INTERLINK
NETWORKS

Wireless LAN Access Control and Authentication

802.11b Wireless Networking and
Why It Needs Authentication

Authors:

John Vollbrecht, Founder
Interlink Networks, Inc. 5405 Data Court, Suite 300, Ann Arbor, MI 48108, jrv@interlinknetworks.com
Robert Moskowitz, Senior Technical Director
TruSecure Corporation, 15210 Sutherland Ave., Oak Park, MI 48237, rgm@trusecure.com

Revision D. 12-02.

Trademark Information

Interlink Networks, Inc.

5405 Data Court, Suite 300
Ann Arbor, MI 48108
Phone: 734-821-1200
Sales: 734-821-1228
Fax: 734-821-1235
info@interlinknetworks.com
sales@interlinknetworks.com
www.interlinknetworks.com

Table of Contents

Wireless LAN Access Control and Authentication

802.11b wireless networking and why it needs authentication

1 INTRODUCTION

1.1 OVERVIEW

Wireless networking is emerging as a significant aspect of internetworking. It presents a set of unique issues based on the fact that the only limit to a wireless network is the radio signal strength. There is no wiring to define membership in a network. There is no physical method to restrict a system in radio range to be a member of a wireless network. Wireless networking, more than any other networking technology, needs an authentication and access control mechanism.

The IEEE 802.11 group has defined standards for Wireless LAN implementation including both radio standards and networking protocol standards. The intent of these standards is to provide a wireless Ethernet capability. The 802.11 standard has specified the use of 802.1x authentication mechanisms for authenticating user access to the LAN. Parts of both 802.11 and 802.1x are being updated and clarified based on experience with its initial deployments. This paper looks at 802.11 access authentication issues, the existing and proposed technologies, and scenarios for use. It also provides our understanding of proposed changes to the standard to make it more secure and robust. It does not deal with radio standards.

1.2 RELATION TO IEEE STANDARDS

IEEE 802.11 is the wireless LAN Standard. The original 802.11 standard included support for “Wired Equivalent Privacy” to protect messages going over the air. WEP requires a shared key to protect messages, and the original standard assumed that these keys would be configured in the devices. Later versions of the standard have add the use of 802.1x for authenticating users attempting to connect to the network and as part of the authentication creating “dynamic” keys for WEP. Currently work in the IEEE is addressing several areas having to do with access authentication for 802.11 wireless networks. This paper focuses on two areas of standards work.

1. **Device (STA) authentication via 802.1x and remote RADIUS.** This leverages off of work done in the IETF, most notably RADIUS and its Extensible Authentication Protocol (EAP). Work on EAP and 802.1x is being done in the EAP working group of IETF and the 802.1 task group of IEEE to deal with issues raised by deployment of 802.11 LANs.
2. **Per-packet authentication (message integrity) and encryption technology.** This is to replace Wired Equivalent Privacy (WEP). The initial WEP algorithm has been shone to be relatively easy to attack.

The revised WLAN standards, properly deployed, will make authenticated wireless networking a safe computing environment.

This paper describes the current state of access control with existing 802.11 devices, our understanding of the ways the standards will change, and highlights some of the issues that are in the process of being resolved. The paper also describes how we expect wireless services to evolve with the revised standard.

1.3 STRUCTURE OF THIS PAPER

- **Section 2** describes the basic wireless infrastructure and defines terms in the 802.11 context.
- **Section 3** covers risks associated with current wireless LAN services.
- **Section 4** describes the access control tools used with wireless LANs today.
- **Section 5** covers the 802.1x-based authentication that is beginning to be deployed.
- **Section 6** is about problems being addressed by standards bodies and their likely fixes.
- **Section 7** covers standards issues with access points, focusing especially on issues with roaming across access points without forcing reauthentication.
- **Section 8** summarizes and draws conclusions.

The paper was written to be read sequentially but someone with good knowledge of wireless may pick and choose from the separate sections.

2 WIRELESS INFRASTRUCTURE

2.1 SCOPE

This paper concentrates on authentication services for 802.11 (WLAN) in what is referred to as Infrastructure mode. In this mode all wireless station communication is passed through an access point whose function is similar to that of a wired hub. This paper will also cover privacy and integrity services triggered by the authentication services and how the authentication services themselves benefit from these privacy services.

The application of these authentication services to practical wireless networking situations will be covered in separate papers.

2.2 TERMINOLOGY

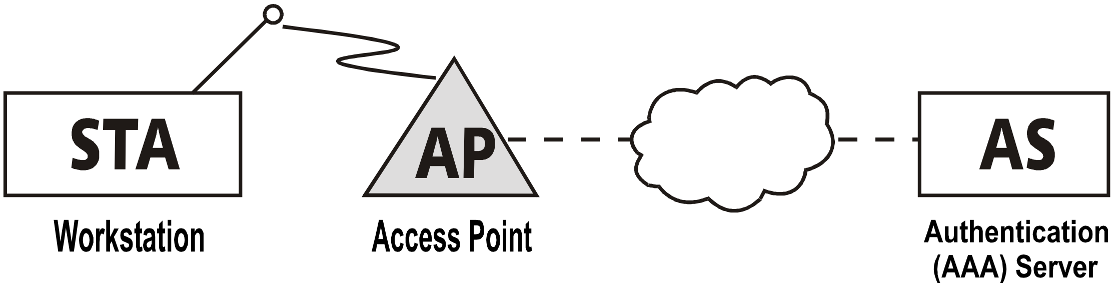

Figure 1. Wireless LAN access terminology.

AP Access Point. An 802.11 hub/bridge that provides star topology control on the wireless side and access to a wired network.

AS Authentication Server. An 802.1x component for performing authentication services for devices requesting admittance to a network. Implementations include RADIUS and other AAA servers.

STA Wireless Station. Any 802.11 device other than an access point.

2.3 TYPES OF WIRELESS NETWORKS

The 1999 version of the 802.11 standard defines 3 types of wireless networks with a simple set of authentication and privacy features:

2.3.1 Ad hoc network

A network composed solely of stations within mutual communication range of each other via the wireless medium. An ad hoc network is typically created in a spontaneous manner and exists for a limited time in a small area (to avoid the hidden node problem). The proper 802.11 term for ad hoc networks is an Independent Basic Service Set (IBSS).

2.3.2 Basic Infrastructure network

A set of wireless stations controlled by a single coordinator called an Access Point. All communication is through the AP, which functions as a hub. The proper 802.11 term for a basic infrastructure network is a Basic Service Set (BSS).

