Security in Wireless Local Area Networks*

T. Andrew Yang+ **Yasir Zahur**

1. Introduction

Following the widespread use of the Internet, especially the World Wide Web since 1995, wireless networking has become a buzz word at the beginning of the new millennium. New terms such as wireless communications, wireless local area networks (WLANs), wireless web, wireless application protocols (WAP), wireless transactions, wireless multimedia applications, etc. have emerged and become common vocabulary for computer and information professionals. Among the emerging wireless technologies, WLANs have gained much popularity in various sectors, including business offices, government buildings, schools, and residential homes. The set of IEEE 802.11 protocols (especially 11a, 11b, and 11g), nicknamed *wi-fi*, have become the standard protocols for WLANs since late 1990s.

Increasing number of 802.11 based WLANs 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 [1], which link homes and offices in isolated locations to the global Internet.

The further widespread deployment of WLANs, however, depends on whether secure

---

* This paper was adapted from one of the authors' earlier publications: Wireless LAN Security and Laboratory Designs. *The Journal of Computing Sciences in Colleges, Volume 19 Issue 3*. Jan. 2004.

+ The authors may be contacted by sending an email to YANG@CL.UH.EDU.

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 802.11 WLANs, is known to be easily cracked by commonly available hacking software. WLANs suffer from various security vulnerabilities such as eavesdropping, resource stealing, denial of service attacks, static WEP keys, absence of mutual authentication and session hijack attack, etc. To deploy a secure WLAN, it is necessary to implement an alternative security mechanism, such as SSL, VPN, Wi-Fi Protected Access (WPA), or the being-developed IEEE 802.11i protocols.

In this paper, the security aspects of WLANs are studied. We first give an overview of the various types of WLANs and the respective vulnerabilities of various protocols, followed by a discussion of alternative security mechanisms that may be used to protect WLANs.

2. Types of WLANs

The 1999 version of the 802.11 standard [2] defines three types of wireless networks: IBSS, BSS, and ESS.

1) **Independent Basic Service Set (IBSS), i.e., ad-hoc network:** "An *ad-hoc* network is a network composed solely of stations within mutual communication range of each other via the wireless medium." [2]

As shown in Figure 1, in an ad-hoc wireless LAN, end nodes communicate without any access point and thus without any connection to a wired network. Node 2, for instance, may communicate directly with node 1 and node 3. Node 3 and node 1, however, cannot have direct communication with each other since they are outside each other's communication range. An ad hoc network is typically created in a spontaneous manner, allowing non-technical users of the

wireless devices to create and dissolve the ad-hoc network conveniently. It is useful in allowing quick setting-up of a wireless network among end users.

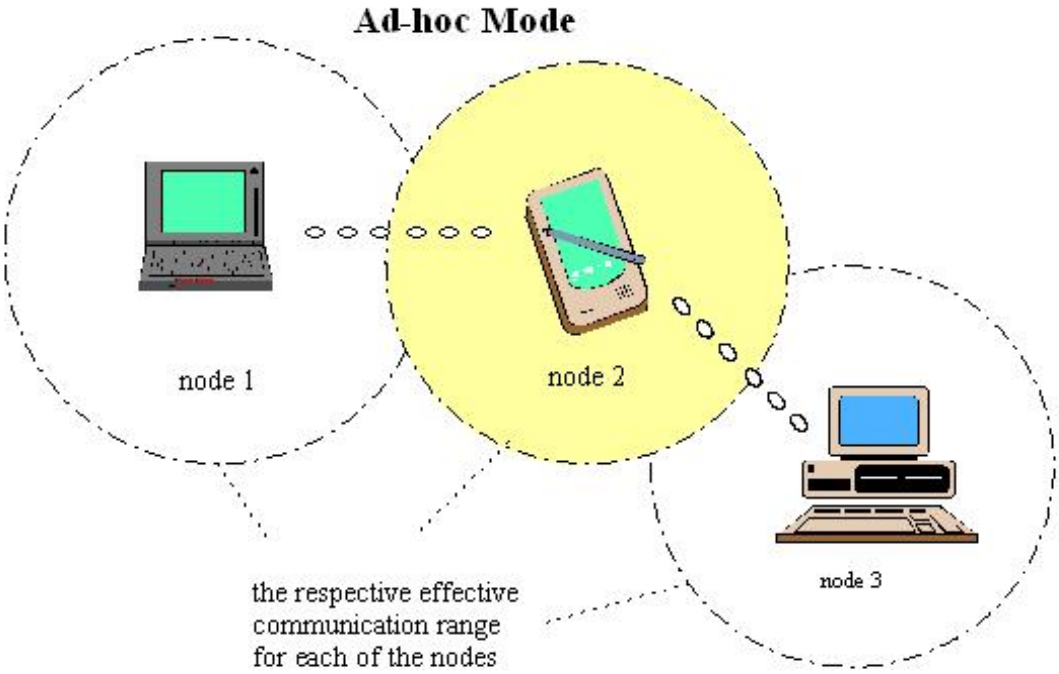

Figure 1 Ad-hoc Mode

As noted in the 1999 edition of the 802.11 specifications [2], "The principal distinguishing characteristic of an ad hoc network is its limited temporal and spatial extent." To achieve a more permanent wireless network, with larger communication range, infrastructure modes (see below) are often used.

2) **Basic Service Set (BSS):** A BSS is "a set of stations controlled by a single coordination function". [2]

A BSS (commonly referred to as an *infrastructure network*) consists of a single access point and a number of end nodes as shown in Figure 2. All the communication between any two nodes has to pass through the AP. The coverage area is greatly increased as compared to an IBSS. Mobile nodes A, B and C, for example, cannot communicate with each other via ad-hoc mode,

because they are outside each other's communication range. However, by communicating through the access point, they effectively form a WLAN for data communications. The access point behaves in a way similar to a hub in a star topology network.

