Security for Corporate Wireless Local Area Networks

Janet Geldermann, James Magee, Kenneth O'Donnell
INFS 612 Summer 2006

Abstract

Wi-Fi networks, or more specifically, networks using the 802.11b standard have become more and more popular for a number of reasons including: low cost, widely available 802.11b networking cards/adapters/devices, widely available 'hot spots', and increasing home and office use of 802.11b. With the increasing number of corporations considering 802.11b as more cost effective method for implementing a local area network, security issues should be addressed. In the last several years, many security vulnerabilities in 802.11b have been discovered including weaknesses in encryption and authentication, which lead to several methods of attack, by hackers. This paper addresses many of the weaknesses of 802.11b and how the security mechanisms of the IEEE standard 802.11i and WPA2 improve the security of wireless networks. In addition to the newer protocol, corporations should consider implementation of a layered security approach.

1.0 Brief History of 802.11

In 1985 the FCC designated portions of the electromagnetic spectrum for use without a government license. This spectrum designation was the first step towards using radio networks for computer networking. These radio frequencies already had been allocated to equipment like microwaves. To limit interference and to make communication harder to intercept the FCC required that communications in these radio frequencies had to use 'spread spectrum' technology. Spread spectrum technology had been first used in World War II to make jamming and intercepting radio communication difficult. This move by the FCC opened up a possibility of using radio waves for computer networking for any organization.

IEEE

In 1990 the Institute of Electrical and Electronics Engineers (IEEE) formed the 802.11 committee also know as the Wireless Local Area Networks Standards Working Group. This committee set about formulating standards for what a wireless network would be. The 802.11 working group defined the specification for the Physical Layer and Media Access Layer for computer communications in a wireless environment.

802.11a/b/g

The 802.11 working group published the first standard for 802.11 in 1997. 802.11 networks started out with speeds of 1-2 Mbps. In two years two variations of 802.11 emerged; 802.11a, which operates in the 5.3 – 5.8 GHz

range offering transfer speeds up to 54 Mbps, and 802.11b, which operates in the 2.4 GHz range, offering transfer speeds of 11 Mbps. Both of these specifications greatly improved performance levels. Further improving performance was 802.11g, which also operated in the 2.4 GHz range offering transfer speeds up to 54 Mbps. There are now many standards for 802.11 and there continues to be new work, improving both security and throughput transfer speed of 802.11.

Standard	Frequency Range	Throughput Speed
802.11a	5.3 – 5.8 GHz	54 Mbps
802.11b	2.4 GHz	11 Mbps
802.11g	2.4 GHz	54 Mbps

Figure 1: 802.11 Standard Frequencies and Throughput Speeds

WLAN

Wireless Local Area Networks or WLANs that used the 802.11a/b/g standards became popular very quickly. Low cost, ease of use, and an ever-increasing number of home users with broadband connections all contributed to the popularity of 802.11a/b/g networks. Many businesses implement 802.11a/b/g networks because it is cheaper to install than a wire based network. Some business (for example coffee houses) offer free 802.11a/b/g access to attract customers. Many households are turning to 802.11a/b/g to share their new high-speed internet connection with more than one computer, or to have the freedom to move about while still connected to the internet. In a study conducted by RSA Security found that in 2005 WLAN adoption rates for London increased 57% and Paris grew 119% in two years ending in 2005.

2.0 Weaknesses of 802.11a/b/g

There are a number of security weaknesses in a 802.11a/b/g network. Since a 802.11a/b/g network uses radio waves as a medium of communication between devices, wireless networks are susceptible to security attacks that might not exist in a traditional (wired) computer networks. The types of attacks that might occur to a 802.11a/b/g network can be grouped into the following categories: passive attack, man in the middle attack, hijacking attack, and denial of service attack.

Passive Attacks

A passive attack or eavesdropping attack occurs when an attacker intercepts data being transmitted on the 802.11a/b/g network. Easily available network tools allow an attacker to capture traffic for analysis. Since the traffic in an 802.11a/b/g network is comprised of radio waves, the attacker can be safely away from an organization's premises and still have access to sensitive information. Figure 2 shows where an passive attack can occur. For example, an attacker could park outside of a residence or office and have access to the 802.11a/b/g network. This type of attack can be used in conjunction with other attacks. In networks where encryption is used the attacker can capture a large set of data and then decrypt it at a latter time.

