GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Wireless LAN Security Concerns

SANS Security Essentials Network Security
GSEC V1.4
vanleng001

Albert Van Lengen

Abstract

Wireless Local Area Networks are becoming as ubiquitous as wired LANs. Wireless technology is allowing the network to go where wire cannot go. The purpose of this paper is to assist IT Managers in the decision process when implementing a Wireless Network. My intention is to give IT managers a primer on 802.11-based LANs and the potential security risks that an enterprise can open itself to if they do not take appropriate precautions before implementing this technology. This includes conducting an adequate risk analysis before implementing wireless network technologies.

Technology such as "Bluetooth" is often thrown into discussions on wireless networks. However, Bluetooth and similar technologies are intended to be "cord-replacement" technologies, such as replacing a USB or Parallel cable to connect a PDA, Cell Phone, Printer or other devices. Bluetooth is working within the IEEE 802.15 Personal Area Network standards. It is intended to be short range (30 feet, slower data rates 1 Mbs), compared with 300 feet or more and 11 Ms with 802.11- based technologies. Again, this paper will focus on the 802.11-based wireless networks.

© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Introduction to Wireless LANs

"International corporate IT industry spending on wireless applications will reach an average of $680,000 in 2002, a dramatic 94 percent rise over $360,000 in 2001." (According to a new report by the World Information Technology and Services Alliance (WITSA) and the Wireless IT Research Group (WIRG) released at the 2002 World Congress on IT in Adelaide, Australia)

Why are wireless networks becoming such a draw? First, you no longer have to drop cable to every desktop and, second, your users can connect from just about anywhere on your corporate campus. Wireless LAN's provide always-on network connectivity while allowing office workers to roam throughout a building without being bound by wires. Wireless LANs seem to be low cost and easily deployed.

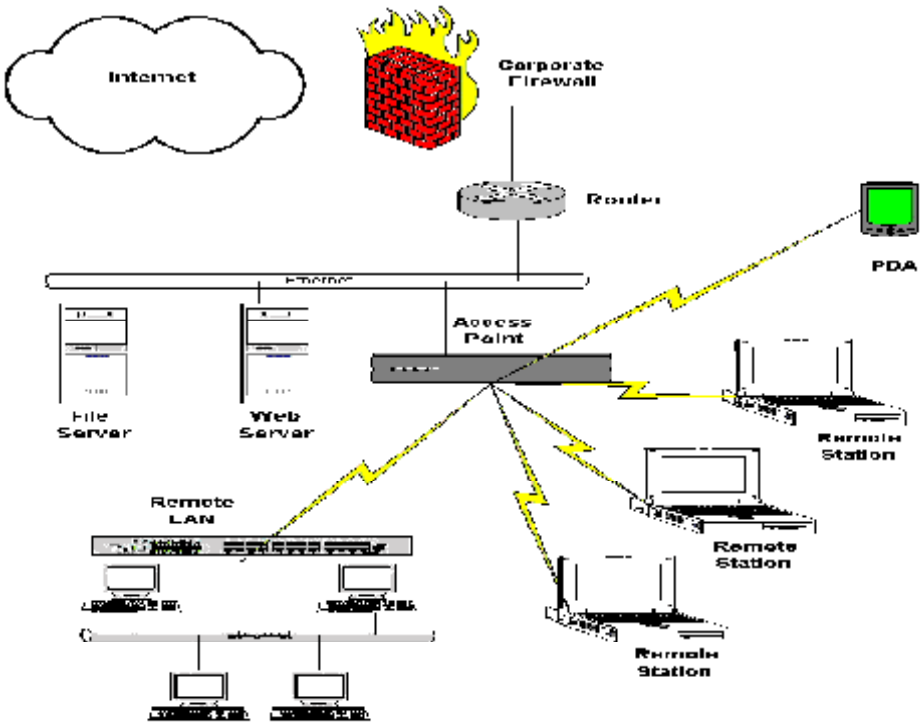
However, organizations are rapidly deploying wireless infrastructures without thoroughly understanding the technology and the inherent risks. "Wireless LANs are broadcasting secrets of enterprises that have spent millions on Internet security." - John Pescatore, Gartner research director.

