Global Information Assurance Certification Paper

Securing Wireless LANs
With
802.1x and EAP authentication

GIAC Security Essential Certification (GSEC)
Version 1.4c August 2004
Option 1

Submitted by

Ahmad Davari-nejad
November 15, 2004

Abstract

Wireless networks are widely used both at homes and in business environments. The security risks associated with these networks are a major concern especially in the corporate networks. There are different types of wireless networks and protocols in use such as Wireless Application Protocol (WAP), Bluetooth, Blackberry and 802.11. The focus of this paper is on security issues related to IEEE 802.11 wireless standard in an infrastructure architecture. Wireless LAN security has drastically improved in recent years and there are many different methods available to effectively secure such networks.

This paper will give a brief overview of IEEE 802.11 wireless networks and the general risk categories associated with them. WEP and its weaknesses will be discussed along with WPA and 802.11i standard. The focus of this paper however, will be on discussing 802.1x and EAP protocols and how they secure wireless networks. Different EAP methods will be explained along with their strength and weaknesses. In conclusion, wireless security is put in perspective in relation to a broader security program.

Wireless LAN

Wireless networks that are based on IEEE 802.11 standard are relatively easy to implement and are low cost compared to wired networks. These networks provide convenience for users and allow them to be more productive by not being restricted to a physical location. Users can move from one conference room to the another and still be able to connect to the network without worrying about being wired. Wireless networks are ideal for locations that can not accommodate new wiring requirements.

The IEEE 802.11 extension was ratified in 1997 and supported data rates of 1 or 2 Mbps operating at 2.4 GHz. In 1999, 802.11b and 802.11a extensions were ratified to offer higher data transmission rates of 11 Mbps and 54 Mbps respectively. These wireless standards were to enhance and complement the wired networks rather than replacing them. The complete documentation for 802.11 standards can be obtained from IEEE's web site by clicking on the following link, choosing a standard, selecting a user type and accepting the terms: http://standards.ieee.org/getieee802/802.11.html

Wireless networks are inherently insecure because the data is transmitted over radio air waves rather than wires. The physical security that could be imposed on wired networks is almost impossible to enforce with regards to WLANs. Radio waves travel well beyond the intended physical perimeters of the work place making it harder to secure.

According to a technical white paper by Internet Security Systems (ISS), "Wireless LAN Security – 802.11b and Corporate Networks", most of the risks to 802.11 wireless networks fall in these basic categories:

- Insertion attacks
- Eavesdropping
- Denial of Service attacks
- Encryption attacks

Insertion attacks are related to placing an unauthorized Access Point on the network. This could be done by either an uninformed employee that is not aware of the risks or by a person trying to do harm.

Eavesdropping refers to the fact that wireless signals can be sniffed by unauthorized persons and confidential information could be compromised. High gain directional antennas can be used to sniff the traffic from far away.

Denial of service attacks can happen to wireless networks much like the wired networks. An attacker with the right equipment can jam the wireless signal making it unavailable for use.

Encryption attacks are attempts to capture the encryption key. WEP is especially vulnerable to these types of attacks.

