CHAPTER

SECURITY IN WIRELESS LOCAL AREA NETWORKS

Mohammad O. Pervaiz, Mihaela Cardei, and Jie Wu

Department of Computer Science &Engineering, Florida Atlantic University
777 Glades Road, Boca Raton, Florida 33431,USA
E-mail:{mpervaiz@, mihaela@cse., jie@cse.}fau.edu

Over the last years, wireless local area networks (WLANs) have experienced a tremendous growth, becoming an integral part of enterprises, homes and other businesses. One of the most important issues in the development of WLANs is providing a secure communication. Because of the broadcast nature of the wireless communication, it becomes easy for an attacker to intercept the signal or to disturb the normal operation of the network. Although the early versions of WLANs were not designed for security, standards and methods are emerging for securing WLANs. In this chapter, we study the security aspects of WLANs. We start with an overview of WLAN technology and a discussion of security services and challenges in WLANs. We continue with an overview of the main WLANs security attacks, followed by a discussion of alternative security mechanisms that can be used to protect WLANs.

1. Introduction

1.1. Introduction to Wireless LAN

Over the last years, wireless networks, specifically those based on IEEE 802.11 standard have experienced tremendous growth. This has happened mainly due to the timely release of the IEEE 802.11 standard [1], the low cost of the hardware, and high data rate (11 Mbps for IEEE 802.11b and 54 Mbps for IEEE 802.11a). Many organizations are finding that WLANs (Wireless Local Area Networks) are an indispensable adjunct to traditional wired LANs, needed to satisfy requirements for mobility, relocation, ad hoc networking, and coverage of locations hard to wire.

Applications areas for WLANs can be classified in the following categories [34]: LAN extension, cross-building interconnect, nomadic access, and ad hoc wireless networks. WLANs are being largely used in education, healthcare, financial industries, and various public places such as airline lounges, coffee shops, and libraries. Although the technology has been standardized for many years, providing the wireless network security has become a critical area of concern. Due to the broadcast nature of the wireless communication, it becomes easy for an attacker to capture wireless communication or to disturb the normal operation of the network by injecting additional traffic [35].

The further widespread development of WLANs depends on whether secure networking can be achieved. In order to be able to deliver critical data and services over WLAN, reasonable level of security must be guarantee. The WEP (Wired Equivalent Privacy) protocol originally proposed as the security mechanism of the IEEE 802.11 standard is known to be cracked by commonly available hacking software. Alternative security mechanisms such as IEEE 802.1x, WPA (Wi-Fi Protected Access), IEEE 802.11i, and VPN, provide mechanisms to enhance security in WLANs. In this chapter, we study the security aspects of WLANs. We start with an overview of WLAN technology and a discussion of security services and challenges in WLANs. We continue with an overview of the main WLANs security attacks, followed by a discussion of alternative security mechanisms that can be used to protect WLANs.

1.2. WLAN Architecture

An IEEE 802.11 WLAN is a group of stations (wireless nodes) located within a limited physical area. The IEEE 802.11 architecture consists of several components that interact to provide a WLAN that supports station mobility. The general architecture is presented in the Figure 1.

The basic building block of IEEE 802.11 LAN is the basic service set (BSS), which consists of some number of stations executing the same MAC protocol and competing for access to the same, shared wireless medium. The association between a station and a BSS is dynamic. When getting out of the range, a station may disassociate to the current BSS, and it may associate later to another BSS. The component that interconnects BSSs is the distribution system (DS). The DS can be a switch, a wired network, or a wireless network. A BSS connects to a DS through an Access Point (AP). An AP functions like a bridge, moving data between its BSS and the DS. A set of BSSs and the DS form an extended service set (ESS) network. Stations within an ESS may communicate and mobile stations may move from a BSS to another. The EES appears as a single logical LAN at the logical link control (LLC) level. The integration of IEEE 802.11 architecture with a traditional wired 802.x LAN is accomplished through a portal.

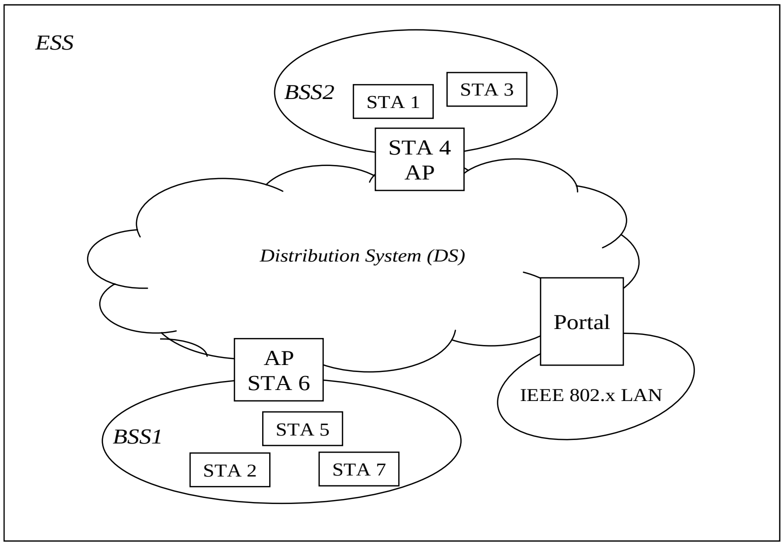

Figure 1. IEEE 802.11 Architecture

There are two types of WLANs: infrastructure-based WLANs and ad hoc WLANs. The vast majority of installations use infrastructure-based

WLANs. The focus of our security discussion in this chapter is on infrastructure-based WLANs. In the infrastructure-based organization, a BSS contains a Point Coordinator (PC) station, which acts as a polling master that dictates the access to the wireless medium. Usually, the same station serves both as PC and as AP of a BSS.

An ad hoc wireless network is typically created in a spontaneous manner, for a limited time duration and for a specific task. For example, in an organization, a group of employees participating in a meeting can organize their laptops in an ad hoc wireless network to facilitate communication and information exchange. Two stations in an ad hoc wireless network can communicate directly if the receiver is within the communication range of the sender, or can use a multi-hop communication otherwise. Communication in an ad hoc wireless network is performed using a wireless routing protocol.

