Enhancing Security of WI-FI Network

Dr. R.N. Rajotiya¹, Pridhi Arora²

¹Advance Institute of Technology and Management, Palwal, India
²Advance Institute of Technology and Management, Palwal, India, 09911696962

ABSTRACT

Wireless networks have gained rapid popularity in last few years. It has become a popular way of accessing the Internet. It does have the advantage of being inexpensive and highly convenient. This paper discusses Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2). WPA2 is the most secured protocol for wireless networks today. It completely implements IEEE 802.11i and has addressed the vulnerabilities of previous protocols WEP and WPA. The objective of this paper is to provide the solution for WPA2 shortcomings and thus, providing protection to wireless networks from several attacks.

Key words: WEP, WI-FI, WPA, WPA2.

1. INTRODUCTION

Today, wireless networks are one of the rapidly emerging areas of growth. WLANs have gained rapid popularity because of ease of deployment, mobility and reduced costs. But, security risks like eavesdropping, data modification and replay attacks are still there. As the popularity of accessing the internet via wireless increases, the amount of protection must also increase. Communication is done by transmitting and receiving messages through the air by radio waves in wireless network. A outsider can intercept if the messages being sent are not encrypted securely [1].WPA2 has implemented block cipher AES to provide stronger data encryption but still vulnerable to several attacks due to transmission of unencrypted management and control frames and sharing of Group Temporal Key (GTK) among peers connected to wireless network. For securing the wireless network, the first protocol introduced was Wired Equivalent Privacy (WEP) which will be covered in Section 2, Wi-Fi Protected Access (WPA) will be discussed in Section 3 and Wi-Fi Protected Access 2 (WPA2) will be discussed in Section 4. Section 5 presents solution to vulnerability of WPA2.

2. WIRED EQUIVALENT PRIVACY

WEP was the first protocol for securing wireless network and was introduced in September 1999 as part of IEEE 802.11 security standard. WEP was intended to give wireless users a security scheme that is equivalent to being on a wired network. WEP uses RC4 stream cipher to provide confidentiality and CRC-32 for data integrity [1]. The standard specified for WEP provides
support for 40 bit key only but non standard extensions provides support for key length of 128 and 256 bits as well. An initialization vector of 24 bit value is also used by WEP for initialization of the cryptographic key stream.

2.1 WEP Shortcomings

(i) WEP does not provide key management and thus, same keys are used for longer duration and tend to be of poor quality [12].
(ii) The standard specified for WEP provides support for 40 bit key only, thus it is prone to brute force attacks.
(iii) Initialization vector is reused and thus, data can easily be decrypted without the knowledge of encryption key using various cryptanalytic methods.
(iv) Analysis of captured traffic can easily reveal the shared key used by WEP. This shows the weak cryptography.
(v) An attacker can send large number of messages to access point (AP) and thus, preventing the AP from processing the traffic [27].
(vi) WEP does not provide any protection measures against packet forgery.
(vii) Denial of services attacks can be launched by using a powerful transmitter to generate powerful radio signals that interfere with WLAN transmission which makes wireless devices unable to use the radio path [15].

3. WI-FI PROTECTED ACCESS

Wi-Fi Protected Access (WPA) was introduced to overcome the flaws of WEP in 2003 by the Wi-Fi (Wireless Fidelity) alliance [2]. WPA was meant to solve the cryptographic problems of WEP without requiring new hardware [1]. WPA adopts TKIP to fix flaws in WEP protocol and includes packet integrity [15].

WPA has following improvements over WEP [1] [8]:
(i) The Temporal Key Integrity Protocol (TKIP) provides improved data encryption.
(ii) TKIP uses a new algorithm called Michael to compute its new Message Integrity Code (MIC).
(iii) The extensible authentication protocol (EAP) provides user authentication which WEP lacks.
(iv) WPA has built-in secure key management, which lacks in WEP.
(v) The Initialization vector length has been increased to 48 bits from 24 bits to reduce the likelihood of reusing keys.

