

White Paper

WIRELESS NETWORK SECURITY

Much attention has been focused recently on the security aspects of existing Wi-Fi (IEEE 802.11) wireless LAN systems. The rapid growth and deployment of these systems into a wide range of networks and for a wide variety of applications drives the need to support security solutions that meet the requirements of a wide variety of customers. This paper discusses traditional security methods, introduces two new enhancements that will soon improve upon WEP, focuses on some practical details of the 802.1x wireless security mechanism, addresses possible security concerns with 802.1x, and closes with a discussion of how to best secure your wireless network using Proxim ORiNOCO products with 802.1x solutions that are available today.

Traditional Security

Wireless security can be broken into two parts: Authentication and encryption. Authentication mechanisms can be used to identify a wireless client to an access point and vice-versa, while encryption mechanisms ensure that it is not possible to intercept and decode data. For many years, MAC access control lists have been used for authentication, and 802.11 WEP has been used for encryption.

Authentication

ORiNOCO access points support MAC authentication of wireless clients, which means that only traffic from authorized MAC addresses will be allowed through the access point. The ORiNOCO access point will determine if a particular MAC address is valid by checking it against either a RADIUS server external to the access point or against a database within the nonvolatile storage of the access point. This is a somewhat weak authentication mechanism because it is can be circumvented, and because authentication is unilateral.

It can be circumvented for two reasons. First, software exists to change the MAC address of some 802.11 cards. Second, authentication is tied to the hardware that a person is using and not to the identity of the user. Therefore, it could be possible to steal a legitimate user's PC and gain illegal access to a network.

Unilateral authentication means that the access point authenticates the user, but the user does not authenticate the access point. This unilateral authentication is a problem because an unsuspecting user could associate to a rogue access point and begin passing network usernames and passwords through the illegitimate access point. This would allow hacker to capture the unsuspecting user's credentials to gain access to other network resources.

Encryption

Much attention has been paid recently to the fact that Wired Equivalent Privacy (WEP) encryption defined by 802.11 is not an "industrial strength" encryption protocol. Papers by Borisov¹ and Walker² have discussed the vulnerabilities of WEP. The Fluhrer³ results have resulted in easy to mount

¹ Brewer, Borisov, et al, "802.11 Security", <http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>

² Walker, Jesse, "Unsafe at any Key Size: an analysis of the WEP encapsulation, November 2000 "

³ Fluhrer, Mantin, Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4", August 2001.

passive attacks.⁴ Despite these findings, WEP is still in general use today either because administrators are not concerned about hackers, or because the wireless network is secured by other means. Virtual Private Networking mechanisms (VPNs) are the most common means to secure wireless networks that are either using WEP encryption or no security at all.

The most recent cracks have been implemented in the above referenced AirSnort program which exploits a specific weakness within WEP: weak initialization vectors (IVs). The actual WEP key that is used to encrypt user data is combined of two parts: a 24-bit IV and a 40, 104, or 128-bit user-defined key. The IV is combined with the user key to create the key that is used to encrypt user data. The weak IV problem was solved in ORiNOCO 802.11b products soon after the weakness was discovered, and the solution was labeled ORiNOCO "WEPplus". ORiNOCO WEPplus enabled equipment chooses not to use these weak IVs during transmit cycles. The transmitting device determines IVs, and the receiving device just follows the transmitting device's instructions. This does not create any compatibility issues between ORiNOCO WEPplus equipment and other vendors less secure equipment. Because the algorithm only functions during transmit cycles, although there are no compatibility issues between ORiNOCO WEPplus and other vendors' equipment, weak-key avoidance is only fully effective if ORiNOCO products are used on both ends of the transmission. Both client and access point must use ORiNOCO radios for WEPplus to be effective in both transmit and receive directions.

Many wireless administrators elect to forgo WEP altogether and use VPN software for encryption. This option is preferable for public wireless hotspot providers that are trying to attract as many users as possible by keeping client configuration as simple as possible. Hotspot customers use VPN software to connect to their company's network. The VPN option is also preferable to many enterprise administrators because VPN solutions offer the best commercially available encryption strength. VPN software uses advanced encryption mechanisms, such as AES, so that decryption is virtually impossible.

