# The CSIRT and Wireless Security Breaches – Specialized Methods, Tools, and Techniques for Proactive and Reactive Wireless LAN Incident Response

**Lance Hayden**
**Advanced Services - Network Security**
**Cisco Systems, Inc.**
**lhayden@cisco.com**

**Marcus Sitzman**
**Advanced Services - Network Security**
**Cisco Systems, Inc.**
**msitzman@cisco.com**

**Abstract**

The growth of wireless networking has created a rapidly expanding infrastructure of public, private, and enterprise connectivity. Unfortunately these infrastructures are often deployed and maintained, deliberately or not, with minimal security any many users and administrators do not understand the security implications of the technology. Wireless technology can be implemented securely when properly planned and designed, but incident response specialists should also be prepared for an increase in security events enabled by wireless LAN (WLAN) deployment. A strategy of proactive efforts and reactive preparation, as well as familiarization with technologies and techniques that enable such efforts, is necessary to help ensure that an organization does not suffer damage or loss as a result of a WLAN enabled security breach.

## 1. The Growth of Wireless LANs

In recent years, Wireless LAN (WLAN) deployments using 802.11 technology have exploded, with corporate WLAN implementations, home and other private installation in conjunction with broadband Internet access, and WiFi "hotspots" springing up in coffee shops, book stores, airports, and a variety of other consumer venues. Setting aside wireless mobile phone infrastructures, which also have growing data capabilities, and focusing strictly on 802.11 WLAN infrastructures still allows for a remarkable increase in available infrastructure. A recent survey conducted by Intel identified the 10 most wired cities in the United States, with the San Francisco Bay area in the top position [1]. Bert Sperling, the survey author, summarizes the growing trend well. "Now, people can e-mail vacation photos from the campground, surf the Web from the local coffee shop or get driving directions without having to stop and ask a gas station attendant" [2].

WLAN implementations are predicted to increase over the coming years as businesses and other organizations deploy infrastructures for both internal and remote access. The market for WLAN access points and network interface cards alone is expected to increase by over US$500 million in the next two years [3]. All indications are that WLAN infrastructure growth will continue to create wireless access within and between enterprise and other organizational networks, public networks and "hot spots", and the Internet.

## 2. Security Challenges with Wireless Networking

One of the most important challenges to the rapid deployment of 802.11 network technologies is security. Security issues with WLAN infrastructures have been widely discussed and encompass problems with underlying protocols, with deployment, and often with a general misunderstanding of the nature of a wireless network. Given that 17% of Internet users have utilized a wireless device for their access (28% of younger Internet users) [4], it becomes easy to see that wireless security issues are quickly becoming issues of concern to the larger Internet community.

Depending on the orientation of the researcher or security professional, wireless security issues may be seen to be technical, administrative, or educational in nature. The fact is that all three of these

perspectives must be taken into account when making an examination of WLAN security and attempting to build security strategies around networks in general, and 802.11 networks in particular.

### 2.1 Technical Security Issues

A number of security researchers have focused on the security problems of the 802.11 protocol and associated authentication or encryption features such as Wireless Equivalency Protocol (WEP) [5, 6, 7]. These studies, as well as others, serve to demonstrate mechanisms by which WLANs may be compromised by sophisticated technical attackers (or less sophisticated attackers employing sophisticated tools). These attacks represent attempts to exploit flaws in the fundamental infrastructure.

Other technical attacks involve the physical realities of wireless networking, namely the fact that it is a non-bounded radiating medium, which may or may not represent an actual technical flaw. The example of the "parking lot" attack in Arbaugh, et al., where an attacker takes advantage of the fact that the WLAN extends beyond the physical corporate perimeter, is representative of such an attack. The use of specialized antennae, including those made from common items such as potato chip containers (see illustration), has received media attention for this type of attack.

Homemade Wireless Antenna:

Wireless hacking has developed into a robust subculture within the black hat community, prompting similar specialization on the part of white hat hackers and network security professionals. The innovation demonstrated by hackers in this area does not stop with examples such as the potato chip antenna above. Information devoted to "wardriving" (using an automobile to search for unsecured WLANs) [8], "warflying" (using a plane to search) [9], and "warchalking" (marking discovered WLANs with specialized graffiti) [10] is readily available on the Internet.

### 2.2 Administrative Security Issues

Many security concerns around WLAN deployments are less a function of inherent vulnerabilities and instead involve how the technology is deployed and configured. For instance while WEP has been shown to be vulnerable to certain attacks, those vulnerabilities are rendered moot if WEP is never enabled on the WLAN to begin with. Failing to enable or choosing not to deploy certain security functions, or not taking into account signal ranges when deploying access points (just inside an external wall versus more centrally located within the building) can create security issues by allowing easier access to unauthorized network users. Similarly, poor or nonexistent policies around the network (including WLAN infrastructures) may create gaps in security and limit an organization's ability to enforce acceptable deployment and use of wireless technology. The installation of "rogue" WLAN access points (AP) by individuals within the organization is an excellent example of such an

administrative problem. Such rogue APs are often doubly problematic in that they are often implemented to provide connectivity to existing "wired" internal networks, and have little or no security enabled, thereby providing an external attacker with a backdoor into the internal network.

