WIRELESS LAN SECURITY AND LABORATORY DESIGNS[*]

Yasir Zahur and T. Andrew Yang
University of Houston Clear Lake
Houston, TX 77058
yang@cl.uh.edu

ABSTRACT

For the past couple of years, increasing number of wireless local area networks (WLANs), based on the IEEE 802.11 protocols, have been deployed in various types of locations, including homes, schools, airports, business offices, government buildings, military facilities, coffee shops, book stores, as well as many other venues. One of the primary advantages offered by WLAN is its ability to provide untethered connectivity to portable devices, such as wireless laptops and PDAs. In some remote communities, WLANs are implemented as a viable *last-mile* technology [4], which link homes and offices in isolated locations to the global Internet. The further widespread deployment of WLANs, however, depends on whether secure networking can be achieved. In order for critical data and services to be delivered over WLANs, reasonable level of security must be guaranteed. The WEP (*Wired Equivalent Privacy*) protocol, originally proposed as the security mechanism of 802.11b WLANs, is known to be easily cracked by commonly available hacking software. Alternative security mechanisms, such as SSL, VPN, Cisco's LEAP, 802.1x, and the being-developed 802.11i protocols, provide mechanisms to enhance security in WLANs. In this paper we study the security aspects of WLANs, by starting with an overview of the WLAN technology and the respective vulnerabilities of various protocols, followed by a discussion of alternative security mechanisms that may be used to protect WLANs. At the end we present a sequence of laboratory designs, which are used as platforms on which attacks at WLANs can be simulated and studied, and alternative security solutions can be implemented and tested.

1. INTRODUCTION

We are designing a new course on *'Wireless Computing and Security'*, in which WLANs and related security issues are a major component. One of the goals in designing the course is to include practical hacking and defense laboratories in the course as student projects. To supplement studying of the theoretical fundamentals of wireless computing, it is desirable that students would be able to use simple hardware and software to set up WLANs and test the various hacking and defense methods. We have conducted a survey of the WLAN standards, their features and vulnerabilities. Another survey of security mechanisms for WLANs revealed that SSL (Secure Socket Layer), VPN (Virtual Private Networks), Cisco's LEAP (Lightweight EAP) and the new 802.11i protocols are viable protection methods that may be adopted to enhance WLAN security. Based on the two surveys, we then designed a sequence of labs that use simple hardware and software configurations to provide various test beds on which the vulnerabilities and security mechanisms of WLANs can be studied.

The rest of the paper includes the result of our study and research, starting with a survey of the WLAN standards and their respective vulnerabilities, followed by discussions of alternative protection mechanisms, and laboratory designs which provide various configurations of platforms for students to launch attacks and to implement security solutions in a closed WLAN. Appendix A contains a mini dictionary with common WLAN-related terminology.

2. WIRELESS LANS

In general, a WLAN consists of a central connection point called the *Access Point* (AP). It is analogous to a hub or a switch in traditional star-topology-based wired LANs. The AP transmits data between different nodes of a WLAN and, in most cases, serves as the only link between the WLAN and the wired networks.

IEEE has specified various WLAN standards, some of which are summarized below in Table 1 [19].

Standard	Description	Approved
IEEE 802.11	Data rates up to 2Mbps in 2.4GHz ISM band	July 1997
IEEE 802.11a	Data rates up to 54Mbps in 5GHz UNII band	Sept 1999
IEEE 802.11b	Data rates up to 11Mbps in 2.4GHz ISM band	Sept 1999

Table 1: IEEE WLAN Standards

The security features provided in 802.11b standard are as follows [16]:

1) SSID (*Service Set Identifier*)

SSID acts as a WLAN identifier. Thus all devices trying to connect to a particular WLAN must be configured with the same SSID. It is added to the header of each packet sent over the WLAN and verified by the AP. A client device cannot communicate with an AP unless it is configured with the same SSID.

2) WEP (*Wired Equivalent Privacy*)

According to the 802.11 standard, WEP was intended to provide "confidentiality that is subjectively equivalent to the confidentiality of a wired local area network (LAN) medium that does not employ cryptographic techniques to enhance privacy" [7]. IEEE specifications for wired LANs do not include data encryption as a requirement. This is because approximately all of these LANs are secured by physical means such as walled structures and controlled entrance to buildings, etc. However no such physical boundaries can be provided in case of WLANs, thus justifying the need for an encryption mechanism.

3) MAC Address Filters

In this case, the AP is configured to accept association and connection requests from only those nodes whose MAC addresses are registered with the AP. This scheme provides an additional security layer.

3. VULNERABILITIES OF IEEE 802.11 WLANS

Ubiquitous network access without wires is the main attraction underlying wireless network deployment. Although this seems to be enough attraction, there exists other side of the picture. In this section, we discuss how WLANs could be vulnerable to a myriad of intrusion methods.

