Global Information Assurance Certification Paper

Wireless network security, does it really exist?

Vedette Morris
GSEC Practical v1.4c
November 11, 2004

Abstract

This paper is targeted at individuals who are new to wireless networking. It's purpose is to highlight the security standards that have been available to wireless network administrators and introduce the recently approved 802.11i standard. It aims to provide readers with a basic knowledge of the problems that have been associated with providing a secure wireless network and also to highlight the steps that have been taken to ensure that the security of a wireless network is comparable to the security of a wired network.

To achieve this I will discuss the standards that have been used in the lead up to the approved 802.11i standard and will give an overview of the new encryption protocols that have been included in the 802.11i standard.

Introduction

In June 2004, after many years in the planning, the Institute of Electrical and Electronics Engineers (IEEE) approved the 802.11i security standard, for wireless networks. Many groups believed that the 802.11i task group was taking too long to approve and implement the standard, as the wireless networking environment had a critical need for the extra security that the standard would ensure.

This paper will first give its readers a background on the previous security standards used by wireless networks, including the interim standards that have been implemented in an effort to improve wireless network security, prior to the release of the 802.11i standard. These include:

- Wired Equivalent Privacy (WEP);
- 802.1x; and
- Wi-Fi Protected Access (WPA).

Next it will introduce the new encryption algorithm and the new encryption protocols that have been introduced under the 802.11i standard. These are:

- The Advanced Encryption Standard (AES);
- The mandatory encryption protocol of CCMP; and
- The optional encryption protocol of WRAP.

The aim is to prove to the reader that wireless network security does exist, however it is necessary to implement the highest security standards in order to achieve this.

Wired Equivalent Privacy

Protecting the privacy of data on a wireless network, presents new challenges to network administrators when compared to the traditional wired network. This is due mainly to the fact that wireless networks don't have defined physical boundaries. The ease of access and the mobility that makes wireless networking attractive to business, also makes it attractive to the network intruder.

When the IEEE 802.11 standard was introduced in 1997, the members behind its implementation understood that the network boundaries had been changed forever and incorporated in the standard an optional "privacy" capability. This was supposed to provide a similar level of privacy to wireless network users, to that currently enjoyed by users of wired networks. The result was Wired Equivalent Privacy (WEP), it should be noted that the authors of the standard, never intended that WEP would provide a secure network protocol,[1] the objective was to provide privacy from the casual or accidental network intruder, not to provide security from the determined hacker.

While not designed as a secure network protocol, WEP was designed in order to provide the basic communications security requirements to the wireless network. These requirements are: Confidentiality, Integrity and Authentication.

Confidentiality was provided by encrypting the transmitted frames. Integrity was provided by an Integrity Check Value, appended to the end of the frame body, its task was to verify that the data had not been tampered with in transit. Finally, authentication was provided based on the knowledge of the shared secret key and the MAC address of the mobile terminal.[2]

How WEP Works

At to root of WEP encryption is the RC4 stream cipher. A stream cipher generates a stream of bits called a key-stream, which is then combined with the plain text message to produce cipher text. The stream cipher takes a short secret key and expands it into a pseudorandom key-stream the same length of the message.[3]

In order for a mobile unit to communicate with an access point using WEP both units must have access to the same shared secret keys. The original 802.11 standard stipulated that WEP would use a 40 bit secret key,

---

[1] Dubrawsky, Ido. "Wireless (In) Security" April 2002
URL: http://www.unixreview.com/documents/s=2427/uni1020280760693/

[2] Gast, Matthew. "802.11 Wireless Networks: The Definitive Guide" (" (Sebastopol CA, 2002) p. xi

[3] *Ibid* – pg 87

although some long key versions of WEP using a 104 bit key have been released. The 802.11 standard did not stipulate how the shared secret keys should be distributed among users of the network and in the majority of cases the WEP key is a static key that is physically typed into each individual access point and mobile unit associated with the service set.

To encrypt data, the 40 bit WEP secret key is augmented with a 24 bit Initialization Vector (IV). This therefore, produces a 64 bit key to be used to encrypt the packet with the RC4 stream cipher. The sender then XORs the data to produce the cipher text and the packet is then sent to the intended recipient. As knowledge of the IV is required in order for the recipient to be able to decrypt the cipher text, the IV is included in the packet as plain text, positioned in the packet between the frame header and the frame body. When the packet reaches the recipient it is then decrypted using the stored WEP secret key and the IV attached to the packet.[4]

WEP Vulnerabilities

There have been many different vulnerabilities associated with WEP. These include:

a. Re-use of Initialisation Vectors;
b. Distribution and rotation of static keys;
c. The ease with which mobile units and access points can be forged;
d. The method with which the integrity of the message is proved; and
e. The RC4 stream cipher itself.

