

Columbitech White Paper

August 2004

Security Threats in Wireless LAN

To streamline business processes and thereby increase overall productivity, organizations are deploying wireless enabled devices with online access to central back office systems. However, with increased mobility comes new security threats. A wireless network is highly exposed to attacks and is more difficult to manage than traditional wired technology. This, in combination with Wireless LAN products that implement weak security standards, composes a threat to the entire corporate network.

The intent of this whitepaper is to analyze the security threats associated with wireless LAN in a corporate environment. More specifically it addresses the problems related to securing wireless LAN in the vertical sectors, where the infrastructure, in whole or in part, is composed of legacy units and systems. This whitepaper uses the term “corporation” as a general entity to represent enterprises, organizations, institutions, etc.

Security Threats in Wireless LAN

Introduction.....	3
Security Threats in Wireless LAN	4
Availability	4
Integrity.....	5
Confidentiality.....	6
Security – Always About the Whole Picture	8
Identifying the Weakest Link.....	8
Securing a Legacy Environment	10
Approaches to WLAN Security	11
Built-in Security	11
Vendor Specific.....	12
VPN	13
Conclusions.....	14
References.....	15

Introduction

A wireless LAN architecture consists of a set of access points and wireless-enabled mobile units. Even though the software used to manage the system and the hardware used to operate the wireless infrastructure come from different vendors, they should interoperate seamlessly and provide a homogeneous and secure communication platform. In the real world however, wireless LAN products from different vendors do not necessarily interoperate seamlessly, instead they provide different capabilities in terms of performance and, more importantly, security. This is particularly true when the solution includes legacy units. The legacy unit may for many reasons not support the latest security standards and protocols required for a secure wireless LAN deployment. The reason could be a non-standard operating system, lack of processing and memory capabilities, old RF technology, or lack of a proper user interface.

A common scenario is an environment with a mix of different wireless units, some of which may support strong security algorithms, such as IPSec, WPA and 802.1x, and some of which may not. The IT security department is thus forced to use the least-common-factor approach, enforcing a level of security that all units can provide. Since a system is never more secure than its weakest link, this approach does not always provide a security level that complies with the corporate security policies. What good is it to use 802.1x security on the Pocket PC based handhelds when the network has to be left practically wide open to allow access for legacy units?

The following paragraphs briefly describe some of the various attacks that can be mounted on a wireless LAN system, why it is so important to take measures to protect against those attacks, and the different security mechanisms available today.

Security Threats in Wireless LAN

In order to deploy an effective corporate security policy it is important to first initiate and execute a proper threat analysis. Not only is it important to define the potential security threats but also to define what services and assets that need to be protected, as well as the value of those assets, the cost of having them compromised, and what security services are required to protect them. Critical security services are usually divided into:

- *Availability* – prevents disruption of a service.
- *Integrity* – prevents unauthorized modification of systems and information.
- *Confidentiality* – prevents unauthorized disclosure of sensitive information.

Availability

To disrupt or disable a system or service, an attacker can mount a *Denial-of-Service (DoS) Attack*. A DoS attack aims to prevent or deny legitimate users access to a system resource. Instead of attempting to access critical data at the target systems, DoS attacks try to overwhelm the target system with bogus and/or defective data to prevent it from working properly. The attacker seeks to consume all available resources or to exploit bugs in the target computer's operating system. DoS attacks come in a variety of forms and can be divided into three basic types:

- Consumption of scarce, limited resources.
- Destruction or alteration of configuration information
- Physical destruction or alteration of network components.

Some DoS attacks can be launched on a sophisticated high-end system or network by using only very limited resources. Such an attack is often called an asymmetric Denial-of-Service attack and it allows a hacker with a standard PC or slow modem to disable a much larger system.

A large-scale DoS attack may involve hacking into a large number of computers that are to be used in the actual attack on the target system. This type of attack is called *Distributed Denial-of-Service attack (DDoS)*. There are as many flavors of DoS attacks as there are Hackers, but some of the attacks have been extensively executed and are widely known, for instance:

SYN-ACK Attacks or TCP-SYN Flooding

An attacker exploits the 3-way TCP connection establishment mechanism by initiating a large number of connections without responding to the server's acknowledgments. Since TCP is a stateful protocol, SYN-ACK attacks force the server to store each acknowledgment packet in a backlog queue. Finally the server's queue will be overflowed and the server can no longer respond to new connections.