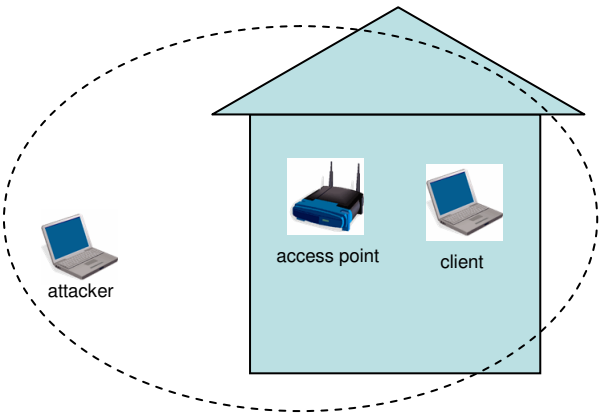

Figure 2: Passive Attack Diagram

Man in the Middle

The man in the middle attack or rouge access point attack is where an attacker will masquerade as a valid access point. By placing themselves in-between a valid client and a valid access point, an attacker will act as an access point having the valid client try to authenticate with the rouge access point, thus an attacker can obtain authentication information and then access the network. This type of attack allows the attacker access to the 802.11a/b/g network as a valid client.

Hijacking/Spoofing

A hijacking attack or spoofing attack is one where the attacker will assume the identity of a valid user. A hijack can be done by either using the valid user's IP or MAC address. The attacker can then spoof the IP or MAC address accessing the network as the valid user. This type of attack allows the attacker access to the 802.11a/b/g network as a valid client.

Denial of Service

A denial of service attack is very much like a denial of service attack for a more traditional (wired) network. An attacker floods the network with a large amount of information, shutting down the network functions. Figure 3 displays a Denial of Service attack. Since an 802.11a/b/g network is a shared network where all the users must share the same available bandwidth this attack will affect all the users of the network. In addition, with an 802.11a/b/g network, a user does not have to have authorized access to the network to cause a denial of service; jamming the radio frequencies for 802.11a/b/g will effectively shut down the network.

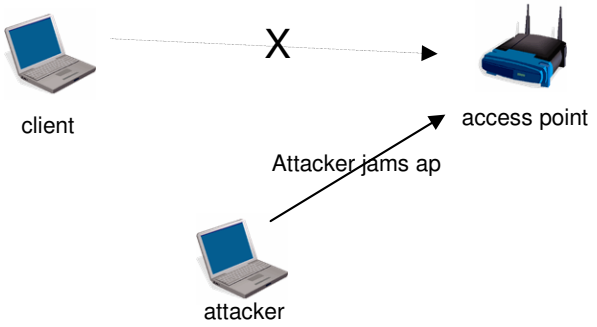

Figure 3: Denial of Service Attack Diagram

3.0 802.11a/b/g Security Mechanisms

There are tools in place within the 802.11a/b/g specification that will lessen the possibility that an attack on an 802.11a/b/g network will be successful. Some of the tools that can be used to help protect an 802.11 a/b/g network include disabling Service Set Identifiers (SSIDs) broadcast, Media Access Control (MAC) filtering, Wired Equivalency Privacy (WEP), and Wi-Fi Protected Access (WPA). Of these, some are beneficial and some prove to be very easily broken.

SSIDs Broadcast

An 802.11a/b/g network by default will send out a beacon frame with its Service Set Identifiers (SSIDs). The access point and the client must have the same SSIDs in order to communicate. This information is sent in clear text and allows a client to connect to the access point easily. By disabling this broadcast, the network is essentially hidden. This change will require that clients connecting to the 802.11a/b/g network to already know the SSIDs before any communication can occur.

MAC Filtering

Although it was never part of the formal specification, many 802.11a/b/g access points allow an administrator to filter access to the network by client's Media Access Control (MAC) address. Every 802.11a/b/g device including clients and access points have a MAC address that uniquely identifies it. Many access points can be set to only allow clients with MAC addresses that match an approved list of MAC addresses to connect to the network. This approach makes it difficult for an attacker to access the network unless the attacker can mimic a valid MAC address. Unfortunately mimicking a MAC address is not difficult.

WEP

Wired Equivalent Privacy (WEP) was intended to address many of the vulnerabilities of 802.11a/b/g, but failed to do so. WEP can be used for authentication or for authentication and encryption of data in an 802.11a/b/g network. There are however, several significant problems with WEP, which include the weakness of the RC4 encryption algorithm, reuse of Initialization Vectors, static key use, and poor authentication flexibility. These weaknesses have rendered WEP ineffective in fully protecting an 802.11a/b/g network.