3.1 General Wireless Network Vulnerabilities

1) Invasion & Resource Stealing

Resources in a network include access to various devices (such as printers and servers) and services (such as connectivity to an intranet or the Internet). To invade a network, the attacker will first try to determine the access parameters for that particular network. Hacking techniques such as *MAC spoofing* [9] [20] may be used to attack a WLAN. For example, if the underlying network uses MAC-address-based filtering of clients, all an intruder has to do is to find out the MAC address and the assigned IP address for a particular client. The intruder will wait till that client goes off the network and then start using the network and its resources while appearing as a valid user.

2) Traffic Redirection

An intruder can change the route of the traffic and thus packets destined for a particular computer can be redirected to the attacking station.

3) Denial of Service (DOS)

Two types of DOS attacks against a WLAN can exist. In the first case, the intruder tries to bring the network to its knees by causing excessive interference. An example could be excessive radio interference caused by 2.4 GHz cordless phones [16]. A more focused DOS attack would be when an attacking station sends 802.11 *disassociate* message or an 802.1x *EAPOL-logoff message* (captured previously) to the target station and effectively disconnects it (as in "Session Hijack" attacks). The later type of DOS attack is described in more detail in section 3.3.3.

4) Rogue Access Points

A rogue AP is one that is installed by an attacker (usually in public areas like shared office space, airports, etc.) to accept traffic from wireless clients to whom it appears as a valid Authenticator. Packets thus captured can be used to extract sensitive information, or for launching further attacks by, for example, modifying the content of the captured packet and re-insert it into the network.

3.2 IEEE 802.11b Vulnerabilities

The above stated concerns relate to wireless networks in general. The security concerns raised specifically against IEEE 802.11b networks are as following [7]:

1) *MAC Address Authentication:* Such sort of authentication establishes the identity of the physical machine, not its human user. Thus an attacker who manages to steal a laptop with a registered MAC address will appear to the network as a legitimate user.

2) *One-way Authentication:* WEP authentication is client-centered or one-way only. This means that the client has to prove its identity to the AP but not vice versa. Thus a rogue AP may successfully authenticate the client station and then subsequently will be able to capture all the packets sent by that station through it.

3) *Static WEP Keys:* There is no concept of dynamic or per-session WEP keys in 802.11b specification. Moreover the same WEP key has to be manually entered at all the stations in the WLAN, causing key management issues.

4) *SSID:* Since SSID is usually provided in the message header and is transmitted in clear text format, it provides very little security. It is more of a network identifier than a security feature.

5) *WEP Key Vulnerability:* WEP key based encryption was included to provide same level of data confidentiality in wireless networks as exists in typical wired networks. However a lot of concerns were raised later regarding the usefulness of WEP. Some of them are as following:

a. Manual Key Management: Keys need to be entered manually on all the clients and Access Points. Such key management overhead may result in WEP keys that are not changed frequently.

b. Key Size: The IEEE 802.11 design community blames 40-bit RC4 keys for this and recommends using 104 or 128-bit RC4 keys instead. Although using larger key size does increase the work of an intruder, it does not provide completely secure solution [17].

c. Initialization Vector (IV): IV is used to avoid encrypting two identical plain texts with the same key stream and thus result in the same cipher text. By combining a randomly generated IV with the key, the probability of two identical plain texts being encrypted into identical cipher texts is minimized.

In WEP encryption the secret WEP key is combined with a 24-bit IV to create the key. RC4 takes this key as input and generates a key sequence equal to the total length of the plain text plus the IV. The key sequence is then XOR'ed with the plain text and the IV to generate the cipher text.

According to findings reported in [17], the vulnerability of WEP roots from its initialization vector and not from its smaller key size. WEP is based on RC4 algorithm, which is a stream cipher algorithm. Two frames that use the same IV almost certainly use the same secret key and key stream. Moreover, since the IV space is very small, repetition is guaranteed in busy networks.

d. Decryption Dictionaries: Infrequent re-keying and frames with same IV result in large collection of frames encrypted with same key streams. These are called *decryption dictionaries* [4]. Therefore, even if the secret key is not known, more information is gathered about the unencrypted frames and may eventually lead to the exposure of the secret key.

3.3 IEEE 802.1x Protocol and Vulnerabilities

IEEE 802.1x is a port-based authentication protocol. There are three different types of entities in a typical 802.1x network, including a *supplicant*, an *authenticator* and an *authentication server* [13]. To permit the EAP traffic before the authentication succeeds, a dual-port model is used in IEEE 802.1x specifications. In an unauthorized (uncontrolled) state, the port allows only DHCP and EAP traffic to pass through.

When applied to 802.11b, the 802.1x specification includes two main features: (1) logical ports and (2) key management [8]. In the rest of this section we first discuss these two features, followed by a discussions of vulnerabilities unveiled by some researchers.

3.3.1 Logical Ports

Unlike wired networks, wireless stations are not connected to the network by physical means. They must have some sort of association relation with an AP in order to use the WLAN. This association is established by allowing the clients and the AP to know each other's MAC address. This combination of MAC address of the AP and that of the station acts as a logical port. This then acts as a destination address in EAPOL protocol exchanges.