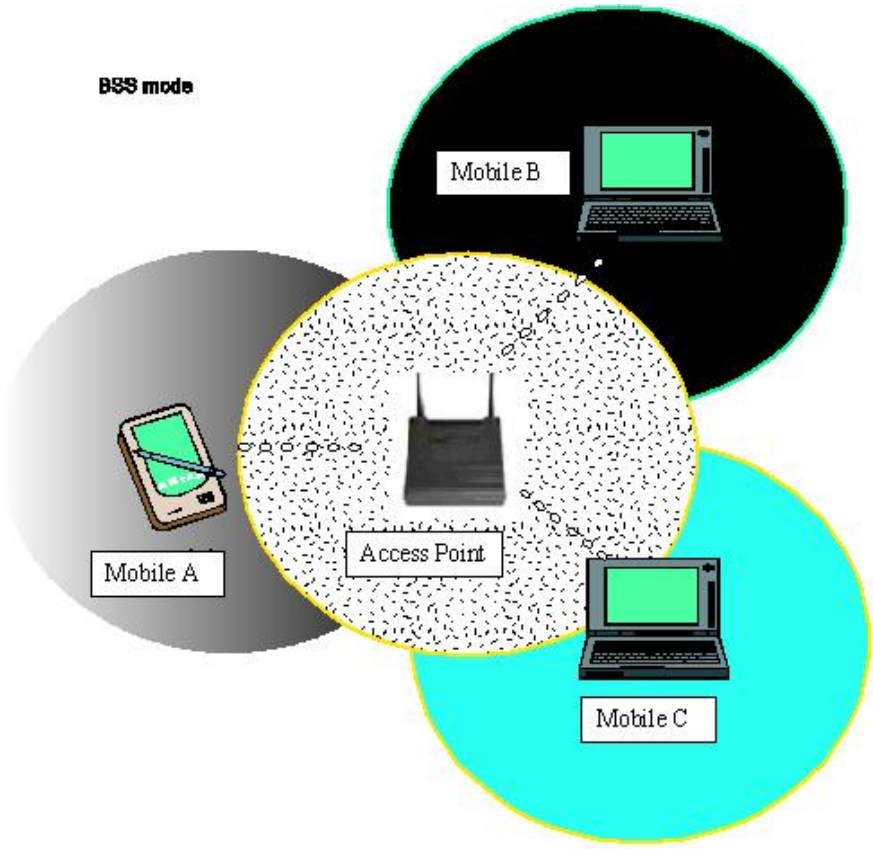

Figure 2. Basic Service Set

3) **Extended Service Set (ESS):** An ESS is "a set of one or more interconnected basic service sets (BSSs) and integrated local area networks (LANs) that appears as a single BSS to the logical link control layer at any station associated with one of those BSSs". [2]

As shown in Figure 3, an ESS consists of multiple BSSs each having a single access point. The access point in each BSS is connected to a distribution system that is usually a wired Ethernet network. An ESS is a hybrid of wireless and wired LANs, and extends a wireless station's connectivity beyond its local access point.

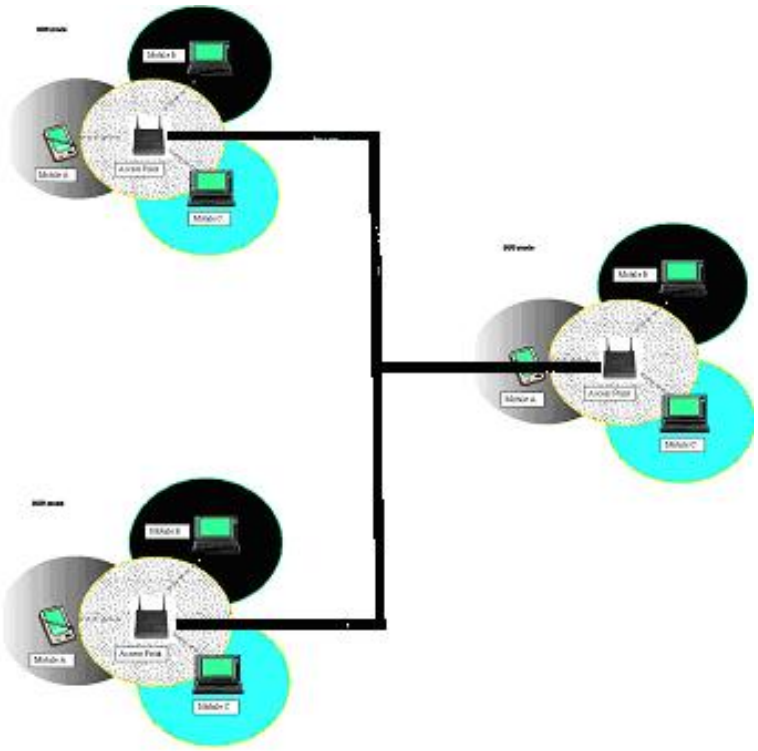

Figure 3. Extended Service Set (ESS)

With the exception of ad-hoc wireless networks, a WLAN typically consists of a central connection point called the *Access Point* (AP), which transmits data between different nodes of a WLAN and, in most cases, serves as the only link between the WLAN and the wired networks.