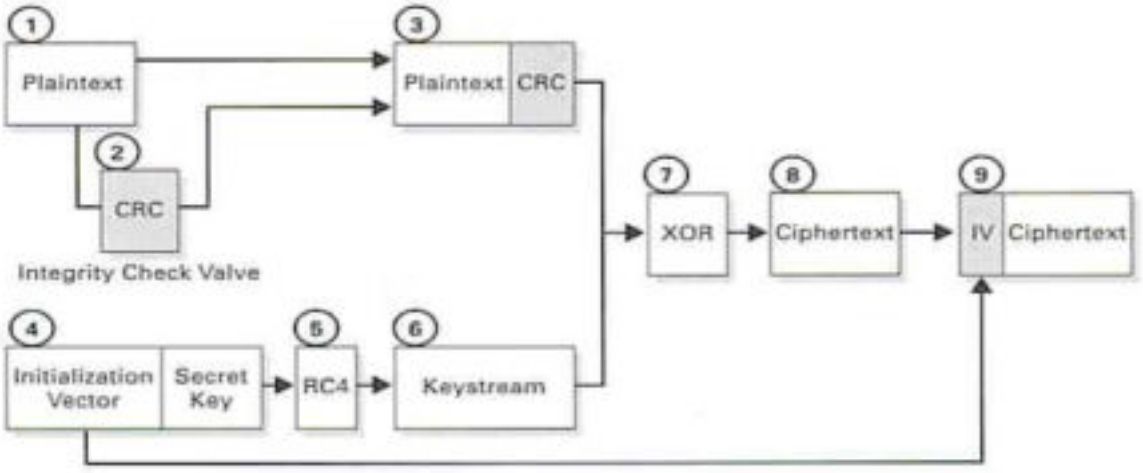
WEP

The 802.11 standard for wireless networks included an encryption method known as Wired Equivalent Privacy (WEP), to protect link-layer communications from eavesdropping. WEP was intended to provide the same level of security as the traditional wired LANs and it was not meant to resolve all security issues related to wireless networks. At first, the main problem with WEP was that the encryption key (shared secret) had to be known and used by all clients connecting to the wireless network. The static WEP key was used for authenticating users and encrypting the communication between the clients and the access points. If for any reason this key was compromised, the new key had to manually be entered into all clients and APs participating in the wireless network. This may have not been a big problem in a small office environment, however, in an enterprise network with hundreds, or perhaps, thousands of users this was an impractical task. The WEP protocol did not provide any mechanism for implementation of a dynamic key generation and distribution.

Soon after, a major vulnerability with WEP was identified that would potentially allow attackers to capture the WEP Key. This was first documented in a paper titled "Weaknesses in the Key Scheduling Algorithm of RC4" by Scott Fluhrer, Itsik Mantin, and Adi Shamir.

WEP uses the RC4 Stream Cipher from RSA which is also widely used for secure communications on the World Wide Web (Secure Socket Layer, SSL). Two key sizes are used: 40 bit and 104 bit and a 24 bit key called Initialization Vector (IV) is added to each that is transmitted in clear text.

The diagram below from a book by Lee Barken called; "How Secure Is Your Wireless Network?" demonstrates the encryption process:



The WEP vulnerability is related to how RC4 cipher is implemented. An attacker can exploit a weakly constructed IV to capture the WEP key. AirSnort and WEPCrack are two software tools that could recover WEP keys.

802.11i and WPA

With the shortcomings associated with WEP, IEEE 802.11i Task Group started the work on developing a replacement. In October 2002, the Wi-Fi Alliance announced Wi-Fi Protected Access (WPA), essentially a subset of the 802.11i specification. An article in the Network World Fusion, "What's in WPA?" by Joanie Wexler, identifies the following components that are included in WPA and 802.11i:

- 802.1x authentication framework
- AP-to-client communications security
- Key management
- Temporal Key Integrity Protocol (TKIP)
- A new cipher (AES)

There are three main elements of TKIP for enhancing encryption (Barken):

- A per-packet key mixing function
- An improved Message Integrity Code
- An enhanced Initialization Vector

AES is the encryption engine to replace RC4 and is compliant with the Federal Information Processing Standards (FIPS). AES is a much stronger encryption and as a result it required new hardware which made it not to be backward compatible. AES, much like TKIP, uses a 48 bit IV. Unlike TKIP, AES is mandatory in 802.11i specification.

EAP Authentication

Extensible Authentication Protocol, EAP, was developed out of necessity. Most enterprises wanted to be able to use stronger authentication methods than just user IDs and passwords. EAP is an authentication protocol that supports multiple authentication mechanism such as MD5, One-Time Passwords, LEAP, PEAP, TLS, TTLS and others. While EAP was originally developed for use with Point to Point Protocol (PPP), it is also in use with IEEE 802. EAP simplifies the interoperability and compatibility of authentication methods and it is a critical framework for the security of wireless networks.

802.1x

The IEEE 802.1x standard was originally designed for wired networks to provide port-level (layer 1) access control. 802.1x is a framework that defines network access control based on a client server model and authentication in which only authorized access to the LAN is granted through the physical ports.

With port-based authentication, even if an intruder by-pass the site security and gain access to a network port, the intruder still has to be authenticated before the access is granted. 802.1x can also be used to greatly enhance the security of wireless networks by enabling port-based authentication as well as dynamically varying the encryption key.

