Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

# Corporate Wireless LAN: Know the Risks and Best Practices to Mitigate them

In recent years, the hottest high tech trend which has received a lot of publicity and hype is the term Wireless LAN (WLAN). There are more and more organizations of all sizes implementing and using wireless networks or Wi-Fi (Wireless Fidelity) networks. This is due in part to its flexibility and mobility, ease of installations and lower implementation costs compared to installing wired cables. Not only can Wi-Fi technology be seen implemented on private wireless networks, it is also being deployed rapidly on the publ...

Copyright SANS Institute
Author Retains Full Rights

AD
CounterTack
Counter Tack Active Forensics for In-Progress Attacks
GET THE WHITE PAPER NOW >>>

# GIAC Security Essentials Certification (GSEC)
# Version 1.4b
# Option 1

# Corporate Wireless LAN:
# Know the Risks and Best Practices to Mitigate them

**By Danny Neoh**

**December 12th, 2003**

© SANS Institute 2004, Author retains full rights.

**Table of Contents**

1.0 Abstract

2.0 Introduction to WLAN Technology
- 2.1 Different types of WLAN Components
- 2.2 WLAN Standards
- 2.3 Typical Wireless Topology

3.0 Why Wireless is used
- 3.1 Wireless Strengths
- 3.2 Wireless Weaknesses

4.0 Types of Attacks on WLAN
- 4.1 Eavesdropping
- 4.2 Man-In-The-Middle Attack
- 4.3 Spoofing and Session Hijacking
- 4.4 Denial-of-Service (DoS) Attack

5.0 Wireless Security in 802.11 Standards
- 5.1 Wired Equivalent Privacy (WEP)
- 5.2 Wi-Fi Protected Access (WPA)
- 5.3 802.11i

6.0 Recommendations on Wireless Security Best Practices in a Corporate Environment
- 6.1 First Layer – Security Policy
- 6.2 Second Layer – Network Level Security
- 6.3 Third Layer – Host Level Security
- 6.4 Forth Layer – Application Level Security
- 6.5 Fifth Layer – Logging and Auditing

7.0 Conclusion

References

© SANS Institute 2004, Author retains full rights.



© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

## 1.0 Abstract

In recent years, the hottest high tech trend which has received a lot of publicity and hype is the term Wireless LAN (WLAN). There are more and more organizations of all sizes implementing and using wireless networks or Wi-Fi (Wireless Fidelity) networks. This is due in part to its flexibility and mobility, ease of installations and lower implementation costs compared to installing wired cables throughout the organization's infrastructure. Not only Wi-Fi technology can be seen implemented on private wireless networks, it is also being deployed rapidly on the public wireless network via hotspots. These wireless locations can be found in hotels, airports, cafes and restaurants around the world. In fact, WLAN technology has been the fastest growing technology since the Internet. According to Gartner Group research, "The corporate move to wireless is expected to be the biggest technology shift of 2003, 'taking off with a vengeance' in 2004" [1]. However, the benefits of using wireless LAN are not without security risks. Corporations are beginning to realize wireless LANs have been poorly implemented or configured with disregard to information security. Problems include limited to non existent encryption of the network traffic from wireless access points and users setting up illegal rogue access points within their corporate network. There was a recent study conducted by AirDefense in three cities around the United States. They found that 57% of the access points were not using any type of encryption. In addition, there were 9% unauthorized rogue access points found [2].

In response to the number growing of security threats and vulnerabilities on wireless LANs, data security and unauthorized corporate access is something network administrators and information security managers of big and small companies have to worry about. This paper will focus on the risks wireless networks pose and methods for a secure implementation of corporate wireless networking to mitigate the risks. This paper will start by giving an introduction on WLAN technology which includes a brief overview of its standards and components. The paper then covers the advantages and disadvantages of WLAN, then moves into attacks that can take place in a WLAN environment. Lastly, the paper will provide methods on securing corporate wireless networks, which includes wireless security standard and recommendations on wireless security best practices. While it is very difficult to have a 100% secure wireless LAN, this paper will provide some guidance to network administrators to ensure they have a secure wireless LAN to help protect their sensitive data and protect against unauthorized access into their environment.

## 2.0 Introduction to WLAN Technology

The purpose of WLAN network is the same as the wired network which is to provide users connectivity to the network without having a physical network cable attached to the users' workstations or laptops. In other words, the data is transmitted over the air via radio frequencies. In this section, we will take a quick



© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

look at the WLAN components, the recent standards on WLAN technology and its topology.

### 2.1 Different types of WLAN Components

The two WLAN components are the wireless workstation and the wireless access point. The workstation could be a desktop system, laptop or other mobile device with a wireless network interface card (NIC). The wireless NIC will communicate with the WLAN via radio frequencies [3]. They can connect in a ad-hoc mode which is client-to-client or in a infrastructure mode which involves access points. We'll discuss more on this later. An access point is essentially a hub that enables wireless clients to connect to the wired LAN. It has an antenna on one end and is connected to the network via a wire on the other end. Therefore, it is a bridge between wired Ethernet and wireless Ethernet (802.11).

### 2.2 WLAN Standards

The wireless network standards used today 802.11 specifications are defined by IEEE (Institute of Electrical and Electronics Engineers). These standards include 802.11b, 802.11a, 802.11g, 802.1x, 802.11e and 802.11i. But the most common standard used in today's industry is the 802.11b standard. It operates in the spectrum of 2.4 GHz and communicates at speeds up to 11Mbps. As for the 802.11a standard, it operates in the spectrum of 5 GHz and provides speeds up to 54Mbps. 802.11g operates in the spectrum of 2.4 GHz like the 802.11b standard, but it also provides speeds up to 54Mbps [4] [5].