Teardrop Attacks

The goal is to hang or crash the target system by purposely sending fragmented IP packets with an overlapping offset value. The target system will be unable to reassemble the packet fragments, and this can sometimes cause the system to crash.

Smurf Attacks

Smurf attacks take advantage of the direct broadcast addressing mechanism by broadcasting forged ICMP echo request packets across multiple subnets using a spoofed IP address. The ICMP echo request and the corresponding reply messages are flooding the network, resulting in severe network congestion.

It is, in general, extremely difficult to protect a system against DoS attacks. If the attacker is dedicated enough the attack will probably be successful, causing the mission critical target system to fail. For example, an attacker with a powerful radio transmitting at the same radio frequencies as the corporate wireless LAN could cause a system to become partially or completely unavailable. A well-designed security architecture would however ensure that the damage caused by such an attack would be limited and temporary.

An effective defense against DoS attacks should include several layers of protection, including strong user authentication and a first line of defense mounted as close to the network edge as possible, preventing a possible DoS attack on centralized systems. It is usually preferable that a wireless switch or edge router takes the beating instead of a central ERP system, since the latter would cause the whole enterprise system to fail.

The most common DoS countermeasure is to deploy a strong firewall policy, preferably distributed as close to the network edge as possible. The cost for managing and operating the system increases with the distributed security, and this cost needs to be included in a general threat analysis.

Integrity

Instead of damaging a system or service by making it unavailable, an attacker can modify, or inject bogus data into, the target system. The attacker does not usually reveal himself and the fact that the system has been compromised may be unknown for a long time. A silent integrity attack can be mounted to compromise the integrity of the data in an ERP system, which could potentially lead to liability issues. There are a number of well known attacks used to compromise a system's data integrity. Examples of such attacks are:

Man-in-the-middle Attacks

In a man-in-the-middle attack the hacker is able to read, and possibly modify at will, messages between two parties without letting either party know that they have been attacked.

Replay Attacks

A replay attack is a breach of security in which an attacker stores and retransmits information to trick the receiver into unauthorized operations, such as false identification or duplicate transactions. Without proper replay protection, it is possible for an attacker to record messages sent during the authentication of a legitimate user and later use these messages to get access to the system.

Injection Attacks

By exploiting a system's lack of integrity control and user authentication, an attacker can silently inject corrupt data into the system. Even though user authentication is

enforced by a specific application, an attacker can utilize the lack of integrity control to inject corrupt data by gaining control over an already authenticated user session.

The attacks mentioned above can be handled effectively by using protocols for strong integrity control as well as by enforcing a policy that allows only authenticated communication. Integrity control is implemented by applying a mechanism that digitally signs each transmitted message. A message that was not properly signed will be treated as a bogus message and will be discarded by the receiving peer. There's a number of different signing algorithms; some provide strong security while others give not more than an imaginary level of security.

The enforcement of strong authentication usually has a negative impact on the end user experience and will most likely not receive a warm welcoming from the people who are going to use the system. Nevertheless, authentication is extremely important and the challenge for the corporate IT security department is to find a solution that provides strong security that does not have a negative impact on the usage of the system.

Confidentiality

Not only is it important to secure the network infrastructure and the services hosted within. It is equally important to protect the information transferred between the mobile units and their corresponding hosts. A fixed local area network environment does not usually require the transmitted data to be protected, unless the information is very sensitive. In a wireless local area network environment, on the other hand, an attacker does no longer need to be onsite to listen in on the network traffic. A standard wireless LAN access point has a range of several hundred meters and special purpose long range antennas can significantly further increase the coverage. Anyone who's within this range and equipped with a compliant radio card can potentially read all the information transmitted on the network.

Today, data networks are used for various services and carry a great deal of sensitive information. It could be credit card numbers, banking information, proposals or sensitive ERP data. Therefore it is of the utmost importance to apply strong encryption when utilizing wireless networks. The security issues related to wireless communication were addressed some time ago in the 802.11 wireless LAN standard by including the WEP security system. WEP specifies a set of algorithms for securing the wireless network from unauthorized access. However, some design flaws in the protocol specification makes WEP totally insecure, allowing a number of different attacks to be successfully mounted on a WEP enabled system.

