An Estimation of Security Risk and Countermeasures in WLAN

Sadqua Ambari
(M.Tech Scholar),
Dept of Electronics & Communication Engg,
Al- Falah University
Dhauj Faridabad Haryana

Mr. Asif Ali
Assistant Professor,
Dept of Electronics & Communication Engg,
Al- Falah University
Dhauj Faridabad Haryana

ABSTRACT

Wireless LANs popularity has been on the rise since the ratification of the IEEE 802.11b standard in 1999. In recent years, wireless LANs are widely deployed in places such as business organizations, government bodies, hospitals, schools and even home environment. Mobility, flexibity, cost-effectiveness and rapid deployment are some of the factors driving the proliferation of this technology. However, the architecture of this technology made it insecure as WLANs broadcast radio-frequency (RF) data for the client stations to hear. This presents new challenges for network administrators and information security administrators.

This study was undertaken to find out if wireless networks are inherently insecure thereby limiting enterprise deployment. If yes, what are the known holes, and can they be fixed? The security mechanisms of wireless LANs were not within the scope of this work. The author tried to answer these questions through comprehensive and broad literature study.

The study shows that wireless LANs are prone to many different kinds of attacks – ranging from passive to active, and that wireless security initiative has come a long way, from weak WEP to a more robust WPA2. It also show that optimal security solution for Wireless LANs involves a combination of security technologies, and that vulnerability assessment and risk analysis are essential for development of effective security policy and determination of appropriate security measures for risk mitigation.

Key words: *Wireless LANs, IEE 802.11, Attacks, Security, Access Point (AP)*

INTRODUCTION

Wireless communication has broken the constraint users used to have with wired technology. The liberty to gain access to corporate network without being bonded, mobility while accessing the Internet, increased reliability and flexibility are some of the factors driving the wireless local area network technology. Other factors that contribute to tremendous growth of Wireless Local Area Networks (WLANs) are reduced installation time, long-term cost savings, and installation in difficult-to-wire areas. Today, Wireless Local Area Network (WLAN) is a choice to reckon in various sectors, including business, education, government, public and individual. IEEE 802.11 dominates the wireless networking technology. This can be attributed to the low cost of the hardware and high data rates that support current applications (from 1 to 54 Mbps) as well as promising future extensions (possibly exceeding 100 Mbps with 802.11n). Increasingly, portable devices (Laptops, PDAs, and Tablet PCs) are being sold with wireless LAN as a standard feature.

However, this technology brings with it important limitations in the field of security. The communication medium of wireless LAN is radio wave, thus it's more susceptible to eavesdropping than wired networks, and as the wireless market grows, the security issues grow along with it. There have been several works on WLAN security since it was discovered that the 802.11 security architecture is weak. However, most of these works were on the security mechanism enhancement.

For an organization to best protect its information there is need for security risk assessment. This will help to determine the threats its information is prone to, and then develop appropriate security measures to counter it.

This thesis assesses the security risks associated with WLANs that limits its deployment in enterprise environment and proffers countermeasures that should be put in place for secure implementation as integral part of LAN.

OBJECTIVES OF THE STUDY

- To find out the known security holes that limit enterprise deployments of a WLAN
- To find out if these known security holes can be fixed

RESEARCH METHOD

This study is descriptive in nature as the problem is well structured and understood. The approach adopted in this research paper is deductive as it looks at the bigger picture (WLAN) and narrows down to security (vulnerabilities and countermeasures). The data is collected from literature and Internet. The subjects of the literature are mainly wireless communications, network security and WLAN security. Most of the literature is published not later than 2002, and the main part of the collected data consists of published articles and papers that were found on Internet. Care was taken to ensure the information from the articles and papers from internet are true and have been published

BASIC WLAN COMPONENTS

For one to set up a wireless local area network, two basic components must be available: wireless network cards and wireless access point(s). The third basic component, wireless bridge, is used to link two or more buildings together.

The wireless network cards are attached to mobile computing devices, and they connect to an access point. An access point is essentially a hub that gives wireless clients the ability to attach to the wired LAN backbone. To maintain a coverage area, more than one access points are used as in cell structures, which are used by cell phone providers to maintain a coverage area. Wireless bridges, on the other hand, enable high-speed long-range outdoor links between buildings. Based on line-of-sight, wireless bridges are not affected by obstacles such as freeways, railroads, and bodies of water, which typically pose a problem for copper and fibre-optic cable.

Wireless Network Interface Card (PCMCIA)
Wireless Access Point

Figure 1 Basic components of WLAN

Source: J. Burrell [8]

WLAN TRANSMISSION TECHNOLOGIES

Wireless LANs are generally categorized according to the transmission technique in use.

All available wireless LAN products fall into one of the categories below:

- **Infrared (IR) LANs:** Infrared light does not penetrate opaque walls; as a result,an individual cell of an IR LAN is limited to a single room. No licensing is required.
- **Spread Spectrum LANs:** Here, spread spectrum transmission technology isused, and in most cases, the LANs operate in ISM (Industrial, Scientific, and Medical) bands so as to avoid licensing requirement as in the United States for example.
- **Narrowband Microwave:** This category of LANs operates at microwavefrequencies. Some operate at frequencies that require FCC licensing, others operate at the unlicensed ISM bands, but they do not use spread spectrum.

INFRARED (IR) LANs

There are three types of infrared transmission: directed beam, ominidirectional, and diffused.

- **Directed Beam Infrared**: Directed beam infrared transmission provides thehighest transmission speed. Here the receiver is aligned with the sender unit to create a point-to-point link. The range depends on the degree of focusing and the emitted power. The light source used in infrared transmission depends on the environment. Light emitting diode (LED) is used in indoor areas, while lasers are used in outdoor areas.

- **Ominidirectional**: In ominidirectional configuration, a single base station iswithin the line of sight of all other stations in the LAN, and this station is typically mounted on the ceiling. This station then acts as a multiport repeater. The ceiling station broadcasts ominidirectional signals which are received by all the other IR transceivers in the area, and these transceivers in turn transmit a directional beam aimed at the ceiling base station.

- **Diffused**: The infrared light transmitted by the sender unit fills the area (e.g.office). Therefore the receiver unit located anywhere in that area can receive the signal.

SPREAD SPECTRUM LANs

In exclusion of very small offices, a spread spectrum wireless LAN makes use of a multiple- cell arrangement. Each of the adjacent cells in the configuration is assigned a different centre frequency within the same band to avoid interference.

With this transmission technology, there are two methods used by wireless LAN products: frequency hopping and direct sequence modulation.

Frequency Hopping: Here, the signal jumps from one frequency to anotherwithin a given frequency range. The transmitter device "listens" to a channel, if it detects an idle time (i.e. no signal is transmitted), it transmits the data using the full channel bandwidth. If the channel is full, it "hops" to another channel and repeats the process. The transmitter and the receiver "jump" in the same manner.