3. The IEEE802.11 Protocols and Built-In Security Features

Between 1997 and 2001, the IEEE had released a series of 802.11 WLAN standards [3], some of which are summarized in Table 1. The first standard, 802.11, was first released in 1997 and revised two years later. The 802.11a and 802.11b standards were released in Sept. 1999. A new standard, 802.11g, was released near the end of 2001, as a high-rate extension to 802.11b.

Depending on the specific standards, the IEEE 802.11 WLAN may run as fast as 2Mbps at 2.4GHZ, or 54Mbps at 5GHZ frequency. Newer wireless standards, currently being developed by various IEEE task groups, may bring the speed of WLANs up to the range of 200-300 Mbps.

Standards	Description / Dates of Approval
802.11	Data rates up to 2Mbps in 2.4GHz ISM band / July 1997: first release; 1999: current edition.
802.11a	Data rates up to 54Mbps in 5GHz UNII band / September 1999
802.11b	Data rates up to 11Mbps in 2.4GHz ISM band / September 1999
802.11g	High-rate extension to 802.11b allowing for data rates up to 54 Mbps in the 2.4-GHz ISM band / Nov 2001: Draft standard adopted; June 2003: Full ratification.

Table 1. The IEEE WLAN Standards

In addition to the major 802.11 standards, as listed in Table 1, there exist other IEEE standards or recommended practices related to the 802.11 protocols, such as 802.11f and 802.11h. There also exist several on-going task groups working on developing protocols related to the performance and/or security of 802.11 protocols, such as 802.11e, and 802.11i. The standards and drafts are available on line from the IEEE web site[1].

- 802.11e (QoS for 802.11): The goal of the IEEE 802.11e task group is to enhance the 802.11 *Medium Access Control* (MAC) layer, in order to improve and manage quality of service (QoS), and to enhance security and authentication mechanisms. These enhancements should provide the quality required for services such as IP telephony and video streaming.
- 802.11f (IAPP): The IEEE 802.11f, released in July 2003, documents IEEE's recommended practice for multi-vendor access point interoperability via an *Inter-Access Point Protocol* (IAPP) across distribution systems supporting IEEE 802.11 operation.
- 802.11h (Power management extension for Europe): 802.11h is an amendment to the IEEE 802.11 protocol. Its goal is to provide spectrum and transmit power management extensions in the 5GHz band in Europe. The standard was released in Oct. 2003.

[1] http://standards.ieee.org/getieee802/802.11.html

- 802.11i (the forthcoming 802.11 security standard): The goal of the IEEE 802.11i task group is to enhance the 802.11 *Medium Access Control* (MAC) layer with security and authentication mechanisms. The current status of that task group is available at IEEE *grouper* site[2]. As of April 2004, the group is working on draft 7.0 of the standard. We will discuss 802.11i in section 5.4.

3.1. Built-in 802.11 Security Features

The security features provided in 802.11 are as follows:

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[3] cannot communicate with an AP unless it is configured with the same SSID.
2) WEP (*Wired Equivalent Privacy*) Protocol: According to the 802.11 standard, "*Wired equivalent privacy* is defined as protecting authorized users of a wireless LAN from casual eavesdropping. This service is intended to provide functionality for the wireless LAN equivalent to that provided by the physical security attributes inherent to a wired medium." [2] 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 the case of WLANs, thus justifying the need for an encryption mechanism such as WEP.
3) MAC Address Filtering: In this scheme, the AP is configured to accept association and connection requests from only those nodes whose MAC addresses are registered with the AP.

[2] http://grouper.ieee.org/groups/802/11/Reports/tgi_update.htm
[3] Throughout the text, the word 'client' is used interchangeably with the word 'station' and the word 'node'. All of these refer to the wireless device used by a user to connect to a WLAN.

Association and/or connection requests sent by other wireless devices will be rejected. Although an unrealistic protection method in an enterprise network environment, MAC address filtering can be an effective method in smaller networks at homes or small businesses.

4. WLANs Vulnerabilities

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.

4.1. General Wireless Network Vulnerabilities

All wireless networks share a unique difference from their wired counterparts, i.e., its use of radio as transmission medium, which contributes to a unique vulnerability, 'Lack of Physical Security'. Besides, wireless networks may suffer other vulnerabilities, some of which they share with wired networks, such as 'Invasion & Resource Stealing' and 'Denial of Service'. The other vulnerabilities, such as 'Rogue Access Points', are associated only with wireless networks.

- Lack of Physical Security: Unlike wired networks, the signals of a wireless network are broadcasted among the communicating nodes. A hacker with a compatible wireless device can intercept the signals when the intercepting device is within the broadcasting range of the communication paths. A hacker with a wireless laptop, for example, may be physically outside a building but can still intercept and then decrypt wireless communications among devices within the building.
- 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* may be used to attack a

WLAN [4] [5]. 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, appearing as a valid user.

- Traffic Redirection: An intruder can change the route of the traffic, causing packets destined for a particular computer to be redirected to the attacking station.
- 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 [6]. A more focused DOS attack would be when an attacking station sends 802.11 *disassociate* message or replays a previously-captured 802.1x *EAPOL-logoff* message[4] to the target station and effectively disconnects it (as in "Session Hijack" attacks). The later type of DOS attack is described in more details in section 5.4, when we discuss the IEEE 802.11i protocol.
- 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.

4.2. IEEE 802.11 Vulnerabilities

The above stated concerns relate to wireless networks in general. Some of the security concerns raised specifically against IEEE 802.11 networks are as follow [7].

- *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

[4] *EAPOL, EAP over LAN*, is a standard for encapsulating EAP messages.

registered MAC address will appear to the network as a legitimate user.