Even when proper encryption is being used, it is possible for someone to eventually break into the system, either by exploiting weaknesses in the encryption algorithm, as is the case with many known attacks on the WEP system, or by guessing the password or encryption key used to protect the data.

Cryptographic Attacks

A cryptographic attack targets a known weakness in the encryption algorithm. A *ciphertext-only attack* is the simplest form of attack. By passively collecting encrypted messages, an attacker could eventually find out the encryption key and thus gain access to the network. Most encryption protocols used today do not allow

ciphertext-only attacks to be executed in a timely fashion, except for the encryption algorithm in the WEP standard. In a *partial cleartext attack*, an attacker collects encrypted messages, in some of which he knows the corresponding cleartext counterpart. With a certain number of cleartext/ciphertext message pairs, the encryption key can be calculated in a reasonable timeframe. Again, this attack assumes some weaknesses in the protocol - this could be known encrypted information that is repeatedly transmitted, or padding areas where the padding data is known to the attacker.

Dictionary Attacks

Also known as *brute force attacks*. Passwords and encryption keys created by a human being often include a name or a word that has some form of meaning. A dictionary attack exploits this fact and uses a dictionary to try to find the right password. A computer with a reasonable amount of computing resources could easily, within minutes or hours, guess a password. It is therefore important to define a strict password policy, requiring the passwords to be of a certain length and complexity. Also, the security system should be able to detect a dictionary attack and take proper actions, for example locking out the user account that is being attacked.

Security – Always About the Whole Picture

When people talk about information security they usually mean data encryption. Although encryption is a core component in any security system, one must not forget that it is just one of several security services needed to make information and services unavailable for unauthorized third parties. As stated before, in order to define a security policy that fulfills the corporate security needs, it is important to make a complete analysis, identifying the services and systems that need to be secured, the security threats against those systems, and the cost of having them compromised or unavailable.

In some cases, the actual data in transit is more or less useless for any third party eavesdropper. It could be pricing information sent from an in-store unit, product IDs or warehouse statistics. So, if the data is not sensitive, why does it need to be secured and why should the corporation bother with implementing a security policy? One needs to look one step further; the data itself may not be very sensitive, but the systems holding the data could be. Once again we need to focus on the threat analysis and more specifically on the part including the cost of having the corporate back office systems offline. Without proper security, an attacker can not only listen in on traffic but also inject false data into the system, compromising the system's integrity, and mount denial-of-service attacks that completely disable a system. Imagine the cost in terms of lost revenue for a large retailer having its point of sales systems off line for a half day due to a disabled back office server. In a best case scenario, the attack did only affect the targeted branch office or local store, in a worst case scenario, the attacked branch office system was used to mount a larger attack to disable vital parts of the global corporate systems.

With this in mind it is easy to see how a non-existing or badly implemented security policy can be a costly mistake. Indeed it is a great challenge to secure a wireless enabled system and the key to success is to realize that no security system is stronger than its weakest link.

Identifying the Weakest Link

As discussed in the previous paragraph, hiding information in transit is just one of several essential security services. Strong access control, user authentication and virus protection are other, equally important components needed to secure a corporate information system. An information system can roughly be divided into the following:

- The data in transit
- The corporate network, including network entities, services and systems
- The mobile device

Equal attention should be paid to each IS component in order to eliminate the weakest link. *Data in transit* is defined as any information sent (possibly through the air) between any two network entities or systems. When the data is sent wirelessly, the need for strong encryption is bigger, due to the higher risk of the data being intercepted. True for all encryption mechanisms used today is that they are breakable

Security Threats in Wireless LAN

in theory, (this is not true for encryption based on the laws of quantum mechanics but those systems are not applicable to a wireless environment). This means that someone with enough computing resources can break any encryption system. However, if a reasonably strong encryption key was used, breaking it would require tens or hundreds of years even for the most powerful computer in the world. Therefore, in practice you could state that an encryption system is totally unbreakable. There are of course encryption standards that can be broken, even in practice. One example of such a system is the built-in security protocol (WEP) in the 802.11 wireless LAN standard. Some serious design flaws in the protocol make it possible for an attacker to break the encryption key and inject modified data into the network.