⁴ <http://sourceforge.net/projects/airsnort>

802.11 Security Enhancements

The IEEE, the organization that created the 802.11 standard, is responsible for keeping the standard current. The IEEE membership includes many vendors that must follow a strict standards-making process and make compromises in order to agree on any final standard. This process takes a long time, so in order to address market requirements more quickly, the Wi-Fi Alliance has created a market standard called Wi-Fi Protected Access that will be implemented ahead of the 802.11i standard.

802.11i

The 802.11 Security Task Group that is creating the 802.11i standard is working to specify stronger encryption algorithms for use in 802.11 networks. Proxim is participating in this effort to ensure that our products will be compliant with the standard when it is ratified. In the current draft specification, a strengthened version of the RC-4 / per-frame encryption algorithm, and a 128-bit AES encryption algorithm are proposed. Improvements based on feedback from the cryptographic community continue to be incorporated into the draft. We expect that the IEEE 802.11i specification will be published at the end of 2003.

Wi-Fi Protected Access⁵

As an intermediate solution that can be applied to existing WLAN hardware, the Wi-Fi Alliance has adopted Wi-Fi Protected Access (WPA). Proxim will implement WPA on client and access point products and make this available in the first half of 2003.

WPA is a specification of standards-based, interoperable security enhancements that strongly increase the level of data protection and access control for existing and future wireless LAN systems. Designed to run on existing hardware as a software upgrade, Wi-Fi Protected Access is derived from, and will be forward compatible with the upcoming IEEE 802.11i standard. When properly installed, it will provide wireless LAN users with a high level of assurance that their data will remain protected and that only authorized network users can access the network. The Wi-Fi Alliance plans to begin interoperability certification testing on Wi-Fi Protected Access products starting in the first half of 2003.

Wi-Fi Protected Access was created with several goals in mind:

- A strong, interoperable security replacement for WEP
- Software upgradeable to existing Wi-Fi certified client products
- Applicable for both home and large enterprise users
- Available immediately.

To meet these goals, 802.11 authentication and encryption were improved using parts of the 802.11i standard draft.

Enhanced Data Encryption through TKIP

To improve data encryption, Wi-Fi Protected Access utilizes the Temporal Key Integrity Protocol (TKIP). TKIP provides important data encryption enhancements including a per-packet key mixing function, a message integrity check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism. Through these enhancements, TKIP addresses all of WEP's known vulnerabilities.

⁵ WECA: http://www.wi-fi.org/OpenSection/pdf/Wi-Fi_Protected_Access_Overview.pdf

Enterprise-level User Authentication via 802.1x and EAP

WEP has almost no user authentication mechanism. Wi-Fi Protected Access user authentication is implemented using 802.1x and the Extensible Authentication Protocol (EAP). Together, these technologies provide a framework for strong user authentication. This framework utilizes a central authentication server, which employs mutual authentication so that the wireless user does not accidentally join a rogue network.

Wi-Fi Protected Access and IEEE 802.11i Comparison

Wi-Fi Protected Access will be forward compatible with the IEEE 802.11i security specification currently under development. Wi-Fi Protected Access is a subset of the current 802.11i draft and uses certain pieces of the 802.11i draft that are ready to bring to market today, such as 802.1x and TKIP. The main pieces of the 802.11i draft that are not included in Wi-Fi Protected Access are secure IBSS (Ad-Hoc mode), secure fast handoff (for specialized 802.11 VoIP phones), secure de-authentication and disassociation, as well as enhanced encryption protocols such as AES-CCMP. These features are either not yet ready for market or will require hardware upgrades to implement. Proxim WPA-compliant access points will be available, and Proxim client products will be upgradeable to WPA soon after the standard is ratified.

802.1x Security Practical Details

Unlike WPA and 802.11i, 802.1x is available and is widely deployed on wireless networks today. There are three primary ways to authenticate using 802.1x: shared secrets (username/password), certificates, and SIM cards. While this paper focuses on the shared secrets method, each authentication method has advantages and disadvantages⁶ and the needs of individual deployments dictate which is used. ORiNOCO products support all three types of authentication, making it possible to retain existing authentication systems, or to maintain the most flexibility while designing new ones.