### 2.3 Typical Wireless Topology

The 802.11 standard typically operate in two modes which include Ad-hoc and Infrastructure networks. Ad-hoc networks are where clients are connected to each other via peer-to-peer network using their wireless NIC without involving access points as illustrated in Figure 1.

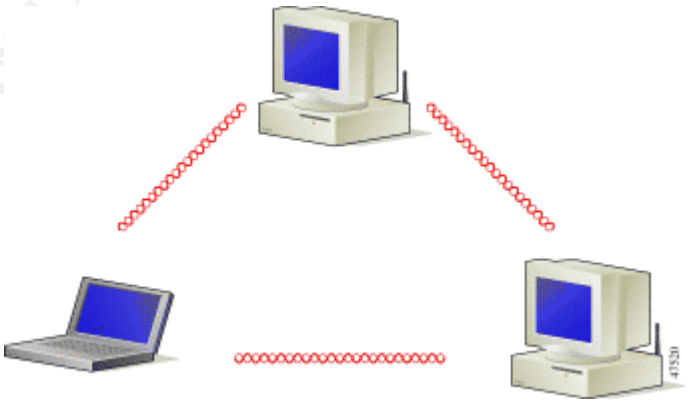

Figure 1: Ad-Hoc Wireless LAN [6]



© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Infrastructure networks involve wireless clients and access points. Wireless clients would connect to each other via one or more access points that are connected to a wired LAN. Infrastructure mode is more common to implement on a larger scale network environment such as within a corporation. Figure 2 illustrates an example of Infrastructure mode.

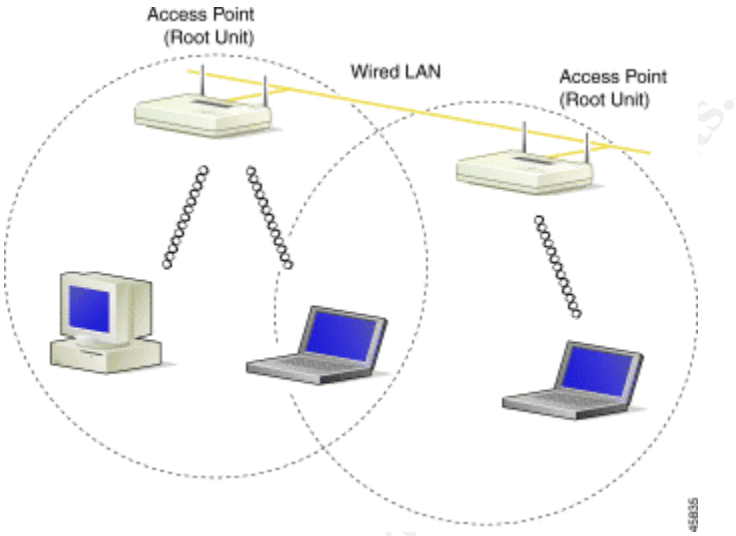


Figure 2: Wireless Infrastructure with Workstations Accessing a Wired LAN [6]

### 3.0 Why Wireless is used

By implementing wireless technology without understanding its associated risks, organizations are prone to hackers' attacks and/or unauthorized access to internal networks carrying confidential data. Using wireless has many advantages due to its flexibility and ease of implementation. Often network administrators overlook the importance of wireless security. Therefore, administrators need to understand the strengths and weaknesses of wireless so they can take the appropriate steps to address those security issues.

### 3.1 Wireless Strengths [7]

- Faster to deploy - Without the hustle and bustle of laying Ethernet cables through walls or ceilings, wireless is definitely easier and faster to implement.
- Reduced Cost of Ownership - In certain corporations that operate under a dynamic environment, which involves frequent moves or changes, then wireless network could help save on overhead costs of relocating or relaying new cables. Additionally, it saves a lot of time to install.
- Mobility and Flexibility - Users who are on the move could actually connect to the network in order to access information that enables them to perform their job more efficiently. Indirectly, this could improve the productivity and effectiveness of an employee.


© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

- Scalability – Wireless LAN is easily configured and changed accordingly to the corporations' needs to run certain applications. In addition, the technology is fairly scalable to meet most needs of any company.

### 3.2 Wireless Weaknesses [8] [12]

- Unauthorized Rogue Access Points - WLAN are sometimes too easy to implement. It only requires an employee to deploy a rogue access within an organization's network. It does not require any form of security measures and can be installed without the knowledge of the IT staff. This opens up a wide window of opportunity for hackers to exploit vulnerabilities.
- Poorly configured Access Points - Access points that are improperly configured could broadcast Service Set Identifiers (SSIDs) of authorized users and allow intruders to steal this information in order to access a corporation's network. SSID resembles an identity where wireless devices need to communicate within the wireless LAN. So in order for a wireless client to connect to an access point, the SSID needs to match.
- Network Abuses – Since the speed of the wireless networks is still less compared to wired networks, any abuse on the wireless network could impact the performance of WLAN. For example WLAN users will encounter network performance degradation due to network congestion when users are doing large file transfer across WLAN. The WLAN 802.11 standard is a shared media until after it gets onto the network. Additionally, the protocol requires large headers for each packet transferred.