2. Security Services and Challenges in Wireless LANs

Providing the network security is an important objective in the design and implementation of WLANs. Communication in wireless network is broadcast by nature and therefore all devices within the communication range of the sender receive the transmission. Thus, it becomes critical to protect data and other resources from unauthorized users. Infrastructure based WLANs assume the use of an AP that dictates the access to the wireless medium. For infrastructure based WLAN, it becomes critical to assure that only authorized users connect to the network, to keep user credentials from being hijacked during authentication, and to assure the privacy of the data being transmitted between the client and the AP.

The main security services in WLAN can be summarized as follows:

- **Confidentiality**: Confidentiality ensures that the data/information transmitted over the network is not disclosed to unauthorized users. Confidentiality can be achieved by using different encryption techniques such that only legitimate users can analyze and understand the transmission.
- **Authentication**: The function of the authentication service is to verify a user's identity and to assure the recipient that the message is from the source that it claims to be from. First, at the time of

communication initiation, the service assures that the two parties are authentic, that each is the entity it claims to be. Second, the service must assure that a third party does not interfere by impersonating one of the two legitimate parties for the purpose of authorized transmission and reception.

- **Access Control**: This service limits and controls the access of a resource such as a host system or application. To achieve this, a user trying to gain access to the resource is first identified (authenticated) and then the corresponding access rights are granted.
- **Integrity Control**: The function of the integrity control is to assure that the data received are exactly as sent by an authorized party. That is, the data received contain no modification, insertion, deletion, or replay.

Designing a secure WLAN is a challenging task due to insecure wireless communication links, user mobility, and resource constraints (e.g. bandwidth, memory, CPU processing capacity). The security requirements also depend on the application. Enterprise network requires a restricted use with strong confidentiality requirements, while public WLANs (e.g. airports, hotels) have less restrictive security requirements. The security schemes must be scalable in terms of the number of users and in terms of the varying mobility of a user from an AP to another.

3. Security Attacks in Wireless LANs

Providing a secure system can be achieved by preventing attacks or by detecting them and providing a mechanism to recover for those attacks. Attacks on wireless networks can be classified as active and passive attacks, depending on whether the normal operation of the network is disrupted or not.

(i) **Passive Attacks:** In passive attacks, an intruder snoops the data exchanged without altering it. The attacker does not modify the data and does not inject additional traffic. The goal of the attacker is to obtain information that is being transmitted, thus violating the message confidentiality. Since the activity of the network is not disrupted, these attacks are difficult to detect. Powerful encryption mechanism can alleviate these attacks, making difficult to read the transmitted data.

(ii) **Active Attacks**: In active attacks, an attacker actively participates in disrupting the normal operation of the network services. An attacker can create an active attack by modifying packets or by introducing false information in the ad hoc wireless network. Active attacks can be divided into internal and external attacks:

- **Internal Attacks** are from compromise nodes that were once legitimate part of the network. Since the adversaries are already part of the network as authorized nodes, they are much more severe and difficult to detect when compared to external attacks.
- **External attacks** are carried by nodes that are not legitimate part of the network. Such attacks can be prevented by using encryption, firewalls and authentication.

Many attacks have been identified in literature on WLANs. Solutions and mechanisms that aim to defense against various attacks are presented later in section 4. Next, we classify the main WLAN attacks into four categories: attacks using impersonation, modification, fabrication, and denial of service (DoS).

3.1. Attacks using Impersonation

In impersonation attacks, an intruder assumes the identity and privileges of another node in order to consume resources or to disturb normal network operation. An attacker node achieves impersonation by misrepresenting its identity. This can be done for example by changing its own MAC address to that of some other legitimate node. Strong authentication procedures can be used to stop attacks by impersonation.

3.1.1. Man-in-the-middle Attacks

In this attack, a malicious node reads and possibly modifies the messages between two parties. The attacker can impersonate the receiver with respect to the sender, and the sender with respect to the receiver, without having either of them realize that they have been attacked. Using an

802.11 analyzer, a person can monitor 802.11 frames sent over the wireless LAN and can learn information about the radio card and AP.

With this information, someone can setup a rogue AP closer to a particular user, forcing the radio NIC to reassociate to the rogue AP, thus allowing the hacker to capture user names and passwords. An attacker can also impersonate a user. By monitoring the frame transmissions, a hacker can program a rogue radio NIC to mimic a valid one. The hacker can then deceive the AP by disassociating the valid radio NIC and reassociating again using the rogue radio NIC. In this way, the rogue radio NIC steals the ongoing session for which the valid user had logged into.

3.1.2. Session Hijacking

Session hijacking attack consists in taking control of a user's session after successfully obtaining or generating an authenticated session ID (or key). The attacker takes control of the legitimate user's application session while the session is still in progress.

3.2. Attacks using Modification

In this attack, the attacker illegally modifies the content of messages traveling from the source to the destination. Such an attack breaks the integrity control security function.

3.2.1. Message Modification in WEP

A message modification attack on WEP (see section 4.1) is described in [4]. The 802.11 standard uses 32-bit CRC to provide data integrity. This is a linear function of the plaintext. Since RC4 is also linear stream cipher, an attacker needs only to XOR the difference quantity <Δ, c(Δ)> to an intercepted ciphertext and a new valid ciphertext is obtained. We note with Δ the binary string corresponding to the desired plaintext difference and c(Δ) is the CRC checksum.

3.3. Attacks using Fabrication

In fabrication attacks, an attacker generates false messages in order to disturb network operation or to consume resources.

3.3.1. Reaction Attack

In reaction attack, the attacker monitors the recipient's reaction to its forgeries. Paper [4] describes a reaction attack for WEP-encrypted TCP/IP traffic. Here, the attacker intercepts a message, flips a few bits in the ciphertext and adjusts the encrypted CRC accordingly. Then the attacker watches to see if the receiver sends back a TCP ACK packet, case in which the modified message passed the TCP checksum and was accepted by the receiver. By carefully selecting the bits to be flipped, additional information on the plaintext is obtained.