3.1 WPA Shortcomings

- It is Prone to threats during Hash collisions because of use of hash functions for TKIP key mixing.
- WPA remains vulnerable to availability attacks like Denial of Service.
- WPA uses old cryptography algorithm RC4 instead of Advanced Encryption Standard (AES).

4. WI-FI PROTECTED ACCESS 2
In September 2004, the Wi-Fi Alliance introduced Wi-Fi Protected Access 2 (WPA2) [7]. Two components of WPA2 standard are encryption and authentication which are crucial to a secure wireless LAN [4]. The encryption mandates the use of AES (Advanced Encryption Standard) but TKIP (Temporal Key Integrity Protocol) is available for backward compatibility with existing WAP hardware. The authentication has two modes: Personal and Enterprise. The Personal mode uses a PSK (Pre-Shared Key) and does not require users to be separately authenticated. The Enterprise mode requires the users to be separately authenticated based on the IEEE 802.1X authentication standard, uses the Extended EAP (Extensible Authentication Protocol) [4].

4.1 WPA2 Shortcomings
(i) Management Frames report network topology and are not encrypted so they provide an attacker the means to discover the layout of the network therefore allowing for more successful DoS attacks against a network [4].
(ii) Prone to availability attacks like Jamming and Flooding since it cannot prevent physical layer attacks [5, 9].
(iii) Control Frames like Request to Send and Clear to Send are also unencrypted making them prone to DoS attacks [4].
(iv) GTK is shared amongst all authorized clients of the network. A malicious authorized client may inject spoofed GTK packets in the network. Thus, an authorized user can sniff and decrypt data of other authorized users and may install malware and compromise other user’s devices [6]. This is known as Hole196 vulnerability.
(v) Deauthentication may lead to MAC address spoofing [4].

5. SOLUTION
In order to address the WPA2 vulnerabilities, algorithm based on stream cipher theory has been proposed. A pseudorandom key stream is used to generate cipher text by utilizing the Substitution box values. This encryption algorithm is based on XOR operation and the steps for the algorithm are described below:

1) Calculate key Numeral for Encryption:
   a) Random number is generated between 1024 and 999999.
   b) Length of number is calculated.
   c) Sum of ASCII value of digits of number is calculated.
   Thus, key Numeral= Length of number + Sum of ASCII value of digits.
2) Calculate \( p_0, p_1, p_2 \) and \( p_3 \) parameters:

\( p_0 = \) Sum of digits at even positions of key numeral
\( p_1 = \) Sum of digits at odd positions of key numeral
\( p_2 = \) Product of digits of key numeral
\( p_3 = \) (key numeral) mod (256)

3) Calculate \( q_0, q_1, q_2 \) and \( q_3 \) parameters:

In order to compute \( q_0, q_1, q_2 \) and \( q_3 \) values, encryption parameters ENP1, ENP2, ENP3 and ENP4 are required which are computed using Table 1:

\[
\begin{align*}
\text{Table 1: Encryption Parameters} \\
| \text{ENP1 parameter} | \text{ENP2 parameter} | \text{ENP3 parameter} | \text{ENP4 parameter} | \\
|----------------------|----------------------|----------------------|----------------------|
| 0, p0 \text{ XOR } p1 | ENP1 + 15 | p2 \text{ XOR } p3 | ENP3 + 55 | \\
| 1, p0 \text{ XOR } p2 | ENP1 + 25 | p1 \text{ XOR } p3 | ENP3 + 65 | \\
| 2, p0 \text{ XOR } p3 | ENP1 + 35 | p1 \text{ XOR } p2 | ENP3 + 75 | \\
| 3, p2 \text{ XOR } p3 | ENP1 + 45 | p1 \text{ XOR } p3 | ENP3 + 85 | \\
\end{align*}
\]

\[
\begin{align*}
q_0 &= \text{ENP1}[0]+\text{ENP2}[0]+\text{ENP3}[0]+\text{ENP4}[0] \\
q_1 &= \text{ENP1}[1]+\text{ENP2}[1]+\text{ENP3}[1]+\text{ENP4}[1] \\
q_2 &= \text{ENP1}[2]+\text{ENP2}[2]+\text{ENP3}[2]+\text{ENP4}[2] \\
q_3 &= \text{ENP1}[3]+\text{ENP2}[3]+\text{ENP3}[3]+\text{ENP4}[3]
\end{align*}
\]