⁶ C. Ellison and B. Schneier, "Ten Risks of PKI: What You're Not Being Told About Public Key Infrastructure," <http://www.counterpane.com/pki-risks.html>.

Terms

Understanding 802.1x requires knowing the names of the different components that make up an 802.1x-secured wireless network. Figure 1 shows the location role of each one of these terms in the authentication process.

Supplicant:	End User System seeking access to the network
Authenticator:	Controls access to the network (access point)
Authentication Server (RADIUS Server)	Authenticates the end user, negotiates key material with the end user, and controls access to the network via the authenticator.
EAP:	Extensible Authentication Protocol: A secure protocol for negotiating other security protocols.
EAPOL	EAP Over LAN: The version of EAP that is used over wireless networks.
PAE	Port Access Entity. PAEs are similar to toggle switches. When the switch is open, no traffic is allowed to pass except for 802.1x traffic. After authentication is successful, the switch closes and user data is allowed to pass.

Basic Operation

The supplicant negotiates the type of security protocol to be used with the authenticator using the EAP protocol. The properties of the different protocols that can be used across EAPOL and RADIUS are outlined in Table 1. We will discuss the practical use of these protocols later. Using the negotiated protocol, the supplicant provides credentials to the authentication server, and the authentication server provides credentials to the client. After each has been authenticated to the other, the security protocol is then used to negotiate session keys, which are used to encrypt user data.

Common EAP types

*IEEE 802.1x, Port Based Network Authentication*⁷ uses the Extensible Authentication Protocol (EAP) as its authentication framework. EAP is a transport mechanism, and any defined EAP method can be used within EAP, enabling support for a wide variety of authentication credentials.

⁷ IEEE: <http://www.ieee802.org/1/files/public/docs2000/P8021XOverview.PDF>

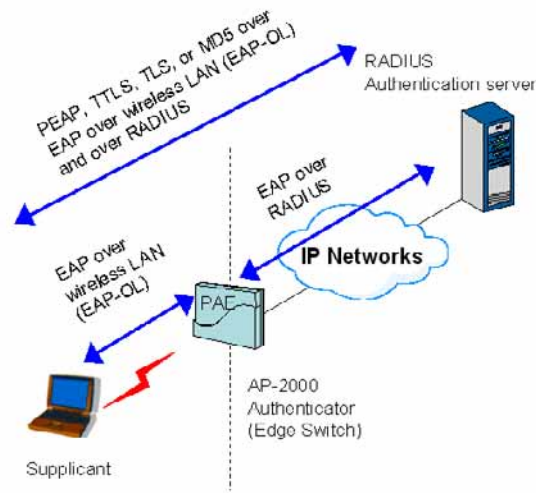


Figure 1: EAP and 802.1x

Common, standards based, non-proprietary EAP authentication methods on the market today include EAP-Transport Layer Security (TLS)⁸, EAP-Tunneled TLS (TTLS)⁹, and EAP-Protected EAP (PEAP). These methods support mutual authentication based on the two common ways to authenticate an end user or device: digital certificates and shared secrets (username/password).

EAP-PEAP is often the easiest to implement because of free client support from Microsoft, and can be just as secure as EAP-TLS if passwords are kept secure. EAP-PEAP does not require the use of client certificates.

EAP-TTLS is similar to EAP-PEAP because it does not require client certificates, but instead is based on client passwords. The disadvantage of EAP-TTLS is that it is not free: server and individual client licenses must be purchased from vendors such as Funk or Meetinghouse. EAP-TTLS became available in February of 2002¹⁰.

EAP-TLS requires certificates on both the RADIUS server and the wireless client. The distribution of certificates to each client can be challenging if the client-to-network administrator ratio is too high.

All three EAP types above have been tested deployed with ORiNOCO access points and client cards. Other EAP types have also been tested and are in use, but they are not mentioned here because their use is not widespread.

Table 1 shows that some 802.1x-based systems pass the username in the clear. In these cases, end-user anonymity is not provided. MD5 is particularly vulnerable because the username, machine name, and hashed password are sent in the clear. When a hash of the password is sent data is vulnerable to an offline dictionary attack. Any EAP type that sends either username or password in the clear is neither secure nor recommended.

