Wireless LAN Security using Interlink Networks RAD-Series AAA Server and Cisco EAP-LEAP

Abstract

Wireless LANs based on 802.11 technology present unique network security concerns. This is due to their susceptibility to eavesdropping by people and devices within radio frequency range of wireless users and access points. Interlink Networks has implemented Cisco Systems' Lightweight Extensible Authentication Protocol (LEAP) on the RAD-Series authentication, authorization and accounting (AAA) RADIUS servers in order to provide a higher level of security for the wireless LAN user.

© 2002 Interlink Networks, Inc.
All Rights Reserved.

This document is copyrighted by Interlink Networks Incorporated (Interlink Networks). The information contained within this document is subject to change without notice. Interlink Networks does not guarantee the accuracy of the information.

Trademark Information

Brand or product names may be registered trademarks of their respective owners.

Interlink Networks, Inc.

775 Technology Drive, Suite 200
Ann Arbor, MI 48108 USA
Phone: 734-821-1200
Sales: 734-821-1228
Fax: 734-821-1235
info@interlinknetworks.com
sales@interlinknetworks.com
www.interlinknetworks.com

INTRODUCTION

The approval of the IEEE 802.11 standard for wireless local area networks (WLANs) and the subsequent fall in prices for wireless network interface cards (NICs) and wireless access points (APs) has caused an explosion in demand for wireless LAN capability. Because of this demand, network administrators have had to deal with two conflicting issues. Network administrators want to provide users with the flexibility and convenience that wireless network access offers while maintaining network security and integrity.

This whitepaper examines WLAN security beginning with the basic 802.11 security features and shortcomings. It continues by exploring the additional security features offered by 802.1x. Finally, it introduces Cisco's LEAP authentication scheme and discusses how using LEAP with Interlink Networks RAD-Series AAA servers offers strong security for WLAN users.

802.11 SECURITY FEATURES

The 802.11 standard provides for two primary security features that, unfortunately, fall short of a truly secure solution. Both of the solutions operate on the data link layer of the network.

SSID – Service Set Identifier

The SSID is a piece of information used to identify a particular access point to stations wishing to use a wireless network. Thus, the SSID is analogous to a common network name shared by the wireless station and access points. The SSID must either be pre-configured or advertised in beacon broadcasts.

Because the SSID is transmitted in the clear in beacon frames by default, it provides very little security. A rogue access point could read the SSID from beacon frames and assume the identity of the legitimate access point. This could potentially allow the hijacking of the stations' traffic.

WEP - Wired Equivalent Privacy

According to the 802.11 standard, Wired Equivalent Privacy (WEP) was intended to provide "confidentiality that is subjectively equivalent to the confidentiality of a wired local area network (LAN) medium that does not employ cryptographic techniques to enhance privacy."

WEP relies on a secret key that is shared between a mobile station and an access point. WEP uses the RC4 stream cipher invented by RSA Data Security. RC4 is a symmetric stream cipher that uses the same variable length key for encryption and decryption. With WEP enabled, the sender encrypts the data frame payload and replaces the original payload with the encrypted payload. The sender then forwards the encrypted frame to its destination. The encrypted data frames are sent with the MAC header WEP bit set. Thus, the receiver knows to use the shared WEP key to decrypt the payload and recover the original frame. The new frame, with an unencrypted payload can then be passed to an upper layer protocol.

WEP provides two main features. It denies access to the network by unauthorized users that do not have the appropriate WEP key. It also prevents the decoding of captured the encrypted WLAN traffic without the possession of the WEP key.

802.11 AUTHENTICATION AND ASSOCIATION

In order for a wireless station to use the WLAN, it must first authenticate itself to the access point. Upon authentication, the station must associate itself with the access point. Once a station has performed these two steps, it may have access to the WLAN resources. 802.11 describes two methods for station authentication.

Open Authentication

With Open Authentication, the station authenticates entirely using clear text. This allows a station to authenticate and associate without having the correct WEP key. The station, however, will not be able to transmit or receive data without the correct WEP key.

Shared Key Authentication

With Shared Key Authentication, a challenge packet is sent to the authenticating station. The station is required to encrypt the packet using the shared WEP key and send it back to the access point. If the challenge packet was encrypted correctly, the station is allowed to proceed to the association phase.

Association

Once the station is authenticated, it transmits an association request to the access point. If the request is accepted, the station is associated with the access point. The access point sends an association reply back to the station.