4) Calculate \( r_0, r_1, r_2 \) and \( r_3 \) parameters:

\[
\begin{align*}
r_0 &= ((\text{ENP1}[q2] \text{ XOR } \text{ENP2}[q2]) \times p_0) + q_2 \\
r_1 &= ((\text{ENP1}[q1] \text{ XOR } \text{ENP3}[q1]) \times p_1) + q_1 \\
r_2 &= ((\text{ENP1}[q0] \text{ XOR } \text{ENP4}[q0]) \times p_2) + q_0 \\
r_3 &= ((\text{ENP2}[q3] \text{ XOR } \text{ENP3}[q3]) \times p_3) + q_3
\end{align*}
\]

5) Calculate Substitution box (S-box) values using Table 2

6) Calculate Message parameter:
Message Parameter = key Numeral (obtained in step 1) + randomly generated key between 1024 and 999999 + Average of p0, p1, p2 and p3 parameters (obtained in step 2) + Average of q0, q1, q2 and q3 parameters (obtained in step 3) + Average of r0, r1, r2 and r3 parameters (obtained in step 4)

7) Message Encryption

i) Reverse the plaintext to be encrypted to obtain Partial Message Encryption 1 (PME1).

ii) Perform PME1 XOR S-box [index] (obtained in step 5) operation to obtain Partial Message Encryption 2 (PME2).

iii) Perform PME2 XOR Message parameter (obtained in step 6) operation to compute Partial Message Encryption 3 (PME3).

iv) Reverse hex encoded value of PME3 to compute Partial Message Encryption 4 (PME4) which is the resultant encrypted text.

Table 2: S-Box values

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>(ENP1[q0] XOR r0) * r0</td>
<td>(ENP1[q1] XOR r1) * r0</td>
<td>(ENP1[q2] XOR r2) * r0</td>
</tr>
<tr>
<td>1</td>
<td>(ENP2[q0] XOR r0) * r1</td>
<td>(ENP2[q1] XOR r1) * r1</td>
<td>(ENP2[q2] XOR r2) * r1</td>
</tr>
<tr>
<td>2</td>
<td>(ENP3[q0] XOR r0) * r2</td>
<td>(ENP3[q1] XOR r1) * r2</td>
<td>(ENP3[q2] XOR r2) * r2</td>
</tr>
<tr>
<td>3</td>
<td>(ENP4[q0] XOR r0) * r3</td>
<td>(ENP4[q1] XOR r1) * r3</td>
<td>(ENP4[q2] XOR r2) * r3</td>
</tr>
</tbody>
</table>

The process of message decryption is identical as the above encryption process. The key used for encryption is being generated randomly in the first step of encryption algorithm.

Also, in the existing scenario, identical Group Temporal Key (GTK) is shared among all peers connected to the network thus, leading to Hole 196 vulnerability. To address the above issue, authenticator can assign random and unique GTK to every peer in network [10]. The access point then generates a unique and random GTK and during a multicast or broadcast communication, sender sends encrypted text using its key to access point. The access point then transmits the encrypted text along with the originating station’s GTK to the recipient stations. The recipient then decrypts the text at their end using this GTK. At the end of the session, a new GTK is assigned to the sender station. As each peer connected to network is unaware of GTK of rest of the peers, hence this overcomes the Hole 196 vulnerability.
6. CONCLUSION
This research presents the various protocols for securing Wireless LAN. WEP is unable to provide security against various threats so WPA was introduced as a solution to the security flaws identified in WEP. WPA2 was introduced to overcome the flaws of WPA. WPA2 provides stronger encryption by using block cipher AES but it is still vulnerable to attacks due to sharing of GTK among clients and transmission of unencrypted control and management frames. In this paper a solution to overcome the Hole 196 vulnerability has been provided.

REFERENCES


