Q&A

PROTECTED EXTENSIBLE AUTHENTICATION PROTOCOL

This document answers questions about Protected Extensible Authentication Protocol.

OVERVIEW

Q. What is Protected Extensible Authentication Protocol?

A. Protected Extensible Authentication Protocol (PEAP) is an 802.1X authentication type for wireless LANs (WLANs). PEAP provides strong security, user database extensibility, and support for one-time token authentication and password change or aging. PEAP is based on an Internet Draft (I-D) submitted by Cisco Systems®, Microsoft, and RSA Security to the IETF. Glen Zorn was the Cisco Systems® lead engineer and coauthor of this I-D.

Q. Is PEAP supported by the Cisco Unified Wireless Network, Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2)?

A. Yes. The Cisco Unified Wireless Network supports several EAP authentication types, including PEAP. Like all EAP types, PEAP can be used with WPA and WPA2 networks.

Q. What is the Cisco Unified Wireless Network?

A. The Cisco Unified Wireless Network is the industry's only unified wired and wireless solution to cost-effectively address the WLAN security, deployment, management, and control issues facing enterprises. This powerful solution combines the best elements of wireless and wired networking to deliver scalable, manageable, and secure WLANs with a low total cost of ownership. It includes innovative RF capabilities that enable real-time access to core business applications and provides proven enterprise-class secure connectivity. The Cisco Unified Wireless Network delivers the same level of security, scalability, reliability, ease of deployment, and management for wireless LANs that organizations expect from their wired LANs.

The Cisco Unified Wireless Network supports an enterprise-ready, standards-based, wireless security solution that gives network administrators' confidence that their data will remain private and secure when they use Cisco wireless products, Cisco Aironet Series products, Cisco Compatible Extensions products or Wi-Fi Certified WLAN client devices. This enterprise-class wireless security solution supports robust wireless LAN security services that closely parallel the security available in a wired LAN. It fulfills the need for consistent, reliable, and secure mobile networking by delivering industry-leading WLAN security services. It mitigates sophisticated passive and active WLAN attacks, interoperates with a range of client devices and provides reliable, scalable, centralized security management. The Cisco Unified Wireless Network allows network administrators to deploy large-scale enterprise WLANs with scalable problem-free security administration that does not increase the burden on the IT staff.

Q. Is PEAP a standard?

A. Not yet. PEAP is based on an I-D submitted to the IETF. Cisco, Microsoft, and RSA Security are actively involved in the IETF standards body supporting a standardized PEAP implementation.

Q. Where can I find information about the PEAP draft proposed to the IETF?

A. Please visit the IETF I-D Search Engine and search for "PEAP."

FEATURES AND BENEFITS

Q. What are the security benefits of PEAP?

A. PEAP provides the following security benefits:

- Relies on Transport Layer Security (TLS) to allow nonencrypted authentication types such as EAP-Generic Token Card (GTC) and One Time Password (OTP) support
- Uses server-side Public-Key Infrastructure (PKI)-based digital certification authentication
- Allows authentication to an extended suite of directories, including Lightweight Directory Access Protocol (LDAP), Novell NDS, and OTP databases
- Uses TLS to encrypt all user-sensitive authentication information
- Supports password change at expiration
- Does not expose the logon user name in the EAP identity response
- Is not vulnerable to dictionary attacks
- Provides dynamic privacy protection when used in conjunction with Temporal Key Integrity Protocol (TKIP) or the Advanced Encryption Standard (AES)

Q. What are the enterprise benefits of PEAP?

A. PEAP is based on server-side EAP-TLS. With PEAP, organizations can avoid the issues associated with installing digital certificates on every client machine as required by EAP-TLS; instead, they can select the methods of client authentication, such as logon passwords or OTPs, that best suit their corporate needs.

DEPLOYMENT

Q. How does PEAP authentication work?

A. PEAP works in two phases:

- In Phase 1, server-side TLS authentication is performed to create an encrypted tunnel and achieve server-side authentication in a manner similar to Web server authentication using Secure Sockets Layer (SSL), a popular and trusted security method. Once Phase 1 of PEAP is established, all data is encrypted, including all user-sensitive information.
- The framework for PEAP Phase 2 authentication is extensible, and the client can be authenticated using methods such as EAP-GTC and Microsoft Challenge Authentication Protocol (MS-CHAP) Version 2 within the TLS tunnel.

Q. What Cisco wireless products support PEAP?

A. A variety of Cisco wireless products support PEAP including: Cisco Aironet autonomous and lightweight access points, Cisco wireless LAN controllers and Cisco Aironet client devices. Cisco Compatible client devices running Cisco Compatible Extensions version 4 or later also support PEAP.

Q. What client operating systems support PEAP?

A. PEAP support is available on Microsoft Windows 2000, Windows XP, and Windows CE. Visit the Cisco Aironet WLAN client software product bulletin Web page for the latest software information and guidelines to enable PEAP on a client machine.