3.3.2. Reply Attack

In the replay attack, an attacker retransmits the same data to produce an unauthorized effect. Such an attack can be mounted against the WEP [4].

3.4. Denial of Service Attacks

In the DoS (Denial of Service) attack, an attacker explicitly attempts to prevent legitimate users from using system services. This type of attack affects the availability of the system. A mischievous person can use a wireless client to insert bogus packets in the wireless LAN, with the intent of keeping other users from getting access to services. The attacker could setup a relatively high power signal generator to interfere and block other users from accessing the medium. Another type of service denial is when an attacker produces fake 802.11 CTS frames. Such a frame is used by an AP to inform a particular user to transmit and all others to wait. As a result, legitimate radio NICs of legitimate end users will continuously delay their access to the medium.

3.4.1. EAP-START Attack

An attacker can attempt to bring down an AP by sensing a large number of EAP-Start messages (see section 4.2. on IEEE 802.1x) to exhaust AP internal resources.

3.4.2. EAP-LOGOFF Attack

Since the EAP-Logoff (see section 4.2. on IEEE 802.1x) frame is not authenticated, an attacker can spoof this frame, logging a user off the AP. By repeatedly spoofing EAP-Logoff messages, an attacker can prevent a user for normal use of network services.

3.4.3. Access Point Overloaded

This attack is based on the observation that in 802.11 a client must be successfully authenticated and associated to an AP before using wireless communication services. AP maintains the client state information in a client-association table. When the table reaches the permitted level of associated clients, the AP start rejecting new association requests. This attack is facilitated by the open system authentication method in 802.11 where an AP authenticates anyone who requests authentication. An attack can be launched if the adversary does a large number of associations with an AP, using random MAC addresses. Since an AP can maintain a limited number of associations, this will prevent other stations from joining the AP.

4. Security Mechanisms and Solutions for Wireless LAN

4.1. The WEP Protocol

The Wired Equivalent Privacy (WEP) [1] protocol is IEEE 802.11's optional encryption standard implemented in the MAC Layer to protect link-level data communication in wireless transmission between clients and access points (AP). WEP was designed in September 1999 to provide security services to wireless LAN users in a same way as available to users in wired LAN. These security services include:

(i) **Confidentiality/Privacy:** The most important goal of WEP is to prevent link-layer eavesdropping. It uses 64 bits RC4 cipher algorithm for providing privacy.

(ii) **Authentication:** IEEE 802.11 standard uses *Open System* and *Shared Key* authentication mechanisms:

- *Open System* authentication is based on request and grant. As the name implies, it authenticates anyone who requests authentication. It is essentially no authentication at all. It simply provides a way for the two parties to agree to exchange data, and provides no security benefits.
- *Shared Key Authentication* is not secure and not recommended for use. It verifies that a station has knowledge of a shared key. The 802.11 standard assumes that the shared key is delivered to the participating wireless clients by mean of a more secure channel, independent of 802.11. Shared key authentication follows the following steps:
    (a) The wireless client sends a frame with its identity and a request for authentication.
    (b) The authenticating node replies with a 128-octet challenge text.
    (c) The client node replies with the encrypted challenge text. Encryption is done using WEP and the shared key.
    (d) The authenticating node decrypts the message received, verifies its CRC, and verifies if it matches the plaintext sent in the step 2. Based on these results it will send the client a status code indicating success or failure.

(iii) **Data Integrity:** Data integrity is used in order to prevent an attacker from tampering with transmitted messages. A 32 bits Integrity Check Value (ICV) field, which is a simple 32-bit CRC, is included for providing data integrity.

4.1.1. WEP Framework

When WEP is activated, the Network Interface Card (NIC) uses a symmetric (secret key) stream cipher *Rivest Cipher 4* (RC4) [9] provided by *RSA Security* to encrypt the payload (frame body and CRC) of each

802.11 frame before data transmission. Decryption is done by the receiving station (i.e. access point) when this frame is received. The data is only encrypted between 802.11 stations. WEP is no longer applicable as soon as frames enter wired part of the network.

As part of encryption process in wireless LAN in 802.11, each packet is encrypted separately with the RC4 cipher stream generated by a 64-bit RC4 key. This key is composed of 40-bit secret WEP key and remaining 24 bits are reserved for random-generated *Initialization Vector* (IV). At the time when the WEP standard was being written in IEEE 802.11, US Government export restrictions [13] on cryptographic technology limited the key size to 40 bits. This 40-bit WEP key is distributed to all stations participating in the data communication. The 24-bit IV is selected by the sender so that each packet is not encrypted in similar manner by RC4 stream cipher. The RC4 stream cipher operates by expanding a short key into a pseudo-random key stream equal to the length of original data.

The encrypted packet or cipher stream is generated by the sender with a bitwise exclusive OR (XOR) [10] of the original packet and the 64 bit RC4 stream as shown in the Figure 2.1. Similarly, receiver obtains the original data by another bitwise exclusive OR (XOR) of the encrypted packet and identical WEP Key as shown in Figure 2.2.

Original Data	0	1	1	0	1	0	1	1	…
XOR									
WEP Key	1	1	0	1	1	0	0	1	…
=									
Encrypted Stream	1	0	1	1	0	0	1	0	…

Figure 2.1. Encryption done by sender in WEP protocol

Encrypted Stream	1	0	1	1	0	0	1	0	…
XOR									
WEP Key	1	1	0	1	1	0	0	1	…

=									
Received Data	0	1	1	0	1	0	1	1	…

Figure 2.2. Decryption done by receiver in WEP protocol

An additional 32 bits Integrity Check Value (ICV), which is simply a 32-bit CRC, is computed on the original packet and it is appended to the end of the frame. The ICV is also encrypted with the RC4 cipher stream but the IV is sent as plain text without any encryption with each packet. The receiving station recalculates the ICV value and compares it with the value received from sender station. If the two values are different, receiver can drop the packet and ask sender to send the encrypted information again.