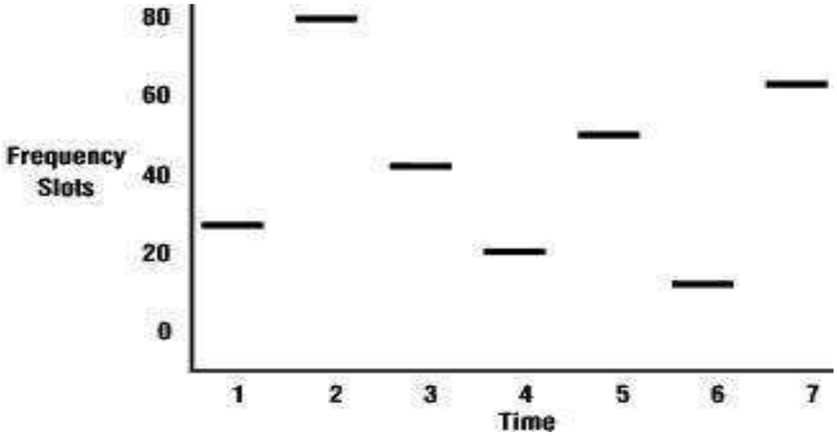

Figure 2 Frequency hopping

Source: WLANA [65]

• **Direct Sequence Modulation**: This method uses a wide frequency band togetherwith Code Division Multiple Access (CDMA). Signals from different units are transmitted at a given frequency range, and at a very low power. A code is transmitted with each signal so that the receiver can identify the appropriate signal transmitted by the sender unit. The frequency at which such signals are transmitted is called the ISM (industrial, scientific and medical) band. This frequency band is reserved for ISM devices. The ISM band has three frequency ranges: 902-928, 2400-2483.5 and 5725-5850 MHz.

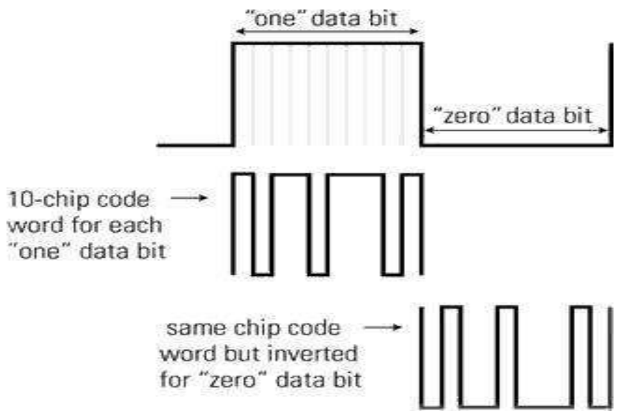
"one" data bit
"zero" data bit
10-chip code word for each "one" data bit
same chip code word but inverted for "zero" data bit

Figure 3 DSSS with CDMA

Source: WLANA [65]

WLAN SECURITY ATTACKS

Attacks on wireless LANs are aimed at the confidentiality and integrity of an information, and network availability. These security attacks can be passive or active.

- **Passive attack**: consist of unauthorized access to an asset or network for thepurpose of eavesdropping or traffic analysis, but not to modify its content. This is tricky to detect because data is unaffected. Consequently, emphasis is on prevention (encryption) not detection.

- **Active attacks**: an unauthorized access to an asset or network for the purpose ofeither making modifications to a message, data stream, or file, or to disrupt the functioning of a network service.

The diagram below shows a general taxonomy of WLAN security attacks.

.

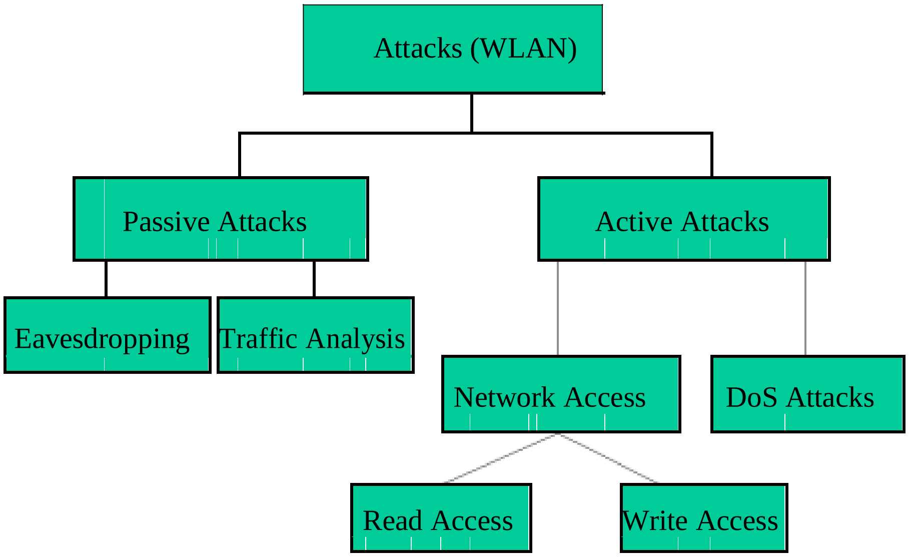

Figure 4 General Taxonomy of WLAN security attacks
Source: K. Fleming [10, 25]

PASSIVE ATTACKS

There are two phases to an attack. The first phase is referred to as the reconnaissance phase, this is a passive attack. During the reconnaissance phase, the goal of an attacker is to discover a target network, and then gather information about the network. The attacker does this in a way that is unnoticeable. However, some of the means of reconnaissance can be detected by an intrusion detection system.

There are two methods used in executing undetectable passive attack: eavesdropping, and traffic analysis.

- **Eavesdropping**: is the capability to monitor transmissions for message content.An attacker listens and intercepts wireless signals between the AP and wireless client.

- **Traffic analysis**: is the capability to gain intelligence by monitoring transmissionfor patterns of communications, or perform packet analysis. This can be carried out even when the messages are encrypted and cannot be decrypted

There abound a lot of sniffing tools that can aid an attacker in achieving his goal. Sniffing tools are the most effective means to monitor what is happening on a network. Undetectable, sniffing can perform two principal functions: packet capture and packet analysis and display. By analyzing a packet, an attacker is informed about the capabilities of a network, and can gather all sorts of confidential information for exploitation of an organization. Packet capture enables an attacker to recover WEP keys in few minutes, thereby providing him with the capability to read all the data passing between the wireless client and the AP. A wide variety of sniffing tools exit - both as priced and freeware.

War Driving is another technique that can be used for reconnaissance. War Driving is the act of searching for the existence of Wireless LAN (802.11) Networks while driving around a city. Simply, it's locating and logging wireless access points while in motion. With programs like NetStumbler (Windows), Kismet or SWScanner (Linux), FreeBSD, NetBSD, OpenBSD, and DragonFly BSD, and KisMac (Macintosh) and GPS, a WLAN can be detected, plotted and posted to a website. Table 1 provides a list of some popular sniffing tools.

