Security Issues of IEEE-802.11 Wireless Networks

Islam, Chowdhury Sajadul
Daffodil International University

http://hdl.handle.net/20.500.11948/753
Downloaded from  http://dspace.library.daffodilvarsity.edu.bd, Copyright Daffodil International University Library
Security Issues of IEEE-802.11 Wireless Networks

Chowdhury Sajadul Islam and M Abdus Sobhan
School of Engineering and Computer Science, Independent University of Bangladesh
E-mail: {chowdhury_iub, sobhan30}@yahoo.com

Abstract: This paper focuses on the WiFi infrastructure mode attacks, vulnerabilities and available protections with respect to data confidentiality, integrity, mutual authentication and availability. It summarizes recent security solutions starting from WEP to IEEE802.11i and discusses the strengths and weaknesses of the solutions of IEEE 802.11 Wireless Local Area Network (WLAN). Generally, security concerns in the LAN world are classified into physical and logical types. There are different types of logical attacks like main-in-the-middle attack and Denial of Service attacks as well as physical security attacks like rouge APs. There are different types of threats such as AP positioning, frequency & transmitter power allocation in WLAN. In the link layer, active and passive eavesdropping, masquerading, message interception, session hijacking, jamming attacks are found to occur. Wired Equivalent Privacy (WEP) was the first logical security solution to secure WLAN, but it has many vulnerabilities. In order to provide securities against vulnerabilities of WEP, the Wi-Fi alliance proposed the TKIP to provide stronger security through a keyed cryptography Message Integrity Code (MIC), an extended IV length and key mixing function and IEEE802.1x protocol used by providing port base security. To provide enhanced security of WLANs, IEEE 802.11i materialized a new MAC layer standard that eternally fixes most of the security problems found in temporary WLAN security solutions. WLANs are becoming more and more secure especially with the arrival of IEEE 802.11i-compliant wireless hardware (a processor used in WLAN card and APs). Attacks on privacy, integrity and authentication can be conquered by IEEE 802.11i, is optionally sustaining TKIP to afford backward compatibility with inheritance systems and with systems that does not support AES hardware.

Index Terms— IEEE 802.11i, Eavesdropping, PEAP, Wi-Fi, WPA2, IPSec.

1. Introduction

The security issues of Wireless Networks (WN) have become a major concern because of its broadcast nature of air communications, which makes it extremely susceptible to malicious interception and motiveless or unintentional interference. In this review paper, an attempt is made to describe and analyze the threats of the security issues of IEEE802.11[1,2]. We stress more importantly on how much protection is available for WN. Attacks on WN can be divided into (i) active and (ii) passive types. Active attacks involve altering data or creating fraudulent streams and passive ones are inherently eavesdropping or snooping on transmission. The major issues are: (i) threats to the physical security of the network; (ii) unwanted access by unwanted parties; and (iii) privacy. [3]

Table-1 shows the key issues, centered on the secure access to WN systems; any breach to it may entail loss of money, national information security, or leak of such information and secrets to unwanted parties including competitors and enemies. If the data carried in the network are sensitive, such as in the networks of financial institutions and banks, e-commerce, e-government, e-health and military network; then extra measures must be taken to ensure security, confidentiality, integrity and privacy effects shown in fig. 4.

It is attempted to extend the discussion on the security attacks and various classes of services of a reliable security system including confidentiality, nonrepudiation, access control, integrity, and availability. The WNs, in general, have security problems due to: sharing, complexity, anonymity, and multiple points of attacks.

To ensure MAC address authentication and to protect against DoS (Denial of Service) attack, a message that causes PTK (Pairwise Transient Key) inconsistent, 4-way handshake key management protocols are used through a fresh session and group key. The Counter Mode /CBC-MAC protocol (CCMP) provides data confidentiality and integrity and replay protection.

WPA (Wi-Fi Protected Access), WPA2 protocols are used in AES algorithm to provide security to IEEE802.11i [3]. WPA is advance-compatible with IEEE802.11i standard. WPA2 seems to be a software security upgrade and momentary solution that
can be adopted faster in the industry while waiting for the IEEE802.11i to be fully implemented in future wireless devices. IEEE802.11i will be improved to achieve communication security but the cost to achieve it will be higher since current hardware cannot sustain AES computations which are the basic building blocks of IEEE802.11i. A new processor is designed that uses wireless NIC and APs, which can proficiently execute IEEE802.11i technologies.