2.3.3 Infrastructure network

When a number of BSSs are connected together through other networking technology (including Ethernet and wireless bridging), they appear to the stations as a single wireless network, or technically an Extended Service Set (ESS). Stations roam transparently from one BSS to another within the ESS. However, there is no standard for packet forwarding for a roaming station in an ESS from one AP to another. IEEE 802.11f is providing a mechanism for AP-to-AP transactions when a station roams. Currently there is no standard way for a STA to roam from one AP to another without reauthenticating to the new AP. A number of proposals for supporting this roaming have been advanced, but so far no 802.11 group is working to develop a standard for this.

2.4 SECURITY OPTIONS FOR WIRELESS NETWORKS

An infrastructure network may have security /integrity requirements. 802.11-1999 only defines a single security option, WEP. Efforts with the IEEE 802.11 workgroup and the vendor WiFI Alliance are producing a number of possible security architecture alternatives. The set of architectures are described below.

2.4.1.1 Wired Equivalent Privacy

WEP was designed to provide:

- **Reasonable Strength:** The security afforded by the algorithm relies on the difficulty of discovering the secret key through a brute-force attack.
- **Self-synchronization:** WEP is self-synchronizing for each message. This property is critical for a data-link level encryption algorithm, where "best effort" delivery is assumed and packet loss rates may be high.
- **Processing efficiency:** The WEP algorithm is efficient and may be implemented in either hardware or software.
- **Exportability:** Every effort was made to design the WEP system operation so as to maximize the chances of approval, by the U.S. Department of Commerce, of export from the U.S. of products containing a WEP implementation. However, due to the legal and political climate toward cryptography at the time of publication, no guarantee can be made that any specific IEEE 802.11 implementations that use WEP will be exportable from the USA.

These design goals for WEP were establish to match the security of a wired network. That is good against external attacks. At the time of its design, 1995, WEP appeared to have met this goal. But by the time the standard was ratified in 1999, WEP was already showing weaknesses so work was begun in 2000 by the IEEE 802.11 workgroup to produce alternatives for WEP.

2.4.1.2 Robust Security Network

An update to the 802.11 specification will define a new set of authentication and privacy features. An ESS or BSS with these features will be called an RSN. An RSN is an ESS/BSS that provides the following authentication and privacy features:

- Enhanced authentication mechanisms for both APs and STAs based on 802.1x
- Key management algorithms
- Dynamic, association-specific cryptographic keys
- Enhanced data encapsulation mechanism, using AES or TKIP

2.4.1.3 Transition Security Network

A Transition Security Network (TSN) is an RSN that also supports unmodified WEP-enabled equipment. A TSN is defined only to facilitate migration to an RSN. A TSN is as secure as WEP, since the WEP-enabled equipment can compromise the larger network. This includes existing WEP networks as well as networks transitioning from WEP to RSN or WPA but including WEP enabled devices. A TSN provides the following authentication and privacy features for RSN-capable equipment

- Support for authentication mechanisms for both APs and STAs based on 802.1x
- Support for key management algorithms
- Support for dynamic, association-specific cryptographic keys

2.4.1.4 Wi-Fi Protected Access

A Wi-Fi Protected Access is an interim alternative to RSN supported by the Wi-Fi Alliance, the 802.11 vendor forum. WPA is NOT an IEEE standard, but is derived from an IEEE draft document. WPA will only work for Infrastructure mode and will include the following:

- Authentication mechanisms for both APs and STAs based on 802.1x
- Key management algorithms
- Dynamic, association-specific cryptographic keys
- Enhanced data encapsulation mechanism, using TKIP

WPA certification may be available to vendors from the WiFi Alliance in the spring of 2003.

3 RISKS WITH WIRELESS LANS

Before going into more detail on access control protocols, this section describes the risks associated with wireless LANs that are addressed by these protocols.

3.1 SNIFFING

The nature of an RF based network leaves it open to packet interception by any radio within range of a transmitter. Interception can occur far outside the users 'working' range by using hi-gain antennas (many of which are standard offerings from some vendors or made from a Pringles ™ can and some coax wire). With readily available tools, the eavesdropper is not limited to just collecting packets for later analysis, but can actually see interactive sessions like web pages viewed by a valid wireless user. An eavesdropper can also catch weak authentication exchanges, like some website logins. The eavesdropper could later duplicate the logon and gain access.

Encrypting data between the STA and AP can mitigate eavesdropping of user data. However, the ability to sniff also makes attacks on encryption easier, and mandates requirements for strong encryption algorithms.

3.2 INVASION AND RESOURCE STEALING

Once an attacker has gained the knowledge of how a WLAN controls admittance, he may be able to either gain admittance to the network on his own, or steal a valid STA's access. Stealing a STA's access is simple if the attacker can mimic the valid STA's MAC address and use its assigned IP address. The attacker waits until the valid system stops using the network and then takes over its position in the network.

This would allow an attacker direct access to all devices within a network, or to use the network to gain access to the wider Internet, all the while appearing to be a valid user of the attacked network.

To mitigate this danger the AP and STA need to support "message integrity", which means that each "signs" every message sent to the other using a shared key.

3.3 TRAFFIC REDIRECTION

An attacking STA can poison the ARP tables in switches on the wired network through the AP causing packets for a wired station to be routed to the attacking STA. The attacker can either passively capture these packets before forwarding them to the attacked wired system, or attempt a man-in-the-middle attack. In such an attack, all the susceptible systems could be on the wired network.

Link-layer authentication stops an outsider from perpetrating this attack. Network-layer (e.g. IPsec) stops an insider from perpetrating this attack.

3.4 DENIAL OF SERVICE

Denial of service attacks against a WLAN can range from simple radio interference (a 2.4Ghz cordless phone is an example of such an attacking device) to more subtle attacks against a single STA or AP. An attacking system could replay a captured 802.11 disassociate message, or an 802.1x EAPOL-logoff message, and effectively disconnect a STA from the WLAN.

It is considered impossible to build a network without some DOS attacks, thus the thrust is to minimize them and to be able to recognize and trace them back to their source.

3.5 ROGUE NETWORKS AND STATION REDIRECTION

An 802.11 wireless network is very susceptible to a rogue AP attack. A rogue AP is one owned by an attacker that accepts STA connections and then at a minimum intercepts traffic if not also performing man-in-the-middle attacks before allowing traffic to flow to the proper network. The goal of a rogue is pulling valid traffic from the WLAN to a wired network for attacking (or to conduct the attack directly within the rogue AP) and then reinserting the traffic into the proper network.

A newer form of a rogue AP is a STA with two wireless cards. With one, it acts as a valid station to the ESS, with the other it acts as an AP to other STAs. Such rogue APs could readily be deployed in public areas as well as shared office space areas.

4 TODAY'S ACCESS CONTROL TOOLS

4.1 SSID – SERVICE SET IDENTIFIER

Each ESS has an SSID that it uses to identify the APs that are a part of the ESS. A common way of configuring a network is to require each STA to know the SSID of the AP to which it wants to connect. By default, all APs broadcast their SSID as an advertisement of their presence.