Note that the authentication and association is done solely on the data link layer between the station and the access point. No knowledge of the user was considered in allowing the station access to the WLAN.

802.11 SECURITY CONCERNS

Using the 802.11 security features certainly increases the security of the WLAN. However, these features alone do not provide a complete wireless security solution. A number of security concerns have been raised. These concerns were motivating factors in the development of Cisco's EAP-LEAP and Interlink Networks' RAD-Series EAP-LEAP support.

MAC Address Authentication

Open and Shared Key Authentication involves the station authenticating to an access point using the station's MAC address. This type of authentication does not consider the identity of the user. Thus anyone stealing a laptop or NIC configured with the WEP keys can obtain network access.

One Way Authentication

WEP authentication is one-way only. The access point does not need to authenticate to the mobile station. This may allow a rogue access point to falsely indicate a successful authentication to a station and hijack that station's data.

Static WEP Keys

No mechanism is defined for key distribution or key negotiation. This requires wireless networks to be hand-configured with WEP keys. The administrative costs of this hand configuration virtually guarantee that these keys will seldom be changed.

WEP Key Vulnerability

Recent papers have described successful attacks on the WEP algorithm. One of these, whose source code is readily available on the Internet, is a passive attack that claims to be able to retrieve a 40-bit WEP key in 15 minutes with an ordinary laptop. Because this attack scales linearly based on key size, a 128-bit key should be able to be cracked in about 45 minutes.

802.1X

The IEEE 802.1x Standard for Port Based Network Access Control was adopted to address some of the current 802.11 security concerns. 802.1x provides two important mechanisms.

User Authentication using EAP

Extensible Authentication Protocol (EAP) is a method of conducting an authentication conversation between a user and an authentication server (e.g. Interlink Network's RAD-Series AAA server). Intermediate devices such as access points and proxy servers do not take part in the conversation. Their role is to relay EAP packets between the parties performing the authentication. 802.1x describes how EAP packets are encapsulated and carried over Ethernet (and Token Ring/FDDI) frames so that EAP authentication conversations may be conducted through Ethernet. EAP supports multiple authentication mechanisms such as token cards, certificates, biometrics, etc. User authentication using EAP solves the MAC address-only authentication security concern described above.

WEP Key Distribution using the EAPOL-Key Frame

This message allows the wireless access point to send one or more WEP keys to the station. Access points can send an EAPOL-Key message at any time after authentication to update the WEP keys at the station. This allows (but does not require) the distribution of per-session keys to access points and stations. It is important to note that this provides a mechanism for rotating WEP keys but does not describe how this is handled. Using the EAPOL-Key frame to rotate WEP keys can help mitigate the static WEP key security risks described above.

The adoption of 802.1x for use in WLANs is an improvement in security over SSIDs and static WEP keys. In order to further improve the security in the WLAN, Cisco has developed EAP-LEAP. Interlink Networks supports Cisco's EAP-LEAP authentication scheme in the RAD-Series AAA servers.

LEAP - LIGHTWEIGHT EXTENSIBLE AUTHENTICATION PROTOCOL

Cisco Systems, Inc. has developed the Lightweight Extensible Authentication Protocol (LEAP), sometimes known as “EAP-Cisco Wireless”. LEAP provides two important security features.

Mutual Authentication Between Station and Access Point

LEAP requires the mutual authentication between stations and access points. This allows a connecting station to verify the identity of the access point with which it is attempting to associate. At the same time, the access point must verify the identity of the station. The station must present a username and password that will be verified by a LEAP-capable RADIUS server such as the Interlink Networks RAD-Series AAA Server. This mutual authentication ensures that only authorized users are allowed access to the network while preventing hijacking of legitimate user sessions by rogue access points. Mutual authentication is a great improvement over the one-way authentication described above.

Distribution of WEP Keys on a Per-session Basis

Upon successful authentication, the LEAP algorithm dynamically generates a unique WEP session key. Both the RAD-Series AAA Server and the Cisco Aironet Network Interface or Cisco Aironet Wireless LAN Adapter independently generate this key. This means that the key is not transmitted through the air where it could be intercepted. The use of per-session WEP keys greatly reduces the possibility of a WEP key being discovered. In the unlikely event that the key is discovered, it is of no use once the current session is over. This greatly decreases the WEP key vulnerability described above.

Using Cisco’s LEAP fills two noteworthy WLAN security holes. The Interlink Networks RAD-Series AAA Server is the authentication server that makes LEAP possible.

CISCO LEAP ARCHITECTURE

There are three key components required for LEAP functionality.

