A

Seminar report

On

Wireless Lan Security

Submitted in partial fulfillment of the requirement for the award of degree
Of ECE

SUBMITTED TO: **SUBMITTED BY:**

www.studymafia.org www.studymafia.org

Acknowledgement

I would like to thank respected Mr…….. and Mr. ……..for giving me such a wonderful opportunity to expand my knowledge for my own branch and giving me guidelines to present a seminar report. It helped me a lot to realize of what we study for.

Secondly, I would like to thank my parents who patiently helped me as i went through my work and helped to modify and eliminate some of the irrelevant or un-necessary stuffs.

Thirdly, I would like to thank my friends who helped me to make my work more organized and well-stacked till the end.

Next, I would thank Microsoft for developing such a wonderful tool like MS Word. It helped my work a lot to remain error-free.

Last but clearly not the least, I would thank The Almighty for giving me strength to complete my report on time.

Preface

I have made this report file on the topic **Wireless Lan Security**I have tried my best to elucidate all the relevant detail to the topic to be included in the report. While in the beginning I have tried to give a general view about this topic.

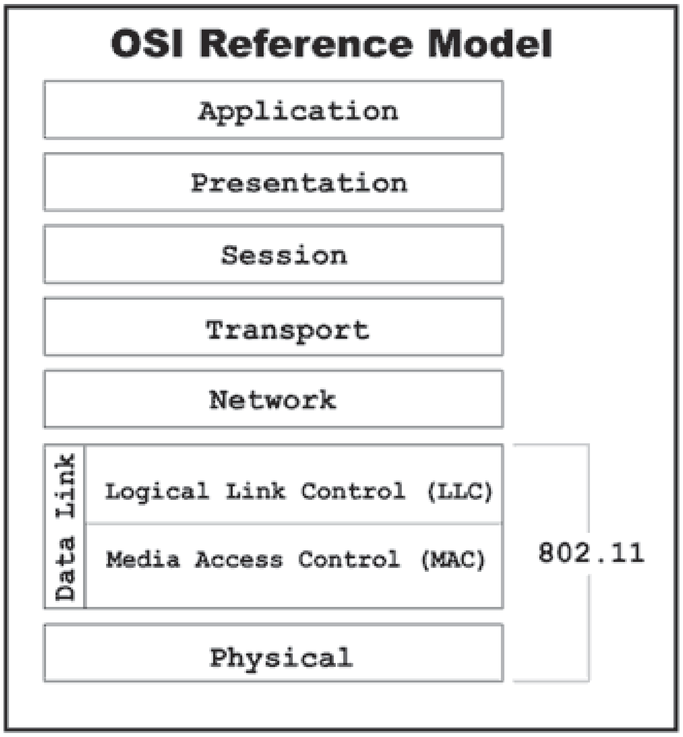
My efforts and wholehearted co-corporation of each and everyone has ended on a successful note. I express my sincere gratitude to …………..who assisting me throughout the preparation of this topic. I thank him for providing me the reinforcement, confidence and most importantly the track for the topic whenever I needed it.

Contents:

I. Introduction

a. The 802.11 Wireless LAN Standard

In 1997, the IEEE ratified the 802.11 Wireless LAN standards, establishing a global standard for implementing and deploying Wireless LANS. The throughput for 802.11 is 2Mbps, which was well below the IEEE 802.3 Ethernet counterpart. Late in 1999, the IEEE ratified the 802.11b standard extension, which raised the throughput to 11 Mbps, making this extension more comparable to the wired equivalent. The 802.11b also supports the 2 Mbps data rate and operates on the 2.4GHz band in radio frequency for high-speed data communications



As with any of the other 802 networking standards (Ethernet, Token Ring, etc.), the 802.11 specification affects the lower layers of the OSI reference model, the Physical and Data Link layers.

The Physical Layer defines how data is transmitted over the physical medium. The IEEE assigned 802.11 two transmission methods for radio frequency (RF) and one for Infrared. The two RF methods are frequency hopping spread-spectrum (FHSS) and direct sequence spread-spectrum (DSSS). These transmission methods operate within the ISM (Industrial, Scientific, and Medical) 2.4 GHz band for unlicensed use. Other devices that operate on this band include remote phones, microwave ovens, and baby monitors.