Table 1 Sniffing Tools [10, 32]

Tool	Capability	Source	Notes
tcpick - v0.2.0	Packet capture	http://tcpick.sourceforge.net/	NETwork DUmp data Displayer and Editor for tcpdump tracefiles (Linux, Free BSD, Open BSD)
Sniffit - v0.3.7b	Packet capture	http://reptile.rug.ac.be/~coder/sniffit/sniffit.htMl	Can track, reassemble and reorder tcp streams (Linux based)

Tool	Capability	Source	Notes
TCPDUMP -v3.8.3	Packet capture & analysis	http://www.tcpdump.org/	Prints out the headers of packets or save packets for later analysis
Sniffit - v0.3.7b	Packet capture	http://reptile.rug.ac.be/~coder/sniffit/sniffit.htMl	Packet capture library (developed on LINUX), has various functions not offered in any other non-commercial sniffer.
SLSNIF - v0.4.1	Packet capture	http://www.azstarnet.com/	Packet capture library (Linux based)
AirSnort	War Driving (Packet capture & analysis)	Open-source: http://airsnort. shmoo.com	Recovers encryption keys (Windows or Linux Based)
WEBCrack	Packet Analysis	Open-source: http://wepcrack. sourceforge.net	Recovers WEP keys (PERL based scripts)
Sniffer Wireless	Packet Capture & Display	Network Associates (commercial product)	Capability to decrypt WEP-based traffic and quickly detect Rogue APs. (Windows and PDA based)
KRIPP - v0.6	Network passwords capture & display	http://konst.org.ua/kripP	Written in Perl, it uses only the tcpdump utility as an underlying traffic interceptor
Net Stumbler	War Driving; Network Discovery; Packet Capture	Open-source: http://netstumbler.com	Records SSIDs in beacons and interfaces with GPS to map a network. (Windows-based)
Kismet	War Driving; Network Discovers; Packet Capture	Open-source: http://kismetwireless.net /	Most complete War Driving tool. Works with most client cards that support Rfmon mode. Operates on most OS systems.
Wellenreiter	War Driving; Network Discovers; Packet Capture	Open-source: http://www.wellenreiter.net	Perl and C++ based for Linux and BSD systems.
httpcapture -v0.4	Packet capture & analysis/display	http://www.steve.org.uk/Software/httpcapture/	Plugins for capturing, decoding, and displaying some network logins
Ethereal - v0.10.4	Packet capture; Protocol analyzer	http://www.ethereal.com/	Free network protocol analyzer for Unix and Windows

ACTIVE ATTACKS

An active attack is one whereby an unauthorised change of the system is attempted. This could include, for example, the modification of transmitted or stored data, the creation of new data streams or limiting an organization's network availability. Active attacks may take the form of one of four types (or combination): masquerading, replay, message modification, and denial-of-service (DoS).

• Masquerading: An active attack in which the attacker impersonates anauthorized user and thereby gains certain unauthorized privileges. It could be attempted through the use of stolen logon IDs and passwords, through finding security gaps in programs, or through bypassing the authentication mechanism. The attempt could come from an insider, an employee for example, or an outsider through the public network. Once entry is made and the right access to the organization's critical data is gained, the attacker may be able to modify and delete software and data, and make changes to network configuration and routing information.

• Replay: Also known as Man-in-the-Middle attack, a replay attack is one wherebythe attacker monitors transmissions (passive attack) and retransmits messages as the legitimate user to trick the receiver into unauthorized operations such as false identification or authentication or a duplicate transaction.

• Message modification: The attacker alters a legitimate message by deleting,adding to, changing, or reordering it.

• Denial-of-service: The attacker prevents or prohibits the normal use ormanagement of communications facilities. DoS attacks can range from physical destruction of equipment, disruption of certain network services to a specific person or system, prevention of a particular individual from accessing a service to flooding a network, thereby preventing legitimate network traffic. Below are some common practices for accomplishing DoS:

- ƒ Deploy radio-jamming equipment
- ƒ Saturate a network' bandwidth by continually broadcasting frames
- ƒ Conduct disassociation/de-authentication attacks
- ƒ Conduct transmit duration attacks by configuring the transmit duration field to a maximum of 30-packets-per-second rate
- ƒ Saturate AP tables by flooding associations
- Setup a rogue AP and associate users to a bogus network to establish a Man-in-the-Middle attack

To accomplish an active attack, an attacker must have access to the target network with a read and write access right. The overall goal is to have access to network resources or to capture and decrypt data - if encrypted. Read access enables an attacker to intercept and read traffic from a network, thereby providing him with the potential to carry attacks on encryption, authentication, and other protection methods. Having discovered a target network through reconnaissance, and having captured unencrypted or encrypted traffic by sniffing, an attacker has the potential to gain key material and recover encryption keys. Acquisition of the encryption keys provide an attacker full access to the target network, and with write access he has the capability to send traffic to a network entity. The following are some goals of an attacker with network read and write access:

ƒ Recover encryption keys

ƒ Recover key streams generated by encryption keys

ƒ Inject data packets: write encrypted data by replaying captured key stream

ƒ Encrypt data with key and inject the data to the network

ƒ Install spying software on a wireless client and have the capability to read the results

ƒ Setup a rogue AP and control network parameters - such as encryption keys

ƒ Bypass authentication schemes:

- By deploying MAC address spoofing to evade MAC address filtering o By deploying shared-key authentication bypass attacks
- By performing LEAP Dictionary attacks if network is using 802.1x forauthentication
- By performing PEAP Man-in-the-Middle attacks if network is using802.1x for authentication

ƒ Install malicious code on a wireless client

WLAN technology on its own has inbuilt security problems in its architecture, as the APs and the clients must advertise their existence through beacon frames. This makes a signal exposed to anyone within range and is capable of listening. Shielding a WLAN by locating it within an area where the RF signals are not cable of escaping minimizes the risk of unauthorized access. However, this is not always a viable solution. As a result other security methods must be deployed such as strong access control and encryption technology.

The techniques for gaining unauthorized access to a WLAN are well-known security issues. Many of these security issues exploiting WLANs have recently been corrected with technology developments in the 802.11i standard. Table 2 is a list of all known security attacks deployed against WLANs categorized by type of threat, and mapped to associated hacker methods and tools.

Access control attacks

These attacks attempt to penetrate a network by circumventing filters and firewalls to obtain unauthorized access. MAC spoofing (also known as identity theft) and Rogue Access Points are more common among these.

Table 2 Wireless Security Attacks [45]

Attack	Description	Methods and Tools
War Driving	Discovering wireless LANs by listening to beacons or sending probe requests, thereby providing launch point for further attacks.	DStumbler, KisMAC, MacStumbler, NetStumbler, WaveStumbler,
Rogue Access Points	Installing an unsecured AP inside firewall, creating open backdoor into trusted network.	Any hardware or software
AP Ad Hoc Associations	Connecting directly to an unsecured station to circumvent AP security or to attack station.	Any wireless card or USB adapter
MAC Spoofing	Reconfiguring an attacker's MAC address to pose as an authorized AP or station.	Bwmachak, SirMACsAlot, SMAC,Wellenreiter, wicontrol
802.1X RADIUS Cracking	Recovering RADIUS secret by brute force from 802.1X access request, for use by evil twin AP.	Packet capture tool on LAN or network path between AP and RADIUS server

Integrity attacks

These attacks send forged/modified control, management or data frames over wireless to mislead the recipient or facilitate another type of attack. Denial-of-service attacks are the most common of the attacks that can be facilitated by this.