## 4.0 Types of Attacks on WLAN

Despite the many advantages WLAN can provide, there are many associated security risks hackers can exploit. Below are a few types of attacks that could take place on wireless networks:

### 4.1 Eavesdropping [9]

Eavesdropping is also known as a passive attack where an attacker monitors the network and intercepts data that is transmitted over the WLAN. This type of attack is the easiest as attackers can easily use network traffic tools such as TCPDump or Airsnort to capture network traffic for their analysis. This can be done at a distance away from an organization's premises. Once the attacker manages to gather enough sensitive information they can gain unauthorized access to an organization's network. An attacker can then launch more damaging active attacks.

### 4.2 Man-In-The-Middle Attack [9]


© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

A man-in-the-middle attack involves an attacker who is impersonating the wireless access point. By placing themselves between an access point and a valid client, attackers are able to intercept data that sent between the two wireless components. The traffic valid clients send to the attacker will be forwarded to an access point and the reply from the access point to the client will be forwarded back by the attacker as well. This way, the attacker will be able to obtain valuable information such as authentication requests or any secret key that may be in use. Figure 3 illustrates an example of Man-In-The-Middle Attack.

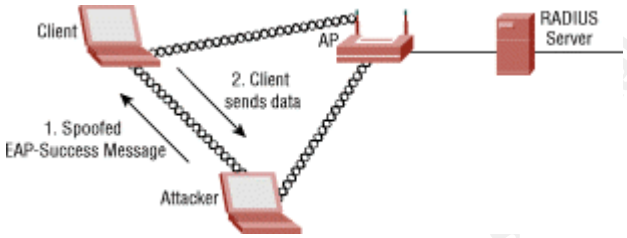


Figure 3: Man-In-The Middle Attack [19]

### 4.3 Spoofing and Session Hijacking [9] [10]

A spoofing attack occurs when an attacker assumes the identity of a valid WLAN user by using their valid IP or MAC addresses to gain access to the corporation network. Once this is done, the attacker can launch a hijacking session by intercepting the connections established by a valid client to an access point. The session can then be used to access sensitive information and resources within the corporation's wireless network. There are methods to prevent unauthorized access into the wireless network. For example, MAC filtering which only allows authorized MAC addresses to connect to the wireless network. However, bear in mind a MAC address on a wireless device can be easily tampered with by changing certain parameters in the registry for Windows and executing root shell commands in Unix. Figure 4 illustrates an example of Session Hijacking Attack.

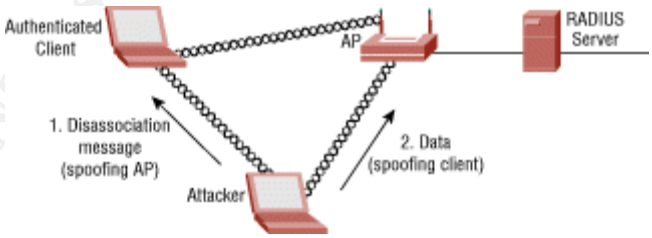


Figure 4: Session Hijacking Attack [19]

### 4.4 Denial-of-Service (DoS) Attack [9][11]

This type of attack is different from most other attacks because the attackers don't intend to gain unauthorized access to your network to steal sensitive information. Their real intention is to bring down your organization's network so valid users cannot access network related services which could have huge business impacts to your corporation. Due to the fact that the WLAN has a


© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

relatively low transmission bit rate (802.11b at 11 Mbps), it is easy for an attacker to launch a DoS attack by sending an ICMP ping flood from the wired network towards the access points via the fast Ethernet interface. This will cripple the access points because they cannot handle the large amount of traffic. In addition, an attacker could also prevent the communications between the access point and the clients by jamming specific radio frequencies. The attackers can achieve this by generating strong radio signals to disrupt the frequency range that is in used.

## 5.0 Wireless Security in 802.11 Standards

With all these security threats towards wireless networking, IEEE has produced and continued to work on security technology to improve the security for wireless networks. We will take a look on the few major security features that have evolved over the past few years which include WEP, WPA and the supposedly silver bullet to wireless security that is 802.11i.

### 5.1 Wired Equivalent Privacy (WEP) [12] [13]

Wired Equivalent Privacy or often known as WEP is the encryption standard for wireless networking. WEP is designed to provide privacy of individual transmission similar to the privacy found on the wired LAN environment. It offers the most basic level of security for WLAN and it is the easiest to implement as well by just enabling the encryption key on the access points as well as clients. By enabling WEP, the data becomes encrypted using the RC4 encryption algorithm before transmission over the air. The receiving end such as access points or wireless clients would decrypt the data through shared key authentication to authenticate the clients. This means only clients who have the same secret key issued by the access points will only be able to decrypt data. However, WEP is known to have security flaws after it was first ratified in September 1999. WEP is vulnerable because it typically uses a weak 40-bit key and relatively short 24-bit Initialization Vectors (IVs) to encrypt data. Since the IVs have only 24-bit long combinations, WEP will eventually use the same IV for multiple data packets once all the key combinations had been used up. It would only take approximately one hour for the IVs to be repeated for a large busy corporate network. This would lead an attacker to easily decrypt any of the 802.11 frames once enough were collected with the same IV. All that is left is to figure out is the same shared secret key, which can be accomplished with the help of some hacking tools. To make the situation worse, WEP uses static shared secret key and no dynamic key distribution. This means that the network administrators and users would use the same keys for a long period of time which allows the hackers enough time to hack into the WEP enabled WLAN.

### 5.2 Wi-Fi Protected Access (WPA) [14] [15] [16]


© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

With so many security flaws on WEP, the IEEE members and the Wi-Fi Alliance had to come out with a temporary fixed with a stronger security standard to address the security flaws found in WEP. This standard is called Wi-Fi Protected Access (WPA). WPA is the subset of the upcoming 802.11i or also known as WPA2 which is to be ratified on the first quarter of 2004. But until then, WPA provides the best enterprise wireless security.