802.1x is a carrier of EAP messages. One can think of the 802.1x as a protocol for communicating EAP over wired or wireless networks.(Barken)

There are three basic components related to 802.1x protocol:
- Supplicant (Client)
- Authenticator (Access Point)
- Authentication Server (RADIUS)

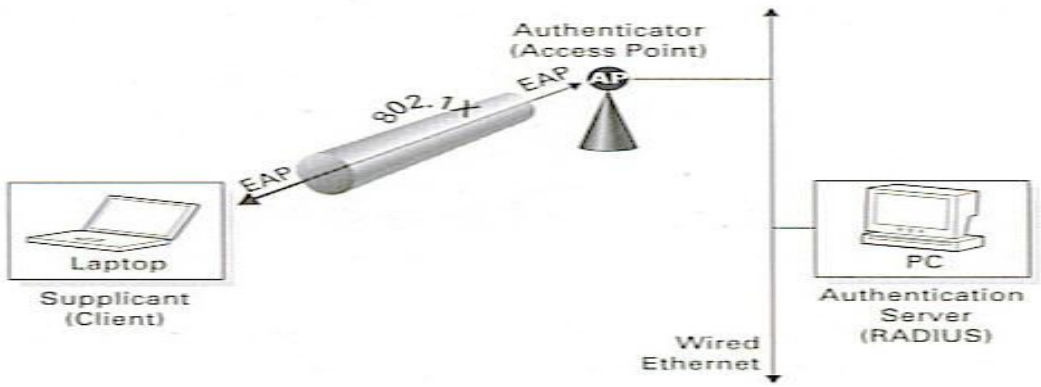


Diagram from “How Secure is your Wireless Network?” by Lee Barken.

Supplicant is the entity that is seeking access to the network. This could be a client or a standalone device such as an IP phone or a network device.

Authenticator is the device to which the supplicant directly connects. Supplicant receives connection permissions through the Authenticator. Authenticator is like a Traffic controller, if you are not authenticated, none of your traffic can go through except for 802.1x traffic. Two virtual ports are used: control port and uncontrolled port. Uncontrolled port is only used for communication between the Authenticator and the Authentication server. The controlled port is like a switch that is in off position. After the client is authenticated, the switch is turned on and traffic can flow through. In a WLAN environment, Access Point is the Authenticator.

Authentication Server is a device that manages authentication information. The authentication server authenticates each client connected to the Authenticator before making available any services offered by the LAN. Authentication Server is usually a RADIUS server. Most RADIUS servers are also capable of passing the authentication requests to a backend source such as NT domain, LDAP or Active Directory.

The following exchange takes place for each client authentication:

1. The client sends an EAP start message to the AP.
2. The AP replies to the client by an EAP Request/Identity message.
3. The client responds to the AP by identifying itself with an EAP Request/Identity message. The AP forwards this message to the RADIUS.
4. RADIUS then sends a challenge back to AP by an EAP Request. This could be a request for credentials such as a password or a certificate, depending on the EAP type. The AP forwards the challenge to the client.
5. The client responds back to AP with a challenge response. The AP forwards the response to the RADIUS.

6. The RADIUS sends an EAP-Success to the AP if the challenge response was okay. The AP then allows the client to connect to the network through the controlled port.

All the communications between the client and RADIUS must go through the AP. The Supplicant and Authenticator communicate by using EAP. The 802.1x defined an encapsulation method for sending EAP packets over Ethernet frames. This method is called EAP over LAN (EAPOL). For this to work correctly, all three components (Supplicant, Authenticator and Authentication Server) must be 802.1x compliant. ("What is 802.1x?" by Joel Snider)

The key regeneration and distribution functionality of 802.1x is especially important to 802.11 wireless networks. One of the main problems with WEP was the fact that the key was static and had to be hard coded in every client and AP. 802.1x provides a key management system that allows the key to be regenerated frequently (per session or per user). Therefore, even if enough packets are captured to compromise the key, it is only for that session.

To sum up, 802.1x allows for user authentication, authorization and accounting. It also, enables us to change the encryption key frequently and it has mechanism for key distribution. Finally, 802.1x allows for enhanced authentication methods beyond just ID and password.

EAP Methods

802.1x and EAP are frameworks for how a session takes place for a secure authentication. There are many different EAP authentication methods available today. For EAP to work, all three components of 802.1x (Supplicant, Authenticator and Authenticating Server) must support the chosen EAP. Some EAP methods are more secure but harder to implement and visa versa. The following are brief descriptions of selected EAP methods and their strength and weaknesses.