### 2.3 Educational Security Issues

Like many other network security problems, education and awareness play a large part in mitigating the potential threat. In the case of wireless networking, this issue can be exacerbated by the rapid proliferation of WiFi hot spots in airports, retail shops, and universities, as well as "freenets" set up in communities to provide Internet access to anyone within range. By their very nature, open WLAN access points have little or not security deployed. The same can be said for supposedly private, but unsecured, access points, be they a wireless AP in a private residence, connected to a cable modem and accessible from surrounding residences, or an enterprise with a large WLAN footprint and no real authentication or security measures in place. In some cases, WLAN administrators may possess a false sense of security due to a lack of understanding of threat issues or the technology. For instance, home users may feel that since they assign a service set ID (SSID) to their WLAN that this functions as a sort of password protection, not understanding that this information is typically broadcast over the WLAN and easily discovered.

In the case of an unsecured WLAN, users may not be aware of the open nature of their communications. Data exchanged with the WLAN is subject to capture, and the wireless computer becomes a potential target of attackers on the net. Should the wireless user at an open hot spot connect back into his or her organization's internal network in a less-than-secure fashion then any attackers or malicious software that may compromise the individual's system may have easy access to other resources. Security issues, privacy issues, and even threats to legal or regulatory compliance may ensue, as a result of this lack of knowledge or awareness. These risks do not affect only the technologically inexperienced or those with little understanding of the Internet or security. "For instance, in a recent IETF meeting, among the hundreds of attendees that carry laptops, a dozens [sic] have been detected to be infected with Code Red worm. When these laptops are later integrated back into their company networks, they can spread the worms from within and deem the firewalls useless in defending this worm" [11].

## 3. The Challenge for Security and Incident Response Professionals

The addition of widespread network infrastructures with often very limited security controls in place is a growing problem for those responsible for securing networks and tracking down and responding to attacks. The ease with which a WLAN can be deployed makes rogue APs a concern of every security administrator. Such an AP, located within the corporate firewall and connected to the wired network, can be an instant critical threat to an otherwise well-secured infrastructure. By the same token, an incident involving such an AP, especially if concealed well, can become very problematic to trace. Consider also the threat to mobile workers connecting to open networks and making themselves vulnerable to local attack or worm infestation and the administrator's headaches just increase. It is important for security professionals to understand and actively pursue security on wireless networks with the same vigor they defend traditional nets, whether they own and deploy those networks themselves or allow their workers to utilize third party connections.

## 4. Proactive Versus Reactive Security Approaches

The proactive versus reactive dichotomy is not new, nor is this paper particularly innovative in once again focusing on it. But the dichotomy is important enough to risk cliché by once again pointing it out. Many organizations find themselves all too easily in reactive mode when it comes to security. Questions of budget, expertise, and where to focus resources may prove daunting and create environments or cultures where problems are ignored until they become crises and action can no longer be avoided. Security incident response professionals specialize in the discipline of reaction, although most such professionals would prefer that their skills be required rarely, if at all. The best

security value is the value of nonoccurrence. However, the nature of business often makes such value difficult to measure or justify. But relying only on reactive defenses is dangerous. "Reactive solutions definitely need to be present to address attacks and security holes. But it shouldn't be a large part of the mix; it should only be an emergency tactic" [12].

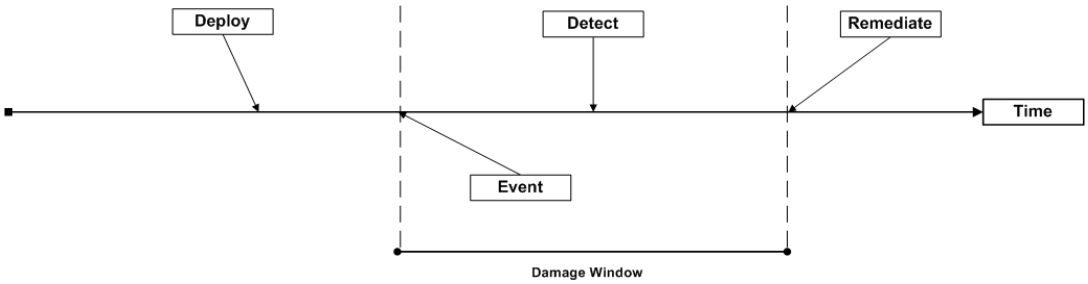
An examination of approaches can prove helpful in identifying the need for proactive, as well as reactive, measures in network security in general and WLAN security in particular.