WPA can be considered an enhanced and improved version of WEP. Not only does WPA increase the initialization vector (IV) from 24-bits to 48-bits so hackers will have a harder time cracking an encrypted message since the number of possible shared keys has increased, WPA also provides a stronger encryption scheme called Temporal Key Integrity Protocol (TKIP). TKIP provides dynamic key distributions. It generates a new encryption key for every 802.11 packet. This will protect against replay attacks. In addition, TKIP also includes a Message Integrity Code (MIC) or sometimes referred to as “Michael”. Basically MIC will check for data integrity using a checksum security technique. MIC compares the numerical value in terms of number of set bits in the transmitted message with the received message. If the numerical value is different, this means that the message has been garbled or manipulated. This would protect against packet forgeries.

Furthermore, WPA also utilizing 802.1X and the Extensible Authentication Protocol (EAP) to strengthen the user authentication process which is not present in WEP. Basically this would allow users to authenticate against a central authentication server such as a Remote Authentication Dial-In User Service (RADIUS) server before being allowed to join into the corporate wireless network to avoid any security breach.

In order to use WPA, it will involve upgrading the firmware of WEP enabled devices. Note: Most corporations with existing wireless networks in place will most likely choose to wait for the release of 802.11i before taking any actions towards upgrading or implementing changes. Although WPA addresses all known problems with WEP, it does not protect against the denial-of-service (DoS) attacks. This will be incorporated later in the paper when discussing the appropriate security practices and strategy in order to avoid a DoS attack in a corporate network environment.

### 5.3 802.11i [15] [16] [17] [18]

The upcoming security standard and maybe the silver bullet to resolve the wireless security issue is 802.11i or WPA2 which expected to be ratified on the first quarter of 2004. This version is quite similar to WPA which is an enhanced security version of WPA. 802.11i will also use the 802.1X/EAP framework similar to WPA to ensure mutual authentication and dynamic key management. In addition, WPA2 features a new encryption scheme which is called Advanced Encryption Standard (AES). AES is a stronger encryption method approved by


© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

the US National Institute of Standards and Technology (NIST). AES is a symmetric block cipher which encrypts data in blocks of 128 bits using variable cipher key lengths of 128, 192 or 256 bits. In addition, 802.11i is more robust than the 802.11 security standard because it has two strong authentication features such as Wireless Robust Authentication Protocol (WRAP) and Counter with Cipher Block Chaining Message authentication code Protocol (CCMP). However, one thing to note is the new investment in hardware or hardware upgrades may be needed for implementing the AES feature from WPA2. Is 802.11i the answer to wireless all security issues that we are faced today? Only time will tell.

## 6.0 Recommendations on Wireless Security Best Practices in a Corporate Environment

Wireless LANs in a corporate environment should be implemented as secure as possible. However the wireless security in 802.11 standards as discussed previously is considered weak and has many security vulnerabilities that can be exploited by an attacker. An organization is subject to monetary loss or even bankruptcy if an attacker is able to successfully penetrate a corporate network via wireless. An attacker can steal sensitive data or launch a malicious virus attack which leads to network services unavailable. The best defense against wireless is to not implement it at all. But with wireless's many advantages especially in a fast pace corporate environment, IT managers are trending toward with wireless deployments. So it is important to ensure you have a secure wireless LAN.

Securing wireless LANs in a large corporate environment is no easy task. This section will provide some guidance to network administrators or IT managers when implementing a secure wireless network. In my opinion, the best method on implementing a secure wireless LAN in a corporate environment is to use the Defense In Depth method as learned from attending the SANS Training seminar. Defense In Depth constitutes a ring architecture with multiple security layers where each layer has its security functions [20]. Figure 5 illustrates Defense In Depth model.


© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

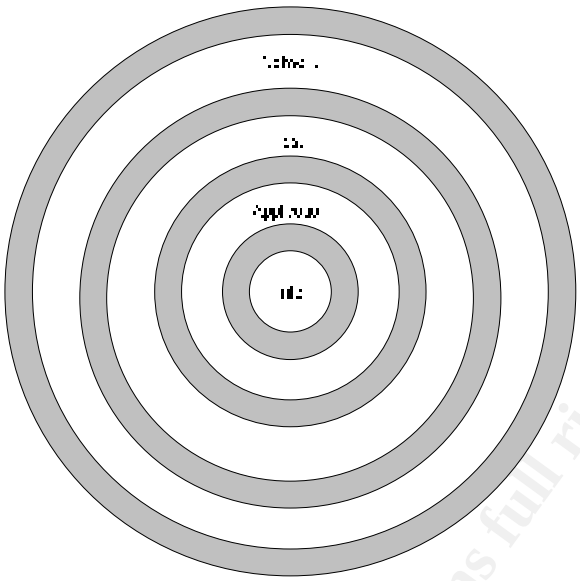

Figure 5: Defense In Depth Model [20]

Based on this model, we would structure the best practices in a layered model which consists of the following:
(Please note that the word 'Layer' mentioned below does not refer to the OSI or TCP model.)