SSID provides a very modest amount of control. It keeps a STA from accidentally connecting to a neighboring AP. It does not, by itself, help with other security issues, and in particular it does not keep an attacker from accessing the ESS or from setting up a "rogue" AP that uses the same SSID as a valid AP.

It is possible to turn off SSID broadcasts. This does make WLAN discover by an attacker harder, but when a station PROBES for an AP SSID, the AP responses with a one-time broadcast, so the patient attacker will still discover SSIDs. SSID hiding is impossible, and is not a security measure.

4.2 MAC FILTERS

Some APs provide the capability for checking the MAC address of the STA before allowing it to connect to the network. This provides an additional layer of control in that only STAs with a registered MAC address can connect. This approach requires that the list of MAC addresses be configured. The list may be kept in long-term memory on the AP, or the AP may send a RADIUS request with the MAC address as the userid (and a null password) to a central RADIUS server and the RADIUS server will check the list. The RADIUS approach is especially appropriate if the MAC addresses are to be used with multiple APs.

Using MAC filters is considered to be very weak security because on many wireless cards it is possible to change the MAC address by reconfiguring the card. An attacker could sniff a valid MAC address from the wireless network traffic and then configure his card to use it and gain access.

4.3 STATIC WEP KEYS

Wired Equivalent Privacy (WEP) is part of the 802.11 specification. Static WEP key operation requires keys on the STA and AP that are used to encrypt data sent between them. With WEP encryption, sniffing is eliminated and session hijacking is difficult (or impossible). STA and AP are configured with a set of 4 keys, and when decrypting each are used in turn until decryption is successful. This allows keys to be changed dynamically.

As described above, keys are the same in all STAs and APs. This means that there is a “community” key shared by everyone in the ESS. The danger is that if any one in the community is compromised, the community key, and hence the network and everyone else using it, is at risk.

As it turns out, the current version of WEP encryption has been proven to be vulnerable. Some additional details of this are described below. A new security component is being developed within 802.11. Until it is available and deployed, WEP is not strong protection, but provides an important first line of defense according to many security professionals.

4.4 DYNAMIC WEP KEYS

There are a number of methods for dynamically setting the WEP keys. The most commonly used now is 802.1x. Kerberos is also used.

4.5 VPNS

Many people use VPNs to protect their connection over a wireless network. This is not strictly a wireless solution—it can be used in any remote access situation. VPNs do provide protection for some of the areas where current Wireless LAN solutions are weak. In particular, VPNs can provide integrity checking and, optionally, encryption of sessions. VPNs only protect the STA traffic routed through the VPN, not the STAs or the network. Without WEP or an equivalent to support Link layer integrity, the connection between the STA and the AP is vulnerable to unsophisticated, easy to mount, denial of service attacks. In addition, the STA and Client are vulnerable to direct attacks. Adding a personal firewall product at a financial and management cost can mitigate the Client risk.

Deploying a firewall between the AP and the network that only allows authenticated VPNs access can provide network protection against attacks, but at a price. The firewall will require each workstation to establish a separate tunnel to the firewall. Authentication of the tunnel is required, and will be managed after the network connection is established, requiring different support in either the client or the AP. A VPN gateway CAN provide this level of protection directly. However, if the user needs to establish an additional tunnel, to a remote corporate firewall for instance, this will require a tunnel over a tunnel, which is expensive in cpu cycles on the STA and for most VPN clients has not been heavily tested.

In most current situations, using a VPN with a single firewall is a good idea whether dialing in from a remote location or connecting via a wireless Access Point. Adding WEP to the wireless session solves the wireless specific issues.

4.6 VENDOR SPECIFIC SOLUTIONS

Several vendors have implemented nonstandard solutions that provide extra security.

- Cisco LEAP is an 802.1x-based solution (see below) that uses a proprietary algorithm to support mutual authentication between a STA and a AAA server. The AAA server and the Client must support the LEAP algorithm for this to work; the Access Point can be any standard AP supporting 802.1x.
- Agere provides a solution that uses a non-standard dialog between the STA and the AP to allow standard PPP authentication methods to be used. This allows any standard RADIUS server to be used to authenticate a user.
- Symbol Technologies supports a service where client, access point and AS are based on Kerberos.
- 3COM provides a way to create a PPTP tunnel and use standard RADIUS to authenticate the tunnel.

5 STANDARDS-BASED AUTHENTICATION ADDITIONS TO WLAN

The open nature of WLAN requires authentication of the STAs to the APs. There are no wires to follow to determine which STAs are part of the network. An authentication process will allow an AP to restrict which STAs can associate with it. However, session authentication by itself, as will be shown, is inadequate for WLAN. WEP lacks message integrity, an essential component in security.

5.1 MESSAGE INTEGRITY

Per-packet message integrity checking (sometimes called per packet authentication) is the only way for an AP to determine that a packet was sent from an authenticated STA and for the STA to determine that a packet came from the authenticating AP. All message integrity algorithms need a key that is shared by the two systems. This, in turn, requires that the STA session authentication process must end with a session key shared by the two systems.

A further analysis of the risks inherent in WLAN places one more stipulation on any WLAN authentication process. Since the STA has no method short of authenticating the AP to trust the AP it associates with, the authentication process must provide explicit authentication of the AP or network.

WEP relies on decryption of a known data frame with a simple check-sum to provide its per-packet message integrity. This has recently been shown flawed and open to attack.

5.2 802.1X AUTHENTICATION

Authentication is a process of binding a name to something known and then using that name in all future interactions. The name in 802.11 is the media access or MAC address; the 48-bit value assigned to the WLAN card by its manufacturer. 802.1x is an authentication dialog between the system needing network services and the network. This dialog uses the IETF Extensible Authentication Protocol (EAP).

802.11 WLAN is now specifying the use of IEEE 802.1x (Port-Based Network Access Control) to provide the station authentication. 802.1x consists of a Port Access Entity (PAE) in all STAs and APs, EAP encapsulation over LANs (EAPOL), and RADIUS Authentication Servers (ASs).

802.1x redefines our traditional understanding of a network interface and adds access authentication services to it. In 802.1x the principal component is the Network Access Port (or just Port) that can either be a physical network interface or a virtual MAC. Above the Port is the Port Access Entity (PAE); the controlling logic that manages which device’s packets will be accepted by another device.