Attack	Description	Methods and Tools
802.11 Frame Injection	Crafting and sending forged 802.11 frames.	Airpwn, File2air, libradiate, void11, WEPWedgie, wnet dinject/reinject
802.11 Data Replay	Capturing 802.11 data frames for later (modified) replay.	Capture + Injection Tools 802.11

Table 3: Integrity attacks

Attack	Description	Methods and Tools
802.11 Data Deletion	Jamming an intended receiver to prevent delivery while simultaneously spoofing ACKs for deleted data frames.	Jamming + Injection Tools
802.1X EAP Replay	Capturing 802.1X Extensible Authentication Protocols (e.g., EAP Identity, Success, Failure) for later replay.	Wireless Capture + Injection Tools between station and AP
802.1X RADIUS Replay	Capturing RADIUS Access-Accept or Reject messages for later replay.	Ethernet Capture + Injection Tools between AP and authentication ser

Confidentiality attacks

These attacks attempt to intercept private or sensitive information sent over wireless associations - whether sent in the clear or encrypted by 802.11 or higher layer protocols. Eavesdropping, WEP Key Cracking, Evil Twin AP (poorly-understood attack) and Man-in-the-Middle (a form of active eavesdropping) are the most common attacks in this category. As shown in general taxonomy of WLAN security attacks (figure), eavesdropping is classified as passive attack whereas the rest are members of active attack class.

Table 4: Confidentiality attacks

Attack	Description	Methods and Tools
Eavesdropping	Capturing and decoding unprotected application traffic to obtain potentially sensitive information.	bsd-airtools, Ethereal, Ettercap, Kismet, commercial analyzers
WEP Key Cracking	Capturing data to recover a WEP key using brute force or Fluhrer-Mantin-Shamir (FMS) cryptanalysis.	Aircrack, AirSnort, chopchop, dwepcrack, WepAttack, WepDecrypt, WepLab
Evil Twin AP	Masquerading as an authorized AP by beaconing the WLAN's service set identifier (SSID) to lure users.	cqureAP, HermesAP, HostAP, OpenAP, Quetec, WifiBSD
AP Phishing	Running a phony portal or Web server on an evil twin AP to "phish" for user logins, credit card numbers.	Airsnarf, Hotspotter
Man-in-the-Middle	Running traditional man-in-the middle attack tools on an evil twin AP to intercept TCP sessions or SSL/SSH tunnels.	dsniff, Ettercap

Authentication attacks

Intruders use these attacks to steal legitimate user identities and credentials to access otherwise private networks and services. Dictionary attack and brute force attack are the two most common techniques employ here by the attackers to achieve their objectives.

Once succeeded, the attacker impersonates (masquerading) as an authorized user, thereby gaining certain unauthorized privileges.

Table 5: Authentication attacks

Attack	Description	Methods and Tools
Shared Key Guessing	Attempting 802.11 Shared Key Authentication with guessed vendor default or cracked WEP keys.	WEP Cracking Tools
PSK Cracking	Recovering a WPA PSK from captured key handshake frames using a dictionary attack tool	coWPAtty, KisMAC, wpa_crack, wpa-sk-bf
Application Login Theft	Capturing user credentials (e.g., e-mail address and password) from cleartext application protocols.	Ace Password Sniffer, Dsniff, PHoss, WinSniffer
VPN Login Cracking	Recovering user credentials (e.g., PPTP password or IPsec Preshared Secret Key) by running brute-force attacks on VPN authentication protocols.	ike_scan and ike_crack (IPsec), anger and THC-pptpbruter (PPTP)
Domain Login Cracking	Recovering user credentials (e.g., Windows login and password) by cracking NetBIOS password hashes, using a brute-force or dictionary attack tools.	John the Ripper, L0phtCrack, Cain
802.1X Identity Theft	Capturing user identities from cleartext 802.1X Identity Response packets.	Capture Tools
802.1X LEAP Cracking	Recovering user credentials from captured 802.1X Lightweight EAP (LEAP) packets using a dictionary attack tool to crack the NT password hash.	Anwrap, Asleap, THCLEAPcracker
802.1X EAP	Downgrade Forcing an 802.1X server to offer a weaker type of authentication using forged EAP-Response/Nak packets	File2air, libradiate
802.1X Password	Using a captured identity, repeatedly attempting 802.1X authentication to guess the user's password.	Password Dictionary

Availability attacks

These attacks attempt to inhibit or prevent legitimate use of wireless LAN services. The most common type of availability attack is the denial-of-service (DoS) attack, known as RF Jamming in the wireless world.

Table 6: Availability attacks

Attack	Description	Methods and Tools
AP Theft	Physically removing an AP from a public space.	"Five finger discount"
RF Jamming	Transmitting at the same frequency as the target WLAN, perhaps at a power that exceeds regulation Equivalent Isotopically Radiated Power (EIRP).	RF Jammer, Microwave oven, AP with Alchemy/HyperWRT firmware
Queensland DoS	Exploiting the CSMA/CA Clear Channel Assessment (CCA) mechanism to make a channel appear busy.	An adapter that supports CW Tx mode, with a lowlevel utility to invoke continuous transmit
802.11 Beacon Flood	Generating thousands of counterfeit 802.11 beacons to make it hard for stations to find a legitimate AP.	Fake AP
802.11 Associate / Authenticate Flood	Sending forged Authenticates or Associates from random MACs to fill a target AP's association table	Airjack, File2air, Macfld, void11
802.11 TKIP MIC Exploit	Generating invalid TKIP data to exceed the target AP's MIC error threshold, suspending WLAN service.	File2air, wnet dinject
802.11 Deauthentic-ate Flood	Flooding station(s) with forged Deauthenticates or Disassociates to disconnecting users from an AP.	Airjack, Omerta, void11
802.1X EAPStart Flood	Flooding an AP with EAP-Start messages to consume resources or crash the target.	QACafe, File2air, libradiate
802.1X EAPFailure	Observing a valid 802.1X EAP exchange, and then sending the station a forged EAPFailure message.	QACafe, File2air, libradiate
802.1X EAP-of-Death	Sending a malformed 802.1X EAP Identity response known to cause some APs to crash.	QACafe, File2air, libradiate
802.1X EAP Length Attacks	Sending EAP type-specific messages with bad length fields to try to crash an AP or RADIUS server.	QACafe, File2air, libradiate

PUTTING ATTACKS INTO PERSPECTIVE: RISK ANALYSIS

Risk is chances of threats in getting benefits from defects or weaknesses which are causes of losses and/or damages to assets or groups of assets, effecting an organization directly or indirectly. Risk analysis is an effective tool in WLAN threat management. With this a good security policy can be derived and implemented to defend the WLAN against possible attacks. On-going monitoring and periodic testing can then be used to verify that a deployed WLAN meets defined objectives. Vulnerabilities discovered in the process are then (re)analyzed so as to refine the policies and/or apply fixes. This iterative process is illustrated in the diagram (figure 5) shown below:

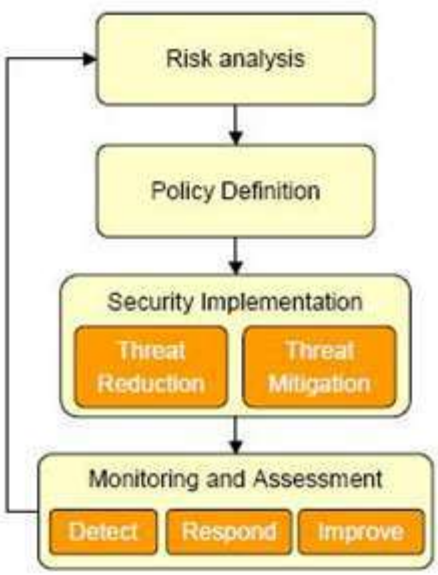

Figure 5 Security as a process

Source: L. Phifer [44]

It’s extremely important to understand the attacks that might affect a network. However, it should be noted that some attacks are less likely or more damaging than others. More also, it should be noted that it is not practical or possible to defend any network against all possible attacks. A more realistic goal is to reduce associated risk to an acceptable level. Risks are put into perspective by identifying one’s own WLAN's vulnerabilities - the probability that attacker will exploit them - and business impact would occur. The following steps/points are necessary in performing risk analysis.