- First Layer – Security Policy
- Second Layer – Network Level Security
- Third Layer – Host Level Security
- Forth Layer – Application Level Security
- Fifth Layer – Logging and Auditing

### 6.1 First Layer – Security Policy

Wireless LAN implementation in a large corporation without any security policies will put the corporation at serious risk. In fact, all organizations should have a security policy in regards to wireless LAN infrastructure in place before reaching the deployment stage. In order to have a strong security policy, an organization should build its wireless LAN policies on its existing corporate security networking policies. Following are some best practices on security policy on wireless implementation: [21] [22]

- Implement a set of policies on wireless network security and clearly identify the ownership of those policies. Review those policies regularly to ensure security control when new risks are identified.
- The placing of access point locations is important. Before implementing a wireless LAN and during the planning phase, you need to know who are your users and where are they seated in order to ensure the access point signal is adequate to cover the necessary areas. This will also help to


© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

avoid the signal to leak outside of the premise where outsiders could detect the wireless network. Make sure when installing the access points, try to avoid outward facing walls or windows and install the access points closer to the buildings' centre. In addition, try to lower the access point broadcast signal wherever it is possible.

- Scanning and detecting for rogue access points on the corporate network regularly is a must. Wireless access points are easy to install. Users could simply just put one access point into the corporate network without properly configured security features. This would leave your corporate network door wide open for hackers to launch attacks. Tools like NetStumbler can be used to scan and search for any unauthorized access points.
- The default management passwords and SSIDs on access points should be changed prior to installing them into corporate network. Strong passwords should be used when changing the passwords with at least 8 characters in length and should include at least one alphabetic, one numeric and one special character.

In order to have a secure wireless network especially in a large corporate environment, everyone in the organization should own the security responsibilities and not only network administrators or IT managers [21]. This means that user education on wireless policies should not be taken lightly.

- Educate users to be aware that corporate security is everyone's responsibility and users will share the cost of any security breaches.
- Enforcing the security policy that employees should not simply install rogue access points into the corporate network without the knowledge of the corporate IT staffs.
- Educate users to be aware of the security risks when using their laptops to connect via ad-hoc mode especially in public places. In addition, they should connect using infrastructure mode when connecting to corporate network environment.

### 6.2 Second Layer – Network Level Security

At this layer, network level security will establish terms of authentication, encryption and authorization on installing wireless network connectivity between wireless clients to the internal protected network via access points.

- **Isolation of Wireless LAN**
  The wireless LAN should be implemented on another network separate from your internal wired LAN. This means that the access points should be installed on a separate network with a firewall in placed between the wireless network and the wired corporate network. The network traffic that travels from the wireless network to the wired network will have to go


© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

through the firewall with authentication verification and strong encryption [23].

- **Securing Wireless LAN with VPN Solution**
  As discussed earlier, there are many security vulnerabilities found with WEP. It is recommended to include Virtual Private Network (VPN) solution into your wireless LAN to ensure secure wireless connections. In other words, VPN allows user from a wireless network environment to establish a secure connection into the corporate private network. VPN forms a tunnel between two communicating points and the data that travels across would be encrypted and protected from unauthorized access and preventing events such as eavesdropping and man-in-the-middle attacks. VPN is considered to be reliable as it uses secure encryption algorithm such as Internet Protocol Security (IPSec) for data packets authentication and digital certificates for public keys validation [23].

- **Authentication and Authorization via RADIUS**
  Before allowing a wireless client to connect and access to the corporate private network, it is a must to validate or authenticate that client. This can be achieved by using 802.1X authentication on a remote authentication dial-in user service (RADIUS) server. The wireless client would communicate with the RADIUS server that is located at the corporate LAN via the access point. The RADIUS server would then validate the client credentials and send data with security keys to the access point to allow secure connectivity with the client, if the client is authorized to connect. Otherwise, the connection would be refused and the wireless client would not be able to connect into the corporate wireless network [23]. This will help defend against attacks such as man-in-the-middle and denial-of-service.

A sample design on a secure wireless network on this layer is illustrated on Figure 6:


© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

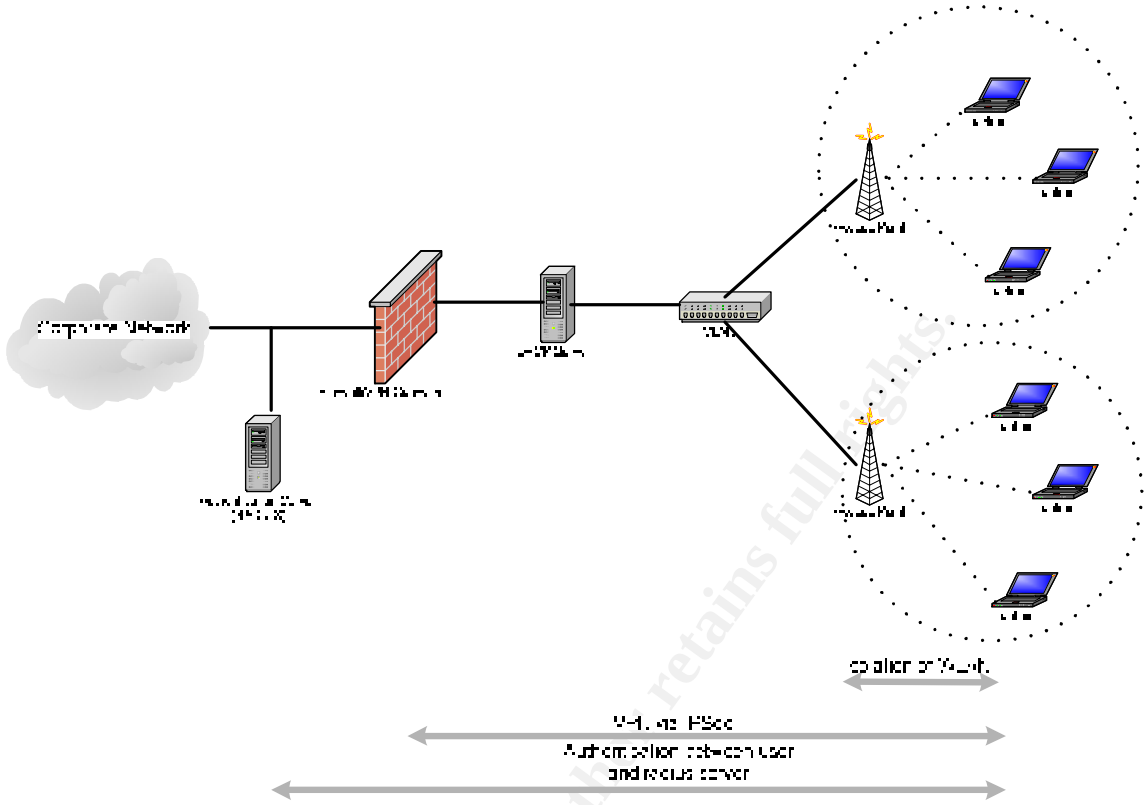

Figure 6: Secure Corporate Wireless LAN [23]

### 6.3 Third Layer – Host Level Security

In this section we will see host level security in terms of access control on the wireless devices such as access points.

- **Handling the SSIDS**
  The default SSIDs on the access points should be changed prior to installation into the corporate network. When changing the SSIDs for the access points, please ensure to use something special and do not use something obvious such as your organization's name. In addition, ensure to change the SSID regularly. In case the SSIDs are compromised by a hacker, they will become unusable in a short period of time. Another important thing to note is to disable the broadcast SSID option where most of the access points are set to broadcast SSID by default. Even though by disabling broadcast on SSID, a hacker will still have a way to sniff the SSID by using Kismet software, but at least it provides an obstacle for potential hackers [22] [24].

- **WEP Encryption**
  WEP encryption should always be enabled with at least 128-bit or higher. Although WEP is considered to have many security flaws, it still provides a


© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

layer of protection to the wireless communication and leaves users better off than no protection at all [22].

- **Access Control via MAC Addresses and IP Addresses**
  Access points can be configured to filter MAC addresses to control users connecting to your corporate wireless network. This means those users with valid MAC addresses that had been configured on access points will be allowed connectivity to the wireless network. Those without valid MAC addresses will be rejected. One thing to bear in mind is that MAC addresses could easily be spoofed by a hacker but at least it requires an additional effort from the intruder to hack into the network.
  Another method of access control is through IP addresses. By using Dynamic Host Configuration Program (DHCP) server to restrict the maximum number of DHCP addresses allocated to the potential maximum number of users on the network. Since IP addresses can be spoofed, if there are users unable to get access into the wireless LAN, there may be some unauthorized access into the wireless LAN that needs investigation [22].

### 6.4 Forth Layer – Application Level Security

Application level security should not be taken lightly as it plays a big role to ensure your wireless network stays secure.

- **Securing wireless clients**
  Normally an attacker would prefer to choose their prey on wireless clients as it bypasses the external firewall. Therefore it is important to have the wireless clients installed with personal firewalls such as BlackIce or ZoneAlarm. This will prevent attackers to hack into the wireless client and use it to access the corporate wireless network environment [25]. In addition, any hotfixes or security patches released on the operating system running on the wireless clients such as Windows XP or Windows 2000 should be applied immediately after certifying in a corporate environment [26].

- **System Hardening**
  Hardening your corporate systems is very important. Please bear in mind that this level of security will be the final defense against intruders. If a hacker managed to hack in via a wireless client and by-pass all security layers described previously, there must be an additional layer of protection before reaching your corporate's vital information or servers. System hardening is taking security measures such as installing and configuring systems and applications to meet strict security requirements. For example it is always a good practice to remove any services on your systems that you do not need to use. Also, try to disable services that you think that you might use it sometime in the future but not currently. In


© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

addition, always remember to patch, patch and patch your systems. Whenever there are new security and application patches available to fix certain security vulnerabilities, you need to apply the patches or hotfixes on the systems as soon as possible. It is a good practice to test the patches or hotfixes on a test environment first before applying onto production systems. Finally, enforce the principle of least privilege. Only allow users restricted permissions and rights to access systems or applications. Allow users enough access to enable them to do their daily jobs [27].

### 6.5 Fifth Layer – Logging and Auditing

After successfully implementing the wireless network with various security measures, it is always a good practice to audit, test, and measures security policies you have established to check for any vulnerability or any improvements required.

- **Test, test and test again**
  Testing is the best method to audit your wireless network. This will allow you to find any vulnerability within your wireless network and enable you to take appropriate actions to overcome any security risks. You should also "War-drive" your own corporation. This means searching around for access point signals that can be used to gain access to your network. Software such as NetStumbler can be used for "war driving" [28]. Another option an organization should consider is to hire external security consultants to test your security implementations as well as review your policies [29].

- **Security Expertise Required**
  Security is the most important element to safe-guard corporate critical information. However security is not an easy task to handle especially in a large corporate environment where it requires experience and capable IT staffs to manage information resources [29]. A suggestion is to establish a Security Operations Center (SOC) consisting of IT employees that are well-trained in security. The team's main responsibility is to attend to all corporate security matters not only on wireless security, but also on information technology (IT) security as a whole.

- **Vulnerability Scanning**
  It is a good practice to have run vulnerability scans on your corporate wireless network regularly for any vulnerability. Scanning regularly will help you identify and resolve vulnerabilities before attackers have a chance to exploit your wireless network. One thing to note is that ensure you have obtained permission and informed the appropriate parties before doing a network vulnerability scan to prevent any false alarms being picked up by the intrusion detection system (IDS) [30].


© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

- **Account Auditing and Logging**
  When an employee is terminated or no longer with the organization, ensure a process in place to revoke that employee's access to network resources as quickly as possible. For example removing their account from the RADIUS authentication server or servers that they have access to previously. This is to prevent disgruntled or hostile employees from doing something malicious towards the organizations critical systems [29]. In addition, it is good practice to audit user accounts against the current list of employees within the organization to ensure that no false accounts were made or old user accounts are found residing within the system. Furthermore, the logging function on the firewall and intrusion detection system (IDS) should be turned on and monitored by the Security Operations Center (SOC) team. The SOC can take appropriate actions or steps according to the corporate security policies in the event of unauthorized access to the wireless network or strange activities taking place on the corporate wireless network.

## 7.0 Conclusion

As more corporations start to implement wireless networks due to user demand, the IT staff for the organization must recognize the security threats wireless poses. Businesses need to plan and take proper security measures before and after implementing wireless networks in their environment to protect valuable data against any potential attack. The wireless security in 802.11 standard such as WEP has so many vulnerabilities, which an attacker could exploit. The recently released WPA has better security functions but is still new in the market. Many corporations that already have implemented wireless would rather wait for 802.11i to be released somewhere in 2004 next year before upgrading their networks.

A corporate wireless network is best protected by following the security best practices using a defense in depth method. This would include security measures at different layers such as network layer, application and host layer. In addition, having a proper wireless network security policy in place and audit your corporate wireless network regularly will also help strengthen the wireless security. If a corporation cannot afford to implement all five security layer approach due to cost or resource reasons, at least prioritize which layered approach is best suited to your corporate environment and implement them accordingly. On the other hand, corporations should add more security measures to their wireless environment whenever they see fit to mitigate the risk of being attacked and not just on the five layers as described in this paper. With that, I shall end this paper with a quote from the instructor Eric Cole during the SANS Seminar on September 2003 in Boston "Keep adding on the security layer and not taking them away. Complement on and not replacing with".


© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

References

[1] Gaudin, Sharon. “Gartner Predicts Wireless Boom” March 11, 2003
URL: http://itmanagement.earthweb.com/erp/article.php/2107961

[2] AirDefense. “War Drive of Atlanta, Chicago & San Francisco:
57 % of Enterprise Wireless LANs Not Encrypted” September 2003
URL: http://www.airdefense.net/eNewsletters/Sept03/feature.shtm

[3] Karygiannis, Tom & Owens, Les. “Wireless Network Security 802.11, Bluetooth and Handheld Devices” section 3-1 to 3-4
URL: http://csrc.nist.gov/publications/drafts/draft-sp800-48.pdf

[4] Burns, Jim & Hill, John. “Evolution of WLAN Security” October 4, 2003
URL: http://www.mtghouse.com/MDC_Evolving_Standards.pdf

[5] Holloway, Damien. “A Guide to Wireless Networking and Deployment” Jaunary, 2003
URL: http://www.hill.com/archive/pub/papers/papers.asp?yr=2003&mn=01

[6] Reference Document. “Cisco Aironet Wireless LAN Client Adapters”
URL:
http://www.cisco.com/en/US/products/hw/wireless/ps4555/products_installation_and_configuration_guide_chapter09186a00801241ec.html#1037868

[7] Reference Document. “What is a Wireless LAN”
URL: http://www.wlana.org/learn/educate1.htm

[8] AirDefense. “WLAN Security Risks”
URL: http://www.airdefense.net/wlans/risks.shtm

[9] Shimonski, Robert J. “Wireless Attacks Primer” February 24, 2003
URL: http://www.windowsecurity.com/articles/Wireless_Attacks_primer.html

[10] Peikari, C & Fogie, S. “Network Attacks”. May 15, 2003
URL: http://www.informit.com/isapi/guide~security/seq_id~20/guide/content.asp

[11] Gast, Matthew. “Seven Security Problems of 802.11 Wireless” May 24, 2002
URL: http://www.oreillynet.com/pub/a/wireless/2002/05/24/wlan.html?page=1

[12] Shimonski, Robert J. “Wireless Security Primer 101” December 16, 2002
URL:
http://www.windowsecurity.com/articles/Wireless_Security_Primer_101.html

[13] Geier, Jim. “802.11 WEP: Concepts and Vulnerability” Wi-Fi Planet June 20, 2002



© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

URL: http://www.80211-planet.com/tutorials/article.php/1368661

[14] Vaughan-Nichols, Steven J. “Protecting Your 80211 Network with WPA” Wi-Fi Planet May 21, 2003
URL: http://www.wi-fiplanet.com/spring03/article.php/2210441

[15] Geier, Jim. “WPA plugs holes in WEP” Network World March 31, 2003
URL: http://www.nwfusion.com/research/2003/0331wpa.html?page=3

[16] Wi-Fi Alliance. “Wi-Fi Protected Access: Strong, standards-based, interoperable security for today’s Wi-Fi networks” April 29, 2003.
URL:
http://www.wifialliance.com/OpenSection/pdf/Whitepaper_Wi-Fi_Security4-29-03.pdf

[17] Eaton, Dennis. “Diving into the 802.11i Spec: A Tutorial” November 26, 2002
URL: http://www.commsdesign.com/design_corner/OEG20021126S0003