### 4.1 Sub-optimized Reactive Approach

In some cases an organization may have little or no formal security or defensive network controls in place. In such a situation, the approach is reactive in that problems will be addressed as they are discovered, but mechanisms may not exist to even discover the problems easily. Sophisticated attackers often eliminate the evidence of attack, perhaps even correcting the original vulnerability that allowed them access in order to secure a more effective and long-term compromise. In such an approach, where intrusion detection and security testing procedures are deficient, significant time may elapse between the security event and its discovery and eventual remediation. This elapsed time is the damage window. A damage window extends beyond just the discovery of the incident. Until the vulnerability or threat is addressed and mitigated the damage window remains open, even if known.

An example of such a situation would be a system vulnerability that allowed an attacker to compromise a host and add a back door account or rootkit to the system. Even if the compromise is discovered and the resulting artifacts completely removed, if the original vulnerability remains in place (by not applying an appropriate patch, for instance) then the damage window remains open as the attacker may be free to re-compromise the host. Another example is a worm mitigation effort that does not remove the enabling vulnerability (MS SQL vulnerabilities, for instance, in the case of the Slammer worm) from all systems, and thereby runs the risk of re-infection and continuing damage from the worm. A sub-optimized reactive approach is illustrated below.

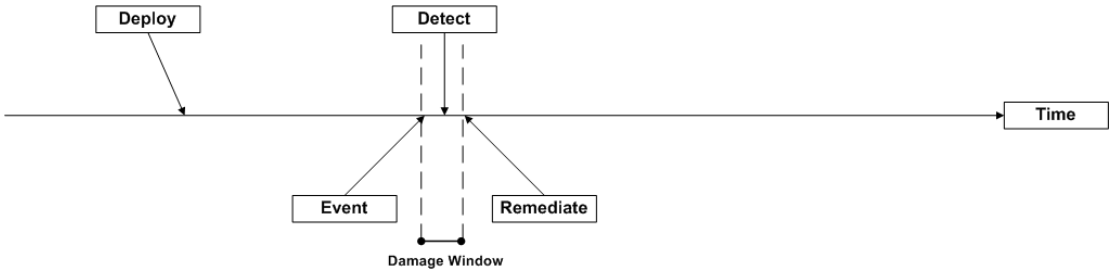
Sub-optimized Reactive Approach:




### 4.2 Optimized Reactive Approach

In optimized reactive approaches, the organization has in place security controls designed to react and alert in the event of an incident, and has defined reaction and remediation plans to ensure that security incidents are given a quick response that removes or mitigates the original vulnerability. Intrusion detection systems, effective log analysis, and incident response procedures are examples of controls and processes that exist in an optimized reactive environment. In an ideal environment, all incidents are detected as they occur, and remediation effected shortly thereafter. This is less than realistic, but the approach holds true in that such efforts should achieve marked improvement over a similar approach with no controls or processes in place. The optimized reactive approach is illustrated below.

Optimized Reactive Approach:

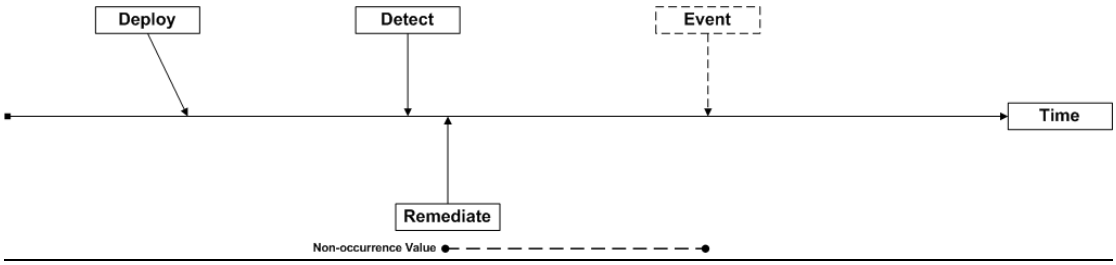



### 4.3 Proactive Approach

Proactive security controls and processes allow an organization to further limit damage windows of network security incidents to the zero point and begin generating non-occurrence value for the organization. Each successful proactive effort at identifying and mitigating network security vulnerabilities prior to their exploitation in a security incident eliminates damage windows and allows the organization to maintain productivity and resources that would otherwise have been devoted to incident response and vulnerability remediation. Increasingly, this value of nonoccurrence is being recognized in industry as a viable and measurable metric. Regulatory compliance and data protection frameworks such as the USA Health Insurance Portability and Accountability Act (HIPAA), the USA Sarbanes-Oxley Act, and the EU Data Protection Directive all require proactive efforts at control of IT infrastructures. And other regulatory environments, such as the Basel II Capital Accord, focus on the concept of "operational risk", including security, in measuring financial and organizational stability [13].

Proactive controls and processes are particularly important in the case of wireless network security, due to the open nature of the technology and the ease with which it may be deployed. Reactive approaches to WLAN security may very well result in extended damage windows as the source of compromise is often more difficult to determine. A strategy that combines robust proactive mechanisms with tested reactive controls represents the best way to implement, improve, and manage wireless network security.