FHSS and DSSS are different techniques to transmit data over radio waves. FHSS uses a simple frequency hopping technique to navigate the 2.4GHz band which is divided into 75 sub-channels 1MHz each. The sender and receiver negotiate a sequence pattern over the sub-channels.

DSSS, however, utilizes the same channel for the duration of the transmission by dividing the 2.4 GHz band into 14 channels at 22MHz each with 11 channels overlapping the adjacent ones and three nonoverlapping channels. To compensate for noise and interference, DSSS uses a technique called "chipping", where each data bit is converted into redundant patterns called "chips".

The Data Link layer is made up of two sub-layers, the Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. The Data Link layer determines how transmitted data is packaged, addressed and managed within the network. The LLC layer uses the identical 48-bit addressing found in other 802 LAN networks like Ethernet where the MAC layer uses a unique mechanism called carrier sense multiple access, collision avoidance (CSMA/CA). This mechanism is similar to the carrier sense multiple access collision detect (CSMA/CD) used in Ethernet, with a few major differences. Opposed to Ethernet, which sends out a signal until a collision is detected before a resend, CSMA/CA senses the airwaves for activity and sends out a signal when the airwaves are free. If the sender detects conflicting signals, it will wait for a random period before retrying. This technique is called "listening before talking" (LBT) and probably would be effective if applied to verbal communications also.

To minimize the risk of transmission collisions, the 802.11 committee decided a mechanism called Request-To-Send / Clear-To-Send (RTS/CTS). An example of this would be when an AP accepts data transmitted from a wireless station; the AP would send a RTS frame to the wireless station that requests a specific amount of time that the station has to deliver data to it. The wireless station would then send an CTS frame acknowledging that it will wait to send any communications until the AP completes sending data. All the other wireless stations will hear the transmission as well and wait before sending data. Due to the fragile nature of wireless transmission compared to wired transfers, the acknowledgement model (ACK) is employed on both ends to ensure that data does not get lost in the airwaves.

b. 802.11 Extensions

Several extensions to the 802.11 standard have been either ratified or are in progress by their respective task group committees. Below are three current task group activities that affect WLAN users most directly:

802.11a

The 802.11a ("another band") extension operates on a different physical layer specification than the 802.11 standard at 2.4GHz.

802.11a operates at 5GHz and supports date rates up to 54Mbps. The FCC has allocated 300Mz of RF spectrum for unlicensed operation in the 5GHz range. Although 802.11a supports much higher data rates, the effective distance of transmission is much shorter than 802.11b and is not compatible with 802.11b equipment and in its current state is usable only in the US. However, several vendors have embraced the 802.11a standard and some have dual band support AP devices and network cards.

802.11b

The 802.11b ("baseline") is currently the de facto standard for Wireless LANs. As discussed earlier, the 802.11b extension raised the data rate bar from 2Mbps to 11Mbps, even though the actual throughput is much less. The original method employed by the 802.11 committee for chipping data transmissions was the 11-bit chipping encoding technique called the "Barker Sequence". The increased data rate from 2Mbps to 11Mbps was achieved by utilizing an advanced encoding technique called Complementary Code Keying (CCK). The CCK uses Quadrature Phase Shift Keying (QPSK) for modulation to achieve the higher data rates.

802.11g

The 802.11g ("going beyond b") task group, like 802.11a is focusing on raising the data transmission rate up to 54Mbps, but on the 2.4MHz band. The specification was approved by the IEEE in 2001 and is expected to be ratified in the second half of 2002. It is an attractive alternative to the 802.11a extension due to its backward compatibility to 802.11b, which preserves previous infrastructure investments.

The other task groups are making enhancements to specific aspects of the 802.11 standard. These enhancements do not affect the data rates. These extensions are below:

802.11d

This group is focusing on extending the technology to countries that are not covered by the IEEE.

802.11e

This group is focusing on improving multi-media transmission quality of service.

802.11f

This group is focusing on enhancing roaming between APs and interoperability between vendors.