4.1.2. Weaknesses in WEP

When WEP was introduced in IEEE 802.11 standard, the committee was aware of WEP limitations but at that time it was the only security mechanism which could be efficiently implemented worldwide. Since then, several security holes have been discovered in WEP, and it is no longer considered secure.

The WEP's IV size of 24 bits provides for 16,777,216 different RC4 cipher streams for a given WEP key, for any key size. With only 24 bits, WEP eventually uses the same IV for different data packets. For a large and busy network, this reuse of IVs can occur within an hour or so. This repetition allows easy decryption of data packets for a moderately sophisticated attacker [2]. In August 2001, Fluhrer-Mantin-Shamir (FMS) [3] and Stubblefield et al [12] confirmed that the combination of revealing 24 key bits in the IV and a weakness in the initial few bytes of the RC4 key stream leads to an efficient attack that recovers the key.

Apart from short and static IV, 40-bit WEP keys are also inadequate for any network. In wireless network security, it is generally accepted that key sizes should be at least greater than 80 bits in length. The longer the key length, the better it stands a chance against a brute-force attack. Some vendors even increased the key size from 64 bits to 128 bits (also known as WEP2) but the move to 128 bit WEP by itself does not solve the inherent weaknesses in WEP, it just makes it harder to crack the key [2, 5]. As key management is not specified in the 802.11 WEP standard, networks use one single WEP key shared between every station on the network. Since synchronizing the change of keys is tiresome and difficult, keys are seldom changed. This increases the chances of the attacker to eavesdrop the network and it will eventually get full access of the network traffic.

In order to provide integrity of data, WEP uses ICV mechanism, which is based on non-cryptographic Cyclic Redundancy Check (CRC-32), an algorithm designed for detecting noise and common errors in transmission. While CRC-32 is an excellent checksum for detecting errors, researchers [11] proved that it is inadequate for providing cryptographic integrity. Better designed encryption systems use algorithms such as MD5 or SHA-1 for their ICVs.

In January 2001, Borisov, Goldberg, and Wagner [4] presented several other attacks including Message Modification and Message Injection attacks. They showed that an attacker could easily modify any encrypted message without even being detected by the WEP, hence undermining the WEP's data integrity. Arbaugh [5] later on turned this into a practical attack that could decrypt any chosen packet in a few hours. Soon after WEP release in 1999, several software tools [6, 7, 8, 17] were available to compute and recover WEP keys by passively monitoring transmissions.

4.2. IEEE 802.1x

The 802.1x [31] standard was approved in March 2001 by IEEE 802.11 Working Group to cover up the weak security mechanism specified in the original 802.11 standard. 802.1x is a port-based standard and it is mainly designed to use *Extensible Authentication Protocol* (EAP) to provide strong authentication, access control, and easy key management. It also helped in WLAN scaling by providing centralized authentication of users or stations. IEEE 802.1x is also called *EAPOL* (EAP encapsulation over LANs).

IEEE 802.1x is designed for wired and wireless LAN authentication. This authentication requires involvement of three important components: *supplicant*, *authentication server*, and *authenticator*. The user/client that has to be authenticated is a *supplicant*. The actual server (i.e. RADIUS [30]) doing the authentication is called an *authentication server*. *Authenticator* is a network device (i.e. wireless access point) that receives information from supplicant and passes this information to authenticator in required format. The authentication server may be collocated in the same system as the authenticator, or it may be located elsewhere, accessible through remote communication. Most of the authentication functionality is implemented in supplicant and authentication server. This makes 802.1x highly favorable for wireless *access points* (AP) which usually have low memory and weak processing power.

4.2.1. Authentication Process and Key Management

The authentication mechanism consists in the following steps:

(i) The client/supplicant sends an *EAP-Start* message to AP for authentication.

(ii) The AP replies with an *EAP-Request* identity message and asks client to provide its identification and until its identification is verified, it has to block all messages like DHCP, HTTP, and POP3.

(iii) The client sends its identity to the authentication server in an *EAP-Response* message. Although EAP supports both client-only and strong mutual authentication but for better security, mutual authentication is usually used in WLAN.

(iv) The authentication server uses selected authentication algorithms (digital certificates or other EAP authentication type) to verify the client’s identification. An *EAP-Success* packet or *EAP-Reject* packet is sent to the AP depending on the results of the authentication.

(v) If the authentication server authorizes the client, then the client is allowed to access the LAN. At this point, the AP switches the client’s port to authorized state and the client is allowed to resume normal network transactions.

From the five authentication steps, it can be observed that 802.1x is just a standard for passing EAP over wired or wireless LAN, as the actual authentication is provided by the EAP, not by 802.1x itself. There are many types of EAP that define how the authentication would take place, such as Transport Layer Security (EAP-TLS) and EAP Tunneled Transport Layer Security (EAP-TTLS). The IEEE 802.1x standard provides an architectural framework based on which various authentication methods can be used, such as certificate-based authentication, smartcards, one-time passwords, etc.

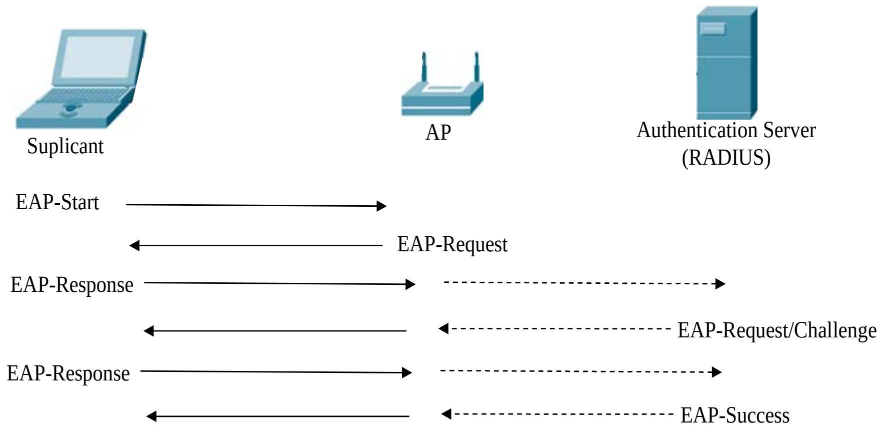

Figure 3. Successful Authentication

In Figure 3, we present an example of a successful authentication. The exchange of EAPOL frames is shown in continuous line and the exchange of EAP frames using a higher layer protocol such as RADIUS is shown in dotted line. The authenticator is responsible for relaying EAP frames between the supplicant and the authentication server, and for performing any repackaging.