Proactive Approach:




## 5. Wireless Network Attack Scenarios

In creating a WLAN security strategy an organization should consider the ways in which their wireless infrastructure (and by extension their entire network, if connected) may be attacked and/or compromised. Such scenario planning is useful in determining appropriate proactive as well as

reactive strategies to help ensure that security problems are identified and addressed prior to an incident and, should an incident occur, that response plans are adequate.

Wireless security incident scenarios will likely fall into one of three categories: incidents of attack against the network that are known or identified; incidents of attack that are unknown or unidentified; and incidents involving the installation of a rogue AP, which may or may not constitute an attack. Each scenario presents its own set of problems, which may overlap, and demands its own solutions, both proactive and reactive. In some situations one scenario may evolve into another.

### 5.1 Known Attack

A known attack is one in which the organization under attack becomes aware of the attack at some level. Such awareness may be relatively complete, with the nature, systems, and damage known or determined; while others may be incomplete, with certain details known but others remaining undetermined. Known wireless attacks may occur as a result of a user or administrator realizing their system has been compromised; by alerts from logs or intrusion detection systems; or perhaps by equally suspicious but less obvious means (for instance, a security guard noticing an individual sitting across the street with a potato chip can connected to a laptop aimed at the organization's facility.)

By definition, a known attack represents a fait accompli: the attack can not be prevented through proactive measures at the time of discovery. Therefore reactive processes must be engaged to mitigate the threat. While reactive solutions such as IDS or system logs may be useful in reconstructing history in this scenario, the primary value in a known attack scenario will come from the organization's incident response plan. This documented process will determine the course of action necessary to meet all technical, functional, and legal needs of the organization in responding to the attack. For wireless attacks, it is important that the incident response plan and computer security incident response team (CSIRT) understand the nature and unique challenges of a wireless attack, and have a defined plan of action for response. Recommendations for such inclusions in the CSIRT strategy are discussed later in this paper.

### 5.2 Unknown Attack

Unknown attacks represent the most significant fear for an organization. While the attack remains unknown or unidentified, the damage window for the organization remains open, allowing the attacker to harm or otherwise compromise the organization's systems, productivity, and potential revenues. While a worm is fairly easy to identify as bandwidth is utilized and connectivity or productivity slows, attackers looking to compromise specific systems may be harder to discover, particularly if they are sophisticated and take measures to avoid detection. In the case of WLAN infrastructures, it may become more difficult to determine the origin and nature of an attack if the attack utilizes a poorly managed (or unauthorized) wireless network. WiFi hotspots allow increased mobility and anonymity for attackers, as well as providing new vectors for attack through mobile workers. Rogue access points (discussed below) can allow backdoors into the network that may mask or otherwise obfuscate the nature or origin (logical and physical) of the attacker.

Discovering and identifying unknown attacks requires a mixed strategy of proactive and reactive solutions. While effective and pre-defined incident response plans are equally necessary in known and unknown attacks, the CSIRT is limited in its effectiveness before an attack is identified. For an unknown attack, the proactive strategy involves actively identifying the attack as quickly as possible. The attack may not be preventable (in the case of a parking lot attack, a less secure deployment of a WLAN may make it difficult to prevent an attacker from attempting to gain access). However, reactive vigilance (such as a security guard patrolling the grounds looking for suspicious activity) may serve to alert the organization to the attack at the opening of the damage window. Technical solutions such as IDS can, in the same way, alert to an attack or attempted attack as the attack begins and allow for a faster response.

The risk of unknown attack is also an important impetus for proactive testing and analysis of the network security posture. A goal of proactive security is to identify and remediate potential attack vectors before they are utilized by an attacker. Effective policies, system patch management strategies, system hardening, and vulnerability assessments are all proactive components designed to identify and mitigate risks before they are leveraged in an attack, thereby closing the damage window completely.

### 5.3 Rogue Access Points

The installation of access points in an ungoverned or unauthorized way constitutes a third likely scenario for WLAN attack. In the case of rogue APs, the installation may not be part of a deliberate attempt at compromise. WLAN deployments are often viewed as contributing to convenience and productivity and an individual or group may deploy an AP to provide this benefit without realizing or considering the potential security problems such a deployment can produce. In other situations the deployment of a rogue AP is very much a component of a deliberate attack. A surreptitious and inconspicuously deployed AP (for instance in an unused cube with a live network connection) can give an attacker with brief or limited physical access (under the guise of a job interview or a repairman) a direct connection into the internal network that does not demand a physical presence. Attackers can be very clever with the placement of rogue APs. These APs may even be disguised as valid wireless network points rather then the attacker trying to hide the unauthorized network from discovery, and an attacker may attempt to assimilate the AP into the wireless network with different more accessible settings for their client.