- Define business needs
- Document who needs WLAN access, and where?

- Identify users or groups permitted to use 802.11 at the office, on the road, and at home.
- Determine resources reached over wireless
- Which applications, databases, and shares must be opened to wireless users, and when?
- Next, quantify new business risks caused by adding wireless.
- What information do those services and databases contain?
- Consider data that resides on wireless stations and flows over wireless links
- For each asset, estimate the likelihood of compromise and potential cost to business, using quantifiable metrics like downtime, recovery expenses, etc

Completion of this process provides a prioritized list of at-risk assets. Base on this, a security policy that defends important assets from wireless-borne attack, balancing cost/benefit and residual risk can be written. Next step is to select, install, and configure countermeasures that implement and enforce the security policy.

CONDUCTING A VULNERABILITY ASSESSMENT

A vulnerability assessment is an explicit study that uses penetration testing and observation to identify security weaknesses that could be exploited, and the risks. The results obtained are then evaluated to determine severity and steps to reduce or eliminate the threats. To be truly effective, assessments should be carried out regularly to spot out newly-introduced vulnerabilities and verify that installed security measures are working as intended. Assessments may be performed by in-house or third- party staff, with full, partial, or no knowledge of the organization network and security implementation.

In the following sections, I present the techniques and tools that can be useful for conducting a WLAN vulnerability assessment: from wireless device discovery and penetration testing, to security event monitoring and spectrum analysis. A sample worksheet, provided in appendix, illustrates how assessment results can be documented for review and remediation.

WLAN DISCOVERY

The first step in any vulnerability assessment is identification of all wireless devices near the site(s) under test. By so doing, all authorized devices will be isolated from the rest - where as the authorized will be subjected to further assessment; the rest will be scrutinized to determine ownership, impact on WLAN operation, and potential threat.

Wi-Fi Stumblers – which are free, easy to use for simple tasks, and available for most Operating Systems – is one of the tools that can be used for this purpose. One limitation of Stumblers is that they can find APs, but not Stations or non-802.11 interference sources. They may supply GPS latitude/longitude, but cannot pinpoint indoor location. For complete vulnerability assessment, a portable WLAN Analyzer that can scan all RF channels, export details about all wireless devices, accurately plot results on floor plans, and make it easy to find newly-discovered devices is ideal.

Using the discovery tools, make a list of observed 802.11 and other devices. Record the following parameters: a) for APs, record their ESSID, MAC address, IP address, channel, SNR, and observed 802.11/802.1X settings, b) generate a similar list of discovered Stations, noting whether they are associated to an Ad Hoc node, probing for multiple ESSIDs, and/or actively associated with specific AP(s). For non-802.11 devices, a spectrum analysis is used to fingerprint type. To locate and indentify the unauthorized devices - including the owner -, use a "find" tool (or WIPS with rogue mapping).

VULNERABILITY/PENETRATION TESTING

The overall objective of penetration testing is to discover areas of the enterprise network where intruders can exploit security vulnerabilities. These tests are typically performed using automated tools that look for specific weaknesses, technical flaws or vulnerabilities to exploit, with the results presented to the system owner with an assessment of their risk to the networked environment and a remediation plan highlighting the steps needed to eliminate the exposures. Various types of penetration testing are necessary for different types of network devices. For example, a penetration test of a firewall is different from a penetration test of a typical user's machine. Even a penetration test of devices in the DMZ (demilitarised zone) is different from performing a scan to see whether network penetration is possible. The type of penetration test should be weighed against the value of the data on the machine being tested and the need for connectivity to a given service.

Tools like Nmap or Superscan are used to scan devices and ports. Active devices are fingerprinted to identify operating systems, server programs, accounts, and shares using tools like Winfingerprint and Xprobe. WEP traffic may be analyzed with a tool like Aircrack-ptw, while PSK authentication messages may be analyzed with coWPAtty. 802.1X/EAP user IDs may be recorded and passwordbased EAPs may be tested using a tool like Asleap.

USING WIRELESS INTRUSION PROTECTION SYSTEM (WIPS) TO MONITOR ACTIVITY

WIPS is a network monitoring tool that runs round the clock and pinpoints attacks or attempted attacks on wireless network. It is an extension of the advanced protection found in wired firewall and virtual private network security systems, but with a focus on wireless local area networks (WLANs). It uses traffic analysis to keep track of attack signatures, protocol errors, atypical behaviour, and policy violations, generating alerts and defensive actions. Within a given RF band, WIPS sensors listen to the air - both in local and remote offices - decoding 802.11/802.1X protocols and analyzing all wireless activity. WIPS servers understand wireless attacks and can enforce real-time wireless security policies - for example, it automatically locks down rogue devices. Intrusion alerts and related evidence are reported to a central database for future reference during routine compliance reporting or post-breach forensic analysis.

WIPS can be extremely useful during a WLAN vulnerability assessment, as WIPS can triangulate a discovered device's location on a floor plan, making searches more efficient. WIPS helps to spot misconfigured devices, actual attacks that may have occurred recently, problem-prone locations and devices that may warrant additional scrutiny and on-going risky user behaviour by generating policy-based alerts. Also during penetration testing, WIPS can confirm that tests are working as expected. It can teach how to recognize signs of attack. It can record information needed for incident investigation or understanding of its impact, long after the attack ends. WIPS can even combine current and past observations to suggest how to mitigate threats. Penetration test results can, in the other hand, help to fine-tune WIPS.

USING WIRELESS ANALYZERS FOR INVESTIGATION

WLAN and spectrum analyzers play important role during vulnerability assessment, from start to finish. A combination gives a tool that offers both performance and security monitoring functions for wireless LANs. Where as WLAN analyzers help capture packet on the air to display important information such as the list of access points and stations, per-node and per-channel statistics, signal strength, a list of packets and network connections, protocol distribution charts, etc., spectrum analyzers dig into non-802.11 transmissions – for example, RF interference coming from microwave oven. Portable (laptop or handheld-based) analyzers are useful while penetration tests are in progress as they provide a mobile platform for device discovery, traffic capture, and other eye-raising wireless activity. Remote analyzers - WIPS sensor or AP-based - can help to further investigate potential vulnerabilities at the end of tests. Portable analyzers are efficient for on-site investigation, while remote analyzers are more cost-effective for off-site investigation.

PUTTING ASSESSMENT RESULTS TO WORK

Wireless vulnerability assessment is an effective tool on which a good security policy that can defend organization assets is hinged on. Assessment reports usually rank identified vulnerabilities by severity and recommend countermeasures. These countermeasures are then installed and configured to implement and enforce the security policy. This is achieved through station and AP hardening, rogue detection and elimination, and deployment of 802.11/802.1X security measures.