802.11h

This group is addressing concerns on the frequency selection and power control mechanisms on the 5GHz band in some European countries.

802.11i

This group is focusing on enhancing wireless lan security and authentication for 802.11 that include incorporating Remote Access Dialing User Service (RADIUS), Kerberos and the network port authentication (IEEE 802.1X). 802.1X has already been implemented by some AP vendors.

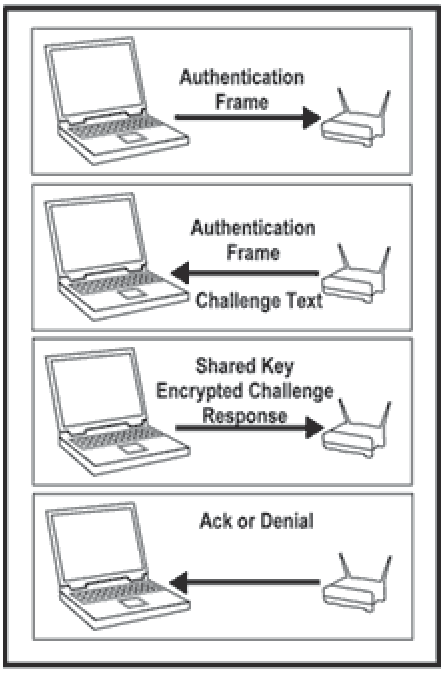
c. 802.11 Security Flaws

802.11 wireless LAN security or lack of it remains at the top of most LAN administrators list of worries. The security for 802.11 is provided by the Wired Equivalency Policy (WEP) at the MAC layer for authentication and encryption The original goals of IEEE in defining WEP was to provide the equivalent security of an "unencrypted" wired network. The difference is the wired networks are somewhat protected by physical buildings they are housed in. On the wireless side, the same physical layer is open in the airwaves.

WEP provides authentication to the network and encryption of transmitted data across the network. WEP can be set either to either an open network or utilizing a shared key system. The shared key system used with WEP as well as the WEP encryption algorithm are the most widely discussed vulnerabilities of WEP. Several manufacturers' implementations introduce additional vulnerabilities to the already beleaguered standard.

WEP uses the RC4 algorithm known as a stream cipher for encrypting data. Several manufacturers tout larger 128-bit keys, the actual size available is 104 bits. The problem with the key is not the length, but lies within the actual design of WEP that allows secret identification. A paper written by Jesse Walker, "Unsafe at any key length" provides insight to the specifics of the design vulnerabilities and explains the exploitation of WEP.

The following steps explain the process of how a wireless station associates to an AP using shared key authentication.



1) The wireless station begins the process by sending an authentication frame to the AP it is trying to associate with.

2) The receiving AP sends a reply to the wireless station with its own authentication frame containing 128 octets of challenge text.

3) The wireless station then encrypts the challenge text with the shared key and sends the result back to the AP.

4) The AP then decrypts the encrypted challenge using the same shared key and compares it to the original challenge text. If the there is a match, an ACK is sent back to the wireless station, otherwise a notification is sent back rejecting the authentication.

It is important to note that this authentication process simply acknowledges that the wireless station knows the shared key and does not authenticate against resources behind the AP. Upon authenticating with the AP, the wireless station gains access to any resources the AP is connected to.

This is what keeps LAN and security managers up at night. If WEP is the only and last layer of defense used in a Wireless LAN, intruders that have compromised WEP, have access to the corporate network. Most APs are deployed behind the corporate firewall and in most cases unknowingly are connected to critical down-line systems that were locked down before APs were invented. There are a number of papers and technical articles on the vulnerabilities of WEP that are listed in the Reference section.

II. Wireless LAN Deployment

The biggest difference in deployment of Wireless LANs over their wired counterpart are due to the physical layer operates in the airwaves and is affected by transmission and reception factors such as attenuation, radio frequency (RF) noise and interference, and building and structural interference.

a. Antenna Primer

Antenna technology plays a significant role in the deployment, resulting performance of a Wireless LAN, and enhancing security. Properly planned placement can reduce stray RF signal making eavesdropping more difficult.