3.3.2 Key Management

IEEE 802.1x specifications do not emphasize on using WEP key for encryption. This is because key information is passed from an AP to a station using *EAPOL-Key* message. Keys are generated dynamically, at a per-session basis.

Typical configuration of a WLAN using IEEE 802.1x is shown in Figure 1.

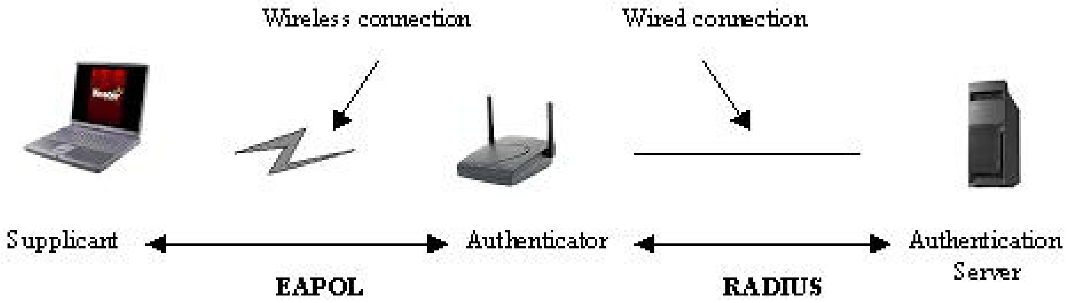

Figure 1: IEEE 802.1x in 802.11 WLANs

The *Supplicant* authenticates with the *Authentication Server* by using EAPOL to communicate with the AP, which acts as the *Authenticator*. Messages are exchanged between the Supplicant and the Authenticator to establish the Supplicant's identity. The Authenticator then transfers the Supplicant's information to the Authentication Server using RADIUS. All communications between the Authentication Server and the Supplicant passes through the Authenticator using EAP over LAN (i.e., EAPOL) and EAP over RADIUS, respectively. This creates an end-to-end EAP conversation between the Supplicant and the Authentication Server.

3.3.3 Vulnerabilities of 802.1x

Recent findings published by researchers from University of Maryland ([11]), however, have unveiled design flaws and the resulting vulnerabilities in such integration of 802.1x with 802.11b. Two of the vulnerabilities identified are 'absence of mutual authentication' and 'session hijacking', which we provide an overview below. For more technical details about the design flaws and other vulnerabilities, please consult the original publication.

1) Absence of *Mutual Authentication*

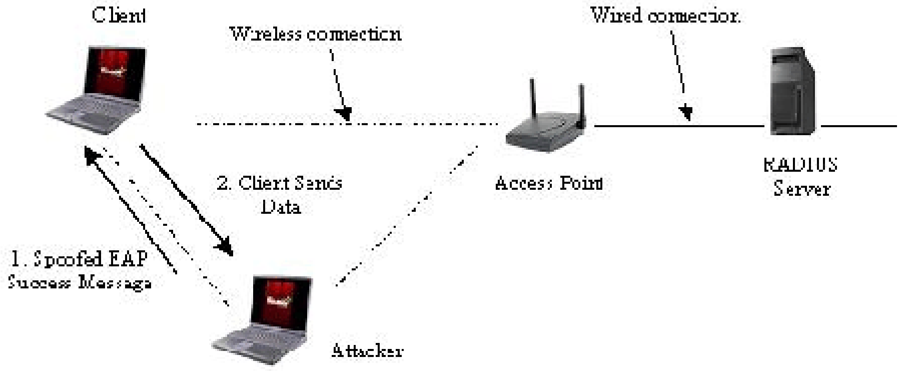

Figure 2: Man-In-the-Middle Attack Setup

According to 802.1x specifications, a Supplicant always trusts the Authenticator but not vice versa. Consider Figure 2. There is no EAP Request message originating from the Supplicant (the *client*). It only responds to the requests sent by the Authenticator (the *AP*). This one-way authentication opens the door for "MAN IN THE MIDDLE ATTACK".

The *EAP-Success* message sent from the Authenticator to the Supplicant contains no integrity preserving information. An attacker can forge this packet to start the attack.

2) Session Hijacking

With IEEE 802.1x, RSN (*Robust Security Network*) association has to take place before any higher layer authentication. Thus we have two state machines. One is classic 802.11 and the other is 802.1x based RSN state machine. Their combined action should dictate the state of authentication. However, due to a lack of clear communication between these two state machines and message authenticity, "Session Hijacking Attack" becomes possible.

