Global Information Assurance Certification Paper

How WPA secures the Wi-Fi connection and eliminates the weaknesses in WEP.

by Hendra Hendrawan
GSEC Practical v1.4b
Oct 22, 2003

Abstract

The growing popularity of wireless network for the past recent years in pervasive. However, the progress of security standards for wireless network has been far behind. Different vendors has introduced different security solutions to the demand from the people in deploying wireless solutions.

This paper will discuss the three security layers of wireless network and the challenges and possible solutions in deploying a secure wireless network solution in an organization.

The weaknesses of Wired Equivalent Privacy (WEP) will be mentioned but not discussed in details. Instead detail discussion will be focused on Wi-Fi Protected Access (WPA). The security discussion will be divided into three major sections or security layers: the wireless LAN layer, the access control layer and the authentication layer.

To complete the discussion, possible practical solutions will also be brought up and analyzed from different point of views, such as deployment strategies, challenges and possible solutions.

Introduction

The insecurity of wireless LAN is always a concern for most organizations. However, the demand for wireless LAN is high enough that some organizations have decided to use third-party or proprietary solutions, deployed insecure wireless network or neglected to use any security solution in the wireless network.

This is due to the fact that the slow progress of security standards or other issues such as different flavors of operating system used by the clients that use the wireless network.

As it has been well known in the community of information security practitioners, Wired Equivalent Privacy (WEP) is no longer adequate to be used to protect the wireless LAN. However, the recent development in wireless security standards, protocols and applications sounds promising.

Weaknesses in WEP

Wired Equivalent Privacy (WEP) has well known insecurity issues. There have been a lot of papers, discussions, and even applications that can be used to break the WEP security. Mainly the areas of concerns are the following:

1. Good authentication

2. Access control
3. Replay prevention
4. Message modification prevention
5. Message privacy
6. Secret key protection.

Obviously, the listed problems above breaks the C-I-A (Confidentiality - Integrity – Availability) model of information security. Therefore, any Wi-Fi security solution must eliminate the above problems.

WPA and other standards

The next generation of wireless security after WEP is IEEE 802.11i. 802.11i defines a better wireless network in terms of security called robust security network (RSN). However, most network devices currently do not support or incompatible with RSN. Hence Wi-Fi protected access (WPA) was introduced as a transition solution towards 802.11i network or RSN.

WPA is a security solution that is based around the current capabilities of existing Wi-Fi products found in the market. WPA in a sense is a subset or RSN.

WPA uses existing and well-known standards and protocol to mitigate the security weaknesses in WEP.

Security layers

This paper will divide wireless network security context into three security layers. The three layers are:

1. Wireless LAN
2. Access control
3. Authentication

The wireless LAN layer deals with the communications between the client and the access point. The access control layer is the one in charged on allowing or rejecting connection from and to the network. It also talks to the authentication server which will be discussed later. The authentication makes the decision whether a wireless device is allowed to join the network.

Access control

WEP does not provide any access control to the wireless network. Wi-Fi Protected Access (WPA) on the other hand overcomes this problem by specifying mandatory protocols for secure wireless network. The mandatory protocols are IEEE 802.1X and EAP and RADIUS. RSN being a superset of WPA does not require RADIUS protocol for authentication server which allows more flexibility for implementation.

IEEE 802.1X

The main purpose of 802.1X is to control access at a point where a client or user joins the corporate network. It is based on a very simple idea that breaks the network into three sections as follows:

1. Supplicant, which is the client device or user who wants to use the network resource
2. Authenticator, which actually controls the access to the network, and
3. Authentication server, which contains information regarding the validity and authenticity of the user willing to join the network. It also makes the final decision whether a user is allow to the network.

How 802.1X solves the access control issue

Originally, 802.1X is designed to work with wired LAN. The objective is to control port access so that not anyone can plug in a wired network card into the jack on the wall and start using the network resource. The idea, however, can be applied to the wireless LAN environment. Each connection request from a client can be considered to be an access to the port via an invisible wire. If the *authenticator* to a wired network is a network switch, or intelligent hub, then the authenticator to a wireless network is the access point. This allows the access point to perform access control similar to the switch because each connection request can be treated as unauthenticated connection until further approved by the authentication server.

Message Passing with EAP

Extensible Authentication Protocol (EAP) was originally designed for Point-to-point (PPP) protocol. It is suitable for the establishing and finalizing the authentication process. In fact, EAP has been used to carry out different authentication protocols such as Transport Layer Security (TLS), Tunnel Transport Layer Security (TTLS), and etc. The benefit of EAP is that it does not depend on a specific authentication scheme and can be easily used to encapsulate other any authentication method.