There are a number of issues that anyone deploying a wireless network needs to be aware of. In most wired LANs, cabling is secured within a building or physical infrastructure so a would-be hacker would have to first defeat physical security measures. Since wireless networks are using radio frequencies that are usually not hindered by physical constraints, would-be hackers have access to your network from your parking lot or maybe even the building next door. To combat this problem, designers developed a user authentication and data encryption system known as Wired Equivalent Privacy, or WEP. Unfortunately, some compromises were made in developing WEP that have resulted in it being much less secure than intended. We will discuss issues with WEP later in the paper.

Wireless LAN Architecture

Basic 802.11-based wireless LANs can be set up in two ways: peer-to-peer (or ad-hoc) and infrastructure (or client/server). In the peer-to-peer configuration, clients running the same specification communicate with similar clients in the general vicinity. This configuration works well for mobile LANs. In the infrastructure configuration, on which this paper will focus, clients communicate through an access point that acts as a bridge between the wired LAN and the wireless clients. If several access points are located in the vicinity of each other, they must communicate on different channels in order to avoid radio interference.

© SANS Institute 2000 - 2005 Author retains full rights.



Typical Wireless LAN Topology

Basic infrastructure wireless LANs can be used as an extension of your wired LAN. It consists of a Basic Service Set (BSS), which includes two or more wireless nodes, or stations (STA's). In the Infrastructure mode, the BSS contains at least one Access Point (AP). The purpose of the AP is to form a bridge between the wireless and wired LANs. STA's communicate with the AP through a wireless Ethernet card.

IEEE 802.11

IEEE 802.11-based wireless LANs come in a variety of flavors: 802.11, 802.11a, 802.11b, and 802.11x. New flavors are also being developed. Each is designed to replace Ethernet cables.

The original specification, 802.11 was adopted in 1997. The specification provided 3 channels of just 2 Mbs wireless connectivity using part of the unlicensed 2.4-GHz radio spectrum. It also included Wired Equivalent Privacy, (WEP).

In 1999, the Internet Engineering Task Force adopted 802.11b. 802.11b provides 3 separate channels in the unlicensed 2.4Ghz range. It improves connectivity to 11 Mbs, which is more than adequate for most business applications. 802.11b is the most commonly used standard today.

The Ethernet Compatibility Alliance developed WiFi to promote standards

© SANS Institute 2000 - 2005 Author retains full rights.

among 802.11b devices. In theory, this should allow companies with WiFi certified Access Points & Ethernet Cards to communicate between one another. I only mention in theory because each product may have proprietary security or other features that may need to be inactivated to properly communicate with another company's product.

802.11a was adopted about the same time as 802.11b. 802.11a operates up to 13 channels in the unlicensed 5 GHz range. It increases connectivity up to a possible 54 Mbs. 802.11a also adapts to a broadcasting technique that breaks the signal into multiple sub-signals to help avoid interference.

Additional 802.11x specifications are being introduced. As of the writing of this paper, 802.11b is the most popular standard, with 802.11a devices starting to enter the market place. In all cases they also include the Wired Equivalent Privacy (WEP).

Wired Equivalent Privacy (WEP)

The intention of WEP was to provide a level of privacy equivalent to that ordinarily present in wired LANs. Wired LANs are usually protected by physical security measures within a facility and do not incorporate encryption. Since wireless LANs are not protected by a physical boundary, their transmissions penetrate walls. WEP was added to the 802.11 standard to provide a level of privacy equivalent to a physical boundary such as a wall.

WEP is an optional encryption scheme that offers a mechanism for securing wireless LAN data streams. WEP uses a symmetric scheme where the same key and algorithm are used for both encryption and decryption of data. For WiFi certification, vendors must support 40-bit encryption keys. Vendors implement encryption and decryption in either software or, vendors such as Cisco, will implement using hardware accelerators to minimize the performance degradation of encrypting and decrypting data streams.

WEP has two main goals, access control and privacy. WEP prevents unauthorized users from gaining access to the network. Unauthorized users would not have the WEP Key. Additionally, WEP provides privacy by encrypting data streams and only users with the correct WEP key can decrypt the data stream.