WEP uses the RC4 encryption algorithm to encrypt and decrypt information. Once thought to be an acceptable encryption algorithm, it was found to be flawed. A paper by the researchers Fluhrer, Mantin, and Shamir found a flaw in the "key scheduling algorithm" of RC4 that makes it fundamentally weak. Since WEP is built upon this algorithm, WEP itself becomes a weak security measure.

WEP is based on a secret key combined with a 24-bit parameter called an Initialization Vector IV. There are two widely used key lengths for WEP, a 64-bit key that is a combination of a 40-bit secret key and the 24-bit IV, or a 128-bit key based on a 103-bit secret key and the 24-bit IV. Since the 802.11a/b/g standard does not specify how the IV is generated and since both the access point and the client need to use the IV to encrypt and decrypt information, The IV is sent in the clear with an encrypted message. Since the IV is only 24-bits long it will eventually be reused. This reuse allows an attacker to easily decrypt any of the 802.11a/b/g frames once enough are collected with the repeating IV.

WEP relies on pre-shared keys as the basis for the cryptographic key. Since this is manually entered on all of the 802.11a/b/g network devices, it is rarely updated if at all. This coupled with the inherent weakness of RC4 and reuse of IVs allows attackers easy access to potentially sensitive information.

WEP authentication is really just a test of the client's ability to encrypt data using the pre-shared key. WEP authentication works by having a client encrypt a clear text message from the access point and sending it back to the access point. If the message was encrypted correctly, the client is authenticated. This may work well for a small organization where an administrator can make sure that all client devices have the correct pre-shared key, however in a corporate environment it becomes burdensome.

WPA

Wi-Fi Protected Access (WPA) sought to fill the holes left behind by WEP. WPA is not part of the formal specifications of 802.11a/b/g, but is available in many 802.11a/b/g devices. WPA improves upon WEP by offering better authentication, and improved security. These two improvements can be used to temporarily secure 802.11 networks before implementation of 802.11i.

WPA is a significant improvement on WEP. However, WPA still relies on RC4, which was found to be fundamentally weak. Future security improvements for 802.11a/b/g will have to improve/replace the RC4 encryption algorithm to ensure security.

4.0 Security Improvements

The result of 802.11a/b/g implementation with its security weaknesses has been underutilization of wireless technologies in corporate or enterprise networks. Solutions and remedies for the vulnerabilities and security risks in 802.11a/bg have been developed in the IEEE standard 802.11i and WPA2. Additionally, a secure corporate network environment must develop a layered security approach to adequately secure their networks.

Security Layers

The most effective way to accomplish security for a corporate network is the Defense in Depth methodology. Defense in Depth consists of multiple security layers each with its own security functionality implementations. Figure 4 shows the minimum layers of security that should be incorporated into a wireless network.

First Layer

The first layer consists of a security policies built on existing corporate network usage policies with specific parameters aimed at a wireless network. Identification of corporate users is the first priority so access point placement is adequate to cover required areas but not so wide that the signals can easily be accessed by an outsider. Access points should be installed closer to the building's center and the signal's power lowered to what is necessary for efficient communications but not so much the network is vulnerable to hackers. If it is necessary to install the access points close to the building walls, the antennas may be directed towards the center to ward off overflow. Rogue access points ought to be watched for on a continuous basis as rogue points may be easily installed. Furthermore, security policies should include changing of default passwords to strong passwords and changing of Service Set Identification (SSIDs) upon wireless installation. Strong passwords are a minimum of 8 characters and include upper and lowercase letters, numeric and special characters such as *&^%$ although researches at the SANS Institute have found that 'passphrases' in length of 14 to 20 characters are much more difficult to crack.

Users must be trained to be aware of how careless actions or violations of corporate security policies could leave the network open to attack. Policies should be clearly defined and enforced.

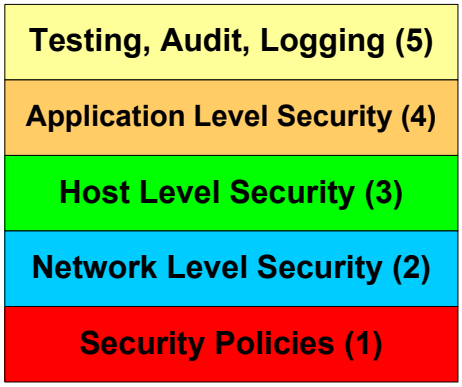

Figure 4: Security Layers for Wireless Networks (1)

Second Layer

Authentication, authorization, and encryption are security measures implemented at this second layer of corporate network security. Terms are established between the wireless clients and the internal protected network. The wireless LAN should be utilized on a network separate from the internal wired LAN with a firewall separating the two as shown in Figure 6. Network traffic that goes through the firewall will have to traverse the firewall with authentication and encryption.