The paper is organized as follows. A short introduction and motivation are given in this section. Logical and physical attacks are described respectively in sections 2.1 and 2.2. In section 3, is described available security protection from WEP to IEEE 802.11i using processor at NIC of AP and STA. The conclusion is drawn in section 5.

Table 1 Analytical attitude towards wireless security issues

<table>
<thead>
<tr>
<th>Wireless Networking Issues</th>
<th>Number of respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Not concerned</td>
</tr>
<tr>
<td>Money loss due to wireless fraud</td>
<td>48 (30%)</td>
</tr>
<tr>
<td>Theft of bandwidth</td>
<td>35 (22%)</td>
</tr>
<tr>
<td>Ensuring personal data is not exposed</td>
<td>23 (14%)</td>
</tr>
<tr>
<td>Ensuring wireless is always available</td>
<td>7 (4%)</td>
</tr>
<tr>
<td>Ensuring personal data is not altered</td>
<td>16 (10%)</td>
</tr>
</tbody>
</table>

2.1 Logical Attacks

Denial-of-Service Attacks
DoS attack is made on physical and MAC layers, and it exploits some protocol weaknesses, or straightforward jamming of the frequency band. [5] Using characteristics of wireless networking, an adversary may launch DoS attacks in several ways:

Attacks on EAPOL-Logoff Frames – The purpose of EAPOL-Logoff frame is to signal disconnection and this is already taken care of by the 802.11 standard; nevertheless an attacker can potentially spoof this frame. As a result, Access Points should filter these messages [4, 5].

Attacks on EAPOL-Start Frames – Access Point (AP) can be down if an attacker is sending a frame with EAPOL-Start frames. To avoid these problems, significant resources should not receive an EAPOL-Start frame. [4, 5]

Attacks on EAP Identifier Space – An Access Point can be down by attacker to consume the EAP Identifier space (0-255). The EAP Identifier is only required to be unique within a single port or 802.11 associations. There is no need for an AP to lock out further connections, once the Identifier space has been exhausted. [4, 5]

Attacks on Premature EAP Packets – A rogue Authenticator sends premature EAP success packets before the mutual authentication has completed, so it creates the opportunity for the attacker to attack.

Supplicant implementations

Spoofing EAP Failure Packets – A Supplicant that receives an EAP-Failure packet from an authenticator outside of an 802.1X exchange can ignore the packet. If the authenticator wishes to remove the supplicant, this will later be followed by a disassociation frame, which can be authenticated.

Modification of EAP Packets – The EAP TLS protocol exchange by encapsulating it within TLS. These protocols are known as Protected EAP (PEAP) and Tunneled TLS (TTLS). To use these protocols, EAP TLS, PEAP or TTLS, a customer can modify the EAP packet so that vulnerabilities still exits [7].

Message Deletion and Interception – An adversary is able to delete the message or remove the packet from the network before it reaches its destination. The receiver’s antenna may think the packet is lost due to noise or error. By this way, the adversary can take the control of travel of a packet [2, 4].

Masquerading and Rogue AP –
An adversary masquerades as an AP by spoofing its MAC address and functioning
appropriately through appropriate Host AP. Alternatively, without masquerading as others, it is possible for a malicious AP to provide a strong signal and attempt to fool a wireless station and leaking private data.

Session Hijacking
Firstly, the adversary disconnects a device from an existing session, and then masquerades as this device to obtain possible connections without the attention of the other device. The adversary is able to receive all packets destined to the hijacked device. 

Man-in-the-Middle Attack (Fig. 1)
The adversary breaks the connection between a wireless station and the AP, then the adversary masquerades as the legitimate station to associate with the AP. When the AP adopts any mechanisms to authenticate the station, the adversary is able to spoof the authentication. Then the adversary, masquerades as the AP to fool the station to associate with it. The adversary played a negative role between them [4].

Authentication Vulnerabilities Use of SSID
An eavesdropper easily determines the SSID with the use of a WLAN packet analyzer, like SnifferPro [24] because it is in plain text. In addition, disabling SSID broadcasts might have undesirable effects on Wi-Fi interoperability for mixed-client deployments so that access point vendor recommends not to use the SSID as a mode of security. [6, 10]

WEP Open Authentication Vulnerabilities
Open authentication system is the most vulnerable system since there is no way of justification in the access point whether a client is valid or not.

WEP Shared Key Vulnerabilities
An eavesdropper can capture both the plain text or challenge text and the cipher-text response. Using an exclusive OR (XOR) function, an eavesdropper can easily derive the key stream just by sniffing the shared key authentication process with a protocol analyzer [4, 6, 9].