Let's assume that the data is encrypted with a strong algorithm that can withstand any cryptographic or brute force attack. The transferred data is thus secured and no unauthorized party can make use of the information. However, this information is eventually stored somewhere, probably in some back office system, located on a server inside the corporate network. If an attack can not be carried out on the data while in transit, an attacker is likely to focus on attacking the target system that holds the information he wants. While one can never prevent someone from picking up transmitted radio waves, it is possible to restrict access to the corporate network and the systems located within. This is usually done by enforcing access restrictions and strong user and/or device authentication. Access to the network can be restricted to specific hosts and applications by deploying firewall technology at the network edge, and user authentication can be made at different levels in the system, ranging from link layer to application access.

Even though firewalls are being deployed at the network edge, the mobile units must somehow be allowed access to their backoffice systems and applications. Thus the firewall must be configured to accept connections to specific hosts and applications. How can we make sure that these "holes" in the firewall are used only by authorized users and not by an attacker? This is when user authentication comes into the picture. Without mechanisms for strong user authentication it is practically impossible to know who is accessing the system and feeding data into it, a fact that should upset any corporate IS manager.

By enforcing data encryption, access control and user authentication, we are able to secure the information and the supporting systems, both when the data is in transit and when it is stored, but is this enough? What about the mobile units? Is it not possible that the mobile unit itself stores some piece of information that could be sensitive in some means, i.e. cached application data, user credentials, or security parameters? What happens if a mobile unit gets stolen? Can someone get access to the network by extracting information stored inside a stolen unit? This is not at all impossible but, in fact, quite likely. Imagine an attack where a virus or some piece of program is loaded onto one of the mobile units. When the device connects to the network, this program can legitimately access some target system and execute a backdoor to be used to later access the system.

As has been showed in this chapter, securing an information system is always about the whole picture. Encryption, authentication, access control, and device management are equally important components in a general security policy. If one of them is missing or is badly implemented, then it won't matter how strong encryption keys the

corporation uses, or how secure the access control mechanisms are. The system will nevertheless be insecure and unable to withstand an attack.

Securing a Legacy Environment

Securing a wireless LAN system is undoubtedly one of the greatest challenges for a corporate IT security department. How do you make sure your system is secure? Or more importantly, how do you realize your system is not? The complexity of the problem can be greatly reduced if the system is homogeneous and built on open platforms.

In a legacy environment however, applications and hardware are usually proprietary technology, often developed for a specific environment or customer. Lack of standardized interfaces and APIs makes integration difficult. As long as the system works and fulfills its tasks it will probably remain in the corporate environment, and without the necessary tools for doing software maintenance and security upgrades they will constitute a real security threat.

Many of these systems were developed as early as in the 80s or even 70s when security was not as big of an issue as it is today. Even though some applications did include security mechanisms, they were usually based on old and deficient standards that can now easily be broken. User credentials and other security parameters are often sent in clear and messages are poorly encrypted. This gives an attacker the possibilities he needs to access a restricted system or to inject data into the network.

Proprietary applications and systems often rely on “*security by obscurity*”, meaning they are not likely to be attacked since they are not based on open platforms. It is true that open platforms are more exposed because the tools and knowledge required to attack them are often available on the public domain. From a security standpoint however, security by obscurity should be avoided. All it takes to break into a low security legacy system is a little dedication, if the information or the system itself is valuable enough to an attacker, no further incentives are needed. Using security protocols that have not been subject to public review is always a risk. Although the implementation of a proprietary security system is unknown to the public, design flaws and bugs in the implementation can be revealed by passively examining the data flow. This information can later be used to compromise the system. If non-standardized security mechanisms are deployed, the corporation can not be certain that the protocols are in fact secure, and that they will be properly maintained and developed for future needs.

A standardized security system on the other hand is not likely to have any serious design flaws and if the implementation has undergone an independent certification process, an attacker will unlikely be able to mount a successful cryptographic attack.

Approaches to WLAN Security

The security threats to wireless LAN communication are both numerous and highly complex. The challenge may seem overwhelming and many corporate wireless LAN deployments have been postponed until the security issues are better understood and resolved. The wireless security industry on the other hand is putting a lot of effort into solving these issues and many approaches exist, ranging from built-in security mechanisms to vendor specific security add-ons to generic VPN solutions. In this chapter we will briefly describe some approaches to securing the wireless LAN, as well as their strengths and weaknesses.