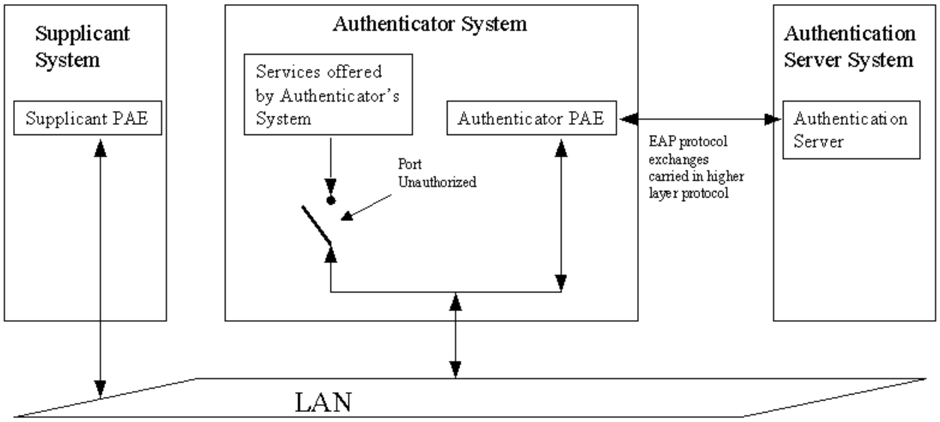
Supplicant System
Supplicant PAE
Authenticator System
Services offered by Authenticator's System
Authenticator PAE
Port Unauthorized
EAP protocol exchanges carried in higher layer protocol
Authentication Server System
Authentication Server
LAN

Figure 2. 802.1x Port Based Network Access Control

There are two types of systems supporting ports and PAEs: supplicants and authenticators (see figure 2.). In WLAN infrastructure usage, STAs are supplicants and APs are the authenticators. In all systems there are two types of Ports: Controlled and Uncontrolled ports. A Controlled port will only accept packets from authenticated systems. That is a packet whose MAC address is on the list of authenticated addresses, whereas an Uncontrolled port will accept any packet. Normally the Uncontrolled port will only use packets to establish authentication; in 802.1x these are EAPOL packets (EAP over LAN and EAPOL key).

This aspect of authentication to a MAC address is fundamental to 802.1x. The authenticator has no other way to identify the supplicant or its packets without a high-layer per-packet authentication mechanism.

The third component is the authentication server (AS). The main function of the authenticator system is to act as an EAP proxy between the supplicant and the AS. That is, it accepts EAPOL EAP packets from the supplicant and forwards the EAP packets to the AS over a protocol like RADIUS. It also forwards all AS EAP packets over EAPOL to the supplicant. In this manner, the supplicant is authenticated to the network. Once this is done, the AS provides the authentication state of the supplicant to the authenticator system via the secure RADIUS channel between the two.

5.3 EAP, RADIUS, AND 802.1X

The standard for Access authorization between a STA and an AP is 802.1x. The de facto standard for communication between the AP and the AS is RADIUS.

The authentication dialog between the STA and the AS is carried in EAP frames. The EAP frames are carried as EAPOL (EAP over LAN) in 802.1x, and as EAP Message attributes in RADIUS.

The standard authorization dialog consists of:

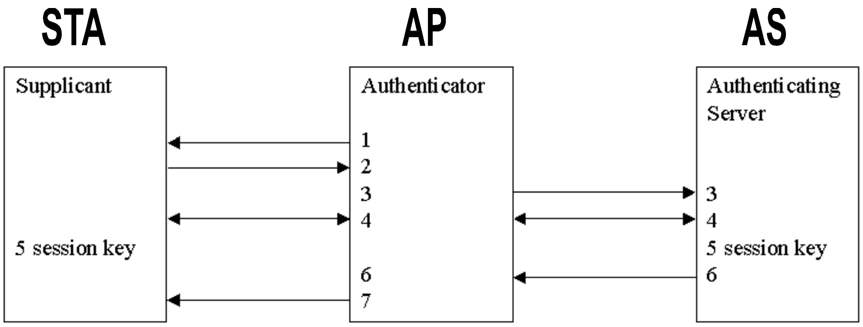

Figure 3. 802.1x standard authorization dialog.

1. AP requests an identity from STA using EAPOL.
2. STA sends its identity to the AP.
3. AP forwards the STA identity to AS via EAP.
4. The AS and STA have an EAP authentication dialog (see next section for types of dialog).
5. If Dialog is successful, STA and AS share a session key.
6. AS sends the session key to the AP in a RADIUS Attribute as part of RADIUS Accept message.
7. AP enables its controlled port for the STA's MAC address and optionally enables a WEP key via the EAPOL-Key packet.

5.4 EAP AUTHENTICATION TYPES

The authentication dialog between the STA and AS must be negotiated between them as part of the EAP dialog. Several EAP authentication methods have been standardized for use with PPP, but good practice for 802.11 requires mutual authentication and the creation of a shared session key as part of the authentication method. In other words, wireless authentication should be explicit mutual authentication: both parties have cryptographic evidence of the other's identity. Current Standard track and Experimental EAP methods are not appropriate for Wireless authentication.

A number of EAP methods that may be appropriate for Wireless authentication have been submitted to the Internet Draft library of IETF. We will discuss some of these below. There are also Vendor proprietary EAP methods that have been rolled out, most notably Cisco's LEAP (Lightweight EAP).

Currently a revision of the Experimental EAP-TLS is the most available implementation appropriate for wireless. There has been discussion of support for strong password authentication with EAP-SRP.

Support for EAP methods must be available in both AAA server and the STA. EAP-TLS support is available in Microsoft XP workstations and as part of the WLAN software for other OSs. Other authentication methods could be added in Workstations either by Microsoft or as addons by the WLAN or Authentication vendors.

Most RADIUS server vendors supporting the WLAN market support TLS (as described in <draft-josefsson-pppext-eap-tls-eap-05.txt>.

5.4.1 EAP-TLS

The EAP-TLS type is currently the most commonly implemented EAP type for WLAN.

EAP-TLS authentication is based on X.509 certificates. In WLAN usage, the STA must have a certificate that the AS can validate. Likewise, the AS will present a certificate to the STA and the STA will have to validate it.

- It is resilient to man-in-the-middle attacks. We do not really care if an attacker is intercepting the exchange. Properly implemented, EAP-TLS resists such attacks.
- It provides explicit mutual authentication between the AS and the supplicant. This is only true if both parties can validate the other's certificate. This is typically done by having both certificates issued by one CA, and for each party to have the CA's certificate and CRL to validate the certificates.
- After the exchange, there is a shared session secret between the AS and the supplicant. Once the AS supplies this to the authenticator system via their secure link, the authenticator system and the supplicant can use it to bootstrap their per-packet authenticated, secure communication.

EAP-TLS requires the complexity of a PKI to support STA authentication. This may be acceptable in large corporate deployments, but is likely to be burdensome for SOHO and small and medium enterprise deployments. A strong password authentication method with User ID and Password is a more practical authentication for many public deployments.