The initial WEP standard specifies the use of a 40-bit key, this is due to the fact that at the time the standard was written, the maximum length of a cryptographic key permitted by law to be exported from the United States of America was a 40-bit key. Due to the short length of the key it was vulnerable to brute-force attacks, enabling the attacker to reveal the secret key. The length of the key was later addressed by the industry with the release of 104-bit key, which made brute-force attacks almost impossible, based upon the technology available to the attacker at the time. However, regardless of the length of the secret key the IV associated with each packet in all cases is only 24-bits in length. This means that the maximum number of times that an IV can be used with the same secret key, without repeating the IV is 2^{24} times, once the same IV is used more than once with the same secret key an IV collision has occurred. If an attacker were to collect all packets going to and from a wireless network access point, they would eventually have enough packets encrypted with the same IV to enable them to obtain the secret key.[5] To make matters worse, some manufacturers do not use random IVs but increment the IV by one for each packet transmitted, there are also some

[4] Borisov, Nikita. Goldberg, Ian. Wagner, David. "Security of the WEP algorithm". February 02, 2001. URL: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

[5] Borisov, Nikita. Goldberg, Ian. Wagner, David. "Intercepting Mobile Communications: The Insecurity of 802.11"
URL: http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf

manufactures that set up their equipment to reset the IVs each time the terminal is reset, both of these practices ensure large numbers of IV collisions.[6]

The WEP standard does not define how the static secret keys are to be distributed and rotated on a network. As such, and as mentioned earlier, some network administrators distribute their network WEP keys by physically going to each access point and mobile unit associated with the service set and typing in the WEP keys. This method of distribution is very time consuming and gaining access to all mobile units in a service set could prove to be a logistical nightmare, these two points are the main reasons that static WEP keys on wireless networks are not changed nearly as often as they should be in order to maintain greater network security. The practice of manually distributing WEP keys introduces more problems with relation to the security of the network, three of the main problems are:

1. It is difficult to prevent the users of the machines from discovering what keys are being used on the network.

2. If staff members can gain knowledge of the secret key, then the key must be changed as often as the staff is changed. If one staff member leaves the organisation the keys must be changed immediately.

3. The more users on the network the harder it is to maintain the secret WEP keys. For example, on larger networks it is necessary for administrators to publish the WEP keys, in order for all intended network users to gain access to the network.[7]

As illustrated above, maintaining the WEP key as a 'secret' key can often be one of the greatest challenges of using WEP on a wireless network.

WEP authentication fails wireless network users due to the fact that authentication is proven by the knowledge of the shared secret key and also with the option of access points maintaining a list of MAC addresses associated with the mobile units permitted to join that particular service set. As listed above maintaining a secret key is one of the challenges of wireless networking, also there are software programs available to anyone who wants to download them that are designed specifically to reveal the secret WEP keys of a service set. The use of a MAC address list is also unreliable as it is easy for an attacker to alter their equipment so that for all intensive purposes it appears to be an authorised machine. Also while the MAC address list may authenticate a machine it does not prove that the user of the machine has permission to be a part of that particular service set. One ploy that attackers use is to set up fake access points, as the access point is not required to authenticate to the user, the user will not be aware that the access point with which they are associated is not actually part of their network.

[6] Dubrawsky, *op. cit*
[7] Gast, *op. cit.* p. 93

To maintain the integrity of messages transmitted over a wireless network, WEP uses an integrity checksum field, the checksum for each packet is obtained by utilising an algorithm known as a cyclic redundancy check (CRC). The CRC checksum is encrypted within the transmitted packet and it is designed to detect single bit alterations within the packet. The CRC however, fails in its task to protect the integrity of the packet, due to the fact that the checksum is calculated using straight forward mathematics, as opposed to a cryptographic hash. This means that an attacker wishing to tamper with transmitted packets is able to predict what effect changing single bits within the packet will have on the CRC calculation.[8]

The final down fall for WEP came when in 2001 a paper was released, written by Scott Fluhrer, Itsik Mantin and Adi Shamir. The paper, titled "Weaknesses in the Key Scheduling Algorithm of RC4", details two major weaknesses in the Key Scheduling Algorithm (KSA) of RC4. The first weakness discovered was the existence of a large number of weak keys. These weak keys allow a small part of the secret key to determine a large amount of the KSA output. It was found that this created a situation where the initial output of the RC4 algorithm was "disproportionally affected by a small number of key bits." The second weakness, which is related to the first weakness, occurs when part of the key presented to the KSA is exposed to the attacker. This action occurs each time a WEP packet is sent as the IV, which comprises 24 bits of the key, is transmitted with each packet in an unencrypted portion of the packet. When the same IV and secret key are used numerous times, an attacker can use the initial word of each key stream to reveal the secret part of the key. [9]

As shown from the problems outlined above, WEP fails dismally in the provision of communications security. Confidentiality is compromised due to the ease with which an attacker can determine the secret key, message integrity is compromised due to the use of the cyclic redundancy check as opposed to the use of a randomly generated cryptographic hash and authentication is compromised due to the fact that the hackers can gain access to the secret key and that using the MAC address of a machine only authenticates the machine and not the user of the machine.