Consider Figure 3. First of all, the *supplicant* and the *authenticator* (the AP) engage in the authentication process (steps 1 through 3), which results in the supplicant being authenticated. An attacker then sends a *MAC-disassociate* message using the AP's MAC address (step 4). The valid supplicant will disassociate when receiving the *MAC-disassociate* message. This causes the RSN state machine to transfer to the *Un-Associated* state. However, since this *disassociate* message was sent by the attacker (impersonating as the real access point), the real access point does not know about it. Thus the 802.11 state machine remains in *Authenticated* state for that particular client in the real AP. The attacker then gains network access using the MAC address of the authenticated supplicant (which is disassociated by now).

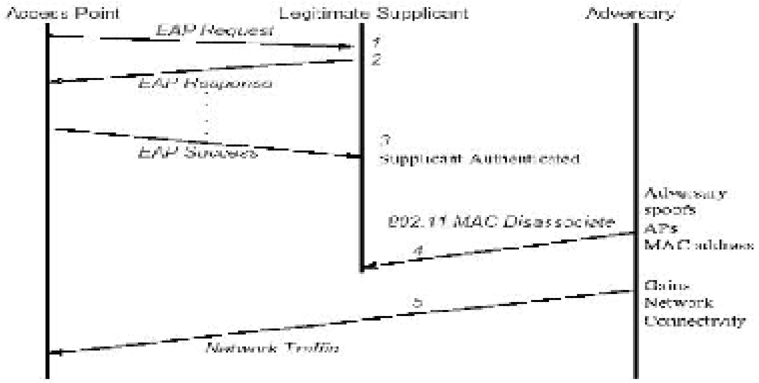

Figure 3: Session Hijack Attack [11]

4. ALTERNATE SOLUTIONS

Given the reported vulnerabilities of IEEE 802.11 protocols, alternate protection methods must be adopted to offer the existing WLANs reasonable security. The new IEEE 802.11i protocol, which is currently under development, is supposed to remedy the vulnerabilities reported in 802.11b and 802.1x protocols. Readers who are interested in the development status of the new 802.11i protocol may refer to [1] and [6], or visit the IEEE 802 Standards site at http://grouper.ieee.org/groups/802/ for more information.

Three alternative solutions for WLANs are discussed in this section: VPN, Cisco LEAP, and SSL.

4.1 Virtual Private Networks (VPN)

VPN technology provides the means to securely transmit data between two network devices over an insecure data transport medium [15]. VPN technology has been used successfully in wired networks especially when using Internet as a physical medium. This success of VPN in wired networks and the inherent security limitations of wireless networks have prompted developers and administrators to deploy VPN to secure WLANs.

VPN works by creating a tunnel, on top of a protocol such as IP. VPN technology provides three levels of security [15]:

- *Authentication:* A VPN server should authorize every user who logged on at a particular wireless station trying to connect to the WLAN using a VPN client. Thus authentication is user based instead of machine based.
- *Encryption:* VPN provides a secure tunnel on top of inherently insecure medium like the Internet. To provide another level of data confidentiality, the traffic passing through the tunnel is also encrypted.
- *Data authentication:* It guarantees that all traffic is from authenticated devices.

4.2 CISCO LEAP (Lightweight EAP)

Cisco *LEAP* (aka *EAP Cisco Wireless*) supports strong mutual authentication between a client and a RADIUS server. LEAP is a component of the *Cisco Wireless Security Suite.* Cisco introduced LEAP in December 2000 as a preliminary way to quickly improve the overall security of wireless LAN authentication.

Cisco has addressed the above described 802.1x vulnerabilities with the LEAP and Cisco WEP enhancements, such as the *message integrity check (MIC)* and per *packet keying* [3].

1) Mutual Authentication between Client Station and Access Point

As described in section 2, the problem of *Rogue Access Points* can be attributed to the one-way, client-centered authentication between the client and the AP. LEAP requires two-way authentication, i.e., a client can also verify the identity of the AP before completing the connection.

2) Distribution of WEP Keys on a Per-session Basis

As opposed to the static WEP Keys in 802.11b specifications, LEAP protocol supports the notion of *dynamic session keys*. Both the Radius Server and the client independently generate this key. Thus the key is not transmitted through the air where it could be intercepted. The attacker posing as the authenticated client will not have access to the keying material and will not be able to replicate the WEP session key. As a result, all frames sent to and from the attacker will be dropped. This effectively mitigates the 'Session Hijack' attack described earlier.

4.3 SSL (Secure Socket Layer)

SSL is an application level protocol that enables secure transactions of data and relies upon public/private keys and digital certificates. When using SSL in WLAN environment, once a wireless client is communicating with an Access Point (using WEP), a user is NOT able to DO ANYTHING on the wireless connection until properly authenticated. This authentication is accomplished using the additional level of SSL security encryption. Since WEP alone does not ensure secure wireless communications, people are encouraged to use applications that provide encryption such as SSL-based secure websites.

5. LABORATORY DESIGN

Laboratory designs presented below serves two purposes: 1) They provide various WLAN setup for students to launch attacks, by exploiting vulnerabilities discussed in sections 3.2 and 3.3; 2) The simple setups allow students to test the alternative protection solutions discussed in section 4.