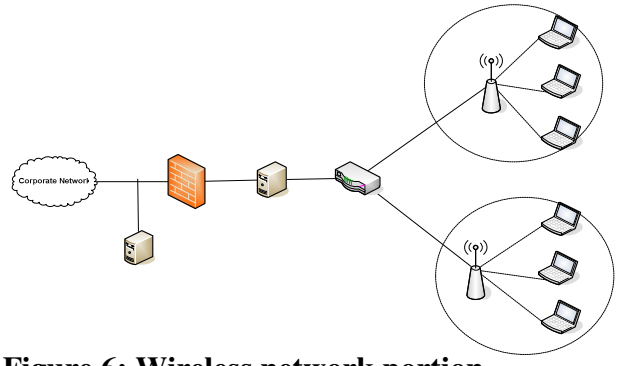

Figure 6: Wireless network portion separated by firewall from the internal network (18)

It is also recommended that a Virtual Private Network (VPN) be utilized to secure the wireless connections. The VPN establishes a secure tunnel connection between two points. The data that crosses the VPN is protected by secure Internet Protocol Security (IPSEC) encryption and thus from man-in-the-middle attacks and eavesdropping.

Third Layer

The third layer of security entails host level security. Default SSIDs should be changed upon installation as part of corporate policy and changed regularly so if the SSID becomes compromised it will be for a short period of time. A unique name should be utilized instead of the corporate name. SSID broadcasts should be turned off to provide an additional obstacle layer to intruders and password sign on implemented.

MAC Addresses can be used to limit connectivity to the network by filtering the MAC addresses that are configured at an access point. Although MAC addresses can be spoofed by hackers, it requires extra effort by the intruder to access the network. Dynamic Host configuration Program (DHCP) servers restrict the allocated number IP addresses accessing the network. If an authorized user is denied access to the wireless network, network or system administrators will be alerted to the network problem and initiate an investigation. MAC addresses are used in conjunction with Access Control Lists. The list contains all the authorized MAC addresses used on the network. Communications that comes by an intruder not on the list will be dropped.

WEP encryption was initially used by 802.11b but contains many security flaws.

Although WEP is better than no security at all, it remains very weak. 802.11i and WPA2 provide an improved solution for secure wireless networks.

Improved Security

Prior to the acceptance of 802.11i, the Wi-Fi Alliance released Wi-Fi Protected Access (WPA). The Wi-Fi Alliance is a non-profit organization of industry leaders formed with the focus of adopting a single worldwide standard for high-speed wireless LANs. WPA consists of three components: Temporal Key Integrity Protocol (TKIP) a data-integrity protocol [10], 802.1x and Message Integrity Code (MIC), designed to address the security limitations in 802.11. The new 802.11i standard called "RSN or Robust Security Network" provides standards that scale better than WEP and can be used internationally. [20]

TKIP is the replacement for WEP "without replacing legacy hardware." [22] Each packet uses a different key by generating a 'per-packet key mixing function' instead of "the concatenation of the IV and the shared secret key." [24] WPA reuses some of the cryptographics of the WEP protocol since these functions are usually hard coded into the wireless network interface hardware and not upgradeable. [24] This reuse ensures compatibility with legacy hardware. WPA reuses the WEP RC4 stream cipher but uses the shared secret key to generate seeds for other keys. This minimizes exposure of the secret key to attacks.

The TKIP per-packet key mixing function is divided into two phases. In Phase One: The sender's MAC address, session key and initialization vector are hashed together. Phase Two: For each packet, the lowest 16-bits and the previously calculated hash are hashed together resulting in a 104 bit per-packet key. The end product is a full 128-bit dynamic key to be used for encryption and decryption in the same manner as WEP. Figure 7 shows a graphic of this key mixing process.

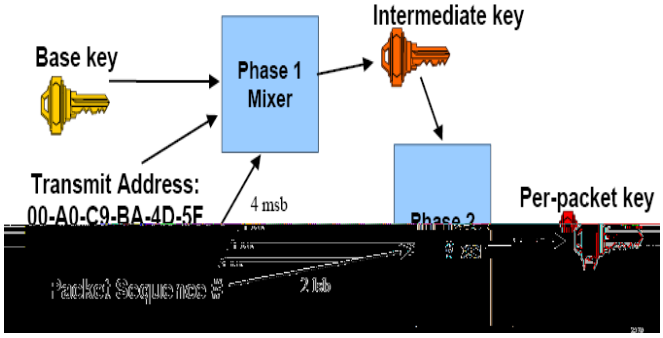

Figure 7: TKIP Key Design [24]

In Figure 8, the intermediate key produced by the Phase 1 mixer, is the TKIP transmit address and key (TTAK) [14]. A ciphertext MAC Protocol Data Unit (MPDU) is the output.