802.1x

The authentication problems associated with WEP were partly addressed when the IEEE released the 802.1x standard. The 802.1x standard was designed to operate with wired networks, however has been incorporated into wireless networks with many advantages over WEP. The standard is not actually a security standard and also the standard itself does not provide the wireless network with authentication, it provides the capability to allow access points to forward requests to an authentication server and forward replies back to the mobile unit. At its root is a standard to implement

[8] Gast, *op. cit.* p. 92
[9] Fluhrer, Scott. Mantin, Itsik. Shamir, Adi. "Weaknesses in the Key Scheduling Algorithm of RC4" URL: http:www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf

the framework for Port-Based Network Access Control.[10] In itself the standard does not provide a secure wireless network, however when used in conjunction with the Internet Engineering Task Force (IETF) Extensible Authentication Protocol (EAP) standard, it provides a wireless network capable of two way authentication (depending on the authentication method used) and also provides options to deal with the problem of static user and session keys.[11]

How 802.1x Works

The purpose of the 802.1x standard is that it,

> "defines a mechanism for Port-based network access control that makes use of the physical access characteristics of IEEE 802 LAN infrastructure in order to provide a means of authenticating and authorizing devices attached to a LAN port that has point-to-point connection characteristics, and of preventing access to that port in cases in which the authentication and authorization process fails."[12]

In order to do this the standard stipulates two distinct roles within the access control interaction; these are the Authenticator and the Supplicant.

1. The Authenticator is the entity that enforces authentication prior to allowing access to the services that are accessible via the port. The Access Point associated with a wireless network service set carries out this role.

2. The Supplicant is the entity that wants to access the services available through the port of the authenticator. The mobile units that are associated with a service set take on the role of the supplicant.

The standard also identifies one more system role, that of an Authentication Server. The authentication server checks the credentials of the supplicant on behalf of the authenticator and indicates whether the supplicant is authorised to access the services provided by the authenticator.

In most cases the authentication process is provided by a Remote Authentication Dial In User Service (RADIUS) server. The access point merely acts as a bridge between the mobile unit and the RADIUS server. The benefit of this system is that the each access point does not have to contain

[10] IEEE Std 802.1X-2001 "IEEE Standard for Local and metropolitan area networks – Port-Based Network Access Control"
URL: http://www.ieee802.org/1/pages/802.1x.html
[11] Ou, George. "At last, real wireless LAN security. Introducing 802.1x and EAP" September 3, 2002
URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2878940-2,00.html
[12] IEEE Std 802.1X-2001 "IEEE Standard for Local and metropolitan area networks – Port-Based Network Access Control"
URL: http://www.ieee802.org/1/pages/802.1x.html

any information about the credentials of any of the mobile units, its actions are based solely on the authentication response from the RADIUS server.

When using the 802.1x standard, access is restricted by the network port until the user is authenticated, the only action that a mobile unit (supplicant) can perform on the network once associated with an access point (authenticator), is that of authentication. For this reason the authentication process takes place using the link layer, as this provides the minimum access required to authenticate while at the same time preventing the supplicant from accessing any other areas of the network in an unauthorised state. Once successful authentication has taken place, the port is then open to the mobile unit and they are able to access all the features on the network, in line with their account privileges.[13]

Extensible Authentication Protocol

The Extensible Authentication Protocol (EAP) is defined in the IETF standard RFC 2284 and as stated previously is used by the 802.1x standard to assist in the security of network transmissions. The advantage of EAP is that it is a general point-to-point protocol (PPP) that has the capability to support multiple authentication mechanisms. It effectively acts as a transport for the different types of EAP authentication methods.

As with WEP, the first action that a mobile unit, or supplicant, must take is to associate with the networks access point, or authenticator. Once associated the authenticator sends a request to the supplicant for authentication, it is here that the EAP authentication method is negotiated.

The EAP Packet

The EAP packet consists of the following fields:

1. Code
2. Identifier
3. Length, and
4. Data…

The code field is one byte in length and its purpose is to identify the type of EAP packet that is being transmitted. The entry in this field ranges from 1 to 4 and the assigned meanings for each entry are:

1. Request
2. Response
3. Success
4. Failure

[13] Phifer, Lisa. "802.1x Port Access Control for WLANs" September 5, 2003
URL: http://www.wi-fiplanet.com/tutorials/article.php/3073201

The identifier field is also one byte in length and assists to match the EAP requests with the EAP responses. This field must be the same if a request is required to be retransmitted, this is necessary so that the retransmitted request can be distinguished from new requests. If it is a new request then this field must be changed.

The length field is two bytes in length and indicates the total length of the EAP packet, taking into account the code, identifier, length and data fields.

The data field can be of any length from zero bytes up, its format is determined by the code field.

A typical request or response EAP packet will contain the code field, indicating either 1 or 2, the identifier field and the length field. It will also contain a type field and a type-data field.