Common terms that are used in describing performance of antenna technology are as follows:

Isotropic Radiator - An antenna that radiates equally in all directions in a three dimensional sphere is considered an "isotropic radiator".

Decibel (dB) - Describes loss or gain between two communicating devices that is expressed in watts as a unit of measure.

dBi value - Describes the ratio of an antenna's gain when compared to that of an Isotropic Radiator antenna. The higher the value, the greater the gain.

Attenuation - Describes the reduction of signal strength over distance. Several factors can affect attenuation including absorption (obstructions such as trees that absorb radio waves), diffraction (signal bending around obstructions with reflective qualities), reflection (signal bounces off a reflective surface such as water), and refraction (signal bends due to atmospheric conditions such as marine fog).

Gain - Describes RF concentration over that of an Isotropic Radiator antenna and is measured in dB.

Azimuth - Describes the axis for which RF is radiated.

Antennas come in all shapes and sizes including the home-made versions using common kitchen cupboard cans to deliver specific performance variations. Following are some commonly deployed antenna types.

Dipole Antenna:

This is the most commonly used antenna that is designed into most Access Points. The antenna itself is usually removable and radiating element is in the one inch length range. This type of antenna functions similar to a television "rabbit ears" antenna. As the frequency gets to the 2.4GHz range, the antenna required gets smaller than that of a 100Mz television. The Dipole antenna radiates equally in all directions around its Azimuth but does not cover the length of the diagonal giving a donut-like radiation pattern. Since the Dipole radiates in this pattern, a fraction of radiation is vertical and bleeds across floors in a multi-story building and have typical ranges up to 100 feet at 11Mbps.

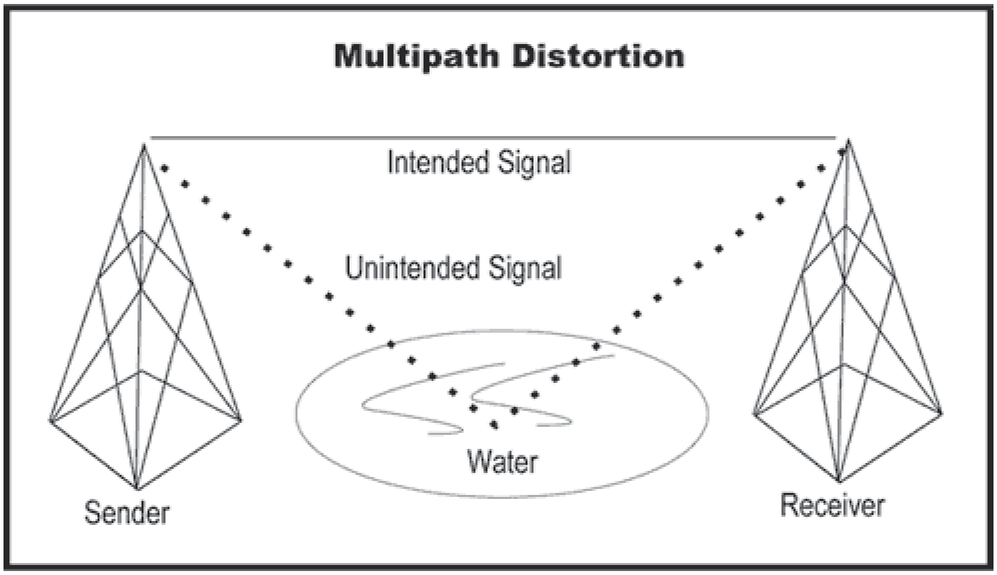
Directional Antennas:

Directional antennas are designed to be used as a bridge antenna between two networks or for point-to-point communications. Yagi and Parabolic antennas are used for these purposes as well as others. Directional antennas can reduce unwanted spill-over as they concentrate radiation in one direction.