LEAP Supplicant

The supplicant is the client software and firmware that authenticates to the WLAN. The software resides on the host device with the WLAN adapter. The firmware resides in the Cisco WLAN adapter. The LEAP supplicant can be configured to store the username and password or to prompt for the credentials at logon time. Storing the username and password in the supplicant may be a security risk since a stolen device would allow access to network resources.

802.1x Authenticator

The authenticator is the software running on the access point (Cisco 340 series and newer). The authenticator acts as a relay, forwarding the EAP messages to the authentication server.

Authentication Server

The authentication server is a LEAP-enabled RADIUS server. The Interlink Networks RAD-Series AAA server implements the LEAP authentication mechanism. The server allows station authentication based on username and password.

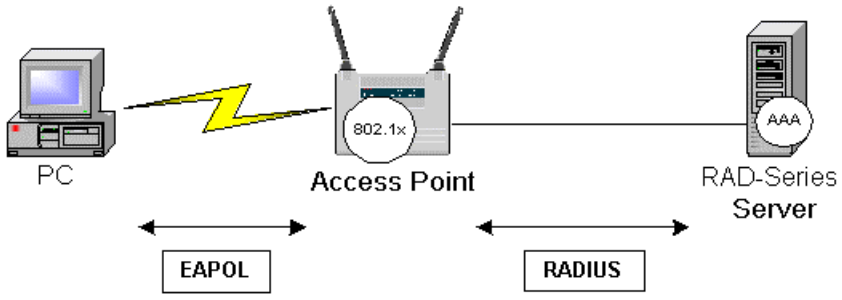

Figure 1 – A client authenticates by using EAPOL to communicate with the Access Point. The Access Point communicates with the AAA server using RADIUS.

THE LEAP AUTHENTICATION PROCESS

The Cisco LEAP authentication and key exchange process occurs in three phases.

The Start Phase

In the start phase, the supplicant begins the authentication by issuing an EAPOW-Start message to the authenticator. The authenticator responds to the supplicant with an EAP-Request/Identity message. The supplicant responds with an EAP-Response/Identity message that delivers its identity to the authenticator.

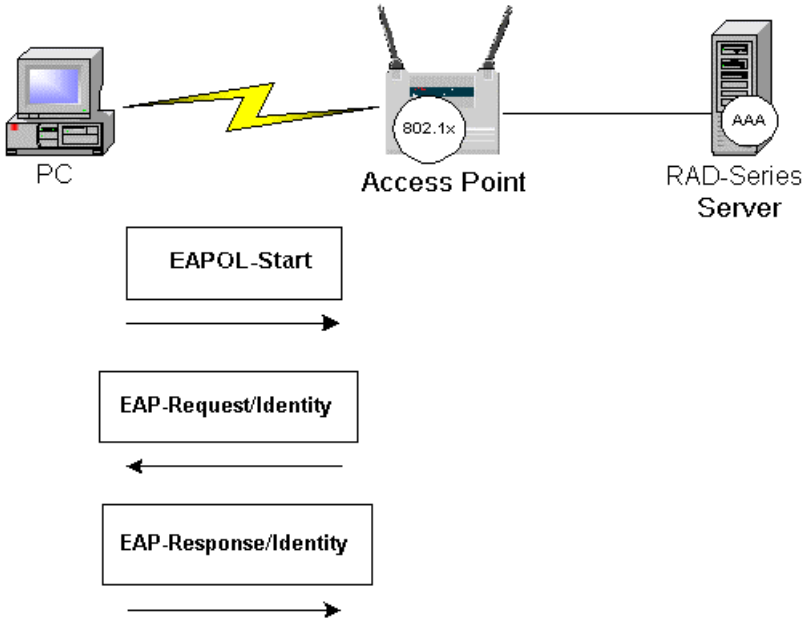

Figure 2 – The Start Phase. The supplicant (client) sends an EAPOL-Start message. The authenticator responds with an EAP-Request/Identity message. Finally, the supplicant responds with an EAP-Response/Identity message which contains the identity of the user.

The Authenticate Phase

The Cisco LEAP authentication is a mutual authentication method. The Authenticator (Access Point) relays EAP messages to the authentication server using a RADIUS Access-Request message with EAP attributes. The Authentication Server responds with a RADIUS Access-Challenge message. The Authenticator relays this message to the Supplicant as an EAP-Request. Next, the supplicant responds with an EAP-Response message that is forwarded to the Authentication Server as a RADIUS message with EAP attributes.