Authentication within the 802.11 standard can either be either Open System or Shared Key. Under the Open System, any STA may request authentication. The AP may grant authentication to all requestors or only to those on an access list. In either case, the entire process is done in clear text. Under the Shared Key authentication, the AP will send the client a challenge test packet that the client must encrypt with the correct WEP key and return to the AP. If the client has the wrong key or no key, it will fail authentication and will not be allowed to

© SANS Institute 2000 - 2005 Author retains full rights.

associate with the AP.

Wireless LAN Vulnerabilities

Security concerns have been raised in the IEEE 802.11 wireless local area network (WLAN) environment. The vulnerability of wireless LANs is increased due to having no real physical barriers. They are susceptible to eavesdropping, jamming, insertion and any other attacks known to wired LANS. Lets look at some of the reasons wireless LANs are vulnerable.

Each AP has a Service Set ID (SSID). A SSID is a string used to define a specific AP or a common roaming domain between multiple AP's. If WEP is not enabled, SSID's are broadcast in the clear, allowing the SSID to be captured by monitoring the network. AP's also come with default SSID's for each manufacturer. If the default is not changed, the AP SSID is easily compromised. SSID's, if configured correctly, can act as a basic password for the client to connect to the network.

As I mention before, WEP defines an authentication and encryption method. Authentication methods are used to protect against unauthorized access to the network. Encryption is used to prevent eavesdroppers from decrypting captured transmissions. WEP can be usually configured in three ways: No Encryption (WEP Turned Off), 40 Bit Encryption, and 128-bit Encryption. Most AP's are shipped with WEP turned off.

WEP encryption is based on RC4, which uses a 40-bit (or a 104-bit) and a 24-bit random initialization vector (64-bit or 128-bit encryption) to encrypt wireless data transmissions. The same key must be used on all clients and access points for communications.

A widely publicized analysis of WEP's security was performed by a team of researchers at the University of California at Berkeley (www.isaac.cs.berkeley.edu/isaac/wep-faq.html). Their analysis suggests that WEP is subject to a variety of attacks using inexpensive off-the-shelf equipment. They suggest that we do not rely solely on WEP for security of our wireless LAN.

Another issue with WEP is that the keys are common among the desktop cards and access points within the same wireless LAN, and they do not automatically change on a regular basis. A hacker using statistical analysis tools can crack a WEP key from a wireless LAN with typical levels of traffic in less than 24 hours. Network managers are reluctant to update WEP keys because it is a tedious process of going to each end user's device to make the changes.

© SANS Institute 2000 - 2005 Author retains full rights.

Implementation Issues of Wireless LANs

Wireless LANs do not include network and security management tools like those with wired LAN infrastructure. Tools that address airwave security, authentication, and user rights are absent from wireless LAN. Therefore, when implementing a wireless LAN, you need to insure you integrate tools between wireless LANs and wired LANs.

Wireless LAN implementation issues can be classified into three categories: Authentication Methods, Key Management, and Security Methods. To insure adequate authentication in a Wireless LAN environment, it is necessary to integrate with existing user administration tools. Utilize tools such as Remote Authentication Dial-in User Service (RADIUS), and Lightweight Directory Access Protocol (LDAP)-based. You should consider creating a group under these tools to enable for wireless access. Only members that belong to the group are granted access. Also, identify users by their user-name not their MAC address to provide monitoring of user level usage, accounting, and auditing

Lack of key management protocol is a limitation to providing IEEE 802.11 security services. Static Keys are difficult to manage on STA's and APs. Proprietary Key management solutions require separate user databases. Current IEEE 802.11 security options for access control do not scale appropriately in a large infrastructure network. Lack of inter-access point protocol (IAPP) further compounds key management issues when STA's roam from one AP to another.

With all of these vulnerabilities, why would you want to implement a wireless LAN? Your workforce is becoming more mobile. There are times when it is not possible or practical to install cables, but network connectivity is required. With wireless LANs, users can access shared information without looking for a place to plug in. Network managers can set up or augment networks without installing or moving wires.

There are many things that can be done to protect your network and lessen the likelihood of an attack. Most of these will fall into two approaches, risk analysis and establish a defense in depth. First address and define the risks, then do what you can to minimize the risks. Second, develop and implement a defense in depth. No single mechanism should be relied upon to provide total security. As with wired LANs, when implementing wireless technology, we must use a layered system of defenses that are integrated to make a hacker's job as hard as possible. These layered systems include risk analysis, administrative and monitoring tools, procedures, policies, and training.