- *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.
- *Static WEP Keys*: There is no concept of dynamic or per-session WEP keys in 802.11 specifications. Moreover the same WEP key has to be manually entered at all the stations in the WLAN, causing key management issues.
- *SSID*: Since SSID is usually provided in the message header and transmitted as clear texts, it provides little security.
- *WEP Key Vulnerability*: Many concerns have been raised regarding the usefulness of WEP in securing 802.11 WLANs. Some of them are as follow:
    a. Manual Key Management - Keys need to be entered manually on all the clients and access points. Such overhead may result in infrequently changed WEP keys.
    b. Key Size - The IEEE 802.11 design community blames 40-bit RC4 keys for the WEP vulnerability, 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 [8].
    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 [8], the vulnerability of WEP roots from its initialization vector and not from its smaller key size. WEP is based on RC4 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* [9] [10]. 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.

With vulnerabilities outlined above, it is reasonable to assume that an 802.11 WLAN protected by WEP alone can be easily cracked by using readily available tools such as *AirSnort* and *WEPCrack*. Alternative security solutions are apparently needed.

5. Alternative Solutions for WLAN Security

In order to secure 802.11 WLANs for critical applications, several alternative solutions have been adopted. Some of the common solutions are discussed in this section, including Cisco's proprietary LEAP protocol, the SSL (Secure Socket Layer), the VPN (Virtual Private Network), the upcoming IEEE 802.11i protocol, and the WPA (Wi-fi Protected Access) protocol.

5.1. The Cisco LEAP Protocol

Cisco *Lightweight EAP*[5] supports mutual authentication between a client and a RADIUS[6] server. LEAP was introduced by Cisco in December 2000 as a way to quickly improve the

[5] EAP, Extensible Authentication Protocol, is a method of conducting an authentication conversation between a user and an authentication server.

[6] RADIUS: *Remote Authentication Dial-In User Service*, a protocol that provides Authentication, Authorization, and Accounting (AAA) services to a network.

overall security of wireless LAN authentication.

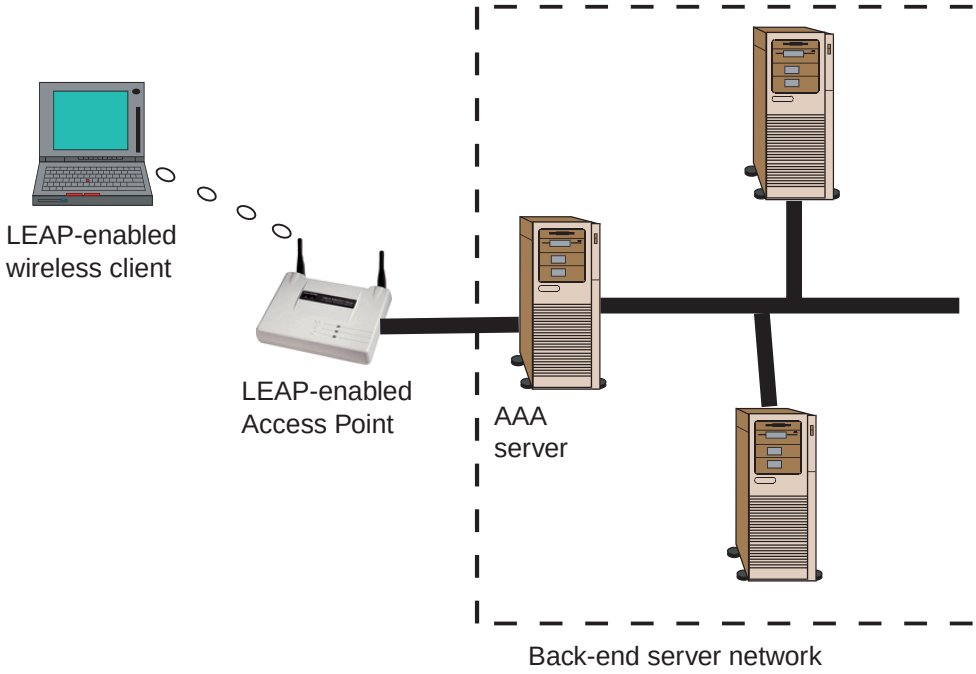

Figure 4. Wireless Security via LEAP

As shown in Figure 4, both the wireless client and the access point must be LEAP-enabled. An authentication server, such as RADIUS, is present in the server network to provide authentication service to the remote user.

Cisco has addressed the above described WEP vulnerabilities with WEP enhancements, such as *message integrity check (MIC)* and *per packet keying* [11]. In addition, LEAP provides the following counter measures against WEP vulnerability in 802.11.

- Mutual Authentication between Client Station and Access Point: As described in section 4.2, 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.
- Distribution of WEP Keys on a Per-session Basis: As opposed to the static WEP keys in 802.11, LEAP supports *dynamic session keys*. Both the RADIUS Server and the client

independently generate this key, so it is not transmitted through the air. An attacker posing as an authenticated client will not have access to the keying material and will not be able to replicate the session key, without which frames sent to and from the attacker will be dropped.

5.2. SSL (Secure Socket Layer)

SSL is an application level protocol that enables end-to-end security between two communicating processes. As shown in Figure 5, in a WLAN environment, the SSL client runs on the wireless station and the SSL server runs on the target application or web server. Once a wireless client is communicating with an access point, a user is not able to access resources over the wireless connection until properly authenticated. This authentication is accomplished via the additional level of SSL security encryption. Once an SSL client is authenticated with an SSL-enabled server, subsequent data transmissions between them are encrypted.