With the popularity of "war driving" (driving around in a car and discovering unprotected WLANs) there is continuing research done on enhancing distances and reducing spill-over by commercial and underground groups. Advanced antennas like the "Slotted Waveguide" by Trevor Marshal, utilizes multiple dipoles, one above the other, to cause the signal radiation to be in phase so that the concentration is along the axis of the dipoles.

b. Deployment Best Practices

Planning a Wireless LAN requires consideration for factors that affect attenuation discussed earlier. Indoor and multi-story deployments have different challenges than outdoor deployments. Attenuation affects antenna cabling from the radio device to the actual antenna also. The radio wave actually begins at the radio device and induces voltage as it travels down the antenna cable and loses strength.



Multi-path distortion occurs in outdoor deployments where a signal traveling to the receiver arrives from more than one path. This can occur when the radio wave traverses over water or any other smooth surface that causes the signal to reflect off the surface and arrive at a different time than the intended signal does.

Structural issues must also be considered that can affect the transmission performance through path fading or propagation loss. The greater the density of the structural obstruction, the slower the radio wave is propagated through it. When a radio wave is sent from a transmitter and is obstructed by a structural object, the signal can penetrate through the object, reflect off it, or be absorbed by it.

A critical step in deploying the WLAN is performing a wireless site survey prior to the deployment. The survey will help determine the number of APs to deploy and their optimum placement for performance with regards to obstacles that affect radio waves as well as business and security related issues.

Complete understanding of the infrastructure and environment with respect to network media, operating systems, protocols, hubs, switches, routers and bridges as well as power supply is necessary to maximize performance and reduce network problems.

III. Wireless LAN Security Overview

As new deployments of Wireless LANs proliferate, security flaws are being identified and new techniques to exploit them are freely available over the Internet.

Sophisticated hackers use long-range antennas that are either commercially available or built easily with cans or cylinders found in a kitchen cupboard and can pick up 802.11b signals from up to 2,000 feet away. The intruders can be in the parking lot or completely out of site. Simply monitoring the adjacent parking lots for suspicious activity is far from solving the security issues around WLANs.

Many manufacturers ship APs with WEP disabled by default and are never changed before deployment. In an article by Kevin Poulsen titled "War driving by the Bay", he and Peter Shipley drove through San Francisco rush hour traffic and with an external antenna attached to their car and some custom sniffing software, and within an hour discovered close to eighty (80) wide open networks. Some of the APs even beacon the company name into the airwaves as the SSID.

a. Authentication and Encryption

Since the security provided by WEP alone including the new 802.1x Port Based IEEE standard is extremely vulnerable, stronger authentication and encryption methods should be deployed such as

Wireless VPNs using Remote Authentication Dial-In User Service (RADIUS) servers.

The VPN layer employs strong authentication and encryption mechanisms between the wireless access points and the network, but do impact performance, a VPN (IPSec) client over a wireless connection could degrade performance up to 25%. RADIUS systems are used to manage authentication, accounting and access to network resources.

While VPNs are being represented as a secure solution for wireless LANs, one-way authentication VPNs are still vulnerable to exploitation. In large organizations that deploy dial-up VPNs by distributing client software to the masses, incorrect configurations can make VPNs more vulnerable to "session hi-jacking". There are a number of known attacks to one-way authentication VPNs and RADIUS systems behind them that can be exploited by attackers. Mutual authentication wireless VPNs offer strong authentication and overcome weaknesses in WEP.

b. Attacking Wireless LANs

With the popularity of Wireless LANs growing, so is the popularity of hacking them. It is important to realize that new attacks are being developed based on old wired network methods. Strategies that worked on securing wired resources before deploying APs need to be reviewed to address new vulnerabilities.

These attacks provide the ability to:

- Monitor and manipulate traffic between two wired hosts behind a firewall
- Monitor and manipulate traffic between a wired host and a wireless host
- Compromise roaming wireless clients attached to different Access Points
- Monitor and manipulate traffic between two wireless clients

Below are some known attacks to wireless LANs that can be applied to VPNs and RADIUS systems:

Session Hijacking

Session hijacking can be accomplished by monitoring a valid wireless station successfully complete authenticating to the network with a protocol analyzer. Then the attacker will send a spoofed disassociate message from the AP causing the wireless station to disconnect. When WEP is not used the attacker has use of the connection until the next time out Session hijacking can occur due to vulnerabilities in 802.11 and 802.1x state machines. The wireless station and AP are not synchronized allowing the attacker to disassociate the wireless station while the AP is unaware that the original wireless station is not connected.