The type field is one byte in length and identifies the structure of an EAP request or response packet. Types 1 to 3 are defined by RFC 2284 as special case types and are explained below, the remaining types identify the authentication method that the authenticator wishes to use:

1. Identity – Used to query the identity of the supplicant attempting to gain access to a network. This will generally be issued by the authenticator as the initial request and the supplicant is required to send a response to this request.

2. Notification – The use of type 2 is optional, when used it enables to authenticator to display a message to the supplicant.

3. Nak – This type is only to be used in the response packet. It is used to convey to the authenticator that the authentication type listed in the request packet is unacceptable to the supplicant.

The type-data field varies in length and is dependent upon the type of the request packet from the authenticator and the associated response from the supplicant.

The success or failure EAP packet will only contain the code field, indicating either 3 or 4, the identifier field and the length field. If the authenticator receives an EAP packet from the authentication server with a code field of 3, then the supplicant is granted access to the network resources associated with his login, if the authenticator receives an EAP packet from the authentication server with a code field of 4 then it disassociates the supplicant.[14]

[14] "RFC 2284-PPP Extensible Authentication Protocol (EAP)" March, 19998
URL: http://www.faqs.org/rfcs/rfc2284.html

Types of EAP Authentication Methods

There are many EAP authentication methods that can be used with EAP, however, I will only be concentrating on the more common methods and detailing the advantages and disadvantages of each. The methods that I will discuss are EAP-MD5, EAP-TLS, EAP-TTLS and PEAP.

EAP-MD5

EAP-MD5 is a form of Challenge-Handshake Authentication Protocol. All systems that support the use of EAP must, as a minimum, support the use of the EAP-MD5 authentication method. If the authentication server wishes to use the EAP-MD5 authentication method, this will be indicated by inserting the number 4 in the type field of the EAP request packet.

The actual challenge-handshake for the EAP-MD5 authentication method follows the following guidelines:

1. The user of the mobile unit (supplicant) transmits their user name through the access point (authenticator) to the authentication server in plain text.

2. The authentication server then validates the user name and transmits a challenge to the mobile unit in the form of a plain text message.

3. The mobile unit uses the EAP-MD5 hashing algorithm to formulate a reply using the challenge and the user's password.

4. This reply is then sent through the authenticator to the authentication server who uses the same hashing algorithm and the stored user password to confirm that the required reply has been received. On the basis of the challenge response an EAP success or failure packet is transmitted.

The advantages of the EAP-MD5 authentication method are:

1. It is easy to implement and configure.

2. A unique "fingerprint" is created to digitally sign each packet ensuring that the messages are authentic.

The disadvantages of using the EAP-MD5 authentication method are:

1. Server authentication is not required, leaving the network open to rouge access points being deployed on the network for malicious purposes. This leaves the network available for man-in-the-middle attacks.

2. Because the authentication process occurs using unencrypted packets the user name, challenge and the challenge reply are susceptible to packet sniffing. [15]

3. Although the user password is not actually transmitted when completing the authentication process, the fact that the exchange is not encrypted leaves open the possibility of password cracking.

Due to the security implications associated with the EAP-MD5 authentication method, it is not recommended for wireless networks.

EAP-TLS

EAP-TLS (Transport Layer Security) utilises Public Key Infrastructure (PKI). This EAP authentication method requires both the mobile unit and the authentication server to exchange PKI certificates. The certificate includes the following data:

1. The name of the entity identified by the certificate.

2. The public key of the entity.

3. The name of the certification authority that issued the certificate.

The most important thing to note when using PKI is that all certificates within a network are issued by a trusted certification authority, this authority has certified that there is a valid combination of entity name and public key contained within the certificate. If the authentication server wishes to use the EAP-TLS authentication method, this will be indicated by inserting the number 13 in the type field of the EAP request packet.

EAP-TLS authentication is carried out using the following steps:

1. After association with the access point (authenticator) the mobile unit (supplicant) then sends their identity through the access point to the authentication server.

2. The authentication server validates the identity of the mobile unit and then transmits its PKI certificate.

3. The mobile unit verifies the received PKI certificate and extracts the authentication server's public key. It then generates a secret session key, encrypts it with the extracted public key and transmits it through the access point to the authentication server.

[15] Meador, William, "Port-based authentication with IEEE Standard 802.1x"
URL: http://www.infosecwriters.com/texts.php?op=display&id=208

4. The authentication server decrypts the secret session key using its private key and then sends a message to the mobile unit encrypted with the secret session key to confirm that there now exists a shared secret session key. This key will be used to encrypt and decrypt all traffic transmitted between the mobile unit and the authentication server for the length of the session.[16]

5. The authentication server also requests the PKI certificate of the mobile unit and then verifies the identity of the mobile unit.

The advantages of the EAP-TLS authentication method are:

1. There is mutual authentication for both the mobile unit and the authentication server, eliminating the prospect of authenticating through a rouge access point.

2. The use of session specific secret keys, provides privacy and minimises the effect that eavesdropping has on network traffic. It also overcomes the problem of key distribution that is one of the weaknesses in WEP.