MAC Authentication Vulnerabilities
802.11 NICs allow the UAA to be overwritten with a LAA. A network attacker can use a protocol analyzer to determine a valid MAC address in the BSS and a LAA-compliant NIC to spoof the valid MAC address. Hacker might be able to subvert the MAC authentication process by "spoofing" a valid MAC address.

IP Redirection Attack
Rogue sniff an encrypted packet and modifies it so that it has a new destination address. The AP decrypts the packet and sends the packet to its (new) destination. Hackers need not only to modify the destination IP address, but also to ensure that the IP checksum in the modified packet is still correct otherwise, the decrypted packet will be dropped by the access point. [4]

Reaction Attacks
When IP redirection attacks are impossible, attacker then monitors the reaction of a recipient of a TCP packet which is accepted only if the TCP checksum is correct, and when it is accepted, an acknowledgement packet is sent in response. Thus, the reaction of the recipient will disclose whether the TCP checksum was valid when the packet was decrypted [4].

2.2 Physical Attacks
Physical Positioning of APs
The Crackers use highly directional dishes to blast through the thick wall of a building or even 20-25 miles away from the top of a hill to enter in to the network and capture the data [1,8]. Attackers can take position behind the Yagi or even a directional dish and still be able to discover the network and eavesdrop passing traffic. Default AP configuration has many Rogue.

Frequency Selection Problems
If users run the same frequency close to others, any AP could legitimately receive signal by accident. To evaluate the LAN security, WEP cracking tool such as WEP Cracker, AirSnort is run.

Radio Signal Interference
Microwave signal (2.4GHz) delays the user by either blocking transmissions from stations on the LAN or causing bit errors to occur in data being sent. Bluetooth radio technologies also operate in the 2.4GHz band and can cause interference with WLANs, especially in fringe areas not well covered by a particular wireless LAN access point [1, 9].
Jamming Attack

The legitimate traffic cannot reach clients or AP due to the fact which overwhelms the frequency. Attackers flood the unlicensed frequency brand originating from outside the service area of the AP or from other wireless devices installed in other areas that degrade the strength of the signal.

Passive Eavesdropping

An adversary sniffs and stores all the traffic in WLAN if the message fields are found to be redundant [2, 4]. Through traffic analysis technique, a recorded packet or knowledge of the plaintext can be used to reveal the encryption key, decrypt complete packets and gather other useful information.

Active Eavesdropping (Message Injection)

An adversary can generate any chosen packet, modify contents of a packet, and completely control the transmission of the packet. Furthermore, by inserting some well-chosen packets, the adversary might be able to learn more information from the reaction of the system through active eavesdropping [2, 4].

3.1 Wired Equivalent Privacy (WEP)

The WEP protect wireless communication from eavesdropping. WEP is based on RC4 algorithm and relies on a secret key (40 bit), which is shared between a mobile STA and an AP to encrypt packets before they are transmitted, and an integrity check IV (24 bit) is used to ensure that packets are not modified. Most installations use a single key that is shared between all STA and APs. To avoid this kind of problem, an alternative of WEP2 (64 bits) is used which contains 128 bit encryption key; so more security can be provided in this way; but still it has some pitfalls [6]. Adding a per-packet key mixing function, a message integrity check and a re-keying mechanism enhances WEP.

Open Authentication- If the WEP key of a STA is matched with the AP WEP key, then the STA is authenticated otherwise authentication is not possible.

Shared Key Authentication- The AP uses locally configured WEP key to encrypt the challenge text and reply with a subsequent authentication request. If the AP can decrypt the authentication request and retrieve the original challenge text, then it grants the client access. [9, 11, 16]

3.2 MAC Address Authentication (Fig. 2)

The MAC address authentication technique verifies the client's MAC address against a locally configured list of allowed addresses or against an external authentication server. MAC authentication is used to supplement the open and shared key authentications provided by 802.1x, further reducing the probability of unauthorized devices accessing the network [7,13].

3.3 IEEE 802.1x Authentication & Encryption Security

Temporal Key Integrity Protocol (TKIP)

TKIP encryption replaces WEPs small (40-bit) static encryption key, manually entered on wireless APs and client devices, with a 128-bit per-packet key. TKIP does not provide complete resolution for its weaknesses but significantly reduces WEPs vulnerabilities.

LEAP helps to eliminate the security vulnerabilities through the use of the following techniques:

Mutual Authentication – AP authenticates the network and the network needs to authenticate the AP.