Optionally, the 802.1x implementation supports the ability to transmit new key information to the supplicant following a successful authentication. This is performed using the *EAP-Key* message. This message is encrypted using a session key, for example using WEP.

4.2.2. Weaknesses

Recent research works [32, 33] show that there are flaws in the way 802.1x works with 802.11. Session hijacking, man-in-the-middle, and denial of service are possible attacks for 802.1x. The 802.1x standard provides a one-way authentication, where only the supplicant is authenticated to the AP. This is because the standard assumes that the authenticator is a trusted entity. The lack of mutual authentication can be exploited to perform a man-in-the-middle attack [32], with an adversary acting as an access point to the supplicant and as a client to the AP.

Session hijacking is another attack that can be successfully mounted against 802.1x. This attack exploits the lack of encryption in the management frames in IEEE 802.11 and 802.1x. The attack proceeds as follows [32]. First, the supplicant authenticates itself. Then an adversary sends an 802.11 MAC disassociate message using the AP's MAC address. This cause the supplicant to get disassociated, while the AP still remains in the authenticated state. Thus, the adversary gains the network connection and can use the network connection using supplicant's MAC address.

There are a number of attacks that could cause DoS (denial of service) for users or network availability. An adversary could spoof the supplicant's MAC address and send EAP-Logoff request to the AP. The AP then disassociates and thus denies services to the supplicant. The attack can also be performed at the MAC layer, when adversary sends a MAC disassociate message. Another message that can be explored is the EAP-Failure message, sent from the AP to the supplicant when the authentication process at the authentication server fails. If a supplicant receives an EAP-failure message, it must stay in an idle state for at least 60 sec. If an adversary spoofs the EAP-failure message every 60 sec, it will prevent the supplicant for being authenticated. Another DoS attack is when an adversary is continuously sending EAP-Start requests to the AP. Then the AP becomes busy with the authentication dialog and thus unable to handle legitimate traffic.

Another type of DoS attack is AP overload, where an adversary does a large number of associations with an AP using random MAC addresses. Since an AP can maintain only a limited number of associations, this will prevent other stations from joining the AP.

4.3. The WPA Protocol

In 2003, the Wireless Fidelity (Wi-Fi) Alliance announced Wi-Fi Protected Access (WPA), a security mechanism to address the cryptographic shortcomings of WEP. WPA is actually a subset of 802.11i wireless security standard, which was still under development when WPA was released as a short-term solution. The Wi-Fi Alliance, realizing that the long wait of 80.11i is not good for security in WLAN, launched WPA. The security services offered by WPA are:

- **Confidentiality/Privacy:** Confidentiality is provided by using Temporal Key Integrity Protocol (TKIP) [20] along with RC4 stream cipher.
- **Authentication:** WPA is available in two modes. In *Enterprise* mode, it uses 802.1x and EAP authentication while in the *Consumer* mode it makes use of Pre-Shared Key (PSK) to provide authenticity to the wireless network.
- **Data Integrity:** WPA provides *Message Integrity Check* (MIC) for data integrity to protect data from forgery and bit-flipping attacks.

4.3.1. WPA Framework

The most important new feature of WPA is the appearance of the Temporal Key Integrity Protocol (TKIP) [20] in place of WEP's basic RC4 encryption. Like WEP, WPA continues to use RC4, but in a more secure way than WEP. The size of initialization vector in TKIP is increased. Per-packet key mixing feature is also added to make it more resistant to security attacks, and a Message Integrity Check (MIC) is added to confirm that a packet has not been tampered in transmission.

TKIP protocol requires two different keys: a 128-bit key, which is used by a mixing function to produce a *per-packet* encryption key, and a 64-bit key for providing message integrity. One of the main weaknesses of WEP was the small size of IV. In TKIP, size of IV is increased from 24 bits to 48 bits. With bigger key size and dynamic key encryption, WPA stands much better chance against different attacks. Apart from that, keys in TKIP have a fixed lifetime and they are replaced frequently. The *per-packet key mixing* function and *re-keying* mechanism makes sure that keys are often changed when used for RC4 (every 10,000 packets). In fact, WPA uses a unique key for each 802.11 frame. Therefore, even if any key is lost to an attack, Wi-Fi claims that it will not be as useful to an attacker as it was in WEP.

Instead of using CRC, which is considered as a weak cryptographic method [11], WPA provides message integrity by *Message Integrity Code* (MIC) which uses *Michael* algorithm [18]. It solves the bit flipping attack by appending 64 bits MIC with the ICV. It divides packets in two blocks of 4 bytes each. It then uses shifts, exclusive OR, and as a final output of 64 bits of authentication tag. In order to minimize the performance impact, the Michael algorithm limits the instruction set.

TKIP is designed specifically to plugholes in WEP and it is forced to use the same stream cipher RC4 used by the WEP. This also suggests that only a software upgrade is needed to implement TKIP on the already in use networks.

4.3.2. Weaknesses in WPA

Although WPA is much more secure than WEP, it still has some weaknesses. It is designed in such a way that security completely relies on the secrecy of all the packet keys [16]. Even if one packet key is lost to the attacker, it is easily possible to find the MIC key. Similarly, if two packets with same IV are disclosed [16], an attacker can do anything for the duration of the current temporal key.