- Rogue Management: In most cases, during vulnerability assessments, someunknown wireless devices are discovered. Assessment results always list all the discovered devices and their observed properties to facilitate threat assessment, classification, and elimination. For rogue management, a report for example might recommend classifying low-SNR APs as Neighbors so as to use ACLs to block unauthorized associations. It may, as well, recommend physical removal of discovered high-SNR APs connected to the corporate network without permission and stand-alone draft 802.11n APs installed by employees. As a proactive measure rogue management, a report can recommend adding suspicious stations to WIPS watch list to escalate any future alerts pertaining to them. Also, automated actions - like network connectivity checks and temporary wireless blocking - may be configured for malicious rogues that lie off-premises but within RF range.

- WLAN Infrastructure Hardening: Wireless access points (WAPs), switches,gateways, web portals, DNS/DHCP servers, and other devices connected to WLANs often need to be hardened to resist network-borne attacks. Recommendations of penetration test results might be countermeasures, like: changing AP defaults, disabling unnecessary services, eliminating unused ports, using stronger admin passwords or authentication methods, disabling wireless-side management and restricting wired-side to specific IP addresses and/or VLANs, using AP filters to prevent route updates or LAN broadcasts from getting to the wired network, fine-tuning DoS thresholds, and applying firmware upgrades/patches.

- Station Hardening: Wireless clients such as laptops, PDAs, wireless-enabled desktops, scanners, cameras, printers, VoFi phones, and field terminals also require hardening. Countermeasures and best practices - like personal firewalls - typically used to defend Internet-connected clients, are generally recommended for WLAN clients as well. WLAN-specific vulnerabilities indentified during penetration tests might require that further recommendations like configuring stations to associate only to corporate ESSIDS in infrastructure mode, checking 802.1X server certificates to avoid rogue AP is necessary. Deployment of host-resident Wi-Fi Intrusion Prevention program on every client helps to disconnect unsafe associations automatically. Also, WEP-only capable wireless adapters need to be scraped, and those with vulnerable drives should be patched.

- Securing Data In Transit: Assessments help to verify adherence to the corporatesecurity policy, and also identify weaknesses in that policy – if there is any. Test results should be able to list all wireless devices that associate without the mandatory corporate encryption technique. Recommendation could be blocking of employee associations to guest WLAN if the risk analysis shows that the risk is too high. In alternative, guests might be advised to protect themselves with VPN tunnels. Tests report may recommend alternatives to reduce over-the-air vulnerabilities and comply with data privacy regulations. WPA is advised for WLANs with legacy products. However, WPA2 is better for robust data privacy and integrity. But the best practice here is to secure data using VPN for off-site and WPA2 for on-site.

- Controlling Network Use: Also, assessments exercise should test the WLAN'sAccess Control and Authentication mechanisms to determine if there is a breach. And if yes, where? Test results may list plain user identities and crackable credentials that need to be strengthened. One of the consequences of cracked user credentials is unauthorized access to other systems in the corporate network. Here again, recommendations can be made to mitigate vulnerabilities, based on the WLAN's defined security policy. For example, if corporate policy stipulates authentication by PSK, test results should list ESSIDs with weak PSKs, recommending replacement with stronger PSKs or perhaps 802.1X

Table 7 below shows some of the wireless attacks listed in table 7 above matched against the specific countermeasures to mitigate them. As can be seen from the table, there exists more than one countermeasure for each attack – some are simple, some are complicated. To mitigate an attack, you don’t need to implement all, war driving for example.

However, a combination of measures makes the network more robust and secured against the attack.

Table 7: Wireless attacks and countermeasures

Attack	Category/Target	Countermeasures
War Driving	Network Access	Change the Access Point default Admin password, always update the Access Point firmware and drivers for the wireless Adapter(s); Use the highest level of WEP/WPA (WPA2/802.11i strongly preferred); Authenticate wireless users with protocols like 802.1X, RADIUS, EAP (including EAP-PAX, EAP-PSK, EAP-TLS, EAP-TTLS, EAP-FAST, EAP-POTP, EAP-IKEv2, PEAP, and EAP-SIM); Use strong encryption for all applications that run over the wireless network, e.g., use SSH and TLS/HTTPS; Encrypt wireless traffic using a VPN (Virtual Private Network), e.g. using IPSEC or other VPN solutions; Create a dedicated segment for Wireless Network, and take additional steps to restrict access to this segment; Use a proxy with access control for outgoing requests (web proxy, and others).
MAC Spoofing	Network Access	Use of 802.11i (TKIP and CCMP) or VPNs (Session Encryption); AP Authentication; User based Authentication; Static ARP Mapping; Port Security.
802.11 De-	Network Availability	Requires strong authentication of management

authentication Flood		and control frames.
Rogue Access Points	Network Access	Wireless Security Policy; Physical Security; Wired and Wireless Network Separation; Corporate Security Policy/Users Separation; Authentication; Use of Wireless Intrusion Prevention Systems (WIPS); Network Connectivity Checks and Temporary Wireless Blocking; Disabling Unused Ports.
Eavesdropping	Message Confidentiality	Physical Security; T802.1x or VPNs; 802.11i (TKIP & CCMP)
WEP Key Cracking	Message Confidentiality	WPA & 802.11i i.e. TKIP (known as WPA1) and CCMP (also known as WPA2)

Attack	Category/Target	Countermeasures
Man-in-the-Middle	Message Confidentiality	Physical Security; T802.1x or VPNs; Strong Authentication Protocols: PKI, Mutual Authentication, Secret Keys, Passwords e.t.c.
RF Jamming	Network Availability	Mac Filtering; Firewalls (wired); IDS (Wired), DMZ architecture; 802.11i; Dynamic Channel Assignment.
Dictionary Attacks (Crack passwords)	Network Access	Strong Password Policy, 802.1x and VPNs
802.11 Frame Injection	Network Availability	WPA & 802.11i (MIC Algorithm)
Evil Twin AP	Message Confidentiality	Use of Wireless Intrusion Detection or Prevention System; Use of 802.1X Port Access Control for robust mutual authentication; Use of strong Extensible Authentication Protocol (EAP-TLS, EAP-TTLS, or PEAP) to check servers' signature; Use of product like Wavelink Avalanche or Windows Active Directory Group Policy Objects to administer 802.11 and 802.1X parameters on Windows PCs for centrally-manage PCs; Users' education.
Session Hijacking	Network Access	802.11i, 802.1x & VPNs
AP Phishing	Message Confidentiality	Use of Wireless Intrusion Prevention System (WIPS); Use of strong Extensible Authentication Protocol (EAP-TLS, EAP-TTLS, or PEAP) to check servers' signature; Use of Personal Firewalls for Wireless Devices

In summary, there are ten steps that need to be taken in order to deploy a secured enterprise wireless LAN after an assessment has been carried out. They are:

f Document a wireless security policy

f Break the wireless network into SSIDs

f Implement access controls

f Deploy authentication credentials

f Encrypt wireless data

f Harden WLAN infrastructure

f Defend wireless clients

f Monitor wireless traffic

f Prevent wireless intrusions

f Enforce network security [28]

CONCLUSION

This work was done to find out if there are known inherent insecurities that limit enterprise deployments of a WLAN. And if yes, are there countermeasures that can be put in place to fix these known security holes for secure enterprise deployment of wireless networks

WLAN technology has inbuilt security problems in its architecture, as the APs and the clients must advertise their existence through beacon frames, thereby exposing the signals to attackers

There exist a wide range of attacks – from passive to active- on wireless LANs, and are aimed at the confidentiality and integrity of an information, and network availability as shown in table 7. Some of the attacks are less likely or more damaging than others, and some are more common than others. Vulnerability assessment is necessary to determine the combination of measures that should be implemented to mitigate the risks associated with the use of wireless technologies.