3. Message integrity is maintained with the use of a Message Authentication Code. This is devised using the message content and the session secret key, without knowledge of the session secret key the message can not be amended clandestinely by a third party. If the message is corrupted or modified during transmission, the content of the message will not match the message authentication code and the message will automatically be discarded.[17]

The disadvantages of the EAP-TLS authentication method are:

1. Maintaining a Public Key Infrastructure network is extremely time consuming and complex. The larger the network the greater the workload is with maintaining the PKI network.
2. The mobile units user identity is exposed to sniffing.

EAP-TTLS

EAP-TTLS (Tunnelled Transport Layer Security) builds upon the EAP-TLS authentication method. Like EAP-TLS it uses PKI certificates, however with this method of authentication only the authentication server is required to hold and transmit a valid PKI certificate. If the authentication server wishes to use the EAP-TTLS authentication method, this will be indicated by inserting the number 21 in the type field of the EAP request packet.

[16]Iona Orbix 2000 SSL/TLS Programmers Guide "How TLS provides Security" V 2.0 URL: http://www.iona.com/support/docs/orbix2000/2.0/tls/html/index.html
[17] *Ibid*

EAP-TTLS was proposed by Funk and Certicom, it is their propriety authentication method produced to deal with the administrative overheads of EAP-TLS. The initial authentication process follows steps 1 to 4 of the EAP-TLS authentication process. Once the secure tunnel is in place the mobile unit can be authenticated by the authentication server using any number of other authentication methods. The authentication process supports mutual authentication, however only the authentication server is authenticated using the PKI certificate.

The advantages of EAP-TTLS authentication are:

1. Once the server is authenticated, the mobile unit can be authenticated using legacy password based authentication methods with the exchanges being protected by the secure tunnel.

2. The administration of PKI certificates is greatly reduced due to the fact that only the server is required to hold a valid PKI certificate.

3. A shared secret key is produced for use between the authentication server and the mobile unit and is only known by those two entities for use during that particular session.

The disadvantages of EAP-TTLS authentication are:

1. They are susceptible to man-in-the-middle attacks by rouge EAP-TTLS authentication servers.

2. The EAP-TTLS server certificate can be subject to compromise. However this can only have an effect if the server's private key is also known.[18]

PEAP

PEAP (Protected EAP) is similar to EAP-TTLS, in that it also utilises PKI for server authentication while offering a variety of authentication methods to the mobile unit. If the authentication server wishes to use the PEAP authentication method, this will be indicated by inserting the number 25 in the type field of the EAP request packet.

PEAP is very similar to EAP-TTLS in the protection that it provides wireless network users. PEAP was developed by Microsoft, CISCO and RSA Security, in truth it could be referred to as their propriety version of EAP-TTLS. Like EAP-TTLS it provides mutual authentication, client identity protection and key generation. Like EAP-TTLS the PEAP authentication is carried out in two phases, the initial phase where the PKI certificate of the server is exchanged

[18]Funk, Paul "EAP Tunnelled TLS Authentication Protocol (EAP-TTLS)" November, 2002 URL: http://www.watersprings.org/pub/id/draft-ietf-pppext-eap-ttls-02.txt

and the second phase where the client is authenticated within the secure tunnel using an EAP authentication method.

The advantages and disadvantages of PEAP are similar to those of EAP-TTLS. The one disadvantage that PEAP has over EAP-TTLS is that user authentication must be carried out using a form of EAP authentication. Unlike EAP-TTLS which also supports a wide variety of legacy authentication methods.

One of the main things that should be looked at when designing a network is that the methods used for network authentication are widely available and used. The disadvantage of using a propriety based authentication method is that not all companies will support the use and implementation of that particular method. The PEAP authentication method at first was restricted to use with Microsoft products, however PEAP is now widely supported by Cisco, Funk, Interlink Networks and Meetinghouse, to name a few of the support vendors.[19]

802.1x Considerations

One of the most important things to remember about the 802.1x standard is that it provides the standard for port based authentication; it does not provide the actual authentication mechanism. While some of the more common methods of EAP authentication have been described in this paper, there are many others that have not been touched on. It is important that when choosing the method of EAP authentication that will be used on your network, you take into account the equipment used on the network. Some methods of EAP authentication methods have been developed by companies from within the industry and as such may not be compatible with the equipment provided by all manufacturers.

Although there are disadvantages with many of the EAP authentication methods, the 802.1x standard goes a long way to improving the problems that have been experienced on wireless networks. The major benefit of 802.1x is that it provides network administrators with a method of key distribution. This means that, depending of which EAP authentication method is used, the capability exists for each session to have a unique session key and this solves the problem of static WEP keys.

The confidentiality, integrity and authentication problems associated with WEP are partially addressed by the possible use of encrypted tunnels and by the use of two way authentication and the use of server PKI certificates. The 802.1x standard has been incorporated into both the Wi-Fi Protected Access and the 802.11i specifications.