Defending against rogue APs, like defending against unknown attacks, requires a mixed proactive/reactive strategy. WLAN deployment policies are necessary to ensure that everyone within an organization understands the policy on wireless networking, as well as physical security precautions that should be taken to avoid allowing malicious placement of the AP. In the rogue AP scenario, configuration of WLAN components plays an important role. WLANs should be configured properly with security and authentication controls necessary to ensure that any AP connected to the internal network is properly vetted and identified, and an AP may not simply be installed and run with both internal and external connectivity.

Testing also comes into play in the rogue AP scenario. Organizations should include testing for rogue WLANs and APs as part of their proactive security strategy. A number of tools and techniques exist for doing so, which will be discussed later in the paper. Finally, should a rogue AP be discovered, the CSIRT and incident response plan should have inclusions for handling this threat. Identifying the nature of the incident (benign deployment versus malicious compromise); risk analysis (how long the rogue AP has been in place and likelihood that it has been utilized by an attacker); and appropriate response (both technical and procedural) all must be considered, preferably prior to the discovery.

## 6. Recommendations and Remediation for WLAN Security

Many best practices for securing wireless networks are similar or identical to practices for securing wired infrastructures, but there are additional controls and processes that an organization can deploy to ensure that WLAN security is incorporated into the larger network security strategy.

### 6.1 Effective and Specific WLAN Security Policies

Perhaps the most important component of WLAN security is an appropriate set of policies that defines and enforces appropriate behavior and activities in deploying, administering, and using wireless network infrastructures. Policies should be developed as part of an overall risk analysis and business justification for the deployment of wireless technology. According to guidance from the National Institute of Standards and Technology (NIST), a U.S. government agency responsible for setting best practices for other government agencies:

> Agencies should not undertake wireless deployment for essential operations until they have examined and can acceptably manage and mitigate the risks to their information, system operations, and continuity of essential operations. Agencies should perform a risk assessment and develop a security policy before purchasing wireless technologies, because their unique security requirements will determine which products should be considered for purchase [14].

Important specific policies for the deployment of 802.11 infrastructures that should be developed by an organization prior to deployment should include:

- **AP deployment and configuration policies** – these policies should limit deployment of 802.11 access points to only those individuals authorized to do so; should require centralized management and accountability for AP installations; and should specify mandatory security configurations and physical locations for any AP deployed.
- **Client and mobile worker end systems policies** – policies should be created to ensure that wireless-enabled mobile systems including laptops and PDAs possess mandatory security functions such as firewalls, virus protection, intrusion prevention, and virtual private networking. These policies should be designed to protect the system and user in open wireless environments such as WiFi hot spots.
- **Acceptable use policies** – organizational acceptable use policies should be extended to specifically include activities conducted over wireless network connections. Users must understand the nature of WLAN technology and that they retain responsibility for their network activities even if they are not physically located within the organization while they are connected.

### 6.3 Wireless Security Configuration Recommendations

Many vendors have implemented standard 802.11 functionality into their products. Security, however, is not always implemented by vendors in the same way, and the first step in secure configuration is to be aware of these differences. Some vendors rely on proprietary, internally developed security protocols to achieve security in WLAN deployments using their products. Such security controls usually require specialized software for the client end system and may not be compatible with other vendors' products. Other 802.11 implementations rely on standards-based security protocols, established by industry and expert communities, and will usually be compatible with other vendors' implementations of the same security protocols in their respective products.

In selecting wireless networking technologies, or in securing WLANs built on these products, it becomes important to realize the specifics of the 802.11 security controls implemented, along with pros, cons, and specific issues inherent in specific products or solutions. In a similar fashion, every WLAN implementation is different, and will have different requirements that bind the configuration options for that wireless network. For example, an "open" commercial hot-spot in a local coffee shop will have a significantly different wireless implementation then a healthcare organization in which wireless users will be sending or receiving medical records or other confidential information over the WLAN. Organizations must understand their unique security requirements, as well as other factors such as industry regulation in deciding configurations of their wireless technology.

Securing a wireless network must start with the network infrastructure, specifically the wireless access point itself. Although APs are layer two devices, they should have an IP address defined for management and for implementing security protocols. Device management should be secured prior to enabling any wireless traffic traversing the device. Every AP should additionally provide a secure means of management for the device itself, in which all management traffic is encrypted, and management traffic should not traverse the wireless network itself.

To this end, most APs have a web server running to allow HTTP management of the device. If the web interface is used for management, Secure Sockets Layer (SSL) or Transport Layer Security

(TLS) should be utilized to protect traffic. This will require a certificate to be accepted by the administrator to authenticate the AP to be managed. Another acceptable management protocol for the AP is Secure Shell (SSH). This will allow the establishment of an encrypted session to the device with proper user authentication. The AP should require a username and password for device access. A strong password policy should be enforced for all users who have access to the device. SNMP, if employed, should follow the same guidelines in terms of using a string for AP access. If available, all management traffic should be routed through a management VLAN that is designated as such and carries no user traffic.