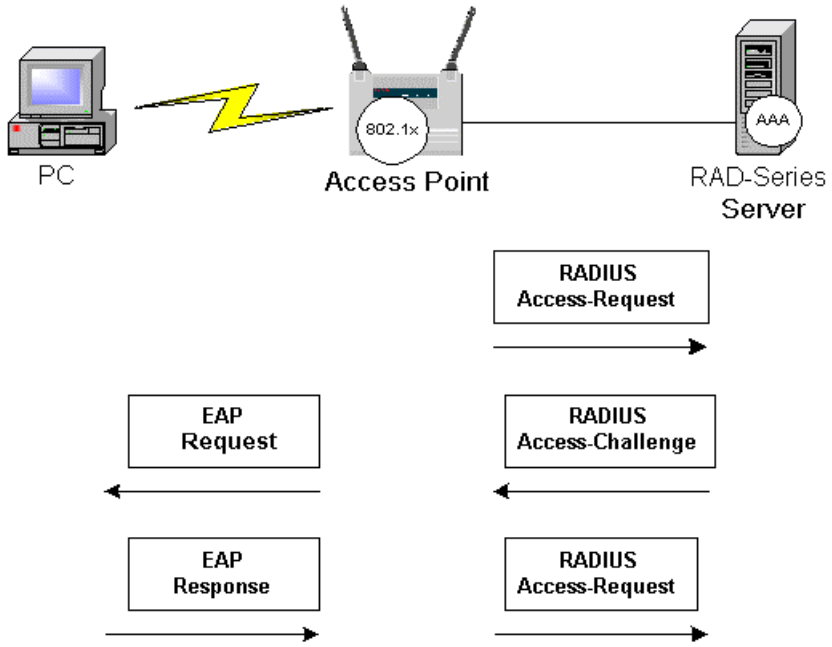

Figure 3 – The Authenticate Phase. The authenticator sends a RADIUS Access-Request message. The AAA server issues a challenge that is carried via EAP to the supplicant. The supplicant responds and the authenticator issues another RADIUS access request.

The Finish Phase

If the user is not valid, the Authentication server sends a RADIUS Deny packet with an EAP fail message. If the user is valid, the Authentication Server sends a RADIUS access accept packet with an EAP success attribute. The RADIUS-Access-Accept message contains the MS-MPPE-Send-Key attribute to the Authenticator. The Authentication Server and the Supplicant are able to derive a key from the user's password. The key derivation technique creates a longer key than will be used for the session. Upon receipt of the key from the Authentication server, the Authenticator transmits an EAPOL-Key message to the Supplicant. This message is a key index and key length that the supplicant can use to calculate the session key to be used.

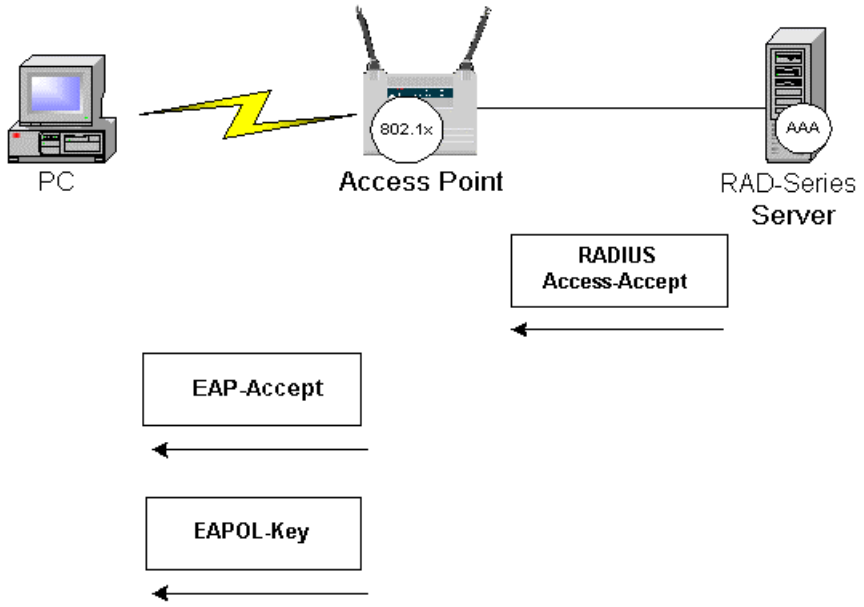

Figure 4 – The Finish Phase. After the AAA server issues a RADIUS Access-Accept message, the authenticator can send and EAP-Accept message along with a key index and length.