EAP-MD5

MD5 was originally used with PPP to authenticate the dial-up users. It is the weakest of all EAP types and it is identical to CHAP. Mutual authentication between client and server is not performed. Only a one way authentication is performed to authenticate the client with ID and password. MD5 is relatively easy to implement. It is vulnerable to password related attacks such as brute force and dictionary attacks. Since mutual authentication is not done, it is also vulnerable to Man-in-the-Middle attack. EAP MD5 does not support dynamic WEP key generation and it should not be used in production environments. (Barken)

LEAP

Lightweight EAP is a Cisco proprietary protocol. Although based on 802.1x, LEAP was Cisco's pre 802.1x attempt to put forward an interim solution to mitigate the risks associated with WEP. In order to implement LEAP, the network card (NIC), Access Point and the RADIUS server must all be Cisco brand. LEAP supports mutual authentication based on a shared secret (user password). Client authentication is done by user ID and password. LEAP supports dynamic key generation per session and per user. LEAP is also vulnerable to password related attacks such as dictionary attack. An article, in ComputerWorld by Bob Brewin, "Cisco releases WLAN security protocol", describes the vulnerability. As stated in the article, a tool called asleap developed by Joshua Wright with SANS Institute in Bethesda, Md., exploits this vulnerability. Here is the link to the tool: http://asleap.sourceforge.net/. Cisco has acknowledged this weakness and released a "patch" to fix the problem. The "patch" is a new protocol called EAP-Flexible Authentication via Secure Tunneling (EAP-FAST). Here is the link to "Cisco Security Notice: Dictionary Attack on Cisco LEAP Vulnerability": http://www.cisco.com/warp/public/707/cisco-sn-20030802-leap.shtml#revision

EAP-TLS

Tunneled Layer Security (TLS) creates an end to end (Supplicant to Authentication Server) encrypted tunnel before user credentials are exchanged. EAP-TLS is based on mutual authentication. Both the client and the server must use valid digital certificates for authentication. The certificates must be X509 compliant. A Public Key Infrastructure (PKI) must be in-place to manage the certificates. EAP-TLS also supports dynamic key generation and distribution. EAP-TLS is not vulnerable to Man-in-the-Middle, eavesdropping, session hijacking, dictionary and encryption attacks. Currently, it provides the strongest security possible. However, if a PKI is not already in-place, it is hard to implement and is costly.

EAP-TTLS

Tunneled Transport Layer Security (TTLS) is an extension of EAP-TLS developed by Funk Software and Cirticom. EAP-TTLS establishes an encrypted TLS tunnel between the client and server for a secure transport of authentication data. Once the tunnel is established, other authentication methods can be used such as PAP, Chap, MS-Chapv2 or other EAP types. EAP-TTLS supports mutual authentication. The server is authenticated with a digital certificate and the client is authenticated using user name and password. EAP-TTLS is not vulnerable to Man-in-the-Middle, eavesdropping, session hijacking, dictionary and encryption attacks. There is no native operating system support for EAP-TTLS. Additional software must be installed on all clients. EAP-TTLS is nearly as secure as EAP-TLS but it is relatively easier to implement (PKI is not necessary).

PEAP

Protected EAP is an IETF draft backed by Microsoft, Cisco and RSA. It is very identical to EAP-TTLS. Mutual authentication takes place between the client and server. The server must authenticate with a digital certificate and the client can use ID and password. Client's credential is passed after a secure TLS tunnel is created between the client and the server. Therefore, other EAP types can be used. Because of the mutual authentication, PEAP is not vulnerable to Man-in-the-Middle attack. Also, PEAP is not vulnerable to Session hijacking, eavesdropping, dictionary and encryption attacks. PEAP is nearly as secure as EAP-TLS. It is supported natively on Windows XP with SP1 and does not require additional software.

Conclusion

From a security standpoint, any one of these three methods, EAP-TLS, EAP-TTLS and PEAP, could provide for a secure implementation of an 802.11 wireless network.

Although a secure implementation of an enterprise wireless network is absolutely essential, it must be part of a broader security program. To be more effective, security must be applied in layers. A robust security program will include the following elements:

- Policies, Standards and Procedures.
- Secure perimeters
- Access control
- Vulnerability assessment
- Intrusion detection and incident handling
- Education
- Penetration testing

Here is how these elements apply to WLANs:
A clear Policy must be in place to state the role of the IT organization in implementation of enterprise wireless networks. To ensure proper configuration and secure implementation, it should clearly be stated that the IT organization is responsible for implementation and installation of the corporate WLAN. The Policy must also address the connection of unauthorized wireless access points/bridges to the corporate network. A usage Policy is needed on the types of wireless devices allowed (Laptops, PDA, Blackberries, etc.) by the users. These Policies must effectively be communicated to the user community to educate them on potential risks and make them aware of the consequences.