Risk Analysis and Risk Mitigation

The best time for a risk analysis is before you have implemented a technology

© SANS Institute 2000 - 2005 Author retains full rights.

and before you have been hacked. Regardless of whether or not you are implementing wireless technologies, it is essential to undergo risk assessment and mitigation procedures. Not all risk can be mitigated, therefore we must determine how to reduce risk to an acceptable level and take prudent measures to avoid unnecessary risks that might damage the enterprise. Acceptable risk must be defined within the context of an organization and the legal environments in which they operate. If we are going to implement a wireless LAN, we must identify and understand the risks so that they can be minimized. As with any risk analysis, we measure the risk for severity so that we may implement appropriate counter measures.

Risk analysis is critical in determining what security controls should be put in place. An effective risk analysis team must involve a mix of senior management, business operations, and security professionals along with IT professionals. They should address the following questions:

1. **What are you trying to protect?** First we conduct an asset inventory. This requires a complete inventory of all of your informational assets: people, hardware, software and data (paper and electronic). This is called an asset inventory.

2. **Who or what are you trying to protect it from?** This next step is referred to as a ***threat*** analysis. For each of the assets listed, identify all of the possible things that can threaten the asset. This includes threats of nature, physical threats, internal and external threats, mistakes, sabotage, viruses, hackers and cyber terrorism etc…

3. **What would be the business impact (cost) if we lost that asset?** To put it a different way, calculate the value of the informational asset. In many cases, it is not practical or feasible to calculate a dollar value for the asset; in most cases, it is sufficient to assign a number (1…5) or a code (High, Medium or Low) for the value.

4. **What is the likelihood of loss or compromise?** This is a ***vulnerability*** assessment. Think of as many weaknesses and vulnerabilities as you can. Include physical access, training, passwords, oversight, bad programming, accidents, malice (both internal and external) etc…How likely is it for you to have a compromise?

5. **Can we live with that?** Calculate the risks. Risk is a probability representing a degree of uncertainty for loss or harm. It is generally calculated using: **Risk = *Threat x Vulnerability*** The values assigned to threat and vulnerability are often very subjective. Regardless, this simple formula shows that a high threat tied to a low vulnerability will yield a low level of risk.

© SANS Institute 2000 - 2005 Author retains full rights.

Risks should be listed in descending order. For each risk, a determination must be made as to whether the risk is an acceptable or unacceptable risk.

Risk mitigation requires that for every risk, one or more ways be implemented to reduce the risk. These are often called counter measures. A cost vs. benefit calculation should be performed for each counter measure.

There are many ways to mitigate risks but they all require good policies and procedures. Other counter measures may include using good passwords, installing anti-virus software, keeping patches up to date, deploying firewalls and network intrusion detectors, using trip wire or other file integrity testers, developing check lists for system administrators to follow – just to name a few.

Information security policies and procedures are the single most important risk mitigation technique. Security policies and procedures put into writing, the organization's overall security posture, assign responsibility, grant authority and describe the organization's risk mitigation strategies. Policies and procedures are also required before "monitoring and detection" and "incident response" strategies can be implemented. For example, a system administrator should not test the strength of user passwords, by running a password cracker, unless an approved written security policy authorizes him or her to do so. From SANS Institute:

A. "Policies must be implementable and enforceable."
B. "Be concise and easy to understand."
C. "Balance protection with productivity."
D. "State reasons why policy is needed."
E. "Describe what is covered by the policies."
F. "Define contacts and responsibilities."
G. "Discuss how violations will be handled."

The risk mitigation and security policies must provide for some means to monitor, detect and report security incidents. The most common means of monitoring and detecting are through daily log analysis, network based intrusion detection systems and host based intrusion detection systems. When a security incident is discovered, there should be mechanisms in place to report the incident and, if necessary, activate an incident response plan.