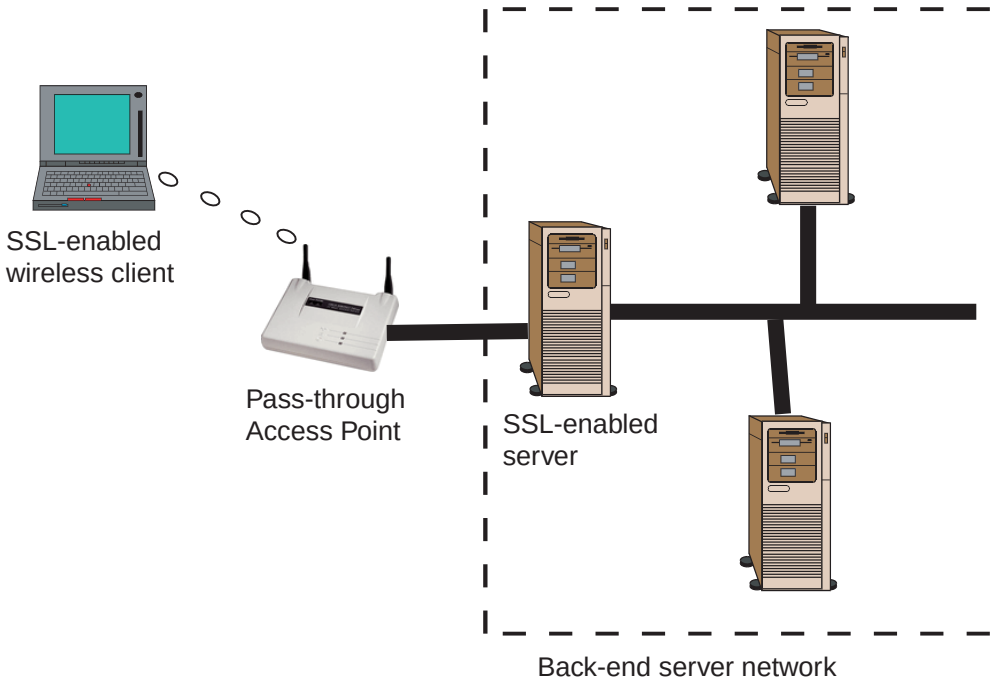

Figure 5. Wireless Security via SSL

Being an application level protocol, SSL provides the system implementers selective authentication for some of the back-end applications or servers behind the access points. In

comparison, most other wireless security solutions, including LEAP, VPN, 802.11i, and WPA, are network or lower level protocols, which typically enforce across-the-board implementation of secure access to the network behind the access point.

5.3. VPN (Virtual Private Network)

VPN technology provides the means to securely transmit data between two network devices over an insecure data transport medium [12]. VPN has been used successfully in wired networks, especially when using an insecure network, such as the Internet, as a communication medium. The success of VPN in wired networks and the Internet have prompted developers and administrators to deploy VPN to secure WLANs. As shown in Figure 6, when used to secure a WLAN, the VPN client software runs on the wireless client machine, while the VPN server runs on one of the back-end servers. An encrypted tunnel is formed between the VPN client and the VPN server, thus ensuring the confidential data transmission over the wireless network.

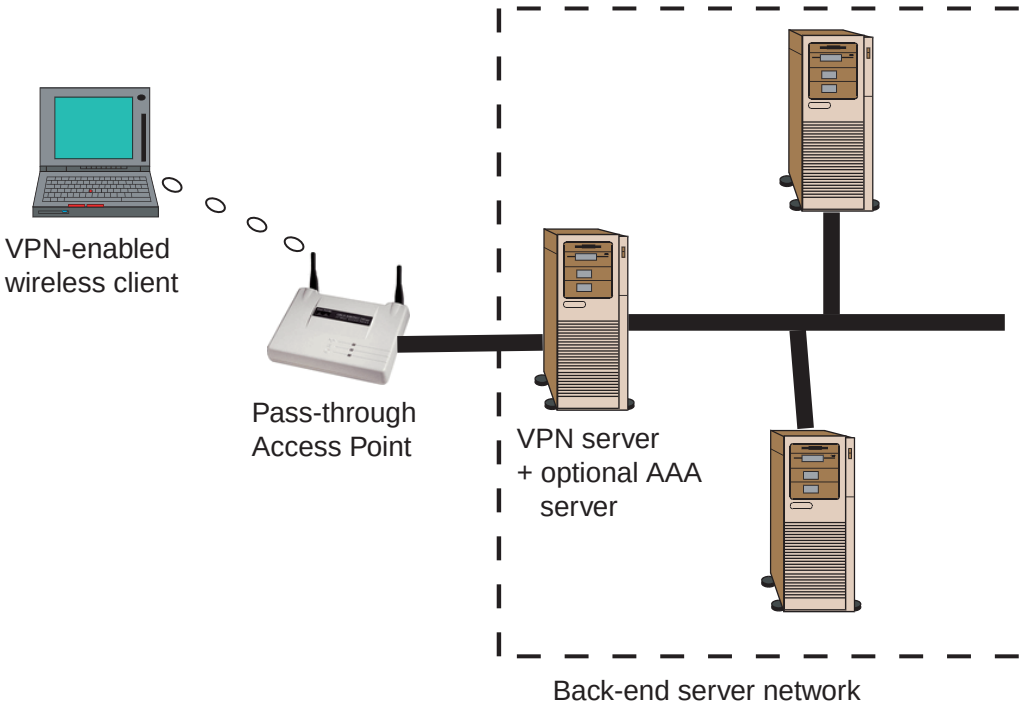

Figure 6. Wireless Security via VPN

VPN works by creating a tunnel, on top of a protocol such as IP. VPN technology provides

three levels of security [12]:

- *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.