[19] Mircosoft.com, "The Advantages of Protected Extensible Authentication Protocol (PEAP)" July 6, 2004
URL: http://www.microsoft.com/windowsserver2003/techinfo/overview/peap.mspx

Wi-Fi Protected Access

Wi-Fi Protected Access (WPA) is the interim industry response to the wireless networking problems. Announced in October 2002, it was created as a subset of the then draft 802.11i standard. The main purpose for implementing the WPA specification was that a solution for the WEP problems needed to be available to wireless network users in the short term and the time frame for the approval of the 802.11i specification looked to be a long way in the future. It was designed to be both backward compatible with the existing 802.11 wireless networking products and also forward compatible with the 802.11i specification.

WPA looked at the 802.11i draft and implemented a version that utilised the more stable elements available at the time. With regards to the elements of WPA that increase the security of the wireless network, WPA uses the 802.1x standard which allows for key management and authentication and it also brings to the wireless network users a data privacy protocol called the Temporal Key Integrity Protocol (TKIP) which will be discussed in further detail below.

TKIP

TKIP is seen as an interim security measure and was required to be implemented in order to assist in the provision of wireless network security until the 802.11i standard was officially endorsed and available for use to wireless network clients.[20] In order for it to be backward compatible to all other wireless network equipment currently in use it was necessary for it to be implemented using the RC4 cryptographic algorithm. This is the algorithm that is used by WEP and the equipment that currently use WEP would require only a software or firmware upgrade to be able to utilise TKIP. This meant that the wireless network users did not have to outlay a large amount of money for an interim security measure. It offers the wireless network administrator three new features that are used as a package to counter the main problems associated with WEP. A brief outline of each of these features is described below.

1. The first feature of TKIP to be discussed is the Message Integrity Code (MIC). TKIP uses a 64 bit cryptographic MIC called Michael. This replaces the 32 bit Cyclic Redundancy Check (CRC) associated with WEP, it enables the prevention of forged data packets and assists in ensuring the integrity of data packets transmitted on the network. Michael is transmitted as a keyed hash, making it cryptographically secure, which is a major improvement on the CRC of WEP.

   If a station receives a data packet which it cannot verify the integrity of and believes that it may have been forged, it will discard the

[20] Kawamoto, Wayne. "Encrypting for the Future" August 9, 2002
URL: http://www.wi-fiplanet.com/columns/article.php/1443911

packet. If a station detects two failed forgeries within one minute, then it assumes that it is under active attack and initiates counter measure actions. It will immediately delete keys established at the beginning of the session and disassociate itself from the wireless network. After one minute it will then reassociate with the network and establish new session keys.[21] It should be noted that while this effectively protects the traffic that is transmitted over the network, it also makes the network extremely susceptible to denial of service attacks. This in the long run could have the possibility of major disruptions to the wireless network.

2. TKIP introduces the concept of a per-packet key. This means that no two packets should be encrypted using the same key. To do this it begins with a 128-bit temporal key, which is shared between the mobile units and the access points. The temporal key has a fixed lifetime and is changed every 10000 packets. It takes the temporal key and combines it with the MAC address of the unit and then it adds a 48-bit Initialisation Vector. This produces the key stream that will be used by that unit to encrypt any packets it transmits. By producing the key in this fashion, it ensures that no matter how many units have access to the temporal key, there will always be a different key stream used to encrypt packets transmitted from different units. It also provides protection for the packet IV by encrypting the IV prior to transmission.

The per-packet key method implemented by TKIP protects the data packets in two phases. First it removes the possibility of the same key stream being used by different units by using the units MAC address as part of the key stream. Then second it encrypts the IV of each packet which means that it becomes more difficult for an attacker to relate packet IVs and per-packet keys.

3. In order to counter the problem of traffic being captured by an attacker and then replayed on the network, TKIP introduces IV sequencing. Each time the temporal key is changed the units IV number is reset to zero. It then increments this by one for each message that is transmitted from the unit. In effect the IV also acts as a packet sequence number. The receiver is required to keep note of the IVs of the packets that it receives from a unit and if it receives a packet that is lower than or equal to the IV of a packet that has already been received, then it will treat the packet as a replayed packet and will discard the packet.[22]

As illustrated above the use of TKIP and the 802.1x standard within Wi-Fi Protected Access greatly improves security to the wireless network. It counters most of the main problems associated with WEP such as the re-use

[21] Trapeze networks, "Enterprise Wireless LAN Security: Making Sense of the Options" http://trapezenetworks.com/technology/whitepapers/WLANsecurity3.asp

[22] Leira, Jardar. "TKIP" URL: http://www.uninett.no/wlan/tkip_mic.html

of IVs, the distribution and rotation of static keys, the ease with which mobile units and access points can be forged, and the method with which the integrity of the message is proved. The main thing that WPA does not address is the RC4 stream cipher itself, although it uses a much more robust implementation of RC4 than WEP, the fact that the RC4 cipher stream is considered to be broken, means that the use of TKIP can only be seen as an interim measure.