5.1 Desktop Computers

When designing the WLAN labs, we have used two Intel based desktop computers. Both of them are associated with the Access Point to create an Infrastructure based WLAN. One of them acts as a server hosting a program that generates sample data. It also acts as a VPN server and/or as an authentication server, etc., depending on the underlying method being employed in an experiment. The second computer acts as a client of VPN, LEAP or SSL, etc., again depending on the underlying method being employed in an experiment.

A. Hardware Configuration

- Processor: Intel Pentium II 400MHz
- RAM: 256MB
- Network Adapter: Cisco Aironet 350 Series Wireless LAN Adapter

B. Software Configuration

- Operating System: Windows 2000 Professional
- ACU (Aironet Client Utility): This utility comes with the Aironet card. It is used to perform user level diagnostics on the Cisco Wireless LAN adapter card. It allows us to upgrade firmware, view current device status, view current device statistics and perform a link test to assess the performance of RF link at various places.
- IPSU (IP Setup Utility): It is used to get the IP address of a wireless Ethernet device based on the device MAC ID. The user may also use this utility to set the IP Address and the SSID if the device is still in the default state.

5.2 Laptop Computer

An Intel-based laptop is used as the attacking device used by a potential attacker trying to crack the WEP key in the WEP-enabled WLAN configuration (see Figure 4). Depending on the type of attacks, it usually hosts a hacking program, such as AirSnort (for cracking the WEP key).

A. Hardware Configuration
- Processor: Intel Pentium III 600MHz
- RAM: 256MB
- Network Adapter: Cisco Aironet 350 Series Wireless LAN PCMCIA Adapter

B. Software Configuration of the laptop is the same as the desktop.

5.3 Access Point

An AP is absolute necessity in wireless LANs running in Infrastructure mode. All traffic between the two computers in the wireless network has to pass through the AP.

- Make and Model: Cisco Aironet 350 Series
- Data Rates Supported: 1, 2, 5.5, 11 Mbps
- Network Standard: IEEE 802.11b
- Uplink: Auto-Sensing 10/100BaseT Ethernet
- Frequency Band: 2.4 to 2.497 GHz
- Network Architecture: Infrastructure
- Wireless Medium: Direct Sequence Spread Spectrum (DSSS)
- Supports IEEE 802.1x-based Extensible Authentication Protocol (EAP) services that provide centralized, user-based authentication and single-user, single-session encryption keys
- Supports Automatic channel selection, Cisco Discovery Protocol (CDP), Dynamic Host Configuration Protocol (DHCP), and BOOTP services to simplify installation and management of WLAN infrastructures

5.4 Other Software Required

We have created a Java application, which is to be executed on the server side when testing each of the security mechanisms described in section 4. For security testing and analysis, the server-side application continuously dumps data to the client. Alternatively, third-party network monitoring and analysis software, such as *NetPerf* and *Chariot*, may also be used. Some of these mechanisms will require additional software configurations in the AP, which may be achieved by using the Cisco client software setup (e.g., in case of WEP and LEAP) or alternatively by employing third party software. The set of third party software includes:

- *Airsnort* utility for cracking of WEP key. (Currently widely used version of Airsnort is Linux based. If windows version could not be obtained then one of the desktop PCs would be installed with Linux operating system.)

- *Radius (AAA) Server*. This is an absolute requirement in the case of Cisco LEAP approach and can also be used in the VPN approach.
- *VPN* server and *VPN* clients for the VPN approach. Any shareware distribution of VPN server and client can be used for this purpose.
- *SSL* enabled client and server for the SSL based approach.

5.5 Configuration of Labs

As discussed in section 4, there are three solutions suggested in response to the WEP vulnerability problems. WEP and 802.1x based configurations will be implemented in order to emphasize and practically demonstrate the vulnerability in these approaches. Various test configurations are discussed and illustrated below.

Table 2 contains symbols and notations used in the lab design charts presented in this section.

Symbol/Notation	Meaning
------	represents security control
——	represents data flow
—ÿ	represents interceptions or attacks;
SP	(Server-side program) represents a Java program that exchanges sample data with the client.

Table 2: Legends used in Lab Design Charts

1) *WEP-based Approach*

In this approach, WEP keys will be manually configured in both the desktops and the AP, in order to enable WEP-based encryption. As shown in Figure 4, the SP will generate sample data and send the data over to the client. The laptop, armed with hacking software, will try to break the WEP key.