In *consumer* mode of WPA, *Pre-Shared Key* (PSK) is used for authentication instead of 802.1x but the PSK used in WPA is vulnerable to an *offline dictionary attack* because of the broadcasting of critical information required for creation and verification of a session key. In order to eliminate the 802.1x/RADIUS infrastructure, WPA also eliminates the strong authentication that comes with these services. In November 2003, Robert Moskowitz [14] found out that any key generated from a pass phrase in PSK mode of WEP is highly vulnerable to attacks if it is smaller than 20 characters. Tools like [17, 21] are easily available to exploit this vulnerability of PSK in WPA. Wi-Fi alliance [15] in fact strongly advises to use PSK only for home user.

WPA is also vulnerable to the following DoS attack. WPA uses mathematical algorithms to authenticate users to the network in such a way that if a malicious user is trying to get in and sends two packets of unauthorized data within one second, WPA will assume it is under attack and automatically shut down itself.

Even though WPA addresses almost all weaknesses in WEP, it is still using the flawed RC4 cipher stream algorithm [19]. Drawbacks in PSK determined its replacement by 802.11i.

4.4. IEEE 802.11i

In June 2004, the IEEE 802.11i security standard was ratified. It is also known as WPA2 since WPA was designed as it subset. It defines data confidentiality, mutual authentication, and key management protocols intended to provide enhanced security in the MAC layer of a wireless network. This set of protocols together defines a Robust Security Network Association (RSNA).

- **Confidentiality/Privacy.** IEEE 802.11 supports three cryptographic algorithms to protect data: WEP, TKIP (Temporal Key Integrity Protocol) and CCMP (Counter-mode/CBC-MAC Protocol). WEP and TKIP are based on RC4 algorithm, and CCMP is based on AES (Advanced Encryption Standard).
- **Authentication.** An RSNA supports authentication based on IEEE 802.1x or pre-shared keys (PSKs). IEEE 802.11 uses EAP to authenticate the client and the authentication server with one another.
- **Key Management.** To enhance confidentiality, data authentication, and to protect against the data replay attack, fresh keys are generated using 4-Way handshake and Group key handshake protocols. Keys are established after 802.1x authentication has completed, but might change over time if needed.
- **Data Integrity.** Data integrity is provided by Cipher Block Chaining Message Authentication Code (CBC-MAC) protocol and Message Integrity Check (MIC).

4.4.1. IEEE 802.11i Framework

Unlike WEP and WPA which used faulty RC4 stream cipher algorithm, 802.11i uses 128 bits *Advanced Encryption Standard* (AES) [28, 29] in *Counter with CBC-MAC* (CCM) [23] mode. AES is one of the most secured encryption standards and now it is approved by the United States federal government as *Federal Information Processing Standard* (FIPS).

The 802.11i specification defines two different classes of security algorithms: *Robust Security Network Association* (RSNA), and Pre-RSNA. Main difference between them is that Pre-RSNA security consists of *Wired Equivalent Privacy* (WEP) and does not uses the *4-Way Handshake* [24] authentication. On the other hand, RSNA provides two data confidentiality protocols, called the *Temporal Key Integrity Protocol* (TKIP) and the *Counter-mode/CBC-MAC Protocol* (CCMP) [26, 27], 802.1X authentication, 4-Way handshake authentication, and key management protocols. The use of TKIP is optional and it is only included because it was a standard that could easily be implemented over the existing hardware. On the other hand, the use of CCM/CCMP is mandatory in 802.11i.

Integrity is provided by CCMP through *Message Integrity Check* (MIC) in the same manner as TKIP but it uses another algorithm that shows better results than Michael does. If even single bit is altered, the checksum value will be completely different.

The CCMP is based on the CCM mode of AES. It was designed by D. Whiting, N. Ferguson, and R. Housley for implementation in 802.11i. It handles packet authentication as well as encryption of wireless data. AES based encryption can be used in a number of different modes or algorithms. In order to provide confidentiality, CCMP uses AES in counter mode while integrity and authentication is provided by Cipher Block Chaining Message Authentication Code (CBC-MAC) [23]. The CBC-MAC field size is 64 bits and nonce size is 48 bits while 16 bits are reserved for IEEE 802.11 overhead. The 64 bits CBC-MAC, 48 bits nonce and 16 bits of overhead makes CCMP 128 bits larger than an in-secured packet but this larger (and slower) packet is worth the price for the strong security provided. CCMP also includes the packets source address and destination address with each packet. This eliminates the possibility of replaying packets to different destinations in 802.11i. Like TKIP, CCMP also sends a 48-bit IV called *Packet Number* (PN) in the header of each frame being encrypted [22]. This IV or PN value is a counter used to initialize AES cipher for frame encryption as well as MIC calculations. Even though AES can be implemented in sizes of 128-bit, 192-bit, and 256-bit, only 128-bit AES is supported by the 802.11i standard.

4.4.2. Weaknesses of IEEE 802.11i

The 802.11i security standard was designed to cover up for all the weaknesses of WEP. In this regard, it has fulfilled its obligation. It offers effective data confidentiality and integrity when CCMP is used. Implementing all the advance features of 802.11i means that a hardware and software upgrade is mandatory. This can be complex and very expensive task. As a result, some users have decided that WPA is good enough for them even though 802.11i offers better security.

As none of the IEEE standard was designed to provide network *availability* service, 802.11i is vulnerable to DoS attack. When 802.11x is implemented with all its features, it increases the chances of mounting DoS attack on 802.11i. Forging of EAP-Start, EAP-Logoff, and EAP-Failure messages becomes easier but attacker needs expensive equipments and huge power supply to disturb the network flow. Attacker can send 255 authentication requests simultaneous and 8-bit space of EAP packet identifier will be exhausted, thus network will be under DoS attack. Similarly, the efficient 4-Way Handshake authentication method of 802.11i is prone to *reflection attack* if wireless device has to perform as authenticator and supplicant at the same time. Mitchell et al [25] identified two more types of DoS attacks: *RSN Information Element* (RSN IE) *Poisoning* and *4-Way Handshake Blocking*. Apart from providing countermeasures to these attacks, they also mentioned different tradeoffs related with *Failure-Recovery* strategy in 802.11i.