802.11i

A full implementation of the 802.11i standard is called a Robust Security Network (RSN). While RSN still supports TKIP encryption in order to maintain compatibility with legacy hardware and uses the 802.1x port authentication standard to authenticate wireless network entities and to provide for dynamic session keys, it also introduces two new encryption protocols to the wireless network administrator. These are:

1. Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), which is a mandatory for all 802.11i implementations; and

2. Wireless Robust Authentication Protocol (WRAP), which is optional for 802.11i implementations.

An important feature of both of these new encryption protocols is the fact that there is a move away from the RC4 cryptographic algorithm to the Advanced Encryption Standard (AES). AES, CCMP and WRAP will be discussed in further detail below.

Advanced Encryption Standard

AES is a symmetric key block cipher, which means that it encrypts data in fixed-sized blocks. While the 802.11i standard is a 128-bit block, AES is also capable of encrypting 192-bit and 256-bit blocks. AES uses an encryption algorithm known as Rijndael, which is capable of having a key-size of 128-bits, 192-bits or 256-bits, however as per the block size the 802.11i standard is a key-size of 128-bits.[23] AES is the U.S. governments approved successor to the Data Encryption Standard (DES) and is defined in Federal Information Processing Standard (FIPS) Number 197 dated 2001, as the U.S. federal government approved encryption algorithm.

Rijndael was chosen as the encryption algorithm for AES as a result of a "contest-like" selection process. The National Institute of Science and Technology (NIST), on behalf of the National Security Agency (NSA), invited candidates from the public and academic sectors to submit algorithms which could be used with AES. After receiving and evaluating twenty-one responses, Rijndael, devised by Joan Daemen and Vicent Rijmen was selected.[24]

[23] "The Advanced Encryption Standard (Rijndael)"
URL: http://home.ecn.ab.ca/~jsavard/crypto/co040401.htm
[24] "Advanced Encryption Standard (AES)" Updated October 26, 2004 URL:
http://www.informit.com/guides/content.asp?g=security&seqNum=65

The National Institute of Science and Technology compares AES to DES in the following fashion:

> "If you could build a machine that could recover a DES key in a second, it would take that machine 149 trillion years to crack a 128-bit AES key."[25]

AES is currently one of the strongest encryptions available for use in a non-military application.

The major disadvantage associated with the use of AES is the fact that it will require upgrades to the network equipment. Existing wireless networks may choose to go with WPA due to the fact that it is backward compatible and there are fewer associated costs.

CCMP

CCMP uses a 128-bit key, with a 48-bit initialisation vector (IV). It was designed by N. Ferguson, R. Housley and D. Whiting and is based upon the CCM mode of the AES algorithm. CCMP uses a combined authentication and encryption mode to provide privacy and authentication. The Counter Mode (CTR) component of CCMP is the algorithm that provides data privacy, while the Cipher Block Chaining Message Authentication Code (CBC-MAC) component of CCMP provides data integrity and authentication.

In order for the AES-CCM protocol to function correctly it requires the presence of two different variables. The first is an AES key, which is used both to encrypt the packet and to compute the Message Integrity Code (MIC). The second is a 48-bit packet sequence counter, which is used to construct both the counter mode encryption counter and the CBC-MAC IV.

A CCMP implementation provides a secure network in the following ways:

1. The MIC check ensures that forged packets are not able to be inserted into the network, the MIC also protects the source and destination addresses from modification;

2. The packet sequence check prevents the possibility of replay traffic; and

3. AES-CCM never reuses a counter value or an IV with the same key.[26]

---

[25] Trapeze networks, "Enterprise Wireless LAN Security: Making Sense of the Options" http://trapezenetworks.com/technology/whitepapers/WLANsecurity3.asp

[26] Walker, Jessie. "Part III: AES-based Encapsulations of 802.11 Data" URL: http://cache-www.intel.com/cd/00/00/01/77/17770_80211_part3.pdf

The disadvantage of using CCMP is the fact that it requires to different operations to be performed in order to provide privacy and authentication. This increases significantly the time and processing resources required to carry out the encryptions process. However an advantage of CCMP is the fact that its authors have released any intellectual property rights to CCM to the public domain, which means that there are no licensing or propriety overheads with its use.

WRAP

WRAP is the optional encryption protocol used in 802.11i implementations and like CCMP it uses a 128-bit key. Also like CCMP, WRAP uses AES encryption however instead of using AES-CCM mode it uses the AES-OCB (Offset code book) mode. AES-OCB provides both privacy and authentication and as such it is termed an authenticated-encryption scheme.

Similar to AES-CCM, the AES-OCB protocol also requires the presence of two different variables to function correctly. The first is an AES key, used to encrypt and decrypt data and the second is a 28-bit packet sequence counter used to construct the nonce. The nonce is a 128-bit number which AES-OCB uses instead of requiring a random IV. The nonce is constructed using a joining of the source and destination MAC addresses, the quality of service traffic class and the packet sequence number. The nonce protects all the elements used to construct it from modification and forgery. As the nonce is constructed using the packet sequence number, the nonce value should never be used more than once with each AES key.