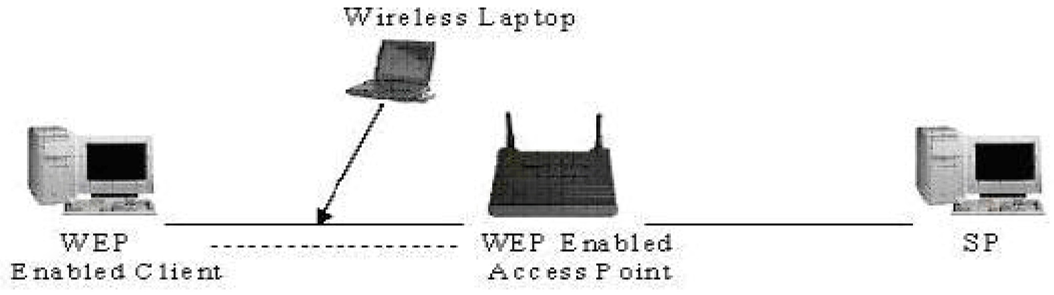

Figure 4: WEP-enabled Set-up

2) *IEEE 802.1x Based Approach*

Two types of attacks that may be launched against an 802.1x WLAN are 'Man-In-Middle' attacks and 'Session Hijack' attacks.

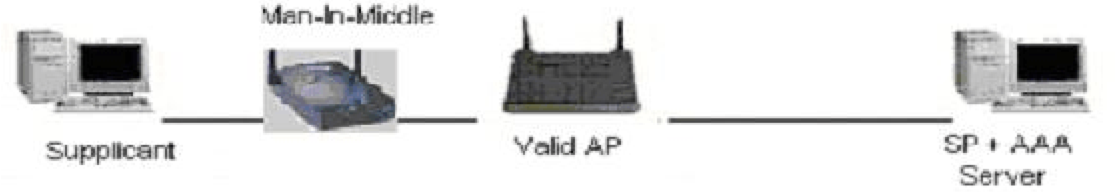

Figure 5: Man-In-the-Middle Attack Set-up

- Man-In-the-Middle Attack

As shown in Figure 5, "Man-In-the-Middle" attacks can be accomplished by using a wireless computer or an AP as the attacking device.

- Session Hijack

As illustrated in Figure 6, a "session hijack" attack is launched by an attacker who sends a MAC disassociate message to a client to cause the client to disassociate from the AP. It then impersonates itself as the client. Without knowing the 'real' client having being disassociated, the AP accepts the attacker as the client without authentication. The attacker then gains access to resources originally granted to the valid client.

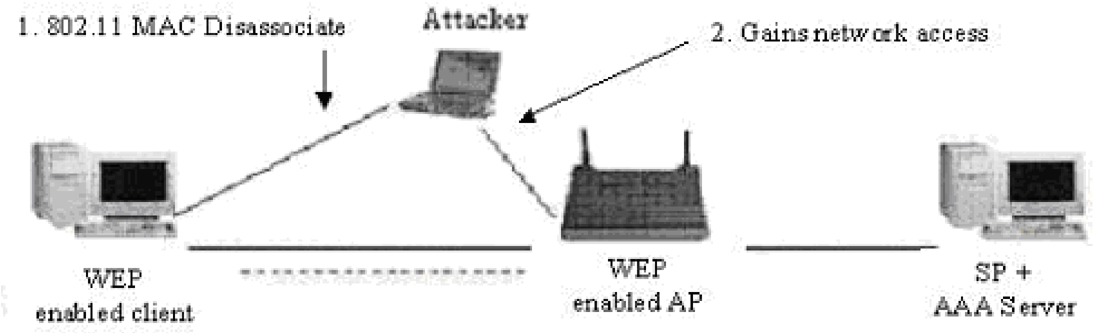

Figure 6: Session Hijack Attack Set-up

3) *LEAP-based Approach*

In this approach one of the desktops will act as a RADIUS server, while the client will be configured to use LEAP (see Figure 7). The Cisco Access Point that we use is already LEAP-enabled, so no additional work needs to be done with the AP.

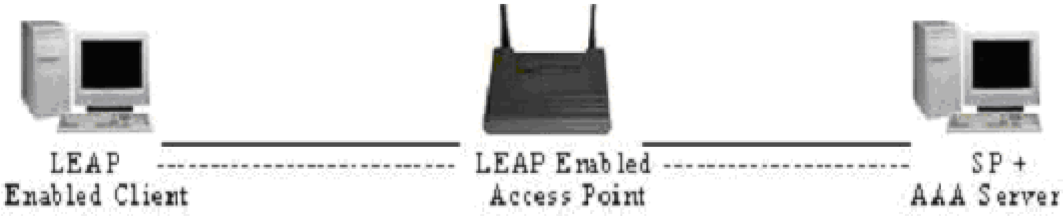

Figure 7: LEAP-enabled Set-up

4) VPN-based Approach

In the VPN approach, the AP will be VPN-aware, i.e., it will only accept and forward VPN traffic to a desktop computer configured as a VPN server (and an optional AAA server). As shown in Figure 8, the second desktop computer will be installed with VPN client software, which communicates with the VPN server by passing through the AP.