REFERENCES

1. W. Stallings, *Wireless Communications and Networks*. Pearson Education, India, 2006, pp 448-492.

2. R. Pejman, & L. Jonathan, *802.11 Wireless LAN fundamentals: A Practical Guideto understanding, designing and operating 802.11WLANs.* Cisco Press, Indiana,pp 21-34.

3. W. Noonan, *Hardening Network Infrastructure: Bulletproof Your Systems BeforeYou are Hached!* , McGraw-Hill Professional, New York, 2004.

4. W.Stallings, *Cryptography and Network Security Principles and Practice*, 4th edn, Pearson Education, India, 2006.

5. C. Doru, ‘Telecommunication System: Wireless Local Area Network’, Blekinge Institute of Technology, Nov. 2005, pp 1-54.

6. Y. Jui-Hung, C. Jyh-Cheng & L. Chi-Chen, ‘WLAN Standards: In Particular, The IEEE 802.11 Family,’ *Potentials, IEEE,* Vol. 22, Issue 4, Oct.-Nov. 2003, pp 16 – 22.

7. D. Smith, ‘What Makes up a WLAN’, Techrepublic, May 2007, retrieved 27 June 2008, < http://articles.techrepublic.com.com/5100-10878_11-1048092.html>

8. J. Burell, ‘Wireless Local Area Networking: Security Assessment and Countermeasures: IEEE 802.11 Wireless Networks’, Dec. 2002, retrieved 16 May 2008, <telecom.gmu.edu/publications/Jim-Burrell-December-2002.pdf>

9. G. Ollman, ‘Securing WLAN Technologies: Secure Configuration Advice on Wireless Network Setup’, Technicalinfo , retrieved 18 April 2008, <http://www.technicalinfo.net/papers/SecuringWLANTechnologies.html>

10. K. Fleming, ‘Wireless Security Initiatives’ May 2005, retrieved 16 May 2008, < http://telecom.gmu.edu/publications/Kieth-Fleming-Wireless-Security-Project-f2-May-2005.doc>

11. J. Epstein, ‘802.11w Fills Wireless Security Holes’, Network World, April 2006, retrieved 05 July 2008, http://www.networkworld.com/news/tech/2006/040306-80211w-wireless-security.html

12. F. Mlinarsky, ‘802.11T Puts WLANs To The Test’, Network World, March 2006, retrieved 05 July 2008, http://www.networkworld.com/news/2006/031306-wireless-lans-80211t.html

13. D. Molta, ‘802.11r: Wireless LAN Fast Roaming’ *The Promise of Secure Wi-FiMobility*, Network Computing, April 2007, retrieved 02 July 2008,<http://www.networkcomputing.com/showArticle.jhtml?articleId=198900107>

14. D. Stanley, 'Standards Corner: IEEE 802.11m - 802.11 Standard Maintenance', The Edge, June 2007, retrieved 04 July 2008, <https://edge.arubanetworks.com/article/standards-corner-ieee-802-11m-802-11-standard-maintenance>

15. D. Halasz, 'IEEE 802.11i and wireless security', Embedded.com, August, 2004, retrieved 06 July 2008, <http://www.embedded.com/columns/specialreports/ 34400002?_requestid=402884>

16. C. Jyh-Cheng, J. Ming-Chia, & L. Yi-wen, 'Wireless LAN security and IEEE 802.11i' *Wireless Communications, IEEE,* Vol. 12, Issue 1, Feb. 2005, pp 27 – 36.

17. IEEE 802.11i: WLAN Security Standards, Javvin Network Management & Security, retrieved 01 July 2008, < http://www.javvin.com/protocol80211i.html>

18. WiFi – Introduction, Kioskea, retrieved 01 July 2008, <http://en.kioskea.net/wifi/wifiintro.php3>

19. B. Mitchell, 'Wireless Standards - 802.11b, 802.11a, 802.11g and 802.11n' *The802.11 family explained,* About.com, retrieved 02 July 2008,<http://compnetworking.about.com/cs/wireless-80211/a/aa80211standard.htm>

20. B. Mitchell, 'IEEE 802.11 Working Group Standards', About.com, retrieved 02 July 2008, <http://compnetworking.about.com/cs/wireless80211/a/aa80211standard _2.htm>

21. J. Mallery, J. Zann, P. Kelly, W. Noonan, P. Love, E.S. Seagren, R. Kraft, & M.O'Neill, *Hardening Network Security: Network Security,* McGraw-Hill Professional, New York, 2005, pp 323-349.

22. K. Sankar, Cisco *Wireless LAN Security: Expert Guidance for Securing Your802.11 Networks,* Cisco Press, Indianapolis, 2004, pp 125-155.

23. J.Koziol, *Intrusion Detection with Snort,* Sams Publishing, Indianapolis, 2003.

24. E. Sithirasenan, S. Zafar, & V. Muthukkumarasamy, 'Formal Verification of the IEEE 802.11i WLAN Security Protocol*', J. IEEE Computer Society,* Issue 18-21, April 2006, pp 181-190.

25. D. Welch, & S. Lathrop, 'Wireless Security Threat Taxonomy', *J. IEEE Systems,* Issue 18-20, June 2003, pp 76 – 83

26. Sinha, I. Haddad, T. Nightingale, R. Rushing, & D. Thomas, 'Wireless Intrusion Protection System Using Distributed Collaborative Intelligence' *J. IEEE IPCCC,* Issue 10-12, April 2006.

27. S. McQuerry, *Wireless LANs: Extending the Reach of a LAN*, Cisco Press, 2008, retrieved 09 July 2008, <http://www.ciscopress.com/articles/article.asp?p= 15668&seqNum=3>

28. L. Phifer, *Ten Steps to Wireless LAN Security*, Search Networking, retrieved 09 July 2008, < http://searchnetworking.techtarget.com.au/tips/24729-Ten-steps-to-wireless-LAN-security>

29. Network security- Learning Space, *Threats to Communication Networks,* retrieved 10 July 2008, <http://openlearn.open.ac.uk/mod/resource/view.php?id=183172>

30. B. Potter & B.Fleck, *802.11 Security: Attacks and Risks*, Search Networking, 2003, retrieved 10 July 2008, <http://searchnetworking.techtarget.com/generic/0,295582, sid7_gci1050371_tax303099,00.html>

31. NetworkDictionary, *How to Install Network Sniffing Tools for Effective TrafficMonitoring?*, retrieved 11 July 2008, < http://www.networkdictionary.com/howto/NetworkSniffer.php>

32. LOT3K, Sniffing Networks: *The Complete Documentation*, retrieved 11 July 2008, <http://www.l0t3k.org/security/tools/sniffing/>