Network perimeter security is the first line of defense against the big bad "enemy" from outside (the Web). This is the main point of entry to the network. A good bit of IT resources are dedicated to ensure a secure perimeter. These may include

border routers, firewalls, DMZs and intrusion detection sensors. However, an unauthorized Access Point connected to the corporate network can potentially undo all the security measures that IT had put in-place. Therefore, we must consider the security of wireless Access Points as part of our perimeter security and dedicate sufficient resources to maintain a secure environment.

Access control can be achieved by implementing a wireless security based on 802.1x and a strong EAP (EAP-TLS, EAP-TTLS or PEAP) implementation. Users must be authenticated through a back-end server (RADIUS) before they are allowed to connect to the network. Authorization and accounting should also be implemented. Both EAP-TTLS and PEAP clients use ID and password to authenticate to the RADIUS server or a backend database such as NT domain, LDAP and Active Directory. Therefore, strong password policies must be implemented along with account lock-outs for invalid logons.

Vulnerability assessment ensures that all Access Points and Authentication Servers are configured properly and all known vulnerabilities are patched promptly.

Intrusion detection is even more critical with the presence of enterprise wireless network. Intrusion detection should include positioning of wireless sensors for detection of unauthorized/rogue APs. This could potentially be very costly depending on the size of the area that needs to be monitored. Also, a systematic "war-driving" should be conducted to identify and remove rogue APs. Although, "war-driving" could be very inefficient and time consuming specially in a dispersed environment, it is an important activity that should be performed.

Education must be an integral part of any security program. It is a proactive measure that if done properly and frequently, it could save the IT security professionals a lot of time and resources. Creative measures must be adopted to inform users of potential risks associated with connecting unauthorized access points to the corporate network. Also, technical help and instruction should be available to remote users to securely configure home wireless LANs. These users remotely connect to the corporate network and therefore become an extension of it. It is important to educate users on security issues related to home and public (airports, hotels, etc.) wireless networks.

Wireless penetration testing and vulnerability assessment should be performed by an outside source on an annual basis. These independent tests could identify vulnerabilities within the enterprise wireless network that would otherwise go unnoticed. These exercises could also be a great source of knowledge transfer for the IT security personnel to become familiar with the latest techniques.

Wireless networks are a fact of life. Since we can no longer fight them, we might as well secure them.

References

IEEE Standards Association, IEEE 802.11 LAN MAN Wireless LANS. URL: http://standards.ieee.org/getieee802/802.11.html

Fluhrer, Scott; Mantin, Itsik; Shamir, Adi. "Weaknesses in the Key Scheduling Algorithm of RC4". URL: http://www.crypto.com/papers/others/rc4_ksaproc.pdf

RSA Security. "What is RC4 Stream Cipher?" URL: http://www.rsasecurity.com/rsalabs/node.asp?id=2250

Lee Barken. "How Secure Is Your Wireless Network?: safeguarding your Wi-Fi LAN". Prentice Hall PTR. 2004

Internet Security Systems. A Technical White Paper. "Wireless LAN Security – 802.11b and Corporate Networks". URL: http://documents.iss.net/whitepapers/wireless_LAN_security.pdf

Wexler, Joanie. Network World Fusion. "What's in WPA?", URL: http://www.nwfusion.com/newsletters/wireless/2002/01626699.html

Extensible Authentication Protocol, EAP. URL: http://www.faqs.org/rfcs/rfc2284.html

Extensible Authentication Protocol. URL: http://www.ietf.org/rfc/rfc2284.txt?number=2284

Snider, Joel. Network World Fusion. "What is 802.1x?", URL: http://www.nwfusion.com/research/2002/0506whatisit.html

Brewin, Bob. ComputerWorld, "Cisco releases WLAN security protocol"(http://www.computerworld.com/mobiletopics/mobile/story/0,10801,92203,00.html?f=x68)

A hacker tool by Josh Wright. Asleap. URL: http://asleap.sourceforge.net/

Cisco Systems. "Cisco Security Notice: Dictionary Attack on Cisco LEAP Vulnerability": URL: http://www.cisco.com/warp/public/707/cisco-sn-20030802-leap.shtml#revision

EAP-TLS, an IETF draft. URL: http://www.ietf.org/rfc/rfc2716.txt

EAP-TTLS, an IETF draft. URL: http://www.ietf.org/rfc/rfc2026.txt

PEAP, an IETF draft. URL: http://www.ietf.org/internet-drafts/draft-josefsson-pppext-eap-tls-eap-10.txt