5.4.2 Protected EAP methods

To mitigate the complexity and cost of deploying the user certificates required to support EAP-TLS, two methods have been proposed that use a server side certificate to allow authentication of the server and creation of an EAP-TLS tunnel that then carries other authentication methods over the tunnel. The two methods that have been proposed are EAP-PEAP (Protected EAP) and EAP-TTLS (Tunneled TLS). These are very similar methods, and most observers expect only one to become commonly implemented. It is not yet clear which one it will be.

Protected EAP methods tend to take many round trips to complete. This can be mitigated in part by using the resume feature of TLS.

Recently a Man-in-the-Middle attack has been described which can be mounted against these methods in certain circumstances.

5.4.2.1 PEAP

PEAP (Protected EAP) extends the TLS challenge to carry an EAP exchange. Once the initial TLS exchange is complete which authenticates the server to the user, any other EAP method can be used to authenticate the user to the server. Thus traditional EAP methods like MD5 or MSCHAP can be used in conjunction with PEAP. Some PEAP characteristics:

- Two EAP exchanges, 1st to set up TLS, second to use TLS for protection
- Provides Certificate-based AS authentication by using standard TLS methodology.
- Authenticates the STA's AS to the STA.
- STA authentication using any EAP type within EAP-TLS tunnel.
- STA Identity hiding by using generic Identity in outer EAP and real Identity within TLS
- Fast reconnect using TLS session resume.

PEAP avoids much, but not all of the PKI complexity of TLS. AS's must have Certs and STAs MUST be configured with the root cert of the AS to validate the AS name within the AS certificate in order to avoid the SSL man-in-the-middle attack from Rogue APs. STAs MUST also use some form of certificate validation to be sure the AS certificate has not been revoked. For example: CRLs or OCSP are both protocols for checking Certificate Revocation.

In Windows XP clients, the user interface for PEAP is EAP, as PEAP presents EAP to XP.

"Inner" EAP Success and Failure messages are protected within TLS tunnel, EAP-failure is clear text if "outer" EAP-TLS fails. This is different than TTLS (see below) where all EAP Success and Failure messages are in the clear.

5.4.2.2 EAP-TTLS

EAP-TTLS (EAP Tunneled TLS Authentication Protocol) uses TLS to provide a secure channel for traditional PPP authentication methods like CHAP, MS-CHAP, MS-CHAP-V2, and EAP/MD5- Challenge. This can reduce the certificate requirements (as with PEAP only the AS needs one) and leverage legacy RADIUS authentication methods (PAP and CHAP). This is perhaps the most appealing feature of TTLS - the ability to continue using existing "legacy" RADIUS servers to authenticate wireless LANs, by inserting a RADIUS/EAP-TTLS Server between the Wireless APs and the legacy RADIUS server. Some characteristics of TTLS:

- Provides Certificate-based AS authentication by using standard TLS methodology.
- Authenticates the AP's AS to the STA. As opposed to TLS that only authenticates the STA's AS to the STA.
- STA authentication using 'weak' standard PPP methods as well as any EAP type within PPP.

- STA Identity hiding by using generic Identity in outer EAP and real Identity within EAP-TLS tunnel

TTLS avoids much, but not all of the PKI complexity of TLS. AS's must have Certs and STAs MUST be configured with the root cert of the AS to validate the AS name within the AS certificate in order to avoid the SSL man-in-the-middle attack from Rogue APs. STAs MUST also use some form of certificate validation to be sure the AS certificate has not been revoked. For example: CRLs or OCSP are both protocols for checking Certificate Revocation.

In Windows XP clients, the user interface for EAP-TTLS is RAS, as TTLS looks like a link-level interface to XP.

5.4.3 EAP-SRP

EAP-SRP is a "Strong Password" method that may be an alternative to TLS. SRP has not gotten as much interest as other methods because of potential Intellectual Property issues. SRP is a User ID and password based authentication, which is resilient to attack. Since it only uses User ID and passwords it is easier to deploy in many organizations than something requiring a CA is. Unlike TLS or TTLS, there is no explicit authentication of the AS by the STA; that is SRP only provides implicit mutual authentication. This may limit SRP's applicability to situations where either the AS is resilient to user database theft, or lose of the user database can be readily rectified.

5.4.4 Future Authentication Types

A number of authentication types have been mentioned as possible methods for Wireless LANS. Some of these are listed below and others will likely emerge. This is the area where the future is the cloudiest. It is not clear whether one or more of these authentication methods will become the defacto standard or if there will be different authentication methods used by different applications, NIC cards, and authentication vendors.

5.4.4.1 Smart/challenge cards

Vendor specific methods will likely be implemented to support mutual authentication and work with EAP. In these cases the user may authenticate with the vendor specific method and the network (AAA) may authenticate itself with another method.

5.4.4.2 Kerberos

Kerberos can be used for mutual authentication and key generation. A problem to be overcome with Kerberos implementations is that many Kerberos implementations require an IP address for the requestor, and in this mode the IP address is often assigned after authentication rather than before.

5.4.4.3 SIM

SIM cards are used by Mobile devices to authenticate to Cellular networks. A SIM card holds a secret known only to a central registry. An EAP-SIM method has been proposed to allow the SIM card and its information to be used to authenticate users accessing the network. The proposal is getting vigorous review and new versions of the Internet Draft describing have recently been published. SIM may be a protocol that will run over PEAP, or the revised SIM method may be strong enough to run as a "Strong Password" authentication method with the SIM key as the password.

5.4.4.4 Other EAP Methods

The Internet Draft Directory contains documentation for a number of other EAP methods, including AKA, SKE, and SecureId.

6 ISSUES WITH CURRENT WLAN SECURITY MECHANISMS

The 802.11 and other standards groups are working on a number of issues. Most of these have been mentioned explicitly or implicitly above. Some of the issues are spelled out in more detail in this section.

6.1 MESSAGE LEVEL INTEGRITY CHECKS

WEP provides encryption of packets, but not message integrity[1]. Proposals for AES, TKIP, and WPA all support message integrity. Not providing Message Integrity allows the following bad things:

1. 802.11 does not provide cryptographic integrity checking of each message. It trusts the MAC address provided by the STA. Since there is no per-packet cryptographic integrity check tied to the authentication key an attacker can spoof the authenticated STA. The attacker can simply note the MAC and IP addresses used, and after the valid STA leaves, start using these values to send packets.
2. A valid STA in the ESS can pose as an AP (typically takes two 802.11 interfaces in the system). Other STA closer to this rogue than a valid AP will associate with the rogue. The rogue could simply send a EAP-Success and start accepting traffic from the mis-directed STA.
3. The absence of integrity checking can also be used as a Denial Of Service attack against a STA by sending WLAN MAC sublayer management frames like the DISASSOCIATE frame.
4. An attacker can readily replace the packet content if it is unencrypted. Even if the packet is encrypted, portions can be replaced in such a manner as to appear as valid frames after decrypting to 802.11, but to be invalid to the application.