5.4. The IEEE 802.11i Protocol

As stated in a page[7] of IEEE 802.11i task group, "The purpose of Task Group I is to: Enhance the current 802.11 MAC to provide improvements in security." To reach that purpose, the IEEE 802.11i Task Group proposed a new protocol called RSN, *Robust Security Network.*

5.4.1. Robust Security Network in 802.11i

RSN uses the IEEE 802.1x port-authentication standard to authenticate wireless devices to the network and to provide the dynamic keys it requires [13]. RSN consists of two basic sub-systems [14] [15]:

i) Data Privacy Mechanism: TKIP, the *temporal key integrity protocol*, is used to patch WEP for legacy hardware based on RC4, while AES based protocol is used for long-term security solution.

ii) Security Association Management: It adopts IEEE 802.1x authentication to replace IEEE 802.11 authentication, and it uses IEEE 802.1x key management to provide cryptographic keys.

As shown in Figure 7, the 802.11i protocol consists of three underlying protocols, organized

[7] http://grouper.ieee.org/groups/802/11/Reports/tgi_update.htm (accessed 4/22/04).

into two layers. On the bottom layer are TKIP and CCMP, the *Counter mode CBC-MAC protocol*[8]. Both encryption protocols provide improved data integrity over WEP. CCMP is an AES-based protocol, chosen to replace the old RC4 protocol in future 802.11 devices. While TKIP is optional in 802.11i, CCMP is mandatory for anyone implementing 802.11i [16].

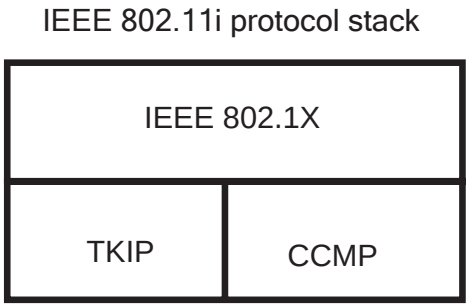

Figure 7. IEEE 802.11i

Sitting on top of TKIP and CCMP is the 802.1x protocol, which provides user-level authentication and encryption key distribution.

5.4.2. The IEEE 802.1x Protocol

IEEE 802.1x is a port-based authentication protocol, which may be used in wired or wireless networks. Figure 8 is an illustration of 802.1x used in a wireless network. There exist three different types of entities in a typical 802.1x network, including a *supplicant*, an *authenticator*, and an *authentication server* [17]. The *authenticator* is the port that enforces the authentication process and routes the traffic to the appropriate entities on the network. The *supplicant* is the port requesting access to the network. The *authentication server* authenticates the supplicant based on the supplied credentials, and is typically a separate entity on the wired side of the network, but could also reside directly in the authenticator. [16]

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

[8] *Counter mode Cipher Block Chaining Message Authentication Code* is an encryption mechanism for data on packet-based networks.

and EAP traffic to pass through.

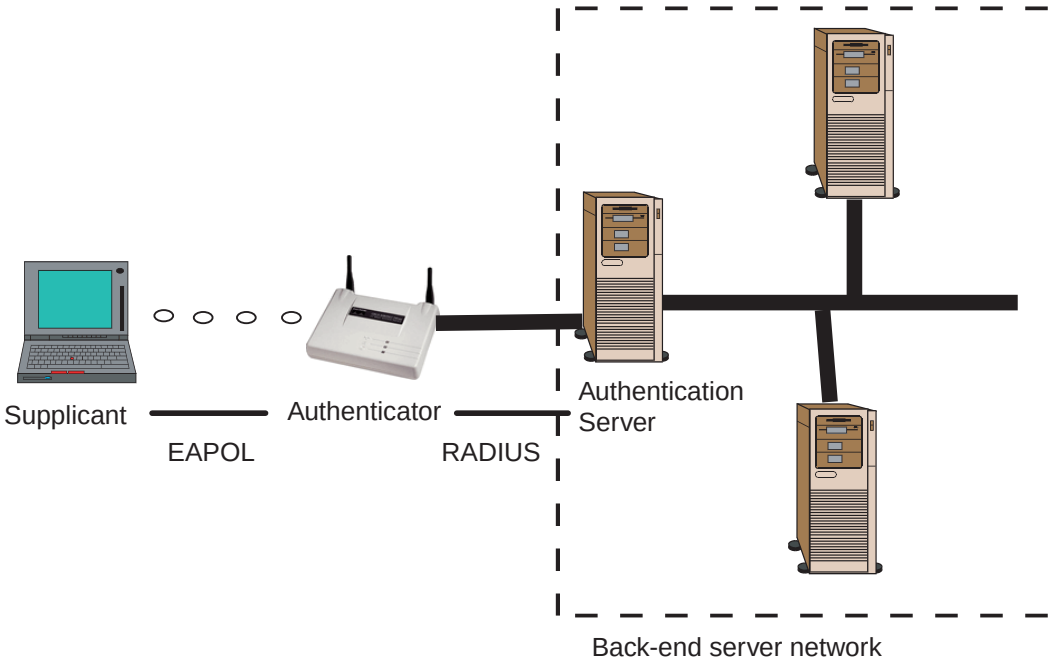

Figure 8: IEEE 802.1x in 802.11 WLANs

When applied to 802.11, the 802.1x specification includes two main features: (1) logical ports and (2) key management [18]. In the rest of this section we first discuss these two features, followed by discussions of vulnerabilities unveiled by some researchers.

- **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.
- **Key Management:** In IEEE 802.1x, key information is passed from an AP to a station using *EAPOL-Key* message. Keys are generated dynamically, at a per-session basis.