Once the AP is properly and securely configured, the WLAN clients can be addressed. The best approach to 802.11 client security is a defense-in-depth strategy. In a layered defense environment, some of the utilized security measure will thwart unskilled or "script kiddie" attackers, but be fairly simple to defeat by a skilled attacker. However, the additional layers of security will make it increasingly difficult for an attacker to penetrate the network unnoticed. A defense-in-depth strategy will make effective use of both proactive and reactive solutions to achieve a balanced security posture, and will regularly test that posture for vulnerability.

A primary step in securing WLAN clients is to restrict access based on physical layer credentials. This step will employ the use of MAC address filtering and/or authentication. This will allow the access point to deny all frames sent out from the AP to MAC addresses that are not included as part of a pre-approved list. Of course, this practice requires the network administrators to register user MAC addresses. MAC address filtering relies on the AP to filter packets destined to a particular MAC based on a filter rules set. MAC authentication will use an authentication server to determine of the MAC address is valid for use on the wireless network. Physical layer credentials provide significant improvement to overall WLAN security by limiting access to the infrastructure.

In addition to device authentication, user authentication is a next logical best practice. User authentication provides a means of identifying the user on the network for specific policies and access restrictions that may be in place, as well as providing an avenue for encrypting wireless traffic. Wireless user-based authentications should be based on an Extensible Authentication Protocol (EAP) standard. The EAP authentication will provide the framework for the use of dynamic encryption keys. Keys will be dynamically changed based on a predetermined re-keying interval. There are several EAP based standards, each of which has distinct properties. User authentication should be protected to ensure the confidentiality of the username and password credentials. There are several EAP standards that will allow for this protected user authentication. Protected EAP (PEAP) is a very good choice for such a WLAN user access model, encompassing all of the strengths noted above.

Compartmentalization of the WLAN from the wired network is an important component of a layered defense, and accomplished by filtering unnecessary traffic between the two networks. The only traffic that should be leaving the AP for the wireless network is AP management frames and traffic returning to a specific user, which is encrypted. Many wireless networks are congested with traffic that is not required for normal operation of the WLAN and can divulge information and pose a security risk. Administrators should filter all outbound routing protocol traffic, Cisco Discovery Protocol (CDP), and any non-IP based protocols that are not used. This filtering is usually configured on the AP itself; however it may sometimes be configured on the neighboring wired network infrastructure.

A final security configuration recommendation within the scope of this paper is AP management traffic. Such traffic is sent from the AP in clear text, and nearly anyone can capture these frames for processing and potential exploitation. The more limiting these frames can be made, the better for WLAN security. Frames should be configured to limit connection rates for clients, and require them to be within a specific area of the AP to negotiate faster connection speeds. The frames should also be configured to cloak the SSID of the WLAN. This action will prevent an attacker from gaining information on the SSID until another client has associated with the AP.

## 7. Tools and Techniques

### 7.1 Wireless Testing and Audit

An important component of a wireless network security strategy is testing. While configuration and proper design are critical, it is only by testing the resulting infrastructures that an organization can be sure that theory meets practice. By subjecting the WLAN to stress of a type similar to that generated by a probe or attack, insight may be gained into areas of vulnerability that were not previously considered or risks that may have been overlooked or improperly addressed.
In a WLAN security test model, system discovery becomes more important. In order to identify all wireless networks within the signal coverage area of a particular site, a survey must be completed. The survey should be one using all non-overlapping channels. For example, in 802.11b, the non-overlapping channels are1, 6, and 11. The wireless card used to perform the survey will need to verify wireless signals on all of these channels while covering the area of the wireless network implementation. The system discovery will be used to verify all authorized APs are operational and have not been altered. The system discovery will also be used to identify APs that have a signal within the general area of the approved wireless network. This could indicate potential rogue access points, or misconfigured APs that are being used by valid users.

A mapping of the APs is necessary to verify points of access to the wireless network. A mapping will show which access points can be used to access the wireless network and which APs are transmitting their signal to distances outside the acceptable use region of the approved coverage area. A mapping will also identify the client distribution. The clients associated with each AP can be evaluated to ensure there are no inconsistencies in expected client association counts.

With a complete mapping of the wireless access points, the next step in a test is to perform active penetration testing on specific access points. These APs can be tested by first analyzing traffic between the clients connected to the AP for encryption and security vulnerabilities. Identity exchanges will provide information regarding the authentication or encryption protocols in use for access to the wireless network. The wireless frame collected for a particular access point can be used in offline analysis to crack user passwords or the encryption keys. Active penetration may also include steps like circumventing MAC address filtering or obtaining an IP address in a static network environment.

Each AP discovered and verified to be an authorized access point to the wired network should have its configuration reviewed. This configuration review should check for consistency in the AP configurations. In cases where configurations are problematic or non-standard, tools exist that can provide centralized configuration management.