⁸ Aboba, B., Simon, D., "PPP EAP TLS Authentication Protocol," IETF RFC 2716, <http://www.ietf.org/rfc/rfc2716.txt>

⁹ Funk, P., Blake-Wilson, S., "EAP Tunneled TLS Authentication Protocol (EAP-TTLS)," <http://www.ietf.org/internet-drafts/draft-ietf-pppext-eap-ttls-02.txt>

¹⁰ See <http://www.funk.com>.

EAP Type	Open/ Proprietary	Mutual Auth	Authentication Credentials		Key Material	User Name	RFC
			Supplicant	Authenticator			
MD5	Open	No	Username/Pwd	None	No	Yes	1321
TLS	Open	Yes	Certificate	Certificate	Yes	Yes	2716
TTLS	Open	Yes	Username/Pwd	Certificate	Yes	No	IETF Draft
PEAP	Open	Yes	Username/Pwd	Certificate	Yes	No	IETF Draft
SIM	Open/GSM	Yes	SIM		Yes		IETF Draft
AKA	Open/UMTS	Yes	USIM		Yes		IETF Draft
SKE	Open/CDMA	Yes			Yes		IETF Draft
LEAP	Proprietary	Yes	Username/Pwd		Yes	Yes	NA

Table 1 EAP Types

802.1x Encryption

Attacks like the one launched by AirSnort are the most troublesome for 802.11 networks, however, they are also the easiest to prevent using two common mechanisms: ORiNOCO's weak key avoidance (WEPlus), together with the key rotation mechanism built into the 802.1x standard and ORiNOCO access points, make it possible to create a secure wireless network.

In the existing pre-802.1x 802.11 specification, neither key distribution nor key rotation mechanisms are specified. With the exception of MD5, all EAP types listed in Table 1 provide a mechanism for the establishment of a session key at the station and the RADIUS server. This session key provides a secure means to periodically transport new encryption keys to the station, so that the keys used to encrypt user data can continuously and securely change.

Attacks against 802.1x

A Arbaugh¹¹ demonstrated two attacks against 802.1x-enabled wireless LAN networks: session hijacking and man-in-the-middle. In addition to the 802.1x attacks described by Arbaugh, it is possible (and more likely) that a hacker might try to use a common AirSnort attack, described earlier in this paper. If encryption with rotating keys is used, none of the attacks described here can be a threat to users of ORiNOCO clients and access points.

Session Hijacking Attack

The session hijacking attack can only be performed on systems that are using 802.1x with encryption disabled. This is not a secure configuration, and Proxim recommends that encryption is always enabled with a key rotation period of less than 30 minutes. When the hijacked session attack is attempted on the EAP-TLS system, the attacker must

1. Wait until the client has successfully authenticated to the network.
2. Send a disassociate message to the client, on the legitimate access point's behalf, using the MAC address of the access point.
3. Send frames to the valid access point, using the MAC address of the valid client.

The hijacked session attack assumes that no encryption is present, because if it were present, the radio perpetrating the attack would not be able to gain access to the network after the hijack because the access point would reject all packets that did not match an encryption key corresponding to a known user. There is not an easy way to decrypt a WEP key generated using 802.1x, so the hijacker cannot create encrypted packets. When no encryption is present, this attack will succeed, allowing the attacker to use the session until the next re-authentication interval. At the next re-authentication time, the attacker would not be re-authenticated. He would then hijack another valid session. 802.1x wireless networks deployed with encryption enabled are not susceptible to this type of attack, and therefore it is not a concern.

Man-in-the-Middle Attack

The scenario used by the attacker to implement this attack is as follows:

1. Place a special rogue access point system to be within radio range of both a valid end user and a valid access point. This rogue system has the capability to simultaneously associate with a legitimate access point, while at the same time acting as an access point itself and allowing a legitimate user to associate to it.
2. Using the rogue system, associate to a valid access point as a client station.
3. Wait for a valid user to associate to the rogue system.
4. Transparently act as a repeater between the legitimate user and the legitimate access point, passing frame received from the user to the access point and vice-versa.