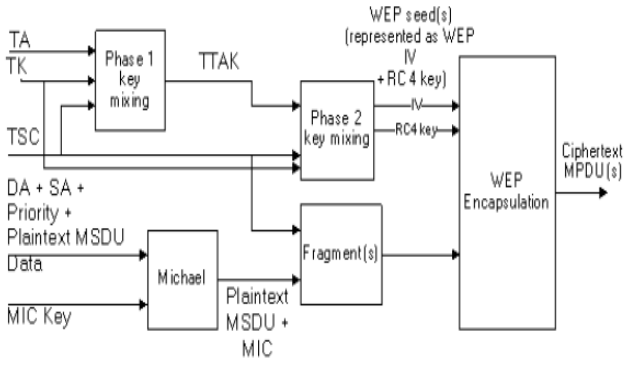

Figure 8: TKIP encapsulation block diagram [15]

Message Integrity Code or MIC protects the data packet integrity by utilizing a keyed hashing function. It is an 8 byte value calculated for the data packet prior to encryption for the purpose of detecting intentional packet modification. The MIC is a new hashing function for use in low power processing devices such as those used in a wireless network. The 20 bit key is considered low protection however. To compensate for the low protection of the hash key, countermeasures are implemented when a packet modification is detected. These countermeasures include disconnection of the wireless link for sixty seconds and/or requesting new session keys.

Advanced Encryption Standard (AES) [1], has been adopted as the standard encryption method, replacing the Data Encryption Standard (DES) by the National Institute of Standards and Technology (NIST). Adoption of AES followed a challenge by the National Security Agency (NSA) for someone to produce a better encryption process. Out of five finalists, AES was selected. AES is "mandatory for protection of sensitive unclassified federal information." [13] The Department of Defense (DoD) and the Committee on National Security Systems (CNSS) mandate the use of National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) require end to end encryption for data transmission utilizing AES-CCMP. [16]

AES use in both software and hardware is fast, easily implemented and not memory usage intensive. The only successful security attacks on AES as of the first half of 2006 have been side channel attacks, which attack the implementation of the cipher not the cipher itself.

Used in combination with AES is Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) provides "confidentiality, authentication, integrity, and replay protection." [14] The data block is not individually encrypted. A value is encrypted and added with a "logical XOR with a data block." [15] Successive blocks are incremented by one and creates a MIC to protect the data. The data block is then encrypted with the process repeating until all the data blocks for a message are processed. The end result has all data blocks combined into a 128 bit block. [24] Figure 9 displays the CCMP encapsulation diagram while Figure 10 shows the decapsulation from the IEEE 802.11i standard document. (MPDU is MAC Protocol Data Unit.)

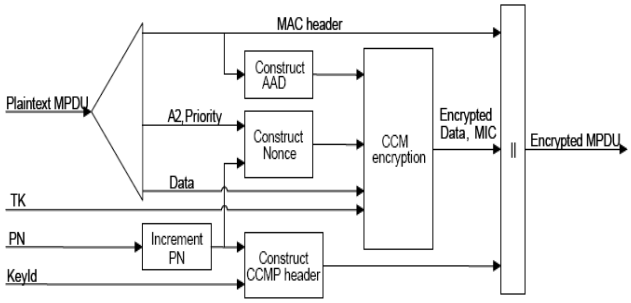

Figure 9: CCMP encapsulation block diagram [15]

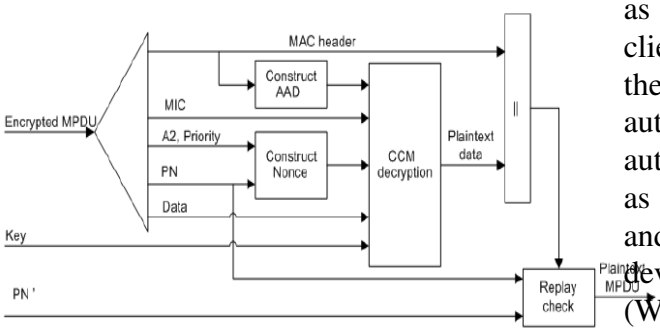

Figure 10: CCMP decapsulation block diagram [15]

It is assumed that a 128-bit encryption is "secured against brute-force attacks." [11] Replay attacks are prevented by CCMP's 48-bit packet number.

