or a hacker in the parking lot. A laptop connecting to a neighboring WLAN can divulge passwords or sensitive documents to anyone on the neighboring network. Accidental associations can even link the two companies' networks together through the laptop as it bypasses all internal security and controls.

If possible, install personal firewalls and VPN clients on end devices to limit upper layer network access, particularly if the device is connected to remote Internet connections and/or can be compromised by a hotspot hacker. Lastly, consider encryption for data at rest on devices that are taken outside the enterprise and may be susceptible to loss or theft.

Rule 4: Protect the Airwaves, Monitor 24x7 in Real-Time

As the only way to know for sure that the WLAN is protected, continuous real-time monitoring of the airwaves is an essential element for securing the WLAN. Policies can become useless if an enterprise does not monitor for policy compliance. Specifically, a monitoring approach based on intrusion *protection* ensures a proactive approach to eliminating vulnerabilities – such as network probes and rogue devices – before hackers can exploit them.

Continuous real-time monitoring is the eyes and ears of the airwaves. First, comprehensive intrusion detection must canvass all types of wireless-specific attacks – probing and network discovery, denial of service attacks, surveillance, impersonation, client intrusions, and network intrusions. Attacks must be detected and reported in real-time, so countermeasures can be implemented immediately.

With the popularity and nature of wireless intruders, security professionals must now move beyond intrusion detection to intrusion protection. Building on intrusion detection, the monitoring functions are completed with proactive vulnerability and rogue assessment on the front end and closed-loop usage auditing and forensic analysis on the back-end. RF monitoring must be blanketed across the enterprise geography to avoid any blind spots, since no one can predict where a wireless hacker will attack next. Moreover, the system must be highly scalable and economical, utilizing next generation system technologies to break cost barriers and minimize overall system expenses.

Summary

It is an unfortunate truth that calculated, targeted attacks are part of today's enterprise landscape. Inevitably, almost every enterprise will be attacked at some point, with the WLAN currently being the most vulnerable area. The response to such dangerous, but as yet unknown, attacks is to develop security solutions that effectively mitigate the risk. Wireless LAN risks are severe because we don't control the medium and we don't control who we connect to. But with vigilant understanding, a well-defined program, and the right tools, WLANs can be secured and their benefits safely and profitably attained.

Continuous real-time monitoring of the radio waves is an essential component to securing the WLAN. Deploy at your peril without it. With the growing sophistication of wireless attacks and the availability of automated tools, monitoring must now move beyond intrusion detection to intrusion protection, part of a proactive process for eliminating wireless vulnerabilities before hackers find them.

Next generation solutions, such as Network Chemistry's RFprotect Intrusion Protection System, complete the "must-have" layers of enterprise wireless security, complementing communications protection and device protection. RFprotect's highly scalable and cost-effective architecture now makes it economical for blanket coverage across both small and large enterprise geographies. The depth and accuracy of its expert detection algorithms plus the flexibility of its user-definable policy rules and open architecture for integration makes it a requirement for enterprise security operations.

Like any network, WLANs cannot be made impervious; someone skilled and motivated can take down the layers of defense. A good defense must adapt. Until the network security professional is equipped with Superhero powers and crystal balls, the next best thing is planning, monitoring, and reacting quickly.