[1] Similar problems were found in IPsec: Steven M. Bellovin, "Problem Areas for the IP Security Protocols", in Proceedings of the Sixth Usenix Unix Security Symposium, pp. 1-16, San Jose, CA, July 1996. http://www.research.att.com/~smb/papers/badesp.pdf

6.2 KNOWING THE ACCESS POINT

With the authentication method described above, the STA never authenticates to the AP, only the AS. In many deployments, the static authentication (via a shared secret) between the AP and the AS provides adequate transitive trust. In a complex deployment with chained ASs, however, the STA never knows the network it authenticated to, as the SSID has no trust relation with the STA.

> Some thought is being given to adding an option to the access sequence where the STA and AP authenticate each other based on information passed to the STA by the AAA server in the access authentication (EAP) dialog. Solving this is not currently a work item in any group we are aware of.

6.3 RADIUS SHARED SECRET ISSUE

RADIUS supports a static secret key between the authenticator (AP) and the AAA server (AS). These secrets are rarely, if ever, changed. This presents an opportunity for an attacker that, through social engineering, learns the key and can intercept the encrypted traffic between the APs and AS or even impose a rogue AP into the network. This attack is being evaluated. RADIUS proxies with this mechanism have been deployed to support remote dial access in many places without problems (at least known by the authors) with this sort of attack. Wireless, however, will be a more visible environment and may draw more attention than previous wired deployments. Methods of supporting key updating for RADIUS have been discussed, but are not currently a work item in any group we are aware of.

6.4 WLAN PACKET PROTECTION

STA and AP authentication is just the first step in access control for WLAN. Each packet on a wireless network may need to be authenticated and optionally encrypted for privacy. Currently WEP provides only packet encryption.

In December 2000, a series of theoretical attacks against WEP were published. In July 2001, code for a simple passive attack against WEP was published on the Internet. A replacement for WEP was well underway prior to the recent attack, but subsequent to it there has been a concerted effort by the major WLAN vendors and a team of cryptographers to develop a fix for WEP that can be deployed on most of the current WLAN cards. These fixes are being designed to provide real security and meet the true per-packet authentication needs of WLAN.

6.5 FIXING WEP

WEP fixes are currently being addressed in the IEEE 802.11i working group. There will be two fixes to WEP. The first is a fix that works within capabilities of the current hardware, which in the remainder of this paper we call TKIP (Temporal Key Integrity Protocol). The second set of changes will not be constrained to existing hardware limitations. The second set is referred to as CCMP (Counter-Mode/CBC-MAC protocol) in the remainder of this paper. The standards process is slow and both vendors and customers need an interim fix. This is the WiFi Protected Access WPA, which is based on a draft version of TKIP see section 2.4.1.4.

6.5.1 TKIP for fixing current hardware

Limitations with current hardware includes the lack of a multiply function (needed by most crytpo algorithms), the RC4 algorithm implemented in hardware, and limited hardware support for security formatting. TKIP will have to fit into the 4 key model in the 1999 specification that restrains the rekeying process.

- TKIP has evolved extensively since it was first proposed in November 2001. TKIP is fairly complex, as it has to work within some sever design constraints. These include:
- Memory and CPU limited devices
- RC4 encryption with a problematic key scheduler (component of RC4 that produces the per-packet encrypting information)
- Limited field size for a strong Message Integrity Check
- Limited key storage model

There are five key elements in TKIP: use of 802.1x for authentication, an 802.1x based keying mechanism using the key established by an EAP method over 802.1x, an RC4 key mixing process with a 48 bit IV, and a MIC (message integrity check).

6.5.1.1 802.1x authentication with TKIP

TKIP and, for that matter, any RSN security method has a reasonable set of requirements on the EAP method used with 802.1x:

- Resilient to Man in the Middle and offline dictionary attacks
- Provide mutual authentication of the AS and STA
- Ends with a secret key shared by the AP and STA

EAP types that meet these requirements include PEAP, SRP, TLS, and TTLS.

6.5.1.2 Rekeying with TKIP

TKIP rekeying requirements are based on the size of the IV. With a 48 bit IV, this is considered large enough that 802.1X authentication will occur before the IV space is exhausted.

6.5.1.3 Roaming with TKIP

TKIP presents three methodologies for roaming between Access Points based on the STA capabilities.

- Reauthenticate with 802.1x after associating with a new AP.
- Preauthenticate to an AP just before associating to it, placing the new keys into the 802.11 key store.
- Preauthenticate to all visible APs, holding the keys on the STA until they are needed after association.

The first method is the easiest on the STA requirements, but may require seconds to complete. This may impact many applications and if the STA is 'bouncing' between APs could result in all resources allocated to authentication with no data communication. The second method works within the limitation of the 4 key model of 802.11, but assumes that there is time as a STA moves toward a new AP to perform the authentication. Again, a bouncing situation may consume all resources. If handled properly, and the STA is only bouncing between two APs, it might just use the keying it has for the two APs. The third method allows a STA to setup keys to all APs it can see (that is detect BEACONs), and authenticate quickly. Even if a STA is bouncing; it simply uses the keys it has for each AP.

There are two methods for the STA to pre-authenticate to other APs.

- Send 802.1x messages directly to the AP without first ASSOCIATING with that AP. This would be a change to the normal operation of only sending Data frames after ASSOCIATING.
- Proxy 802.1x messages for the new AP through the AP the currently ASSOCIATED, using the new AP's BSSID as the destination MAC address. This requires the APs to be on the same layer 2 infrastructure.

6.5.1.4 IBSS support with TKIP

Recent work in TKIP for IBSS has resulted in a complex model that allows each STA to function in an ad-hoc network. This method takes advantage that in ad-hoc, there are no real broadcast frames. Rather a STA sends a broadcast out to each peered DTA individually.

Each STA in a IBSS will contain an 802.1X Supplicant and Authenticator. Thus, depending on the EAP method used, each STA in the IBSS authenticates with all peers, establishing pair-wise keys for unicast traffic and a single key for all of its broadcast traffic.

6.5.1.5 Concerns about TKIP

TKIP is seen to be overly complex by many security professionals. Complexity is the source of many security failures. TKIP relies on RADIUS and EAP to set up the master key between the STA and the AP. Current limitations with RADIUS and EAP types have resulted in a compromised security model. Although pre-authentication and QOS have recently been added to TKIP, the models are not complete, and may have implementation inconsistencies. Finally, the IBSS model is not complete, and in fact the broadcast/multicast security problem may not be solvable in TKIP.