As noted earlier, all EAP types except MD5 provide the ability to establish encrypted sessions. The man-in-the-middle attacker can observe this encrypted traffic, but cannot do anything malicious because it is encrypted. Encrypted traffic is not compromised by this attack and the attacker does not gain access to the network. The attacker only gains the ability to target a particular user for the denial

¹¹ Arbaugh, W., Mishra, A., "An Initial Security Analysis of the 802.1X Standard", <http://www.cs.umd.edu/%7Ewaa/1x.pdf>.

of service attack, which could be more easily perpetrated by a regular access point disconnected from any network.

When encryption is not used, the man in the middle will be able to see the user's traffic. This would have also been possible with a network sniffer. Network sniffers can see network traffic of other users, but if that traffic is encrypted, that traffic is useless to any hacker. Therefore, man-in-the-middle type attacks are not a concern.

Choosing a Security Mechanism

It is possible to compromise any security mechanism with enough brainpower, computer processing power, and time. 802.1x offers greatly increased security measures over standard 802.11 security. Maximum encryption strength today is offered by using VPN on top of a wireless network, however, 802.1x is a generally accepted method to implement wireless security in the enterprise. If a network must have the strongest encryption possible, the best solution is to use. If a more conventional and less restrictive method is appealing, use 802.1x.

Implementing 802.1x requires supplicant software on the wireless station, and a special type of RADIUS server that is capable of 802.1x authentication. Together with an 802.1x-capable wireless client and access point, they make up a complete 802.1x solution. The following ORiNOCO products will function with the 802.1x solutions that will be discussed below:

Wireless client card: Any ORiNOCO 802.11a, 802.11a/b combo, or 802.11b card
Wireless Access Point: ORiNOCO AP-600a, AP-600b, or AP-2000

Today, there are three main commercially available RADIUS server solutions. The 802.1x-capable RADIUS server can interface to other authentication servers if the username and password database resides elsewhere. Microsoft's IAS server interfaces to only to Microsoft Domain and Active Directory servers, while Funk and Meetinghouse servers interface to both Microsoft and non-Microsoft authentication databases.

Listed below are to general combinations of RADIUS servers and supplicants that are used by Proxim customers. Proxim customers are not limited to only the solutions listed below:

Solution 1: Microsoft-Centric

Reason for choice: Cost. Microsoft clients are free, and their servers are relatively affordable.

EAP type: PEAP. Microsoft only supports PEAP and TLS. TLS is unwieldy because client certificates must be installed on each machine. PEAP uses username / password authentication.

RADIUS server: Microsoft Windows 2000 Professional with Internet Authentication Server (IAS) and service pack 3 installed. IAS comes standard with Windows2000 Professional, but it must be explicitly selected during the installation process

Supplicant software: 802.1x upgrades available on Microsoft's web site for WindowsXP and Windows2000. Go to:

<http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/8021xclient.asp>

If other client support is required, Funk and Meetinghouse have feature-rich PEAP clients that work with Microsoft IAS: http://www.funk.com/radius/wlan/wlan_c_radius.asp
<http://www.mtghouse.com/products/index.shtml>

Solution 2: Non-Microsoft Centric

Reason for choice:	Performance / features. In addition to supporting Windows 98 / ME clients, non-Microsoft servers supports the widest range of password protocols and authentication databases, simplifying deployment by permitting the use of any existing authentication system for WLAN user authentication, including Active Directories, token systems, LDAP, and SQL databases.
EAP type:	TTLS. TTLS is more flexible than PEAP, and unlike TLS, it does not require client-side certificates.
RADIUS server:	Funk or Meetinghouse XP, 2k, ME, 98, Pocket PC 2002, Mac OS X, and Linux clients are available. http://www.mtghouse.com http://www.funk.com
Supplicant software:	Client software is typically licensed on a per-client basis

Conclusion

AirSnort and similar types of attacks have proven WEP security provided by the 802.11 standard insecure. The WLAN industry has responded by creating WPA and 802.11i to address these issues in the long term, though these security solutions are not available today. Most of today's security requirements can be met with 802.1x, which provides a solution that is effective and has not yet been broken. Funk, Meetinghouse, and Microsoft all offer 802.1x client and server solutions that are available today and provide security that is adequate for enterprise applications.