User-Based Authentication – LEAP eliminates the possibility of an unauthorized user access by the network through a
preauthorized piece of equipment by the use of usernames and passwords. **Dynamic WEP Keys** – LEAP uses 802.1X to continually generate unique WEP keys for each user. [8]

![Attitude concern comparison](image)

**Protected Extensible Authentication Protocol (PEAP)**
An encrypted SSL/TLS channel between the client and the authentication server is created by PEAP and the channel then protects the subsequent user authentication exchange. To create the secure channel between client and authentication server, the PEAP client first authenticates the PEAP authentication server using digital certificate authentication. When the secure TLS channel is established, one can select any standard PEAP-based on user authentication scheme for use within the channel. After the user is authenticated, the authentication server to the wireless AP supplies dynamically generated keying material. From this keying material, the AP creates new encryption keys for data protection [7, 13].

### 3.4 IEEE 802.11i
The 802.11i specification defines two classes of security algorithms: Robust Security Network Association (RSNA), and Pre-RSNA. Pre-RSNA security consists of WEP and 802.11 entities authentication. RSNA provides two data confidentiality protocols, called the Temporal Key Integrity Protocol (TKIP) and the Counter-mode/CBC-MAC Protocol (CCMP), and the RSNA establishment procedure, including 802.1X authentication and key management protocols.

**Wi-Fi Protected Access (WPA)**
The subset of 802.11i security standard was WPA based on TKIP. WPA focuses the weaknesses of WEP and dynamically generates keys and removes the predictability to exploit the WEP key. WPA also include a Message Integrity Check (MIC), designed to prevent an attacker from capturing, altering and resending data packets [6].

**Wi-Fi Protected Access 2 (WPA2)**
Like WPA, WPA2 supports IEEE 802.1X/EAP authentication. The encryption mechanism is the Counter-Mode/CBC-MAC Protocol (CCMP) called the Advanced Encryption Standard (AES). When a user associates with an access point, WPA2 mutual authentication process is initiated. The mutual authentication process ensures that only authorized users can gain access to the network [6].

**4-Way Handshake Protocol**
The 4-way handshake ensures secure wireless data transmission between supplicant and the authenticator executed to derive a fresh pair-wise Master Key (PMK). This PMK is shared between supplicant and the authenticator at the time of data transmission. Moreover, a fresh Pair-wise Transient Key (PTK) is generated for each session so that a supplicant will have to communicate within the time interval; otherwise it will deauthenticate the supplicant. The AP and the supplicant will silently discard any received message that has an unexpected sequence number [7, 13].

**Internet Protocol Security (IPSec)**
Integrating L2TP with IPSec used as a tunnel protocol to increase the manageability of end-to-end communication. IPSec has many implementations in WLAN. IPSec is widely deployed in VPN as VPN is used to secure wireless network. IPSec has the capability to protect the WLAN from replay attack. IPSec uses shared key for authentication and MD5 or SHA1 for integrity and DES or Triple DES for encryption [10].

4. Conclusions
This paper describes how the Wireless Security Suite can augment 802.11i securities to create secure wireless LANs. Some security enhancement features might not be deployable in some situations, because of device limitations such as application specific devices (ASDs) and 802.11 mobile phones capable of static WEP only or mixed vendor environments. In such cases, it is important that the network administrator understand the potential WLAN security vulnerabilities. Organizations should choose to deploy either IPSec or EAP/802.1x, hereafter referred to as LEAP, but generally not both. Organizations should use IPSec when they have the utmost concern for the sensitivity of the transported data, but remember that this solution is more complex to deploy and manage than LEAP. LEAP should be used when an organization wants reasonable assurance of confidentiality and a transparent user security experience. For Enhancement of security, use the IEEE802.11i protocol in the corporate or in defense. Despite the fact that the wireless networks are not completely secure, its ease of use has always been considered a key factor for their amazing widespread success. Biometric based security schemes have great potential to secure and authenticate access to all types of networks including wireless networks. The IPv6 will be used to create a virtual tunnel backbone and use 3AES instead of using 3DES in IPSec. To solve key management problem, vendors should use the new 8-way handshaking algorithm. And we know that physical security is more secured than the logical one; so we need to maintain device compatibility.

References
[7] An Initial Security Analysis of the IEEE 802.1X Standard Arunesh Mishra, William A. Arbaugh, Department of Computer Science, University of Maryland College, Park Maryland 20742, Feb 2002