Man-in-the-middle

The man-in-the-middle attack works because 802.1x uses only one-way authentication. In this case, the attacker acts as an AP to the user and as a user to the AP. There are proprietary extensions that enhance 802.1x to defeat this vulnerability from some vendors.

RADIUS Attacks

The XForce at Internet Security Systems published vulnerability findings in multiple vendors RADIUS offerings. Multiple buffer overflow vulnerabilities exist in the authentication routines of various RADIUS implementations. These routines require user-supplied information. Adequate bounds checking measures are not taken when parsing user-supplied strings. Generally, the "radiusd" daemon (the RADIUS listener) runs with super user privilege. Attackers may use knowledge of these vulnerabilities to launch a Denial of Service (DoS) attack against the RADIUS server or execute arbitrary code on the RADIUS server. If an attacker can gain control of the RADIUS server, he may have the ability to control access to all networked devices served by RADIUS, as well as gather login and password information for these devices.

An Analysis of the RADIUS Authentication Protocol is listed below:

- Response Authenticator Based Shared Secret Attack User-Password Attribute Cipher Design Comments
- User-Password Attribute Based Shared Secret Attack
- User-Password Based Password Attack
- Request Authenticator Based Attacks
- Passive User-Password Compromise Through Repeated Request Authenticators
- Active User-Password Compromise through Repeated Request Authenticators
- Replay of Server Responses through Repeated Request Authenticators
- DOS Arising from the Prediction of the Request Authenticator

IV. Protecting Wireless LANS

As discussed above, there are numerous methods available to exploit the security of wired networks via wireless LANs. Layered security and well thought out strategy are necessary steps to locking down the network. Applying best practices for wireless LAN security does not alert the security manager or network administrator when the security has been compromised.

Intrusion Detection Systems (IDS) are deployed on wired networks even with the security provided with VPNs and firewalls. However, wire-based IDS can only analyze network traffic once it is on the wire. Unfortunately, wireless LANs are attacked before entering the wired network and by the time attackers exploit the security deployed, they are entering the network as valid users.

For IDS to be effective against wireless LAN attacks, it first MUST be able to monitor the airwaves to recognize and prevent attacks before the hacker authenticates to the AP.

a. Principles of Intrusion Detection

Intrusion Detection is the art of detecting inappropriate, incorrect, or anomalous activity and responding to external attacks as well as internal misuse of computer systems. Generally speaking, Intrusion Detection Systems (IDS) are comprised of three functional areas:

- A stream source that provides chronological event information
- An analysis mechanism to determine potential or actual intrusions
- A response mechanism that takes action on the output of the analysis mechanism.

In the wireless LAN space, the stream source would be a remote sensor that promiscuously monitors the airwaves and generates a stream of 802.11 frame data to the analysis mechanism. Since attacks in wireless occur before data is on the wired network, it is important for the source of the event stream to have access to the airwaves before the AP receives the data.

The analysis mechanism can consist of one or more components based on any of several intrusion detection models. False positives, where the IDS generated an alarm when the threat did not actually exist, severely hamper the credibility of the IDS. In the same light, false negatives, where the IDS did not generate an alarm and a threat did exist, degrade the reliability of the IDS.

Signature-based techniques produce accurate results but can be limited to historical attack patterns. Relying solely on manual signature-based techniques would only be as good as the latest known attack signature until the next signature update. Anomaly techniques can detect unknown attacks by analyzing normal traffic patterns of the network but are less accurate than the signature-based techniques. A multi-dimensional intrusion detection approach integrates intrusion detection models that combine anomaly and signature-based techniques with policy deviation and state analysis.

b. Vulnerability Assessment

Vulnerability assessment is the process of identifying known vulnerabilities in the network. Wireless scanning tools give a snapshot of activity and identify devices on each of the 802.11b channels and perform trend analysis to identify vulnerabilities. A wireless IDS should be able to provide scanning functionality for persistent monitoring of activity to identify weaknesses in the network.