A growing number of tools are becoming available for auditing wireless networks. Some of the tools are commercial, while others are open source and can be used under the GPL license for free. The two most popular wireless network auditing and data collection tools that are available for download and use at no cost are ***Kismet*** and ***Netstumbler***.

Kismet is an open source wireless network sniffing application. This tool is a Linux based tool that will capture wireless network frames in a passive mode, which can then be analyzed in real time or stored and analyzed offline in the standard *pcap* format. Kismet will provide statistics for the detected wireless networks and will allow the user to decrypt traffic on the fly if the encryption key is known.

Netstumbler is a Windows based tool that will identify wireless networks and basic configurations of the APs for each wireless network. This tool provides an easy to use GUI interface that allows the user to quickly identify unencrypted networks and see the clients that are associated with the APs. Netstumbler performs what is referred to as active probing to identify wireless networks. This active probing can be detected and identified by other wireless tools, like kismet, and will alert to the use of

Netstumbler. This probing signature can allow an administrator or other individual to identify the use of Netstumbler in a particular signal area.

### 7.2 Wireless Intrusion Detection

Wireless IDS represents somewhat of a new field at this time. While research is being conducted on WLAN IDS systems [11, 15], few solutions exist at this time, although some commercial tools are beginning to appear [16].

### 7.3 Wireless Incident Response

Should a security incident take place involving an organization's wireless network, it is important to recognize both the similarities and differences between the WLAN and the wired network in conducting incident response activities. For the purposes of this paper, we have selected the ***Response*** phase of the CERT® *Security Knowledge in Practice (SKiP)* methodology to outline these similarities and differences [17]. Regardless of which incident response methodology or plan an organization employs, it is important to include the issues specific to any wireless network infrastructures in that response strategy.

The SKiP methodology is a phased process approach for overall security created and promulgated by CERT®. Phase 5 of the methodology describes steps and actions to take to respond to security incidents, primarily focusing on Analysis, Forensics, Containment, and Public Relations. The Response phase also recommends specific courses of action that can be supplemented to include WLAN technology.

- **Analyze all available information to characterize an intrusion** – in the case of wireless attacks, it may not be possible to isolate the fact that the attack is wireless in nature. However, an organization with WLAN implementations must ensure that these infrastructures are included in incident response plans and that reconstruction of attacks take into account wireless exploitation scenarios. In other cases, it may be obvious that the incident was wireless (discovery of a rogue AP or finding an individual wardriving the organization's parking lot). In these cases, characterizing the intrusion may include physical location of the attacker or the AP, as well as breakdowns in authentication or filtering between the wired and wireless nets.
- **Communicate with all parties that need to be aware of an intrusion** – as with other intrusions, all stakeholders should be kept aware of the incident and progress in response. In some cases, particularly those involving regulatory compliance or other legal issues, the nature of the wireless attack may become important, particularly if sensitive information was mistakenly or negligently transmitted over unsecured wireless networks. Legal guidance should be sought in such situations.
- **Collect and protect information associated with an intrusion** – such collection may be extended to include wireless APs (particularly rogue APs), user access logs, and even surveillance evidence such as security cameras should the attacker have been on or near an organization's property when conducting the attack.
- **Apply short term solutions to contain an intrusion** – actions may include disabling WLAN access or further limiting WLAN and wired network connectivity. Specific users may be identified for scrutiny. Where physical evidence of compromise is discovered (again, rogue APs or unauthorized personnel near premises) it may be necessary to undertake physical sweeps of the organization to ensure that the problem is controlled. In such cases, physical authorities such as security or the police may be necessary to affect the short term solution.
- **Eliminate all means of intruder access** – in addition to mitigating virtual vulnerabilities, the organization may have to consider implementing more robust security controls (see above) within the wireless network. Additionally, the location of APs, physical perimeter

protection, and reviews of building access may require review (in the case of a rogue AP installed by an attacker, it may be necessary to determine how that individual gained physical access to the organization.)

- **Return systems to normal operation** – normal operations may need to include previously unimplemented WLAN security mechanisms and controls, in order to affect this improvement.
- **Identify and implement security lessons learned** – the burgeoning nature of wireless network technology makes it both innovative as well as potentially risky as a technology deployment. Should a wireless incident occur, it may be tempting to simply scrap the technology as too dangerous. This would be an understandable, but ultimately defeatist response. Instead, organizations should take the time to securely deploy wireless infrastructures and test them regularly. An incident is an unfortunate way to learn such a lesson, but such improvements can be achieved.

## 8. Conclusion

Wireless network security poses considerable challenges as WLAN deployments experience seemingly explosive growth. Security and incident response professionals must be aware of the implications and security issues associated with wireless networking regardless of whether or not such networks are being fielded officially in their organizations. The good news is that wireless networks can be made secure with proper planning and diligence. However, given the often less than secure nature of current deployments, incidents are likely to increase as a result of poorly configured or deliberately open WLANs. Properly incorporating this technology into security and incident planning will greatly assist organizations in meeting this challenge.