The detail implementation of EAP can be found in RFC2284. Essentially, EAP specifies four types[1] of message that can be used for the communication purpose.

1. Request: messages coming from the access point to the wireless client/user
2. Response: messages coming from the client to the access point.
3. Success: message from the access point when the network access is granted.
4. Failure: message from the access point when the network access is refused.

The request and response type messages are further divided into six different types. For instance, type 2 is for notification purpose, 1 for identity, etc. (Figure 1)

[1] L. Blunk and J. Vollbrecht. "PPP Extensible Authentication Protocol (EAP)." March 1998. URL:http://www.ietf.org/rfc/frc2284.txt?number=2284 (Oct 10, 2003).

Code	ID	Length	Type	Data

Figure 1 EAP message format for request and response types

Encapsulation of EAP messages with EAPOL

The specification of EAP does not specify how EAP messages are transported from one place to another within the network. Therefore the IEEE 802.1X defines a EAP over LAN protocol namely EAPOL. EAPOL on the other hand provides description on how the EAPOL can be transported over Ethernet (IEEE 802.3).

EAPOL by itself have five types of messages. They are:

1. Start
   This type message is used to search and initiate the authentication process. In a wireless environment the Start type messages are sent to the multicast MAC address to see if there is any respond from the access point.

2. Key
   This is used by the access point to send the encryption keys to the client once the client has obtain the authorization to access the network.

3. Packet
   EAP messages that are going back and forward are encapsulated in this type of EAPOL message. This the main reason for EAPOL to specified in the first place.

4. Logoff
   When the client wishes to disconnect from the wireless network, it sends this type message to the access point.

5. Encapsulated-ASF-Alert
   This type is not used in either WPA or RSN.

Figure 2 shows the format of EAPOL message over the Ethernet (IEEE 802.3) LAN. The type section is where the type of EAPOL messages such as start, key packet or logoff is indicated with a predefined number.

Ethernet Header	Protocol (always 1)	Type	Length of data	Data

Figure 2 EAPOL frame format.

The role of the RADIUS protocol

For small wireless network such as home network there is no such need for a separate authentication server as opposed to a big organization where access points are located in many strategic places called hot spots. So far, the message passing for the access control

layer has been established up to the access point. In the case of a large corporate network, a different way of encapsulating EAP messages further from the access point to and from the authentication server is required. This is where the RADIUS protocol joins the fun.

Similar to EAP, the RADIUS protocol was not originally designed for wireless network. The word RADIUS stands for Remote Access Dial-In User Service. Hence, it was designed for dial-in access. The RADIUS protocol has two important aspects that make it suitable for wireless network. In general, it defines two things:

1. A set of functionality compatible with different types of authentication servers, and
2. The protocol to access the functionalities.

There are a number RADIUS protocol specifications since it was first introduced. But the basic use of the protocol boils down the following four basic message types, which are:

1. Request
2. Challenge
3. Accept
4. Reject

Of all those message types, only the request type message is used for sending messages from the access point to the authentication server. The rest is used by the authentication server to send messages to the access point which is then forwarded to the client or user.

Looking at the RADIUS message format (Figure 3), the important part lies in the attribute part where it defines the type of message it carries and furthermore it is extensible to support vendor specific attributes. The code defines the type of message and the nonce contains a value that's never used more than once.

Code	Nonce	Length	Authenticator	Attributes

Figure 3 RADIUS message format.

The Working EAP, EAPOL and RADIUS

Putting all the pieces together as seen in Figure 4 we have the encapsulation of EAP messages with EAPOL from the user to the access point. And the encapsulation of EAP messages by RADIUS from the access point to the authentication server.

The Authentication Layer

The authentication layer can be considered to be the highest security layer. Both WPA and RSN do not specify or mandate which authentication layers to use. There are many

well known authentication methods such as Transport Layer Security (TLS) and Kerberos. Different authentication methods provide different way of securing the network. The use of key for example in Kerberos is different with TLS. Kerberos is more towards secret key approach while TLS is based on certificate type which will be discussed next.

Transport Layer Security (TLS)

TLS evolved from SSL, which was introduced by Netscape Corporation. TLS later on became a standardized version of SSL which is not vendor specific. The work of TLS is composed of two protocols: record and handshake. The handshake protocol establishes agreement with the other end while the record protocol encrypts/decrypts data that is being sent from both ends.