Built-in Security

Wireline Equivalent Privacy (WEP)

The IEEE community early addressed the security problems in wireless LAN by designing and integrating the WEP security system into the 802.11 standard. Unfortunately, a number of serious design flaws in WEP allow an attacker to break into a WEP enabled system to inject malicious data into the network, decode encrypted messages and to spoof authentication requests [1], [2]. As the WEP system fails to provide an adequate level of security, the wireless industry is clear in its recommendations not to rely solely on WEP for securing a corporate environment.

802.1x

In 2001, the IEEE 802.11 working group passed the 802.1x standard as an effort to improve the security specified in the original 802.11 standard. Combined with an authentication protocol, such as EAP-TLS, LEAP, or EAP-TTLS, IEEE 802.1x is a security framework providing port-based access control, authentication, and dynamic key management. 802.1x is implemented natively in Microsoft Windows XP and some vendors are starting to implement 802.1x support in their access points and network cards. Wireless LAN implementations of 802.1x fall outside the scope of the 802.11 standard, but the 802.11i committee is specifying the use of 802.1x to eventually become part of the 802.11 standard.

Unfortunately the 802.1x protocol is not foolproof. Cisco has published a security advisory [3] regarding some security problems in their 802.1x implementation. Also, researchers at the University of Maryland have published a document proving that 802.1x is susceptible to man-in-the-middle attacks as well as session hijacking. [4]. Neither 802.1x nor EAP was designed with the wireless threat in mind: 802.1x was designed for campus networks and EAP for PPP, it is always dangerous to apply old protocols to new problems without understanding the implications. [1]

WiFi Protected Access (WPA)

WPA is an upgrade to WEP and is now a snapshot of the draft version of 802.11i. WPA includes Temporal Key Integrity Protocol (TKIP) and 802.1x mechanisms to provide dynamic key encryption and mutual authentication. Used correctly, WPA can withstand most known security attacks on wireless LAN. However, some of the WPA configurations allow an attacker to successfully implement a man-in-the-middle attack to get hold of security data. Mutual authentication is not supported when WPA is running in PSK-TKIP (Pre-shared key/ temporal key integrity protocol) mode, allowing rogue access points to be deployed on the network. If a legitimate user

connects to a rogue access point, an attacker gets all the security parameters he needs to get full access to the internal system. Two-way authentication, supported in both SSL and TLS, would effectively prevent such a man-in-the-middle attack. One of the EAP protocols offered in WPA, EAP-TLS does provide two-way authentication, but it is generally only applicable in a more complex environment. A much more serious problem with PSK-TKIP in WPA is described in [5], namely how an attacker can passively discover the network's private encryption key.

Another serious security problem in WPA is the potential of DoS attacks. If at least two incorrectly encrypted messages are sent within a second, a WPA enabled access point will kill all user connections for one minute. This is a defence mechanism designed to thwart unauthorized access. [6]

Vendor Specific

The corporate wireless LAN market's need for enhanced security has driven the major wireless LAN vendors, such as Cisco, Lucent and Symbol Technologies, to implement proprietary security add-ons to WEP. Unfortunately, most vendors do not provide enough information about their specific solutions to determine the overall security assurance that the product will provide. And worse, some solutions suffer from serious security issues that allow attackers to illegitimately access the private network.

Cisco LEAP

LEAP (Lightweight Extensible Authentication Protocol) is an authentication protocol that supports dynamic derivation of session encryption keys. With LEAP, authentication relies on the user's logon password, which is known only by the client and the network. As with most password-based algorithms, Cisco LEAP is vulnerable to dictionary attacks, in which a hacker uses a dictionary to guess the user's password and thereby gain access to the network. The Cisco solution is more vulnerable to a dictionary attack than other password based authentication mechanisms – this is due to a design flaw in the way the password is encrypted during the authentication process. A cryptographic attack can easily reveal the last two bytes in the users' password; and this highly reduces the ability to withstand a dictionary attack, especially if a strong password policy is not enforced. There are now various tools available on the Internet that explore this weakness in the Cisco LEAP implementation to get full network access. Cisco has acknowledged this security vulnerability and has announced the availability of EAP-FAST, an authentication protocol for 802.1x EAP users not vulnerable to dictionary attacks.