At this point, the Supplicant and Authenticator have a common session key that can be used for the duration of the session.

CONFIGURING INTERLINK NETWORKS RAD-SERIES TO USE CISCO LEAP

The RAD-Series AAA server must be configured to use Cisco LEAP. This is accomplished by modifying the following three RAD-Series configuration files.

`/etc/opt/aaa/clients`

This file specifies the RADIUS clients that are recognized by the server. Add a line that specifies the Cisco Network Access Server (NAS) that will be acting as a client

to the RAD-Series server. One must also specify the secret shared between the NAS and the RAD-Series server. The following is an example configuration:

```
w03.mydomain.com          secret            Type=Cisco:NAS
```

`/etc/opt/aaa/users`

This file identifies the users that will be authenticating via LEAP. The Authentication Type must be specified as "Realm". This will allow all users for a given realm to be authenticated using LEAP. One must also add "Check-Items" and "Reply-Items" which define authentication and authorization for the user. The following is an example configuration:

```
joe@mydomain.com  Authentication-Type=Realm,Password=Joepassword
```

`/etc/opt/aaa/authfile`

This file contains a list of realm names and authentication methods for those realms. For each realm, one must associate the realm name with the LEAP authentication method. The following is an example configuration:

```
mydomain.com  EAP   "Cisco LEAP Realm"
   {
   EAP-Type    CiscoLEAP
   }
```

These configurations will allow the authentication of users with LEAP. For more information, please see the RAD-P or RAD-E *Authentication Guide* documentation.

CONCLUSIONS

Wireless LANs provide tremendous benefits in flexibility and convenience but also present a number of serious security issues. Interlink Network's RAD-Series AAA Servers combined with Cisco System's Aironet and LEAP can mitigate the risks associated with wireless equipment, offering the network security and integrity that businesses require.

ABOUT INTERLINK NETWORKS

THE COMPANY

Interlink Networks is a leader in securing access to public and private networks. Our products manage user access to dial-in, broadband, mobile, and wireless LAN networks. Interlink Networks' RADIUS-based access control software provides the authentication, authorization, and accounting infrastructure that enables secure and reliable network access for thousands of enterprise and service provider networks worldwide.

Interlink Networks is headquartered in Ann Arbor, Michigan. We have a worldwide network of resellers and distributors.

OUR MISSION

Interlink Networks' mission is to be a worldwide leader in providing solutions for securing access to public and private networks. By securing access to the network, we provide network operators the first line of defense against unauthorized access to an organization's computing resources.

OUR HISTORY

In July 2000, Interlink Networks was formed by a spin out of technology and developers from Merit Network, Inc., a world-renowned designer, developer, and implementer of Internet technology, hosted at the University of Michigan.

The founders of Interlink Networks spent over a decade defining and developing the world's best carrier-class RADIUS (Remote Access Dial-In User Services) server. Mr. John Vollbrecht, Interlink Networks' Founder and CTO, issued the first RFP for centralized AAA ten years ago, and championed the resulting RADIUS standards through the IETF Standards Groups. Mr. Vollbrecht's name is on many of the RFCs that define RADIUS and AAA.

The charter of Interlink Networks is to expand upon its vision of providing the most advanced authentication products, and to expand its solution set beyond remote access into other network access mechanisms that require authentication and authorization. As networks become more complex, and the means to access networks expands, Interlink will continue to assure that the "interlinks" between users and their networks are protected and secure.

REFERENCES

IEEE Standard 802.11-1999 - Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications

IEEE Standard 802.1x-2001 – Standard for Port based Network Access Control

Intercepting Mobile Communications: The Insecurity of 802.11 - http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf

Weaknesses in the Key Scheduling Algorithm of RC4 - http://www.eyetap.org/~rguerra/toronto2001/rc4_ksaproc.pdf

draft-congdon-radius-8021x-16.txt - IEEE 802.1X RADIUS Usage Guidelines

RFC 2284 - PPP Extensible Authentication Protocol (EAP)

RFC 2548 - Microsoft Vendor-specific RADIUS Attributes

RFC 2865 - Remote Authentication Dial In User Service (RADIUS)

RFC 2866 - RADIUS Accounting

RFC 2868 - RADIUS Attributes for Tunnel Protocol Support

RFC 2869 - RADIUS Extensions

RFC 3079 - Deriving Keys for use with Microsoft Point-to-Point Encryption (MPPE)