As mentioned earlier, 802.11i uses Pre-RSNA and RSNA security algorithms. Pre-RSNA uses WEP so that 802.11i is backward compatible. Implementation of Pre-RSNA and RSNA together can be a complex task and faulty installation might make it easier for *Security*

Level Rollback Attack to occur. Under this attack, an adversary can force the network to use only the WEP as a defense mechanism. Weaknesses of WEP are explained earlier in the chapter and WEP is actually not secured at all.

	802.11	WPA	802.11i
Security Protocol	WEP	TKIP	CCMP
Stream Cipher	RC4	RC4	AES
Key Size	40 bit	128 bit encryption 64 bit authentication	128 bit
IV Size	24 bit	48 bit	48 bit
Key Management	Not Available	IEEE 802.1x/EAP	IEEE 802.1x/EAP
Per-Packet Key	IV Concatenation	Mixing Function	Not Required
Date Integrity	CRC-32	Michael	CCM

Table 1: Comparison of Security Protocols

4.5. Other WLAN Security Mechanisms

Besides IEEE WEP, IEEE 802.1x, WPA and IEEE 802.11i, there are a number of other security mechanisms that can be used to enhance network security. Such security mechanisms include Firewalls, VPN (Virtual Private Networks), Cisco LEAP (Lightweight Extensible Authentication Protocol), TLS (Transport Layer Security), and SecNet (Secure Wireless Local Area Network).

4.5.1. Firewalls

A firewall provides a barrier between a private network and the Internet. A firewall is a device (e.g. a router) installed between the internal network of an organization and the rest of the Internet and it is used to prevent external attackers to send harmful messages to the internal network. A firewall can be used to filter all packets destined to a specific host or server, or it can be used to deny access to a specific host or service. Firewalls can be classified [36] as (1) packet-filter firewall that filters packets at the network or transport layer, and (2) proxy firewalls, which filters packets at the application layer.

4.5.2. VPN

Many companies are creating their own VPN to accommodate the needs of their remote employees and distant offices. VPN is a private network that uses a public network (e.g. Internet) to connect remote sites or users together. VPN technology uses IPSec (Internet Protocol Security) in the tunnel mode to provide authentication, integrity, and privacy. IPSec is a set of protocols developed by IETF to support secure exchange of packets at the IP layer.

To protect access to the private network, a VPN server needs to authorize every user trying to connect to the WLAN using a VPN client. Authentication is user based rather than machine based. The communication between the remote user and the private network uses a secure tunnel on top of an inherently insecure communication protocol such as Internet. To enhance the security, the traffic passing through the tunnel is encrypted.

4.5.3. Cisco LEAP

Cisco LEAP, also known as Cisco Wireless EAP, provides strong mutual authentication between a client and a RADIUS server. This is a two-way authentication mechanism where both the client and the server verify each other’s identity before completing the connection. Authentication uses a username/password scheme. Using a mutual authentication scheme protects WLANs from the man-in-the-middle attack. To increase security and integrity control, Cisco WEP uses Message Integrity Check (MIC) and per packet keying [37]. To mitigate the session hijack attack, EAP Cisco dynamically derives a WEP session key. Both the client and the RADIUS server independently generate the session key, which is not transmitted wirelessly where it can be intercepted by attackers.

4.5.4. TLS

TLS provides endpoint authentication and communication privacy over Internet, using cryptography. The current approved version is TLS 1.1, specified in RFC 4346 [38]. TLS protocol is designed with the objective of preventing eavesdropping, tampering, and message forgery. TLS is used for client/server applications, most commonly using HTTP. It can be used for example to secure world wide web pages for applications such as electronic commerce. TLS protocol has the following characteristics: (1) peer negotiation for cryptographic algorithm support (e.g. RSA, Diffie-Hellman, RC4, MD5, etc.), (2) public key encryption-based key exchange and certificate-based authentication, and (3) symmetric cipher-based traffic encryption.

TLS lies between application layer and transport layer (TCP) and consists of two protocols: the *handshake protocol* and the *data exchange protocol*. The handshake protocol is responsible for negotiating security, authenticating the server to the browser, and defining other communication parameters. Mutual authentication is also supported. The data exchange protocol uses the secret key to encrypt the data for secrecy and the message digest for integrity. The keys information and the algorithm specifications are agreed upon during the handshake phase.

4.5.5. SecNet

SecNet [39] technology, the Harris Corporation's secure communication solution, is capable of delivering secure data, video, and voice over IP at a secret level via a wireless network. Two wireless network interface cards have been designed: SecNet 11 and SecNet 54. The NSA (National Security Agency) certified SecNet 11 card operates on 2.4GHz and provides Type 1 encrypted WLAN communication based on IEEE 802.11b standard. SecNet 11 uses Harris Sierra Encryption module, Intersil PRISM chipset, and Baton encryption algorithm. Both the data and the source/destination addresses are encrypted, preventing traffic analysis on transmitted data. SecNet 11 provides only data encryption and it does not support authentication. SecNet 54 card [39] supports 802.11a/b/g links up to 54 Mbps. SecNet 54 card has a modular architecture with two basic components: a Cryptographic Module (CMOD) that provides the security-critical functions, and an External Module (XMOD) that handles the transport of encrypted data over specific protocols such as wired 802.3 Ethernet, wireless 802.11 and 802.16.

5. Conclusions

The use of wireless LAN is growing rapidly. As wireless LANs are becoming integral part of enterprises, homes and other businesses, it becomes imperative that the wireless components of the network be as secure as the wired networks. Although the early versions of WLANs were not designed for security, standards and methods are emerging for securing WLANs. With 802.1X and 802.11i standards, there are now good choices for encryption and authentication. These emerging security features must be implemented in order to provide the security of the data and information on the wireless network.

Acknowledgments

This works was supported by the DoD Defense-wide RDTE grant on Secure Telecommunication Networks.