These items along with implementation problems found in WPA development are addressed in each interaction of the 802.11I draft. There is a reasonable expectation that the IBSS and broadcast/multicast will work. The pre-authentication methods *may* be inadequate in some cases and it is still too early to know how well the QOS algorithms will work in conjunction with 802.11e.

6.5.2 Pre-TKIP—WPA

WPA is an interim security standard of the WiFi Alliance. It was extracted from a draft of IEEE 802.11i. It is TKIP without the following components:

- IBSS support
- Pre-Authentication for fast roaming support
- QOS support

WPA will present a series of challenges:

- Will TKIP ever get fielded once WPA gets a market foothold?
- If flaws are found in WPA will it impact the credibility of the WiFi Alliance and the IEEE?
- Can WPA become the proving ground for TKIP to improve its security strength and thus market success?

Both WPA and TKIP are viewed as best-effort fixes for the current RC4-based 802.11 hardware. The future for WLAN security should be CCMP.

6.6 WEP FIXES USED WITH 802.1X

Some of the issues noted earlier with 802.1x are directly addressed with TKIP.

With the current WEP, 802.1x APs and STAs are using the EAPOL-Key packet to supply the STA with WEP link broadcast/multicast keys. TKIP continues to use the EAPOL-Key packet but in a new format and in a new protocol that is resilient to attacks.

The inclusion of a replay counter and the MIC defeats all known authentication and substitution attacks. However, it must be applied to some of the WLAN MAC sublayer management frames like disassociation and reassociation in addition to data frames. TKIP does authenticate sublayer management frames where possible. This lessens the management frame attacks, but does not eliminate them.

6.6.1 CCMP—Total WEP replacement

The effort to create a WEP fix for the current hardware platforms will move on to a total replacement of WEP for new, more powerful hardware platforms. It is likely that CCMP, Counter-Mode/CBC-MAC protocol will not work on many of the current shipping cards. CCMP is AES based and many cards lack a multiply function needed by AES. Cards that have the multiply function may lack either the processing power or the memory to support AES. Thus TKIP will have a long field life and CCMP will need to interoperate with TKIP.

To this end, the changes to the management sublayer to support RSN and the key setup mechanism work with both TKIP and CCMP.

The CCMP will have a limited number of encipherment suites based on AES and a few MIC algorithms. Disagreement between WLAN vendors has hampered efforts to have only one suite.

7 ACCESS POINT ROLE AUTHENTICATION SYSTEMS

The APs play a critical role in WLAN authentication systems. This is, in part, the reason for the concern over rogue APs. Rogue APs are your classic Man-in-the-Middle. They are the best place to perform most of these attacks.

All the STA learns about its AP is the SSID it is broadcasting. A SSID is less informative than any other identity string used in networking technologies. Any network can advertise any SSID. An unsuspecting STA associating based on SSID needs other information to trust the AP to carry its data.

7.1 AP AUTHENTICATION ROLE

7.1.1 Relationship of Access Points to Authentication Servers

APs are RADIUS clients for 802.1x. An AP initiates authentication when a Station attempts to associate with it. It maps the EAP messages between EAPOL and RADIUS/EAP to allow the STA and the AS to have an authentication dialog (see section 5.2). The AP accepts the associate request after getting an Access Accept from the AS (RADIUS) server. The current defacto standard is for the AP to also receive a session key in the RADIUS Access Accept in the Microsoft vendor specific attributes (MS-MPPE-send-key and MS-MPPE-recv-key).

7.1.2 Passing authentication server information of station to the access point

As currently implemented in RADIUS, the AP and RADIUS server must share a static configured secret. RADIUS provides message integrity between its client (the AP) and the server with the message authenticator attribute that uses the shared secret. The message authenticator is described in the RADIUS RFCs 2865 and 2869.

RADIUS attributes are used by the AS to send configuration information to the AP. One example is the session key mentioned in the previous section.

7.2 AUTHENTICATION IN MULTIPLE AP RSN

7.2.1 Relationships of Access Points within an RSN for fast roaming

Fast roaming between APs within an ESN should be achievable without resorting to reauthenticating the STA whenever it associates to an AP. The STAs need a methodology to establish security associations with APs before they need to associate. Section 6.5.1.3 covers the basics for a pre-authentication mechanism with TKIP that can also be used with CCMP. For the proxy method of pre-authentication, each AP needs a list of neighboring APs and a method to forward 802.1x packets, either by MAC or IP address. This information should be acquired by the APs as part of the formation of the RSN.

7.2.2 Current model for forming an RSN

The standard approach to forming an RSN is to set each AP up as a RADIUS client. This means that all of the APs have static IP addresses and static RADIUS secrets that are entered into the RADIUS client database. 802.11f, the Inter Access Point Protocol (IAPP), adds to this by having the AP also set up as a RADIUS user. What IAPP brings to an RSN is for the APs and AS to detect a STA roaming from a rogue AP. This helps enforce the integrity of the RSN. 802.11f's initialization process also allows the AS to track an AP that does not have any STAs (802.1x traffic from an AP will identify all APs with STAs to the AS).

7.3 AN ISSUE WITH THE CURRENT RSN FORMATION MODEL

Per RFC 2865, the RADIUS clients MUST have a fixed IP address (i.e. they cannot get their address via DHCP). When applied to APs, this can significantly complicate configuring an RSN, to the point of deterring many from using it. Large enterprises that also use SNMP will not find this requirement burdensome. Moderate-size to small enterprises that currently used DHCP for their APs will resist this change.

7.3.1 A proposal for leveraging the 802.11f relationship to create an RSN

Since every AP is a RADIUS user in 802.11f, the user password could be used in an EAP exchange over IP that would establish an AP boot secret that is used by the AP and AS as the RADIUS client secret. There are a number of methods to work this and there a few proposals being developed. This would allow APs to use DHCP to get their IP address and the address of the RADIUS server (a needed DHCP attribute for this process to work).

8 SUMMARY

This paper focused on two issues concerning the security of 802.11 wireless networking. One deals with the 802.1x framework for authentication of wireless devices when they attempt to associate with an Access Point and connect to the network. The other deals with per frame encryption and integrity check (WEP) issues with the existing standards that are being addressed by the IEEE 802.11 standards committees and others.

The current 802.11 standard does not deal adequately with WLAN access control and authentication. The framework is good; 802.11 specifies the use of 802.1x and RADIUS/EAP (or other AAA protocol supporting EAP) to provide mutual authentication of the STA and the Network (AS or AAA). However, the 802.11 standards group has not provided any recommendations for a standard authentication protocol to be carried by 802.1x and RADIUS/EAP.