**Appendix: Rogue Access Point Detection Tool**

Rogue access point detection is the latest and greatest buzz in wireless security, with wireless product vendors building rogue AP detection into their software in some cases. Rogue AP detection may operate in different ways. Some rogue AP detection is based on the signal strength of a wireless network and will literally "point" in the direction of a signal core. Other tools focus on the complete monitoring of the internal network infrastructure to detect rogue access points. The concept of APs is relatively simple, and the detection of such devices should be simple as well.

The only conclusive method of identifying a rogue access point is to specifically identify the MAC address of the AP on the internal network. The MAC address of the AP is identified in the wireless frame by the wlan.bssid field. In testing for a rogue AP, once an administrator has performed monitoring of the wireless network by capturing wireless frames in the space surrounding the authorized access area, they can determine the listing of APs by MAC address.

This tool is a proof of concept tool to show a simple automated search to identify rogue APs on the internal network. This tool will search internal MAC tables of network switches and routers for the given MAC address of a potential rogue AP. The search will be based on a listing of IP addresses to search, with SNMP community strings providing access to the devices. If the MAC address is found the switch will be identified in order for the administrator to track down the port and disable, monitor, or track down the end device.

This tool is currently in final development. Our hope is to make the tool available at the time of the presentation of this paper at FIRST.

**References**


[1] *2004 Intel report – Most Unwired Cities Survey*, retrieved on April 12, 2004 from http://www.intel.com/products/mobiletechnology/unwiredcities.htm.
[2] Bert Sperling, quoted in William Welsh, *San Francisco Tops Wireless Cities List*, Washington Technology, April 13, 2004, retrieved on April 13, 2004, from http://www.washingtontechnology.com/news/1_1/daily_news/23235-1.html.
[3] Infonetics Research, Inc., *Wireless LAN hardware*, February 19, 2004.
[4]Pew Internet & American Life Project, *Pew Internet Project Data Memo*, April 13, 2004, retrieved on April 14, 2004 from http://www.pewinternet.org/reports/pdfs/PIP_April2004_Data_Memo.pdf.
[5] Nikita Borisov, Ian Goldberg, and David Wagner, *Intercepting Mobile Communications: The Insecurity of 802.11*, retrieved on April 10, 2004 from http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf.
[6] Bill Arbaugh, Narendar Shankar, and Justin Wan, *Your 802.11 Wireless Network Has No Clothes*, retrieved on April 10, 2004 from http://www.cs.umd.edu/~waa/wireless.pdf.
[7] Scott Fluhrer, Itsik Mantin, and Adi Shamir, *Weaknesses in the Key Scheduling Algorithm of RC4*, Eighth Annual Workshop on Selected Areas in Cryptography, August 2001.
[8] http://www.wardriving.com
[9] http://quickwired.com/kallahar/stories/2003-Dec10/warflying.php
[10] http://www.warchalking.org/
[11] Yongguang Zhang, Wenke Lee, and Yi-An Huang, *Intrusion Detection Techniques for Mobile Wireless Networks*, Wireless Networks 9(5), September 2003, 545-556.
[12] William Stearns, quoted in Elizabeth Millard, *The Proactive vs. Reactive Security Approach*, February 20, 2004, retrieved on April 10, 2004 from http://processor.com/proeditorial/article.asp?article=articles%2Fp2608%2F38p08%2F38p08%2Easp&guid=2yceyu6m&searchtype=&WordList=
[13] Dan Geer, *Basel II – Being Security Conscious*, April 15, 2003, retrieved on April 3, 2004 from http://www.itsecurity.com/papers/stake1.htm.
[14] Tom Karygiannis and Les Owesn, *Special Publication 800-48: Wireless Network Security*, National Institute of Standards and Technology, Washington, D.C., November 2002.
[15] Joshua Wright, *Layer 2 Analysis of WLAN Discovery Applications for Intrusion Detection*, retrieved March 10, 2004 from http://home.jwu.edu/jwright/papers/l2-wlan-ids.pdf.
[16] Curtis Franklin, Jr., *Two Paths to Wireless Security*, InfoWorld, April 2, 2004, retrieved April 13, 2004 from http://www.infoworld.com/article/04/04/02/14TCwids_1.html.
[17] http://www.cert.org/security-improvement/skip.html


**Non-cited Resources**


Convery, S., and Miller, D., *SAFE: Wireless LAN Security in Depth*, Cisco Systems, Inc., 2002, retrieved on March 25, 2004 from http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.htm.
Elden, C. and Swaminatha, T., *Wireless Security and Privacy: Best Practices and Design Techniques*, Addison-Wesley, Boston, 2003.
Flickenger, R., *Wireless Hacks*, O'Reilly & Associates, Sebastopol, CA, 2003.
Minoli, D., *Hotspot Networks: WiFi for Public Access Locations*, McGraw-Hill, New York, 2003.