Improved Authentication for Wireless

Wi-Fi Protected Access (WPA) and 802.1X Development

As previously stated, due to the rapid increase in wireless services, security has become a major issue. Wired Equivalent Privacy (WEP) was developed to address security concerns with the wireless technology. However, the WEP standards were quickly determined to be providing insufficient security coverage. One of the bigger problems was with WEP authentication. WEP had two types of authentication, open system authentication and shared key authentication. Open system authentication allows any device to join the network providing that they have the same SSID set up as the Access Point (AP) or the AP is set up to use both. Shared-key authentication requires the client to be using the same type of authentication as the AP. The client encrypts a message sent by the AP and then the AP determines if the message is that same as the one sent. WEP authentication is a client's encryption test. Only if the client has the same key as the AP will they be authenticated. The vulnerability of the authentication and encryption in WEP, such as WEP key recovery, poor key management, and violation of data integrity, led to the development of Wi-Fi Protected Access (WPA), which enhances both encryption and authentication of WLANs. WPA requires changes to software/firmware from those systems implementing WEP. No hardware changes are required until conversion to WPA2 or 802.11i.

WPA uses the 802.1X protocol and an Extensible Authentication Protocol (EAP) to strengthen and provide for the mutual authentication process. This allows clients to authenticate against a central authentication server before they are allowed to join the network. The authentication server is usually a Remote-Authentication Dial-In User Service (RADIUS) server.

There are three entities involved in the 802.1X authentication process. The client or user to be authenticated is known as the Supplicant. The RADIUS server is known as the authentication server. The AP in between the two is called the authenticator.

The mutual authentication in 802.1X involves several steps: [25]

1. A supplicant initiates a connection with an authenticator. The authenticator detects the initiation and enables the port of the supplicant. However, all the traffic except 802.1X, including DHCP, HTTP, FTP, SMTP, and POP3, are blocked.

2. The authenticator then requests the identity from the supplicant.

3. The supplicant then responds with the identity. The authenticator passes the identity to an authentication server.

4. The authenticator server authenticates the identity of the supplicant. Once authenticated, an ACCEPT message is sent to the authenticator. The authenticator then transitions the supplicant's port to an authorized state.

5. The supplicant then requests the identity from the authentication server. The authentication server passes its identity to the supplicant.

6. Once suppliant authenticates the identity of authentication server, all the traffic is forwarded.

The process uses the AP as a middle-man passing messages. The AP does not know whether it is passing a password, PKI certificate, or another form of encryption. However, the mutual authentication that is created by using the AP provides a secure environment. Clients may chose from many different types of specific EAP based on their needs and desired features. We will look at the most popular of the EAP options available.

Types of EAP [8]

EAP-TLS – Transport Layer Security uses SSL to authenticate clients using its digital certificate. Some features include dynamic key exchange, mutual authentication, digital certificates, and encryption tunneling.

EAP-TTLS – Tunneled TLS integrates with a wide variety of password storage formats and existing password-based authentication systems. TTLS can also carry addition legacy authentication methods. These are similar features to TLS except that it does not use digital certificates. TTLS focuses on password-based authentication.

PEAP – Protected EAP is very similar to TTLS but does not provide the legacy authentication methods. Features offered by PEAP are dynamic key exchange, mutual authentication, and encryption tunneling.

LEAP – Lightweight EAP is used for legacy Cisco systems and equipment.

MD5 – Message Digest 5. Passwords are hashed using the MD5 algorithm are deployed for protecting access to LAN switches where the authentication traffic will not be transmitted over airwaves. MD5 can also be safely deployed for wireless authentication inside EAP tunnel methods. The only feature of MD5 is password-based authentication.

MSCHAP - Microsoft Challenge Handshake Accept Protocol: Passwords are hashed using a Microsoft algorithm are deployed for protecting access to LAN switches where the authentication traffic will not be transmitted over airwaves. MSCHAP can also be safely deployed for wireless authentication inside EAP tunnel methods. The main features of MSCHAP are mutual authentication and password-based authentication.

Addressing problems with WEP [11]

WPA using 802.1X manages to address most all of the security concerns that were identified with WEP.

Session Hijacking and Spoofing

Using the mutual authentication of 802.1X, the threat of session hijacking and spoofing is minimized to passive eavesdropping at best. An adversary can disassociate or disconnect an already authenticated client and act as the client with the AP. If the adversary can receive packets this merely becomes eavesdropping. If there is interaction required by the adversary, then they will need to have the client authentication keys. Since the keys are changed each session making them difficult to obtain. Adversaries will not be able to interact or generate any traffic.