The only authentication protocol that supports mutual authentication and is publicly documented is EAP-TLS. Others are being talked about, including EAP-SRP (which is an algorithm using id and passwords rather than public key certificates as TLS does). There is no standards group where algorithms suitable for Wireless LANs are being worked on. An EAP working group has been established to clean up the EAP protocol description, but this group is not chartered to review EAP methods. This lack of a standards group to deal with EAP methods for 802.11 has led to a number of vendor or provider specific solutions, and a push to use solutions borrowed from other areas.

The Issues with existing per frame standards includes the well-documented and publicized problems with WEP. From the Authentication view, the most important issue is to be sure that message integrity is implemented for every packet. Without it, connections can be hijacked by impersonating the MAC address of the STA. This means that the authentication must be bound to a session key (which may be used as a WEP key, or be bound itself to a WEP key).

The combination of a need for WEP and the requirement for authentication to provide dynamic WEP keys leads to the conclusion that to provide secure connections each new wireless LAN access must be authenticated and the authentication should result in a unique shared session key. The session key is used to provide message integrity between the STA and the AP.

Access authentication is a critical part of secure wireless access. It helps with the current WEP weakness and is needed for managing secure access when a WEP replacement is available. The IEEE 802.11 group has provided a framework for access authentication and is fixing problems with WEP. For Wireless LAN authentication to be successfully rolled out, however, additional authentication protocols that work with 802.1x and EAP must also be developed and deployed. It is not yet clear how and where these authentication methods will be developed. They may be developed with support of a standards body, or they may emerge as de-facto standards based on the work of early implementers.

APPENDIX A – GLOSSARY

AAA. Authentication, Authorization and Accounting. A AAA server performs these functions, processing requests using a AAA protocol such as RADIUS.

AES. Advanced Encryption System – An encryption method based on the Rijndael algorithm that will be the basis for future wireless encryption standards.

AP. Access Point – A wireless station that also provides services such as association and distribution of frames to other station or a network.

AS. Authentication Server – A network component that performs authentication. A RADIUS server is an example of an AS.

Authenticator. 802.1X term for an entity that facilitates authentication. Access points act as authenticators.

CA. Certificate Authority – An authority that issues and manages digital security credentials such as public-key certificates.

BSS. Basic Service Set – A set of 802.11 stations that communicate with each other.

BSSID. Basic Service Set Identifier – A unique identifier for a particular BSS. In infrastructure mode, the MAC address of an access point. COPS – Common Open Policy Service – A protocol used for policy control and provisioning.

CRL. Certificate Revocation List – A list of client certificates that were revoked by the authority before they expired.

EAP. Extensible Authentication Protocol – A general protocol for authentication that supports multiple authentication mechanisms.

EAPOL. EAP Over LAN - A technique to encapsulate EAP packets in a LAN environment

IAPP. Inter-Access Point Protocol – A protocol for communicating information between access points in order to support roaming.

IEEE. Institute of Electrical and Electronics Engineers - A non-profit, technical professional association for electrical and electronics engineering.

IETF. Internet Engineering Task Force - The principal body engaged in the development of new Internet standard specifications.

LEAP. Lightweight EAP – A Cisco vendor-specific authentication method that provides mutual authentication and dynamic WEP key generation.

PKI. Public Key Infrastructure – A configuration of systems and components required
to manage and administer a public key environment.

RADIUS. Remote Authentication Dial-in User Service – a protocol used to perform authentication, authorization, and accounting (AAA).

RC4. A variable key-size stream cipher with byte oriented operations. A registered trademark of RSA Security Inc.

SLP. Service Locator Protocol – A protocol which provides a method to discover and select network services.

SRP. Secure Remote Password - A cryptographically strong authentication mechanism suitable for negotiating secure connections and performing a secure key exchange using a user-supplied password.

SSID. Service Set Identifier – An arbitrary string naming an access point or set of access points for purposes of identifying the WLAN to clients.

STA. Wireless Station – Any 802.11 device other than an AP.

Supplicant. 802.1X term for an entity that is being authenticated. Often a synonym for client, workstation, or user.

TLS. Transport Layer Security – A protocol designed to provide privacy and data integrity between two communicating applications. Specifically, EAP-TLS provides protected ciphersuite negotiation, mutual authentication, and key management.

VPN. Virtual Private Network - A method of using encryption and tunneling to securely connect users over a public network.

WEP. Wired Equivalent Privacy – An 802.11 privacy service that encrypts data sent over the wireless medium.

WLAN. Wireless Local Area Network – A network that provides the features of traditional LAN technologies such as Ethernet and Token Ring using wireless technology.

X.509. An International Telecommunications Union (ITU) standard specifying the contents of a digital certificate.

APPENDIX B – REFERENCES

draft-arkko-pppext-eap-aka-00.txt – EAP AKA Authentication

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

draft-ietf-ipsra-pic-03.txt – PIC, A Pre-IKE Credential Provisioning Protocol

draft-ietf-pppext-eap-srp-03.txt – EAP SRP-SHA1 Authentication Protocol

draft-ietf-pppext-eap-ttls-00.txt – EAP Tunneled TLS Authentication Protocol (EAP-TTLS)

draft-ietf-rap-access-bind-00.txt – Framework for Binding Access Control to COPS Provisioning

RFC 1510 – The Kerberos Network Authentication Service (V5)

RFC 2165 – Service Location Protocol

RFC 2246 – The TLS Protocol Version 1.0

RFC 2284 – PPP Extensible Authentication Protocol (EAP)

RFC 2548 – Microsoft Vendor-specific RADIUS Attributes

RFC 2716 – PPP EAP TLS Authentication Protocol

RFC 2748 – The COPS (Common Open Policy Service) Protocol

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 2945 – The SRP Authentication and Key Exchange System

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

RFC 3084 – COPS Usage for Policy Provisioning (COPS-PR)

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

ABOUT INTERLINK NETWORKS

OUR COMPANY

Interlink Networks is a leader in securing 802.11 wireless LAN, mobile, and wired networks. Our standards-based software blocks intruders' access to networks using strong 802.1x authentication. Interlink Networks' offerings range from carrier-class and enterprise level solutions to appliance-ready software—ideal for OEM development designs. 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 the leader in securing and managing access to public and private networks. By verifying user identities, blocking intruder access, and thus securing the network, we provide 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, issued the first RFP for centralized AAA (Authentication, Authorization, and Accounting) 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, and now on EAP (Extensible Authentication Protocol), which is the authentication and key distribution mechanism for 802.1x wireless LAN networks.

FOR MORE INFORMATION

Visit our web site at http://www.interlinknetworks.com, or call us at (734) 821-1200 to learn more about our software and how it can secure your network.