[18] Federal Information Processing Standards Publication 197. “Announcing the Advanced Encryption Standard (AES)” November 26, 2001
URL: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[19] Cisco Aironet Response to University of Maryland's Paper,
"An Initial Security Analysis of the IEEE 802.1x Standard"
URL:
http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_bulletin09186a00800a9e74.html

[20] Cole, Eric., Fossen, Jason., Northcutt, Stephen & Pomeranz, Hal. SANS Security Essentials with CISSP CBK Version 2.1 Volume One. SANS PRESS. Page 292 – 294, A130

[21] Reference Document. “Wireless Security Best Practices”
URL:
http://www.intel.com/business/bss/infrastructure/wireless/security/best_practices.htm

[22] Karagiannis, Konstantinos. “Ten Steps to a Secure Wireless Network” February 25, 2003
URL: http://www.pcmag.com/article2/0,4149,844020,00.asp

[23] Reference Document. “Deploying Secure Wireless Networks: Intel’s strategies to minimize WLAN risk” May, 2003
URL: http://www.intel.com/business/bss/infrastructure/security/secure_wlan.pdf



© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

[24] Reference Document. "Wireless Security—Four Steps You Need to Take" URL: http://www.linksys.com/edu/page10.asp

[25] Cole, Eric., Fossen, Jason., Northcutt, Stephen & Pomeranz, Hal. SANS Security Essentials with CISSP CBK Version 2.1 Volume One. SANS PRESS. Page 670

[26] Cole, Eric., Fossen, Jason., Northcutt, Stephen & Pomeranz, Hal. SANS Security Essentials with CISSP CBK Version 2.1 Volume Two. SANS PRESS. Page 1082, 1264

[27] Norem, Jeff. "Outline for a Successful Security Program" September 26, 2003
URL: http://www.sans.org/rr/papers/index.php?id=1208

[28] Cole, Eric., Fossen, Jason., Northcutt, Stephen & Pomeranz, Hal. SANS Security Essentials with CISSP CBK Version 2.1 Volume Two. SANS PRESS. Page 1321 – 1322

[29] Reference Document. "VPN and WEP: Wireless 802.11b security in a corporate environment" January, 2003
URL: http://www.intel.com/business/bss/infrastructure/security/vpn_wep.pdf

[30] Cole, Eric., Fossen, Jason., Northcutt, Stephen & Pomeranz, Hal. SANS Security Essentials with CISSP CBK Version 2.1 Volume One. SANS PRESS. Page 690, 724 – 725

© SANS Institute 2004, Author retains full rights.



© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Last Updated: May 26th, 2013

# Upcoming SANS Training

**Click Here for a full list of all Upcoming SANS Events by Location**

| | | | |
|---|---|---|---|
| **SANS Malaysia @ MCMC 2013** | **Cyberjaya, MY** | **Jun 03, 2013 - Jun 08, 2013** | **Live Event** |
| **SANS Pen Test Berlin 2013** | **Berlin, DE** | **Jun 03, 2013 - Jun 08, 2013** | **Live Event** |
| **Industial Control Systems Security Training - Houston** | **Houston, TXUS** | **Jun 10, 2013 - Jun 15, 2013** | **Live Event** |
| **Security Impact of IPv6 Summit 2013** | **Washington, DCUS** | **Jun 14, 2013 - Jun 16, 2013** | **Live Event** |
| **SANSFIRE 2013** | **Washington, DCUS** | **Jun 14, 2013 - Jun 22, 2013** | **Live Event** |
| **SANS Canberra 2013** | **Canberra, AU** | **Jul 01, 2013 - Jul 13, 2013** | **Live Event** |
| **Digital Forensics & Incident Response Summit 2013** | **Austin, TXUS** | **Jul 09, 2013 - Jul 16, 2013** | **Live Event** |
| **SANS London Summer 2013** | **London, GB** | **Jul 09, 2013 - Jul 16, 2013** | **Live Event** |
| **SANS Rocky Mountain 2013** | **Denver, COUS** | **Jul 14, 2013 - Jul 20, 2013** | **Live Event** |
| **SANS Mumbai 2013** | **Mumbai, IN** | **Jul 22, 2013 - Jul 27, 2013** | **Live Event** |
| **SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification** | **Washington, DCUS** | **Jul 22, 2013 - Jul 26, 2013** | **Live Event** |
| **SANS San Francisco 2013** | **San Francisco, CAUS** | **Jul 29, 2013 - Aug 03, 2013** | **Live Event** |
| **SANS SEC 560: Network Penetration Testing @ Bangalore 2013** | **Bangalore, IN** | **Aug 05, 2013 - Aug 10, 2013** | **Live Event** |
| **SANS Boston 2013** | **Boston, MAUS** | **Aug 05, 2013 - Aug 10, 2013** | **Live Event** |
| **Critical Security Controls Summit** | **Washington, DCUS** | **Aug 12, 2013 - Aug 18, 2013** | **Live Event** |
| **Industrial Control Systems Security Training - DC** | **Washington, DCUS** | **Aug 12, 2013 - Aug 16, 2013** | **Live Event** |
| **SANS Thailand 2013** | **Bangkok, TH** | **Aug 19, 2013 - Aug 31, 2013** | **Live Event** |
| **SANS Virginia Beach 2013** | **Virginia Beach, VAUS** | **Aug 19, 2013 - Aug 30, 2013** | **Live Event** |
| **Mobile Device Security Summit 2013** | **OnlineCAUS** | **May 30, 2013 - Jun 06, 2013** | **Live Event** |
| **SANS OnDemand** | **Books & MP3s OnlyUS** | **Anytime** | **Self Paced** |