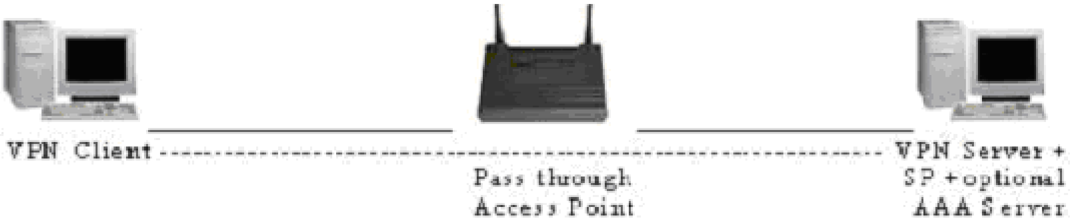

Figure 8: VPN-enabled Set-up

An alternate approach is to have the AP act as a VPN server. However this is not the approach most widely used, primarily because of performance considerations.

5) SSL-based Approach

As shown in Figure 9, one of the desktops will be configured as a server (such as a web server supporting HTTPS). The second desktop will act as a SSL client. Again all traffic must pass through the AP.

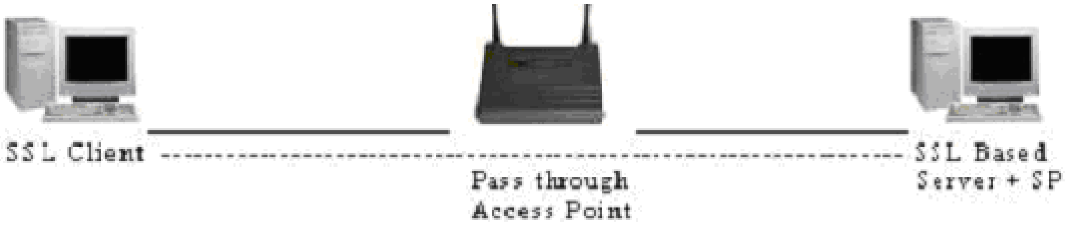

Figure 9: SSL-enabled Set-up

Alternatively, instead of using HTTPS, the client and the server may be set up as SSLSocket client and server, respectively. This approach is useful in application-to-application secure socket communications, which are not HTTP based.

6. SUMMARY

In this paper, vulnerabilities associated with WLAN protocols were discussed, and common security solutions for those vulnerabilities were examined. Also proposed are design of laboratories for studying the vulnerabilities and security of WLANs, which are to be included in a *'Wireless Computing and Security'* course.

Future work related to WLAN security includes studying performance overhead associated with WLAN security solutions, by using the lab configurations proposed in section 5. Furthermore, the security and performance issues in an enterprise-grade hybrid wired/wireless network can be another interesting extension of this work.

REFERENCES

[1] Aboba, Bernard (2002). "IETF/IEEE 802.11i Liaison Report", NIST 802.11 Security Workshop, Dec. 4-5, 2002. http://csrc.nist.gov/wireless/S12_NIST-Status-ba.pdf

[2] Borisov, Nikita, Ian Goldberg, and David Wagner (2001). "Security of WEP Algorithm", ISAAC, Computer Science Department, University of California Berkeley. http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

[3] Cisco Networks (2002). "Cisco Aironet Response to University of Maryland's paper". http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1680_pp.pdf

[4] Cox, John (2002). "Report forecasts WLAN 'last-mile' boom". *Network World Fusion, 08/05/02*. http://www.nwfusion.com/news/2002/0805alex.html

[5] Gust, Mathew S. (2002). 802.11 *Wireless Networks - The Definitive Guide*. O'Reilly, April 2002.

[6] Halasz, Dave (2002). "IEEE 802.11i Draft & Call for Interest on Link Security for IEEE 802 Networks". Nov. 12, 2002. http://grouper.ieee.org/groups/802/linksec/meetings/MeetingsMaterial/Nov02/halasz_sec_1_1102.pdf

[7] Interlink Networks (2002a). "Wireless LAN Security using Interlink Networks RAD Series AAA Server and Cisco EAP-LEAP", Application Notes at *Interlink Networks Resource Library*, 2002. http://interlinknetworks.com/images/resource/wireless_lan_security.pdf.

[8] Interlink Networks (2002b). "Introduction to 802.1X for Wireless Local Area Networks", a white paper at *Interlink Networks Resource Library*, 2002. http://www.interlinknetworks.com/images/resource/802_1X_for_Wireless_LAN.pdf

[9] KLC Consulting (2003), "Change MAC Addresses on Windows 2000 & XP". http://www.klcconsulting.net/Change_MAC_w2k.htm

[10] Mansfield, Brian (2002). "WLAN & 802.11 SECURITY", Internet Developers Group, Netscape Communications, June 18, 2002. http://www.inetdevgrp.org/20020618/WLANSecurity.pdf

[11] Mishra, Arunesh, William A. Arbaugh (2002). "An Initial Security Analysis of the IEEE 802.1x Standard", *CS-TR-4328, Department Of Computer Science, University Of Maryland*, Feb. 6, 2002. http://www.cs.umd.edu/~waa/1x.pdf

