9 in a Series

TTLS and PEAP Comparison

by Matthew Gast

Broadly speaking, the history of 802.11 security is an attempt to address two major problems. The first problem is that the protocols used to authenticate network users were not strong, so unauthorized users could easily access network resources. Second, the Wired Equivalent Privacy (WEP) system proved insufficient for a number of well-publicized reasons. Our white paper “What’s Wrong With WEP?” discusses these in detail. In response to user concerns about weak security, the industry began developing a series of stronger protocols for use with wireless LANs. The key standard is IEEE 802.1X, which provides both stronger authentication and a mechanism for deriving and distributing stronger keys to bolster WEP.

Authentication Protocol Requirements

The dual requirement of strong encryption to prevent eavesdropping and mutual authentication to ensure that sensitive information is transmitted only over legitimate networks, must drive your wireless authentication strategy.

Exchanging user authentication credentials over a wireless network must be done with great care because traffic interception is much easier. Attackers require physical access to the network medium to intercept transmissions, but radio waves cannot easily be confined to a physical facility. Without the security of a direct physical connection, cryptographic safeguards must be built into the protocols for two reasons. First, and most obvious, is to prevent attackers from recovering user credentials as they travel over the radio link. Secondly, unauthorized "rogue" access points may be set up in an attempt to collect credentials from unsuspecting users. Cryptography can provide the necessary assurance that users are connecting to an authorized and secured network.

802.1X is based on the Extensible Authentication Protocol (EAP), and so it offers the choice of several methods to protect authentication exchanges. In practice, authentication methods based on the IETF's well-known Transport Layer Security (TLS) standard can satisfy strict encryption and authentication requirements. Three TLS-based protocols have been developed for use with EAP and are suitable for deployments with wireless LANs: EAP-Transport Layer Security (EAP-TLS), Tunneled Transport Layer Security (TTLS), Protected EAP (PEAP).

EAP-TLS

EAP-TLS uses the TLS handshake as the basis for authentication. TLS itself has many attributes that make it attractive for security-related use. It is well documented and has been analyzed extensively, and cryptanalysis of the protocol has not yet revealed significant weaknesses in the protocol. TLS performs authentication by exchanging digital certificates. The server presents a certificate to the client. After validating the server's certificate, the client presents a client certificate. Naturally, the certificate should be protected on the client by a passphrase, PIN, or stored on a smart card, depending on the implementation.

The central role of certificates is the Achilles heel of EAP-TLS. If no PKI exists, it must be deployed before EAP-TLS can be used in a network. Certificate management is a time-consuming and cumbersome administrative task, especially because certificates must be revoked as users lose access to the wireless network. In addition to issuing certificates, on-line validity checks are mandatory. Furthermore, an existing PKI may be insufficient because most EAP-TLS implementations require the presence of certain attributes that were not defined when early PKI systems were rolled out. A final risk is that EAP-TLS by itself protects the user's authentication material, but not the user identity. The bottom line is that EAP-TLS is secure, but the requirement for client certificates is a large hurdle that makes TTLS and PEAP attractive.

TLS Tunneling with TTLS and PEAP

Both TTLS and PEAP use the inherent privacy of the TLS tunnel to safely extend older authentication methods, such as username/password or token card authentication, to the wireless network. Both are two-stage protocols that establish a strongly encrypted "outer" TLS tunnel in stage one and then exchange authentication credentials through an "inner" method in stage two. Both TTLS- and PEAP-capable RADIUS servers can be used with existing authentication systems. RADIUS proxy abilities can extend existing databases, directories, or one-time password systems for use with wireless LANs.

TTLS uses the TLS channel to exchange "attribute-value pairs" (AVPs), much like RADIUS. The flexibility of the AVP mechanism allows TTLS servers to validate user credentials against nearly any type of authentication mechanism. TTLS implementations today support all methods defined by EAP, as well as several older methods (CHAP, PAP, MS-CHAP and MS-CHAPv2). PEAP uses the TLS channel to protect a second EAP exchange, called the "inner" EAP exchange. Most supplicants support EAP-MS-CHAPv2 for the inner exchange, which allows PEAP to use external user databases. Other common EAP methods supported by PEAP supplicants are EAP-TLS and generic token card (EAP-GTC).

PEAP's major advantage is support from Microsoft, and therefore, built-in support from the operating system. PEAP support is a standard feature in Windows XP and available as a Microsoft feature pack for Windows 2000. Microsoft supplicants (wireless clients) are tightly integrated with the base operating system and can therefore provide single sign on capabilities by using the same user credentials for both Windows sign-on and wireless LAN authentication. Microsoft supplicants, however, do not support the use of token cards. Cisco PEAP supplicants do support EAP-GTC, but Cisco and Microsoft have implemented PEAP in different ways that are not compatible.

Recommendations

Secure wireless LAN deployments require PKI to be deployed in a supporting role. Certificates are used to establish a secure authentication channel in any case. One of the first decisions to be made is whether the cost of issuing client certificates is one worth accepting. In many cases, an existing PKI can be used to support a wireless LAN deployment. Organizations which have not already deployed PKI should consider TTLS or PEAP instead, with an appropriate inner authentication method.

Table: Comparison of TLS authentication methods

	TLS	TTLS	PEAP
Specification	RFC 2716	Internet-Draft, 11/2002	Internet-Draft, 3/2003
Software			
Client implementations	Cisco, Funk, Meetinghouse, Microsoft, Open1X (open source)	Funk, Meetinghouse	Cisco, Microsoft, Funk, Meetinghouse
Supported client platforms	Linux, Mac OS X,Windows 95/98/ME, Windows NT/2000/XP, Mac OS X	Linux, Mac OS X, Windows 95/98/ME, Windows NT/2000/XP	Linux, MacOS X, Windows
Authentication server implementations	Cisco ACS, Funk Odyssey, Interlink Secure.XS, Meetinghouse AEGIS, Microsoft IAS, FreeRADIUS	Funk, Meetinghouse, Interlink	Cisco ACS, Microsoft IAS, Interlink Secure.XS, Meetinghouse, Funk
Authentication methods	X.509 Certificates only	CHAP, PAP, MS-CHAP, MS-CHAPv2, and EAP methods	EAP methods; commonly MS-CHAPv2, generic token card, and EAP-TLS
Protocol operations			
Basic protocol structure	Establish TLS session and validate certificates on both client and server	Two phases: (1) Establish TLS between client and TTLS server (2) Exchange attribute-value pairs between client and server	Two parts: (1) Establish TLS between client and PEAP server (2) Run inner EAP exchange over TLS tunnel
Fast session reconnect	No	Yes	Yes
WEP integration	Yes; generated by RADIUS server and passed through MS-MPPE attributes		
PKI/Certificates			
Server certificate	Required	Required	Required
Client certificate	Required	Optional	Optional
Verification	Certificate chain validation; OSCP is supported by the protocol		
Effect of private key compromise	Re-issue all certs	Re-issue all server certificates and new CA cert	
Client and user auth			
Authentication direction	Mutual: digital certificates both ways	Mutual: Certificate to client, tunneled method for client	Mutual: Certificate to client, tunneled method for client
Protection of user identity	No	Yes	Yes