33. Javvin Technologies, *Network Packet Analyzer CAPSA 6.8*, retrieved 11 July 2008, <http://www.javvin.com/packet.html>

34. CERT, *Denial of Service Attacks*, retrieved 12 July 2008, <http://www.cert.org/tech_tips/denial_of_service.html>

35. TECHWEB, *Replay Attack*, retrieved 12 July 2008, <http://www.techweb.com/encyclopedia/defineterm.jhtml?term=replay+attack>

36. L. Phifer, *Lesson 1: How to counter wireless threats and vulnerabilities*, Search Networking, 2006, retrieved 12 July 208, < http://searchnetworking.techtarget.com/general/0,295582,sid7_gci1172482,00.html?track=wsland>

37. Rapid7, *Penetration Testing Augments Vulnerability Management*, retrieved 12 July 2008, <http://www.rapid7.com/services/pentest.jsp>

38. 3Com, *New 3Com Systems Keep Wireless LANs Safe from Rogue Devices,Hackers and Vulnerabilities*, retrieved 13 July 2008,<http://www.3com.com/corpinfo/en_US/Pressbox/press_release.jsp?INFO_ID=265117>

39. Verisign, *An Introduction to Network-Vulnerability Testing*, retrieved 22 July 2008, <http://www.verisign.co.uk/static/029888.pdf>

40. Motorola, *Enterprise Wireless LAN Security*, March 2008, retrieved 22 July 2008, <http://www.motorola.com/staticfiles/Business/_Documents/static%20files/WLAN_Security_WP_0308_New.pdf>

41. L. Phifer, *Wi-Fi Vulnerability Assessment Checklist*, SearchSecurity, Mar 2006, retrieved 19 July 2008, <http://searchsecurity.techtarget.com/generic/0,295582, sid14_gci1167666, 00.html>

42. Cisco Systems, *Five Steps to Securing Your Wireless LAN and PreventingWireless Threats*, 2006, retrieved 11 July 2008, <http://www.cisco.com/en/US/prod/collateral/ wireless/ps5678/ps6521/prod_white_paper0900aecd8042e23b_ns386_Networking_Solutions_White_Paper.html>

43. R. Apinantrakul, S. Malisuwan, & K. Kasemsan, *The Risk Analysis of WLANSecurity Systems for Organizations in Thailand*, retrieved 21 June 2008,<http://www.rsu.ac.th/ grad/research/paper/2006/RiskAnalysisWLAN.pdf>

44. L. Phifer, *Managing WLAN Risks with Vulnerability Assessment*, AirMagnet, retrieved 11 July 2008, < http://www.airmagnet.com/assets/whitepaper/WLAN_ Vulnerabilities _White_Paper.pdf>

45. L. Phifer, *Wireless attacks, A to Z*, SearchNetworking, April 2006, retrieved 11 July 2008, <http://searchnetworking.techtarget.com/generic/0,295582,sid7_gci1173698, 00. html>

46. Intermec, *Wireless Security: It's Like Securing Your Home*, June 2003, retrieved 11 July 2008, <http://epsfiles.intermec.com/eps_files/eps_wp/WirelessSecurity_wp _web.pdf>

47. M. Kujala, *WLAN Standards and Wireless Networking Security*, May 2003, retrieved 11 May 2008, < http://www.tml.tkk.fi/Studies/T-110.551/2003/papers/3.pdf>

48. Flextronics, *Trends in WLAN Technology*, 2005, retrieved 1 July 2008, http://www.futsoft.com/pdf/wlan_trends_note.pdf

49. 'Wireless *Security* – Information for CIOs', February 2006, retrieved 27 June 2008, <http://www.ag.gov.au/agd/WWW/rwpattach.nsf/VAP/(7A188806B7893EBA0402BC1472412E58)~Wireless+Security++Overview+CIOs.PDF/$file/Wireless+Se curity+-+Overview+CIOs.PDF>

50. N. Chendeb, B. Hassan & H. Afifi, 'Performance Evaluation of the Security in Wireless Local Area Networks (WiFi)', *J. IEEE I&CT*, April 2004, pp 215- 216.

51. S. Radack, *Security for Wireless Networks and Devices*, retrieved 15 April 2008, <http://www.itl.nist.gov/lab/bulletns/bltnmar03.htm >

52. D. Nayak, N. Rajendran, D.B.Phatak & V.P.Gulati, 'Security Issues in Wireless Local Area Networks' *J. IEEE*, vol 3, May 2004, pp 1637 – 1640.

53. B. Issac & L. A. Mohammed, 'War Driving and WLAN Security Issues — Attacks, Security Design and Remedies', *J. ISM*, Vol. 24, Issue 4, January 2007, pp 289 – 298.

54. K.H. Lim, *Security Guidelines for Wireless LAN Implementation*, August 2003, retrieved 18 April 2008, <http://www.sans.org/reading_room/whitepapers/wireless /1233.php>

55. Y. Jiang, C. Lin, H. Yin & Z. Chen, 'A Mutual Authentication and Privacy Mechanism for WLAN Security' *J. Wirel. Commun. Mob. Comput.*, Vol. 8, Issue 1, September 2006, pp 101 – 112.

56. Mishra, N.L. Petroni Jr, W.A. Arbaugh, & T. Fraser, 'Security Issues in IEEE 802.11 Wireless Local Area Networks: A Survey', *J. Wirel. Commun. Mob.Comput.*, vol. 4, Issue 8, November 2004, pp 821-833.

57. N. Wei, J. Zhou, Y. Xin, & L. Li, 'A Security Architecture for IEEE 802.11 Wireless Networks in Large-scale Multinational Corporations', *ITSTelecommunications Proceedings*, June 2006, pp 846-849.

58. R. Zhang, & J. Welch, 'A Survey on Current Practices in Enterprise Wireless Networking and Security Management', *J. Information Systems*, vol. 8, issue 2, 2007, pp 279-382.

59. N. Borisov, I. Goldberg, & D. Wagner, *Security of the WEP Algorithm*, UC Berkeley, retrieved 18 April 2008, http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

60. Symantec, *Wireless LAN Security: Enabling and Protecting the Enterprise*, Symantec Enterprise Security, May 2002, retrieved 24 May 2008, < http://www.symantec.com /avcenter/reference/symantec.wlan.security.pdf>

61. V. Bhargava, & M.L. Sichitiu, 'Physical Security Perimeters for Wireless Local Area Networks', *J. Network Security*, vol.3, issue 2, September 2006, pp124-135.

62. Cisco, *A Comprehensive Review of 802.11 Wireless LAN Security and the CiscoWireless Security Suite*, 2002, retrieved 18 April 2008,<http://www.cisco.com/warp /public/cc/pd/witc/ao1200ap/prodlit/wswpf_wp.pdf>

63. AirWave, *Best Practices Guide: Eight Things You Can Do TODAY to ImproveWireless Network Security*, 2008, retrieved 16 April 2008, < www.airwave.com/resource-center/>

64. EUSSO, *54Mbps Wireless-G Cardbus Adapter: Linking your Computer withWireless G network*, retrieved 16 April 2008,<http://www.eusso.com/Models/Wireless/UGL2454-01R/UGL2454-01R.htm#Diagram>

65. WLANA, retrieved 16 April 2008, <www.wlana.org>