[12] Moskowitz, Robert (2003). "The WLAN's Weakest Link", *Network Computing*, March 5, 2003. http://www.nwc.com/1404/1404colmoskowitz.html

[13] Open Source Implementation of IEEE 802.1x. http://www.open1x.org/

[14] Saindon, Jean-Paul (2002). "Techniques to resolve 802.11 and wireless LAN technology in outdoor environments", a news article at *SecurityMagazine.com*, Aug. 8, 2002. http://www.securitymagazine.com/CDA/ArticleInformation/features/BNP__Features__Item/0,5411,77206,00.html

[15] Trudeau, Pierre (2001). "Building Secure Wireless Local Area Networks", a white paper at Colubris.com, 2001. http://download.colubris.com/library/whitepapers/WP-010712-EN-01-00.pdf

[16] Vollbrecht, John, David Rago, and Robert Moskowitz (2001). "Wireless LAN Access Control and Authentication", a white paper from *Interlink Networks Resource Library*, 2001. http://www.interlinknetworks.com/images/resource/WLAN_Access_Control.pdf

[17] Walker, Jesse R. (2000). "Unsafe at any key size: an analysis of the WEP encapsulation", 802.11 Security Papers at NetSys.com, Oct 27, 2000. http://www.netsys.com/library/papers/walker-2000-10-27.pdf

[18] WLAN Association (1999). "Introduction to Wireless LANs", WLANA Resource Center, 1999. http://www.wlana.org/learn/intro.pdf

[19] WLAN Association (2002). "Wireless Networking Standards and Organizations", *WLANA Resource Center*, April 17, 2002. http://www.wlana.org/pdf/wlan_standards_orgs.pdf

[20] Wright, Joshua (2003). "Detecting Wireless LAN MAC Address Spoofing". http://home.jwu.edu/jwright/papers/wlan-mac-spoof.pdf

APPENDIX A: WLAN-RELATED TERMINOLOGY

- *Authenticator:* The authenticator enforces authentication before allowing access to services that are accessible via that port. The authenticator is responsible for communication with the supplicant and for submitting the information received from the supplicant to a suitable authentication server. It only acts as a pass through for the authentication exchange.

- *EAP (Extensible Authentication Protocol):* The EAP is a method of conducting an authentication conversation between a user and an authentication server. Intermediate devices such as access points and proxy servers do not take part in the conversation.
- *EAP over LAN (EAPOL):* 802.1X defines a standard for encapsulating the EAP messages so that they can be handled directly by a LAN MAC service. This encapsulated form of EAP frame is known as EAPOL. EAPOL in case of WLANs is also termed as EAPOW (EAP over Wireless).
- *ISM:* Industrial, Scientific and Medical Frequency Band.
- *Last-mile technology:* The portion of the cable or telephone company that is wired directly into the customer's home.
  (From http://www.webopedia.com/TERM/l/last_mile.html)
- *MAC (Media Access Control):* In IEEE 802 networks, the Data Link Control (DLC) layer of the OSI Reference Model is divided into two sublayers: the Logical Link Control (LLC) layer and the Media Access Control (MAC) layer. The MAC layer interfaces directly with the network media. Consequently, each different type of network media requires a different MAC layer.
  (From http://www.webopedia.com/TERM/M/MAC_address.html)
- *PAE (Port Access Entity):* A PAE is an entity that has access or is capable of gaining or controlling access to some port which offers some services (http://www.open1x.org/). In 802.1x, a wireless client is the PAE.
- *Port:* A port in this context is a single point of attachment to the LAN infrastructure. Note that in the 802.11 LAN case, an access point manages "logical" ports. Each of these logical ports communicates one-to-one with a station's port.
- *RADIUS (Remote Authentication Dial-In User Service):* A protocol that provides Authentication, Authorization, and Accounting (AAA) services to a network
- *RSN: (Robust Security Network):* It is the main feature of IEEE 802.11i draft. RSN consists of two basic sub-systems [10]:
  - Data Privacy Mechanism
    - TKIP (a protocol patching WEP for legacy hardware based on RC4)
    - AES-based protocol for long term security solution
  - Security Association Management
    - IEEE 802.1x authentication replacing IEEE 802.11 authentication
    - IEEE 802.1x key management to provide cryptographic keys
- *Supplicant:* The supplicant accesses the services accessible via the authenticator.
- *TKIP (Temporal Key Integrity Protocol):* It is sort of a quick fix to existing WEP problems.
  - It never uses the same Initialization Vector (IV) value more than once, thus prevents key stream reuse.
  - It generates new random session key before the IV counter overflows.
  - It provides thorough mixing of IV and session key to generate RC4 key.

  - If re-keying fails, all data traffic is halted and client disassociated.
- *UNII:* Unlicensed National Information Infrastructure Frequency Band.
- *WEP (Wired Equivalent Privacy):* See sections 2.2 and 3.2.