Closed Network Access Control

Lucent has developed a proprietary mechanism for access control that is not part of the 802.11 standard. The network name, or SSID, is not broadcasted on the network and thus only clients with knowledge about the SSID can join the network. In essence, the SSID will act as a shared secret. In general, authentication mechanisms based on shared secrets are robust, as long as the secret is well-protected. With Lucent's access control mechanism, the SSID is sent in clear in some of the management messages, all it takes to break into the network is to sniff for the messages that contain the SSID. [2]

Access Control Lists

Another mechanism (not defined in the 802.11 standard) used by many vendors provides access control based on the client's MAC address. Since a MAC address is easy to spoof, MAC address based access control provides no additional security. [2]

VPN

Companies have successfully used VPN technology for many years to secure their connections to the public Internet. The security implications with deploying wireless LAN (weak built-in security protocols as well as the ability to remotely connect to the network) suggest that any wireless network should be treated as insecure as a connection to the Internet and thus the same security policies should apply. Internet connections are effectively secured by deploying firewalls at the network edge and user access from the outside should require VPN with strong authentication. VPN and firewalls are proven and widely used technology, they are usually based on open and well-known standards, and so the corporation does not have to worry about design flaws or other potential security vulnerabilities.

A VPN is very efficient in providing strong mechanisms for authentication as well as end-to-end encryption. By decoupling security from the link layer, a VPN solution offers a more generic and vendor independent solution than many other WLAN security mechanisms. On the other hand, as VPN software has to be general, supporting a wide range of security protocols and authentication mechanisms, they tend to be a little heavyweight for embedded and legacy systems. According to leading wireless security practices, VPN technology should be used, perhaps in combination with link layer security mechanisms, wherever applicable to provide a homogeneous and efficient security platform. As long as the wireless LAN standards implement weak security, the only fool-proof solution is to deploy firewalls and VPN technology.

Conclusions

Many corporate customers are using 802.11-based wireless LAN to increase their productivity and overall efficiency and there is no doubt that wireless LAN is becoming a vital component in the corporate networking environment. However, along with increased mobility come new security threats. Since the physical medium is shared and possibly extends beyond the corporate's physically secured boundaries, it becomes extremely hard to prevent unauthorized persons to access the network.

This whitepaper suggests taking wireless security to a wider range and not only to focus on securing isolated parts of the information system or dataflow. Most information traversing the wireless network is probably of little interest to an attacker. The network itself and the resources within on the other hand are usually extremely valuable to the corporate and thus a more compelling target. The key to a successful wireless LAN deployment is to make a proper analysis of the threats, which services that need to be secured and the cost of having them compromised. A security system is never stronger than its weakest link, a well designed security architecture should be homogeneous, easy to manage and applicable to the whole target environment, including legacy.

As has been described in this white paper, most wireless LAN security mechanisms suffer serious security issues that make them vulnerable to various cryptographic attacks. Proprietary security add-ons and new draft standards that solve some of the security issues are available, but they do not necessarily apply to a legacy environment. Most new wireless LAN security solutions require major firmware and hardware upgrades, which results in expensive deployments.

As long as there is no generic and proven built-in solution to wireless LAN security, the recommendation from the security industry is clear; treat the wireless LAN as a public insecure connection, much the same as a connection to the Internet. Enforce firewall protection and allow only authenticated VPN enabled users to access the network.

References

- [1] P. J. Craiger. “802.11, 802.1x, and Wireless Security”. GIAC Security Essentials Certification Practical Assignment. June 2002.
- [2] W. A. Arbaugh, N. Shankar, and Y. J. Wan. “Your 802.11 Wireless Network has No Clothes”. Department of Computer Science, University of Maryland. March 2001.
- [3] “Cisco Security Notice: Dictionary Attack on Cisco LEAP Vulnerability”, Document ID 44281, Rev. 2.1. July 2004.
- [4] A. Mishra, W. A. Arbaugh “An initial Security Analysis of the IEEE 802.1X Standard”. Department of Computer Science, University of Maryland. Feb 2002.
- [5] R. Moskowitz, “Weakness in Passphrase Choice in WPA Interface”. WiFi Networking News. Nov 2003. <http://wifinetnews.com/archives/002452.html>
- [6] A. G. Reinhold. “DOS attack on WPA 802.11?”. The Cryptographic Mailing List. Nov. 2002.