TLS Handshake

The following are the general steps which are exchanged during the TLS handshake process.

Step 1: client to server (initiation)
The client sends a message to the server to initiate the process. The message contains a series of cipher suites and other related information supported by the client. It also includes a random number in the message.

Step 2: server to client (initiation)
The server, after receiving the message from the client, also sends a message to the client containing the following a server's random number, which is different from the client's and a session id.

Step 3: server to client (certificate and public key)
Next, the server sends a certificate to the client which contains the public key of the server which can be used by client to encrypt information later on.

This is the most important part in the handshake process because it contains the public key of the server, which is used to encrypt data from the client and can only be decrypted by the server. To guarantee that the public key transmitted to the client is legitimate, certificate issued by Certificate Authority is used as a warranty and assurance.

Step 4: client to server (establishing of shared secret key)
Assuming that the client trusts the certificate and hence the public key from the server. The client can now generate a secret key (or private key) that will be shared by both the client and server for subsequent encryption/decryption process. The shared secret key can also be sent to the server in a secure way because it will be encrypted using the server's public key which only the server knows how to decrypt.

Step 5: client to server and server to client
Both the client and the server can now communicate securely with the secret key.

The establishment of a shared secret key (symmetric key) as opposed to using the public key for both the client and the server has to do with the issue of performance. The steps can be obviously reduced if both the client and the server use public key (asymmetric) encryption. However, public key encryption requires more computing power than private key encryption. Therefore, TLS uses public key encryption to establish a secure private key exchange for later use.

Fitting TLS into WPA

RFC2716 has defined how TLS can be transported over EAP. The RFC defines a number (13) which can be used in the type file (Figure 1) of the EAP message to indicate that the frame is encapsulating a TLS message.

Due to the possibility of TLS packet exceeding the EAP frame, two extra fields are also defined following type file in as shown in Figure 4. The fields are length and flag. The length indicates the total length of the TLS packet and the flag contains three bits indicating the present of the length field, the extra fragments and the start indicator to kick-in the handshake process.

Code	ID	Length	13	Flags	TLS length	TLS data

Figure 4 Encapsulation of TLS Packet in EAP

Traffic Encryption using WPA's Four-way Handshake

Up to this point the authentication process is done. The remaining problems left unsolved are the encryption of the traffic from the user to the access point and a way to verify that the access point is a legitimate access point i.e. not rough access point that is put up for someone with malicious intention to capture personal or otherwise private information.

WPA achieves this by using the four-way handshake to computer a set of keys called the temporal keys. The keys are:

1. Data encryption key
2. Data integrity key
3. EAPOL-Key encryption
4. EAPOL-Key integrity

For some infrastructure wireless network where the user can move from one access point to another without having to reestablish the connection, these keys are recomputed every time there is a re-association between the user and the access point. This is to ensure that every access point is a valid access point.

The computing of temporal keys also prevents packet sniffing because one of the keys can be used to encrypt/decrypt the data that travels in the open air.

The computing of the temporal keys is done by using the shared secret obtained from the authentication process discussed previously, two nonces (never repeated random number), and two MAC addresses. The shared secret key is also known as pairwise master key. So, Secret Key + access point nonce + user nonce + client MAC + server Mac => temporal keys.

The four-way handshake works as follows:

Step 1:
The access point sends EAPOL-Key type message to the user containing the nonce from the access point. The user can now computer the temporal keys because it has all the required information.

Step 2:
The user sends its nonce to the server with the EAPOL-Key integrity key. This ensures the value of user nonce is coming from the legitimate user. The access point is now ready and capable of computing the temporal keys. If the message from the client is not tampered, the values should be same on both sides.

Step 3:
The access point sends a data integrity key to the user and a sequence number to indicate the first encrypted message which will be sent by the access point later on.

Step 4:
The user confirms by sending a message to the access point.

At this point, both parties install the data encryption key and start communicating in a secured environment.

Temporal Key Integrity Protocol (TKIP)

TKIP was created and becomes a part of WPA is because it works around the existing hardware to improve the security, or insecurity, in WEP. It adds certain measures to overcome the weakness in WEP as follow:

1. Message Integrity checking
   This is done by adding a message integrity protocol to prevent tampering which is done on the software level.