Defense in depth is an important concept in information security. The idea behind defense in depth is to not rely upon one form of protection but to develop multiple layers of defense. Deploying a firewall between your network and the internet (at the perimeter), deploying a network intrusion detection system inside the firewall and, installing host based intrusion detection systems on your servers is one example of defense in depth. Running anti-virus software on your mail server, anti-virus software on your file servers and, running anti-virus software on your workstations is another example of defense in depth. Keep

© SANS Institute 2000 - 2005 Author retains full rights.

defense in depth in mind when evaluating counter measures.

Recommendations

As with implementing any technology, conducting an adequate risk assessment and mitigating the risk is essential to good security. As discussed in this paper, 802.11b has several vulnerabilities that you should be aware of before implementing. If you have already implemented 802.11b, here are a few recommendations to assist in protecting your network from attack:

- Enable 128 bit WEP on the AP
- Enable WEP for both authentication and encryption
- Change the WEP key on a regular basis

If your are looking to implement 802.11b in the near future, consider using vendor-offered, proprietary, centralized security management tools for: Central WEP key distribution, STA access control, and IP filtering firewall.

Central WEP Key Distribution: The centralized AP controller can manage the entire wireless network including all security parameters. For Example, all APs can be updated simultaneously with new WEP keys through the centralized management controller.

STA Access Control: Using Remote Authentication Dial-In User Service (RADIUS), or Light-weight Directory Access Protocol (LDAP)-based.

IP Filtering Firewall: The centralized AP controller can implement an IP firewall to protect sensitive network resources. Network administrators can specifically enable access to selected wired network resources; all non-authorized network resources will not be bridged to the wired network.

For long-term security recommendations, implement 802.1x and VPN Tunneling.

802.1x is currently a draft standard for port based network access control. Port-based network access control uses the physical characteristic of the switched LAN Infrastructure to provide a means of authenticating devices attached to a LAN port, and for preventing access where the authentication process fails.

VPN Tunneling is commonly used to create a secure means of communication over an insecure link, such as remote access via the Internet to a company network for e-mail or other network access. It ensures security through both user authentication and encryption with user authentication in the system, where the user name and password are encrypted. The legality of log-on location is checked and the MAC address may be verified as valid. Strong encryption methods such as RC5 and Triple-DES can be used with VPN Tunneling. It also

© SANS Institute 2000 - 2005 Author retains full rights.

maintains interoperability among different AP vendors and 802.11 STAs.

Implementing 802.11 WLAN networks can be burdensome especially when dealing with security issues. Always conduct a Risk Assessment before implementing new technologies.

References

Arbaugh, William; Shankar, Narenda; Wan, Justin Y.C. "Your 802.11 Wireless Network has No Clothes"
Online: http://www.cs.umd.edu/~waa/wireless.pdf

Blackwell, Gary. "Serious WLAN Security Threats: Part1"
Online: http://www.802.11-planet.com/columns/article/0,,1781_949891,00.html

Blackwell, Gary. "Serious WLAN Security Threats: Part2"
Online: http://www.802.11-planet.com/columns/article/0,,1781_947571,00.html

Borisov, Nikita; Goldgerg, Ian; Wagner, David. "Security WEP Algorithm"
Online: http://www.isaac.cs.berkley.edu/isaac/wep-faq.html

CISCO. "Overview, Wireless LAN Security"
Online: http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w_ov.html

Haber, Lynn. "Defend you WLAN"
Online: http://www.zdnet.com/enterprise

Janzen, Eric. "Understanding Basic WLAN Security Issues"
Online: http://www.802.11-planet.com/columns/article/0,,1781_937241,00.htm

Phiffer, Lisa. "Improving WLAN Security"
Online: http://www.802.11-planet.com/columns/article/0,,1781_92871,00.html

SANS Institute. "Information Assurance Foundations: Security Essentials"
Vol. 2.1, Version 1.8, 2001.

Schroeder, Max. "Wireless Security"
Online: http://www.cconvergence.com/article/CTM20011031S0013

Yassmin, Asma. "Known Vulnerabilities in Wireless LAN Security
Online: http://www.tml.hut.fi/Studies/Tik-110.300/1999/Wireless/Vulenerability_4.html

"The Unofficial 802.11 Security Web Page"
Online: http://www.drizzle.com/~aboba/IEEE/

© SANS Institute 2000 - 2005 Author retains full rights.