The first step in identifying weakness in a Wireless LAN deployment is to discover all Access Points in the network. Obtaining or determining each one's MAC address, Extended Service Set name, manufacturer, supported transmission rates, authentication modes, and whether or not it is configured to run WEP and wireless administrative management. In addition, identify every workstation equipped with a wireless network interface card, recording the MAC address of each device.

The information collected will be the baseline for the IDS to protect. The IDS should be able to determine rogue AP's and identify wireless stations by vendor fingerprints that will alert to devices that have been overlooked in the deployment process or not meant to be deployed at all.

Radio Frequency (RF) bleed can give hackers unnecessary opportunities to associate to an AP. RF bleed should be minimized where possible through the use of directional antennas discussed above or by placing Access Points closer to the middle of buildings as opposed to the outside perimeter.

c. Defining Wireless LAN Security Policies

Security policies must be defined to set thresholds for acceptable network operations and performance. For example, a security policy could be defined to ensure that Access Points do not broadcast its Service Set Identifier (SSID). If an Access Point is deployed or reconfigured and broadcasts the SSID, the IDS should generate an alarm. Defining security policies gives the security or network administrator a map of the network security model for effectively managing network security.

With the introduction of Access Points into the network, security policies need to be set for Access Point and Wireless Station configuration thresholds. Policies should be defined for authorized Access Points and their respective configuration parameters such as Vendor ID, authentication modes, and allowed WEP modes. Allowable channels of operation and normal activity hours of operation should be defined for each AP. Performance thresholds should be defined for minimum signal strength from a wireless station associating with an AP to identify potential attacks from outside the building.

The defined security policies form the baseline for how the wireless network should operate. The thresholds and configuration parameters should be adjusted over time to tighten or loosen the security baseline to meet real-world requirements. For example, normal activity hours for a particular AP could be scaled back due to working hour changes. The security policy should also be changed to reflect the new hours of operation.

No one security policy fits all environments or situations. There are always trade offs between security, usability and implementing new technologies.

d.State-Analysis

Maintaining state between the wireless stations and their interactions with Access Points is required for Intrusion Detection to be effective. The three basic states for the 802.11 model are idle, authentication, and association. In the idle state, the wireless station has either not attempted authentication or has disconnected or disassociated. In the authentication state, the wireless station attempts to authenticate to the AP or in mutual authentication models such as the Cisco LEAP implementation, the wireless station also authenticates the AP. The final state is the association state, where the wireless station makes the connection to the network via the AP.

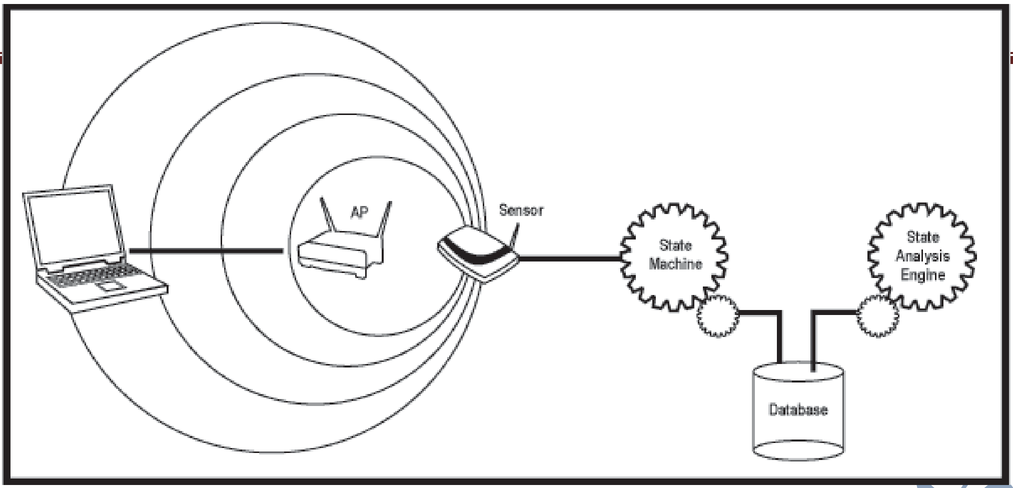
Following is an example of the process of maintaining state for a wireless station:

1. A sensor in promiscuous mode detects a wireless station trying to authenticate with an AP
2. A state-machine logs the wireless stations MAC address, wireless card vendor and AP the wireless station is trying to associate to by reading 802.11b frames, stripping headers and populating a data structure usually stored in a database
3. A state-machine logs the wireless station's successful association to the AP

State Analysis looks at the behavioral patterns of the wireless station and determines whether the activity deviates from the normal state behavior. For example, if the wireless station was broadcasting disassociate messages, that behavior would violate the 802.11 state model and should generate an alarm.

e. Multi-Dimensional Intrusion Detection

The very natures of Wireless LANs intrinsically have more vulnerabilities than their wired counterparts. Standard wire-line intrusion detection techniques are not sufficient to protect the



network. The 802.11b protocol itself is vulnerable to attack. A multi-dimensional approach is required because no single technique can detect all intrusions that can occur on a wireless LAN. A successful multi-dimensional intrusion detection approach integrates multiple intrusion detection models that combine quantitative and statistical measurements specific to the OSI Layer 1 and 2 as well as policy deviation and performance thresholds.

Quantitative techniques include signature recognition and policy deviation. Signature recognition interrogates packets to find pattern matches in a signature database similar to anti-virus software. Policies are set to define acceptable thresholds of network operation and performance. For example, policy deviation analysis would generate an alarm due to an improper setting in a deployed Access Point. Attacks that exploit WLAN protocols require protocol analysis to ensure the protocols used in WLANS have not been compromised. And finally, statistical anomaly analysis can detect patterns of behavior that deviate from the norm.

Signature Detection

A signature detection or recognition engine analyzes traffic to find pattern matches manually against signatures stored in a database or automatically by learning based on traffic pattern analysis. Manual signature detection works on the same model as most virus protection systems where the signature database is updated automatically as new signatures are discovered. Automatic signature learning systems require extensive logging of complex network activity and historic data mining and can impact performance.

For wireless LANs, pattern signatures must include 802.11 protocol specific attacks. To be effective against these attacks, the signature detection engine must be able to process frames in the airwaves before they are on the wire.

Policy Deviation

Security policies define acceptable network activity and performance thresholds. A policy deviation engine generates alarms when these pre-set policy or performance thresholds are violated and aids in wireless LAN management. For example, a constant problem for security and network administrators are rogue Access Points. With the ability for employees to purchase and deploy wireless LAN hardware, it is difficult to know when and where they have been deployed unless you manually survey the site with a wireless sniffer or scanner.

Policy deviation engines should be able to alarm as soon as a rogue access point has been deployed. To be effective for a wireless LAN, a policy deviation engine requires access to wireless frame data from the airwaves.

Protocol Analysis

Protocol analysis monitors the 802.11 MAC protocols for deviations from the standards. Real-time monitoring and historical trending provide intrusion detection and network troubleshooting.

Session hijacking and DoS attacks are examples of a protocol attack. Maintaining state is crucial to detecting attacks that break the protocol spec.

V .Wireless LAN Security Summary

Wireless LANs provide new challenges to security and network administrators that are outside of the wired network. The inherent nature of wireless transmission and the availability of published attack tools downloaded from the Internet, security threats must be taken seriously. Best practices dictate a well thought out layered approach to WLAN security. Access point configuration, firewalls, and VPNs should be considered. Security policies should be defined for acceptable network thresholds and performance. Wireless LAN intrusion detection systems complement a layered approach and provide vulnerability assessment, network security management, and ensure that what you think you are securing is actually secured.

Conclusion

Wireless LAN deployments should be made as secure as possible. Standard 802.11 security is weak and vulnerable to numerous network attacks. This paper has highlighted these vulnerabilities and described how it can be solved to create secure wireless LANs.

Some security enhancement features might not be deployable in some situations because of device limitations such as application specific devices (ASDs such as 802.11 phones capable of static WEP only) or mixed vendor environments. In such cases, it is important that the network administrator understand the potential WLAN security vulnerabilities.

Reference:

www.google.com

www.wikipedia.com

www.studymafia.org