References

1. LAN MAN Standards Committee of the IEEE Computer Society. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Standard 802.11, 1999 Edition, 1999.
2. J. Walker, Unsafe at any key size: an analysis of the WEP encapsulation, Tech. Rep. 03628E, IEEE 802.11 committee, Mar. 2000.
3. S. Fluhrer, I. Mantin, and A. Shamir, Weaknesses in the key schedule algorithm of RC4. *Proceedings of the 4th Annual Workshop on Selected Areas of Cryptography*, 2001.
4. N. Borisov, I. Goldberg, and D. Wagner, Intercepting mobile communications: The insecurity of 802.11. *Proceedings of the International Conference on Mobile Computing and Networking*, pp 180–189, Jul. 2001.
5. W. A. Arbaugh, An inductive chosen plaintext attack against WEP/WEP2. IEEE Document 802.11-01/230, May 2001.

6. Airsnort. Available at http://airsnort.shmoo.com/
7. WEPAttack. Available at http://wepattack.sourceforge.net/
8. WEPLab. Available at http://weplab.sourceforge.net/
9. R. L. Rivest, *The RC4 Encryption Algorithm*. RSA Data Security, Inc., Mar. 12, 1992.
10. E. Dawson and L. Nielsen, Automated Cryptanalysis of XOR Plaintext Strings, *Cryptologia*, Vol. 2, pp 165–181, Apr. 1996.
11. S. G. Stubblebine and V. D. Gligor, On message integrity in cryptographic protocols. *Proc. IEEE Symposium on Research in Security and Privacy*, pp 85–105, 1992.
12. A. Stubblefield, J. Ioannidis, and A. Rubin, Using the Fluhrer, Mantin, and Shamir attack to break WEP, In *Proceedings of the 2002 Network and Distributed Systems Security Symposium*, pp 17–22, 2002.
13. W. Diffie and S. Landau, The Export of Cryptography in the 20th Century and the 21st , *Sun Microsystems Laboratories*, Palo Alto, California, Nov. 2000.
14. R. Moskowitz, Weakness in Passphrase Choice in WPA Interface, ICSA Labs, 2003.
15. Wi-Fi Alliance WPA standard, Section 8.2, Version 1.2, Dec. 16, 2002.
16. V. Moen, H. Raddum, and K. J. Hole, Weaknesses in the Temporal Key Hash of WPA, Mobile Computing and Communications Review, pp. 76–83, Apr. 2004.
17. AirCrack. Available at http://www.grape-info.com/doc/linux/config/aircrack-2.3.html
18. N. Ferguson. Michael: an improved MIC for 802.11 WEP. IEEE doc. 802.11-2/020r0, Jan. 2002.
19. I. Mantin, Analysis of the Stream Cipher RC4, *Weizmann Institute of Science*, Nov. 2001.
20. J. Walker, 802.11 Security Series – Part II: The Temporal Key Integrity Protocol (TKIP), Intel Corporation, 2002.
21. coWPAtty. Available at http://www.wirelessdefence.org/Contents/coWPAttyMain.htm
22. J. Edney and W. Arbaugh, Real 802.11 Security: Wi-Fi Protected Access and 802.11i, *Boston, Addison-Wesley*, pp. 269-272, 2004.
23. D. Whiting, R. Housley, and N. Ferguson, Counter with CBC-MAC (CCM). *RFC 3610*, Sep. 2003.
24. C. He and J. Mitchell, Analysis of the 802.11i 4-Way Handshake, *Proceedings of the ACM Workshop on Wireless Security* (WiSe), Philadelphia, PA, USA, pp. 43-50, Oct. 2004.
25. C. He and J. C. Mitchell, Security Analysis and Improvements for IEEE 802.11i, *The 12th Annual Network and Distributed System Security Symposium* (NDSS'05), pp. 90-110, Feb. 2005.

26. J. Black and P. Rogaway, CBC MACs for arbitrary-length messages: The three key constructions, *Advances in Cryptology — CRYPTO 2000, LNCS 1880*, pp. 197–215, Springer-Verlag, 2000.
27. E. Petrank and C. Rackoff, CBC MAC for real-time data sources, *J.Cryptology*, Vol. 13, No. 3, pp. 315–338, Springer-Verlag, 2000.
28. National Institute of Standards and Technology. FIPS Pub 197: *Advanced Encryption Standard (AES)*, Nov. 2001.
29. Advanced Encryption Standard Development Effort, http://www.nist.gov/aes
30. C. Rigney, W. Willats, and P. Calhoun, RADIUS extensions, *RFC 2869*, Jun. 2000.
31. IEEE Standards for Local and Metropolitan Area Networks: Standard for Port based Network Access Control, *IEEE Draft P802.1X/D11*, Mar. 2001.
32. A. Mishra and W. Arbaugh, An Initial Security Analysis of the IEEE 802.1x Standard, *Technical Report, University of Maryland, CS-TR-4328 and UMIACS-TR-2002-10*, Feb. 2001.
33. P. Ding, J. Holliday, A. Celik, Improving the Security of Wireless LANs by Managing 802.1x Disassociation, *IEEE Consumer Communications and Networking Conference (CCNC04)*, pp 53-58, Jan. 2004.
34. K. Pahlavan, T. Probert, and M. Chase, Trends in Local Wireless Networks, *IEEE Communications Magazine*, Mar. 1995.
35. W. Arbaugh, N. Shankar, and J. Wang, Your 802.11 Network has no Clothes, *IEEE Intl. Conf. on Wireless LANs and Home Networks*, Dec. 2001.
36. B. A. Forouzan, *Data Communications and Networking*, 3rd edition, McGraw Hill, 2004.
37. Cisco Networks, Cisco Aironet Response to University of Maryland's paper, http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1680_pp.pdf, 2002.
38. RFC4366: The Transport Layer Security (TLS) Protocol Version 1.1, http://tools.ietf.org/html/4346, 2006.
39. Harris Corporation, Secure Communication Solutions, http://www.govcomm.harris.com/secure-comm/.