A typical configuration of a WLAN using IEEE 802.1x is shown in Figure 8. The *Supplicant* is the wireless station, which 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.

5.4.3. Vulnerabilities of 802.11i

The design goal of IEEE 802.11i protocol is to achieve enhanced MAC level security by integrating the 802.1x protocol with 802.11. Recent findings by Mishra and Arbaugh [19], however, have unveiled design flaws and the resulting vulnerabilities in such integration. 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.

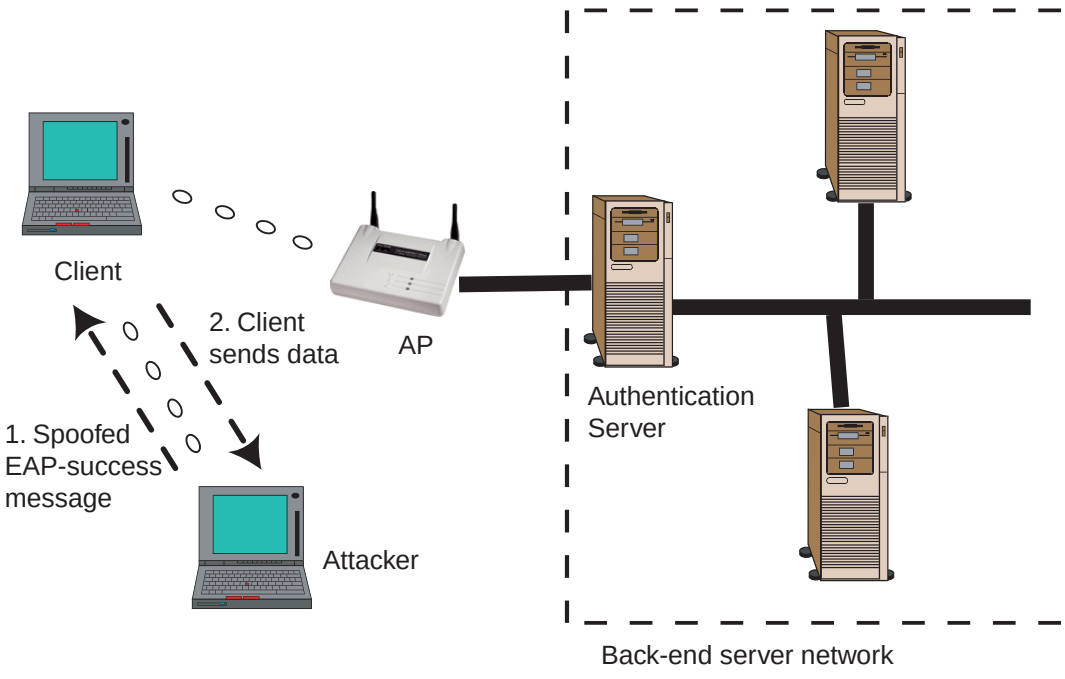

Figure 9. Man-In-the-Middle Attack in 802.11i

1) Absence *of Mutual Authentication*

According to 802.1x specifications, a Supplicant always trusts the Authenticator but not vice

versa. Consider Figure 9. 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. As shown in Figure 9, 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 in 802.11i. 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.

To understand how a session may be *hijacked* in 802.11i, let's refer to Figure 10.

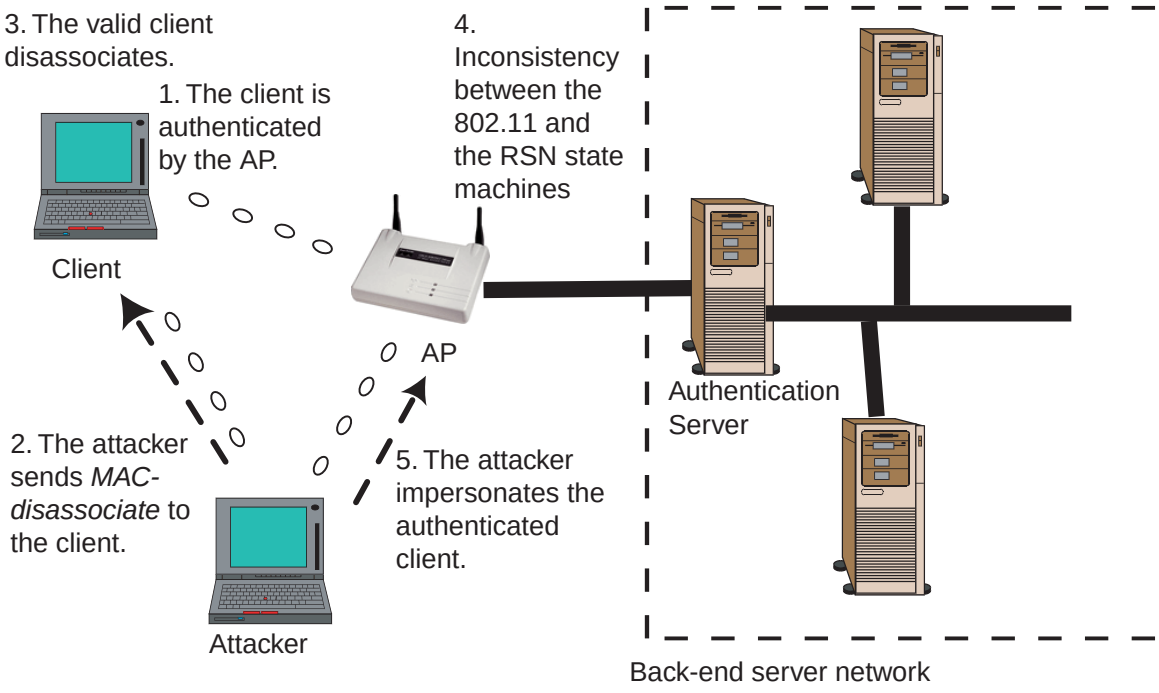

Figure 10. Session Hijack Attack in 802.11i

1) First of all, the *supplicant* and the *authenticator* (the AP) engage in the authentication

process, which results in the *supplicant* being authenticated.