AES-OCB mode operates by augmenting the normal encryption process with the incorporation of an offset value. The nonce is used to produce the offset, first it is subject to the XOR function, the output of which is then encrypted using the AES key, this results in the offset value. AES-OCB also includes a MIC function, however it is calculated using the same function as the encryption, which minimises processing time and resource usage.[27]

The major disadvantage with WRAP is the fact that already three different entities have already applied for patents claiming intellectual property rights, this means that there are additional overheads and uncertainties associated with its use.

Conclusion

It is easy to see the benefits that a full implementation of the 802.11i standard will give to the security of a wireless network. The 802.11i standard overcomes all the problems associated with WEP, and provides the

[27]Cisco Systems. "Wireless LAN Security Solution"
URL:http://www.cisco.com/en/US/netsol/ns339/ns395/ns176/ns178/networking_solutions_white_paper09186a00800b469f.shtml

confidentiality, authentication and integrity that is required for a secure network. While of wireless network security has had many critics in the past, it has come a long way since WEP and is now capable of providing a fully secure network.

While the approval of the 802.11i standard was a long time coming, it is important to note that security standards, like that of security practices and policies in the workplace, should not be rushed. Unless, of course, you are prepared to start the task again, soon after the initial approval, in order to address areas that may have been overlooked in the initial planning stages of the implementation.

I believe that the security provided by the 802.11i standard will not only entice many new users to wireless networking but it may also entice back users who have been disillusioned with wireless networking due to the lack of adequate security.

If a wireless network is administered as a Robust Secure Network it will finally have the confidentiality, authentication and integrity that wired networks have been enjoying for many years. The essential thing for the network administrator and security personnel to remember is that nothing is forever, so the wireless network must be up to date with the current security standards.

References

"Advanced Encryption Standard (AES)" Updated October 26, 2004
URL: http://www.informit.com/guides/content.asp?g=security&seqNum=65

Borisov, Nikita. Goldberg, Ian. Wagner, David. "Intercepting Mobile Communications: The Insecurity of 802.11"
URL: http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf

Borisov, Nikita. Goldberg, Ian. Wagner, David. "Security of the WEP algorithm". February 02, 2001. URL:
http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

Cisco Systems. "Wireless LAN Security Solution"
URL:http://www.cisco.com/en/US/netsol/ns339/ns395/ns176/ns178/networking_solutions_white_paper09186a00800b469f.shtml

Dubrawsky, Ido. "Wireless (In) Security" April 2002
URL: http://www.unixreview.com/documents/s=2427/uni1020280760693/

Fluhrer, Scott. Mantin, Itsik. Shamir, Adi. "Weaknesses in the Key Scheduling Algorithm of RC4"
URL: http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf

Funk, Paul "EAP Tunnelled TLS Authentication Protocol (EAP-TTLS)" November, 2002
URL: http://www.watersprings.org/pub/id/draft-ietf-pppext-eap-ttls-02.txt

Gast, Matthew. "802.11 Wireless Networks: The Definitive Guide" (Sebastopol CA, 2002) p. xi

IEEE Std 802.1X-2001 "IEEE Standard for Local and metropolitan area networks – Port-Based Network Access Control"
URL: http://www.ieee802.org/1/pages/802.1x.html

Iona Orbix 2000 SSL/TLS Programmers Guide "How TLS provides Security" V 2.0 URL: http://www.iona.com/support/docs/orbix2000/2.0/tls/html/index.html

Kawamoto, Wayne. "Encrypting for the Future" August 9, 2002
URL: http://www.wi-fiplanet.com/columns/article.php/1443911

Leira, Jardar. "TKIP"
URL: http://www.uninett.no/wlan/tkip_mic.html

Meador, William, "Port-based authentication with IEEE Standard 802.1x"
URL: http://www.infosecwriters.com/texts.php?op=display&id=208

Mircosoft.com, “The Advantages of Protected Extensible Authentication Protocol (PEAP)” July 6, 2004
URL:
http://www.microsoft.com/windowsserver2003/techinfo/overview/peap.mspx

Ou, George. “At last, real wireless LAN security. Introducing 802.1x and EAP” September 3, 2002 URL:
http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2878940-2,00.html

Phifer, Lisa. “802.1x Port Access Control for WLANs” September 5, 2003
URL: http://www.wi-fiplanet.com/tutorials/article.php/3073201

“RFC 2284-PPP Extensible Authentication Protocol (EAP)” March, 19998
URL: http://www.faqs.org/rfcs/rfc2284.html

“The Advanced Encryption Standard (Rijndael)”
URL: http://home.ecn.ab.ca/~jsavard/crypto/co040401.htm

Trapeze networks, “Enterprise Wireless LAN Security: Making Sense of the Options”
http://trapezenetworks.com/technology/whitepapers/WLANsecurity3.asp

Walker, Jessie. “Part III: AES-based Encapsulations of 802.11 Data”
URL: http://cache-www.intel.com/cd/00/00/01/77/17770_80211_part3.pdf