Man-in-the-Middle Attack (MitM)

If proper mutual authentication controls are used, then MitM attacks are also limited to passive eavesdropping through the relayed information. It is possible for an adversary to disassociate or deauthenticate a client from its authenticated session with an AP. The client will then try to re-establish contact with the AP and after several tries be tied to the adversary connection. The adversary can now operate in the middle of the client and the AP. However, the adversary may not be able to associate itself with either client or AP if it does not have the proper credentials. When that is the case the only thing that the adversary can do is forward credentials between the client and AP or eavesdrops.

Masquerading and Malicious AP

The authentication mechanism (e.g., EAP-TLS) will prevent an adversary from forging, modifying, and replaying authentication packets, eliminating passive eavesdropping, message injection, and message deletion and interception. In order for mutual authentication to occur there must be more than MAC address exchange. Therefore, the new WPA2 eliminates the threat of masquerading or malicious APs because they require more information in order to be a success as opposed to WEP.

Denial of Service Attacks (DoS)

There are several ways that an adversary can still launch DoS attacks even when the EAP mutual authentication is still being used. Adversaries can continuously flood the system with deauthentication messages or association requests. The full compliment of 802.11i is not yet secure enough to defeat all DoS attacks.

Fourth Layer

The application layer comprises the fourth layer of wireless network security. The first line of application defense entails securing the wireless client. Attackers would choose to prey on the clients by bypassing an external firewall. Corporate network personnel should ensure all hot fixes and operating system security patches are installed on client machines. Clients can also utilize personal firewalls to prevent intruders from accessing the corporate wireless network through client vulnerabilities.

'System hardening is done by installing and configuring systems and application to meet strict security requirements.' [1] Functions not needed on the network should be turned off or eliminated. Disable those services that may be needed for potential functionality but are not necessary for current operations. Again, ensure that updates and patches are installed in a timely fashion. Intruders may discover a back door into your system or applications but developers may quickly release a patch to block an attack. Make sure the network is protected. The application layer is the final line of defense against attacks if attackers have managed to bypass all other layers.

Fifth Layer

Testing, logging, and auditing are the fifth layer of defense on the wireless network. Once the previous four layers have been successfully implemented the final objectives are to test and scan the network for vulnerabilities. "War-driving" is a method used to test vulnerabilities at access points to detect if the points can be accessed from outside corporate boundaries. Various commercial products are available to war-drive/walk the corporate wireless network. Outside security experts can also be employed to "penetration" test the corporate network for vulnerabilities. Audit logs that document attempted or successful intrusions should alert network and system administrators to the event so that proactive measures can be taken to plug the hole.

Auditing and logging of user accounts should be used in addition to the above means of auditing. Eighty-seven percent of network hacking or intrusion have be initiated from corporate insiders be it intentional or accidental. Audits and logs of user accounts provides a means to trace and document the event to find out what happened and provide a means to prevent the intrusion from occurring again.

5.0 Recent Vulnerability Discovery

The newest vulnerability in wireless was announced by researchers David Maynor of Internet Security Systems and Jon Ellch of the Naval Postgraduate School in Monterey, CA in late June 2006. By using an open source software program called LORCON (Lots of Radion Connectivity) [16], the researchers hit the wireless drivers with an enormous barrage of packets. This method, called "fuzzing" cause driver programs to fail or "run unauthorized software." [16] This type of attack can be run on a vulnerable laptop from most anywhere and the machine need not be connected to a network. [16] By their nature, wireless cards are constantly searching for wireless access points and thus are open to attacks.

Current driver code is built upon the original wireless code. The threat in the initial code is still there and vulnerable to attack from hackers. Hardware engineers do not always write the drivers with security in mind thus the development of the fuzzing attack.

Maynor and Ellch will present their findings at the Black Hat 2006 convention in August of 2006.

6.0 Conclusion

The vulnerabilities in the IEEE 802.11a/b/g wireless device standards have left corporations open to attack from hackers. Attacks such as Denial of Service, Man in the Middle, passive attacks, and spoofing have become common intrusions into networks costing corporations time and money. Implementation of the IEEE 802.11i and WPA2 standards will help protect wireless networks by increasing the difficulty of breaking the encryption utilized in protecting data, passwords and enhancing the strength of network authentications. In addition to implementing the newer standards, corporations must resolve to use Defense in Depth methodologies. This method uses a layered defense including security policy implementation, education and training of users, patch updates, testing, and auditing of network activities. In addition, by incorporating a wireless network separated by

firewall from the internal corporate network will provide the necessary protections for enterprises to make use of wireless technologies.