2. IV Selection
   Use of IV is done in an incremental manner, and IV value is used to prevent replay attack.

3. Per-packet Mixing
   This is done by using different key for each packet sent.

4. IV Size
   IV Size is increased to increase the time requires to crack the IV value.

Implementation Considerations

As good as it sounds, to be able to provide the above solutions, a couple of things require some practical considerations.

Support for EAP

As far as the access control is concerned, not all operating systems support EAP yet. In a case where an organization does not require the network to support different operating system platforms, this is not an issue. Windows XP has built-in support for 802.1X authentication method. For an organization that is required to support different OS on the other hand, may face a challenge.

Four-way handshake and rouge access point

The four-way handshake theoretically provides a good way of securing the network traffic. Alas, it brings up two implementation issues as well. First, the access point must be able to compute the temporal keys. Second, the distribution of the secret key to the access point must be done securely. Third, certificate may not be effective enough in stop computer illiterate users from accessing rough access point.

Access or Computing or Temporal Keys

Regarding the first and the second issue, if the access point cannot be used to compute or store the secret key, a server that supports EAP and EAPOL can be placed behind all the access points to handle the requests. The third however can only be mitigated by educating the user not to trust any certificate without careful inspection.

TKIP

TKIP can be deployed easily providing the vendor of the Wi-Fi network card provides driver update for the device.

Conclusion

WEP is insecure, WPA as a transition solution provides better security given the current hardware limitation. Eventually, every wireless device will be compatible with the 802.11i and RSN specifications. Unfortunately, the need and demand to use the wireless technology cannot wait for that day to happen. On the bright side, WPA can reduce if not eliminate the weaknesses in WEP without having to reinvest in the new technology.

List of References

Edney, Jon., and William A. Arbaugh. Real 802.11 Security: Wifi Protected Access and 802.11i. Boston: Addisson-Wesley, July 2003.

Fogie, Seth., and Cyrus Peikari, Maximum Wireless Security. Indianapolis: SAMS, December 2002.

Gast, Matthew S. 802.11 Wireless Networks: The Definitive Guide. Sebastopol: O'Reilly, April 2002.

Silverman, Micah. "Securing Wireless Network." Dr. Dobb's Journal. Volume 28 (June 2003): 36 – 44.

"Wi-Fi Protected Access: Strong, standard-based, interoperable security for today's Wi-Fi networks." Wi-Fi Alliance.
URL: http://www.wi-fi.org/OpenSection/pdf/Whitepaper_Wi-Fi_Security4-29-03.pdf (Oct 20, 2003).

"Securing Wi-Fi Wireless Networks with Today's Technologies." Wi-Fi Alliance.
URL: http://www.wi-fi.org/OpenSection/pdf/Whitepaper_Wi-Fi_Networks2-6-03.pdf (Oct 20, 2003).

Dismukes, Trey."Wireless Security Blackpaper." Ars Technica.
URL: http://www.arstechnica.com/paedia/w/wireless/security-1.html (Oct 20, 2003).

"Port-Based Network Access Control." IEEE Standard for Local and Metropolitan Area Network.URL: http://standards.ieee.org/getieee802/download/802.1X-2001.pdf (Oct 10, 2003).

Geier, Jim. "Planning WLAN Operational Support II."
URL: http://www.wi-fiplanet.com/tutorials/article.php/3093811 (Oct 10, 2003).

Geier, Jim "Planning WLAN Operational Support III."
URL: http://www.wi-fiplanet.com/tutorials/article.php/3095581 (Oct 10, 2003).

Schroder, Carla. "Wireless on Linux, Part 1."
URL: http://www.wi-fiplanet.com/tutorials/article.php/3066371 (Oct 12, 2003).

Robinson, Brian. "Gearing Up for Wireless Security." Jan 13, 2003.
URL: http://www.fcw.com/fcw/articles/2003/0113/cov-plug4-01-13-03.asp (Oct 20, 2003).

Blunk, L, and J. Vollbrecht. "PPP Extensible Authentication Protocol (EAP)". March 1998. URL: http://www.ietf.org/rfc/rfc2284.txt?number=2284 (Oct 10, 2003).

Dierks, Tim, and Eric Rescorla. ”The TLS Protocol Version 1.1.” June 2003. URL: http://www.ietf.org/internet-drafts/draft-ietf-tls-rfc2246-bis-05.txt (Oct 10, 2003).

Freier, Alan O., Philip Karlton and Paul C. Kocher. “The SSL Protocol Version 3.0.” November 18, 1996. URL: http://wp.netscape.com/eng/ssl3/draft302.txt (Oct 10, 2003).

Last Updated: July 27th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event