2) An attacker then sends a *MAC-disassociate* message using the AP's MAC address.
3) The valid supplicant will disassociate when receiving the *MAC-disassociate* message.
4) 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.
5) The attacker then gains network access using the MAC address of the authenticated supplicant (which is disassociated by now).

5.5. The WPA (Wi-Fi Protected Access) Protocol

As anticipated by most Wi-Fi manufacturers, the forthcoming IEEE 802.11i protocol, currently still in draft mode, is the "ultimate" security mechanism for 802.11 WLANs. The *Wi-Fi Protected Access (WPA)* protocol, backed by the Wi-Fi Alliance[9], is considered as a temporary solution to the weakness of WEP.

WPA is designed to secure all versions of 802.11 devices, including 802.11b, 802.11a, and 802.11g, multi-band and multi-mode [21]. As a temporary solution prior to the ratification of the 802.11i standard, WPA is forward-compatible with the 802.11i specification, and is actually a subset of the current 802.11i draft, taking certain pieces of the 802.11i draft that are ready to bring to market today, such as its implementation of 802.1x and TKIP.

WPA offers two primary security enhancements over WEP: an improved data encryption, which was weak in WEP, and user authentication, which was largely missing in WEP [20].

- Enhanced data encryption through TKIP: To address WEP's known vulnerabilities (as discussed in section 4.2), TKIP provides important data encryption enhancements including a

[9] Wi-Fi Alliance: http://www.wifialliance.com/OpenSection/index.asp

per-packet key mixing function, a message integrity check (MIC) nicknamed Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

- Enterprise-level user authentication via 802.1x and EAP: To strengthen user authentication, WPA implements 802.1x and EAP. Similar to LEAP, WPA's user authentication framework uses a central authentication server, such as RADIUS, to authenticate each user before allowing them to connect to the network. It also supports mutual authentication to allow a user to authenticate an access point, in order to prevent rogue access points.

The main pieces of the 802.11i draft that are not included in Wi-Fi Protected Access are secure IBSS, secure fast handoff, secure de-authentication and disassociation, as well as enhanced encryption protocols such as AES-CCMP. [20]

6. Summary

Following an introduction to WLAN, we give an overview of the various types of WLANs. Vulnerabilities of WLANs and the IEEE 802.11 protocols are then discussed. That section is followed by a discussion of alternative security solutions that may be used to protect WLANs, including Cisco's LEAP, SSL, VPN, IEEE 802.11i, and WPA. It should be noted that the IEEE 802.11i protocols are yet to be standardized, and vulnerabilities discussed in this paper are associated with the current draft, which will be further revised.

An important issue related to WLANs is the potential impact a security measure may have upon the performance of a given WLAN. Performance of WLANs can be optimized by tweaking various factors like encryption methods, fragmentation threshold, and RTS/CTS, etc. It is also dependent upon external factors like distance, other devices operating in the same frequency range like microwave oven and cordless phones, etc. Readers interested in this line of work may refer to [22].

Acknowledgement

This material is based upon work supported by the National Science Foundation under Grant No. 0311592.

References

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

[2] IEEE 802.11 (1999). Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. http://standards.ieee.org/getieee802/download/802.11-1999.pdf

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

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

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

[6] 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

[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] 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

[9] Gayal, Sangram, and S. A. Vetha Manickam. Wireless LAN Security: Today and Tomorrow. An online report, the Center for Information and Network Security, Pune University.

http://hyatus.dune2.info/Wireless_802.11/wireless-lan-security.pdf

[10] Borisov, N., I. Goldberg, and D. Wagner (2001). Intercepting Mobile Communication: The insecurity of 802.11. In *Proceedings of the Seventh Annual Conference on Mobile Computing and Networking*, pages 180-188, 2001.

[11] 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

[12] 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

[13] Moskowitz, Robert (2003). The WLAN's Weakest Link. *Network Computing (Mar 5, 2003)*.

[14] Cox, Philip. "Robust Security Network: The future of wireless security". System Experts Corporation.

http://www.systemexperts.com/win2k/SecureWorldExpo-RSN.ppt

[15] Mansfield, Brian (2002). "WLAN & 802.11 SECURITY", Internet Developers Group, Netscape Communications, June 18 2002,

http://www.inetdevgrp.org/20020618/WLANSecurity.pdf

[16] Eaton, D. (2002). Diving into the 802.11i Spec: A Tutorial. CommsDesign.com. Nov 26, 2002. http://www.commsdesign.com/design_center/wireless/design_corner/OEG20021126S0003?_loopback=1

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

[18] 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

[19] 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

[20] Wi-Fi Alliance Overview at http://www.wi-fi.org/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf.

[21] *Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks*. April 29, 2003. http://www.wifialliance.com/OpenSection/pdf/Whitepaper_Wi-Fi_Security4-29-03.pdf

[22] Zahur, Y., M. Doctor, S. Davari, and T.A. Yang (2003). 802.11b Performance Evaluation. *The Proceedings of the 2nd IASTED International Conference on COMMUNICATIONS, INTERNET, & INFORMATION TECHNOLOGY (CIIT 2003).* http://sce.cl.uh.edu/yang/research/CIIT03finalPaper.pdf