7.0 References

[1] "Advanced Encryption Standard." Wikipedia, the free encyclopedia. Wikipedia. URL: http://en.wikipedia.org/wiki/Advanced_Encryption_Standard July 3, 2006.

[2] "Attack through Wireless Device Drivers." URL: http://www.networksecurityjournal.com/ Network Security Journal, July 11, 2006.

[3] Biggs, Maggie. "How to Secure the Wireless Fortress," *Federal Computer Week*, vol.20, number 21, pp. 24-29. June 26, 2006.

[4] Branch, Joel W. et al. "Autonomic 802.11 Wireless LAN Security Auditing." *IEEE Security and Privacy.* URL: http://portal.acm.org/citation.cfm?id=1009276&dl=GUIDE&coll=GUIDE&CFID=15151515&CFTOKEN=6184618 June 30, 2006.

[5] Cam-Winget, Nancy, etal. "IEEE 802.11i Overview," NIST 802.11 Wireless LAN Security Workshop. Falls Church, VA. December 4-5, 2005.

[6] "CCMP." Wikipedia, the free encyclopedia. Wikipedia. URL: http://en.wikipedia.org/wiki/CCMP July 3, 2006.

[7] Cole, Eric, et al. "Secure Communications 401.4," SANS *Security Essentials 401*, version 2.5, Module 24. The SANS Institute, February 2006.

[8] "Determining Which EAP Authentication Method to Use," HP.com. URL: http://docs.hp.com/en/T1428-90056/ch11s03.html July 10, 2006.

[9] "Extensible Authentication Protocol." Wikipedia, the free encyclopedia. Wikipedia. URL: http://en.wikipedia.org/wiki/Extensible_authentication_protocol July 3, 2006.

[10] Halasz, David. "IEEE 802.11i and Wireless Security," URL: http://www.embedded.com/showArticle.jhtml?articleID=34400002 July 6, 2006.

[11] He, Changhua and John C. Mitchell. "Security Analysis and Improvements for IEEE 802.11i". Network and Distributed System Security Symposium (NDSS '05), San Diego, February 2005.

[12] "IEEE 802.11i." Wikipedia, the free encyclopedia. Wikipedia. URL: http://en.wikipedia.org/wiki/IEEE_802.11i June 28, 2006.

[13] Kagan, Anna. "How Things Work: WLA Technologies and Security Mechanisms," The SANS Institute, November 7, 2003.

[14] Linask, Erik, "Is Your WLAN Safe?" TMCnet URL: http://www.tmcnet.com/usubmit/2006/05/25/1659577.htm July 12, 2006.

[15] "Local and Metropolitan Area Networks," IEEE Std. 802.11i-2004. *IEEE*, pp 32 – 113.

[16] McMillian, Robert. "Researchers Use Wi-Fi Driver to Hack Laptop." PC

World.com. URL: http://www.pcworld.com/resource/printable/article/o,aid,126204,00.asp July 13, 2006.

[17] "MD5." Wikipedia, the free encyclopedia. Wikipedia. URL: http://en.wikipedia.org/wiki/MD5 July 3, 2006.

[18] Neoh, Danny. "Corporate Wireless LAN: Know the Risks and Best Practices to Mitigate Them," The SANS Institute, December 12, 2003.

[19] "Official IEEE 802.11 Working Group Project Timelines – 06/21/06" ANSI/IEEE URL: http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm (7/12/06)

[20] Perez, Elio. "802.11i (How we got here and where are we headed)." The SANS Institute, August 21, 2004.

[21] "Recommended 802.11 Wireless Local Area Network Architecture," National Security Agency, Systems and Network Attack Center, Ft. George G. Meade, MD., I332-008R-2005, September 23, 2005.

[22] "TKIP." Wikipedia, the free encyclopedia. Wikipedia. URL: http://en.wikipedia.org/wiki/TKIP July 3, 2006.

[23] "Wi-Fi Security Still a Major Issue." Wi-Fi Planet. URL: http://www.wi-fiplanet.com/tutorials/print.php/3609866 June 30, 2006.

[24] Wong, Luis Carlos. "An Overview of 802.11 Wireless Network Security Standards & Mechanisms." The SANS Institute, October, 2004.

[25] Wong, Stanley, "The Evolution of Wireless Security in 802.11 networks: WEP, WPA and 802.11 Standards." The SANS Institute, May 20, 2003.