Q. Is PEAP authentication available on wireless clients from vendors other than Cisco?

A. Yes. PEAP authentication is allowed from any PEAP-enabled supplicants that comply with the proposed PEAP IETF I-D. Cisco encourages customers to verify support and interoperability with vendors before starting installation.

Q. Can I install both PEAP client software from Cisco and PEAP client software from Microsoft on my machine?

A. PEAP client software from Cisco is complementary to PEAP client software from Microsoft. Users may choose to install either of these PEAP implementations on their client machines. When the Cisco PEAP supplicant is installed on a client machine, it completely replaces any existing MS-CHAP Version 2 PEAP supplicant on the machine.

Q. Can I use client certificate authentication with PEAP?

A. PEAP is based on server-side EAP-TLS. Client certificate authentication is not required—only the server is authenticated using certificates.

Q. Does PEAP provide single-login to Windows domains for passwords or OTP?

A. PEAP is compatible with single-login, which is a function of the client supplicant. Single-login function may be available with third-party utilities. The Windows PEAP supplicant (PEAP/MS-CHAPv2) supports single sign-on. Cisco's PEAP/GTC supplicant does not support single sign-on.

Q. How does silent session resume work during a PEAP session?

A. PEAP supports silent session resume (also known as Fast Reconnect) when only Phase 1 of PEAP is executed. In Phase 2, the previous authentication state is reused. Users are not required to reauthenticate until the PEAP session timeout expires. The PEAP session timer is independent of the RADIUS session timer, which is used to control the volatility of dynamic encryption keys with EAP.

Q. Can I use PEAP with LDAP or Novell NDS databases?

A. Yes. PEAP provides interoperability with both LDAP and Novell NDS.

Q. Where can I learn more about deploying PEAP?

A. Please read the Protected Extensible Authentication Protocol Application Note to learn more about deploying PEAP.

Q. Where can I learn more about deploying secure WLANs?

A. Please read the following documents to learn more about deploying secure WLANs:

- Wireless LAN Security White Paper
- Cisco Aironet Technical References
- Deployment Guide: Configuring the Cisco Wireless Security Suite

Q. Where can I learn more about WLAN security?

A. Please read the Cisco Wireless LAN Security brochure to learn more about WLAN security.

EAP TYPE COMPARISONS

Q. What is the difference between the Microsoft PEAP supplicant and the Cisco PEAP supplicant?

A. Both supplicants support PEAP, but each supports different methods of client authentication through the TLS tunnel. The Microsoft PEAP supplicant supports client authentication by only MS-CHAP Version 2, which limits user databases to those that support MS-CHAP Version 2, such as Windows NT Domains and Active Directory. The Cisco PEAP supplicant supports client authentication by OTPs and logon passwords, enabling support for OTP databases from vendors (such as RSA Security and Secure Computing Corporation) and logon password databases (such as LDAP and Novell NDS) as well as Microsoft databases. In addition, the Cisco PEAP client includes the ability to hide user name identities until the TLS encrypted tunnel is established. This provides additional confidentiality that user names are not being broadcast during the authentication phase.

Q. What are the differences between PEAP, EAP-Flexible Authentication via Secure Tunneling (FAST), Cisco LEAP, and EAP-TLS?

A. Table 1 provides a summary comparison of PEAP, EAP-FAST, Cisco LEAP, and EAP-TLS.

Table 1. PEAP, EAP-FAST, Cisco LEAP and EAP-TLS Comparison Chart

	PEAP with Generic Token Card (GTC)	PEAP with Microsoft Challenge Authentication Protocol (MS-CHAP) Version 2	EAP-FAST	Cisco LEAP	EAP-TLS
User Authentication Database and Server	OTP, LDAP, Novell NDS, Windows NT Domains, Active Directory	Windows NT Domains, Active Directory	Windows NT Domains, Active Directory, LDAP (limited)	Windows NT Domains, Active Directory	OTP, LDAP, Novell NDS, Windows NT Domains, Active Directory
Requires Server Certificates	Yes	Yes	No	No	Yes
Requires Client Certificates	No	No	No	No	Yes
Operating System Support	*Driver*: Windows XP, Windows 2000, Windows CE* *With third-party utility*: Other OS**	*Driver*: Windows XP, Windows 2000, Windows CE *With third-party utility*: Other OS**	*Driver*: Windows XP, Windows 2000, Windows CE*** With third-party utility: Other OS**	*Driver*: Windows 98, Windows 2000, Windows NT, Windows Me, Windows XP, Mac OS, Linux, Windows CE, DOS	*Driver*: Windows XP, Windows 2000, Windows CE *With third-party utility*: Other OS
Application-Specific Device (ASD) Support	No	No	Yes	Yes	No
Credentials used	Client: Windows, Novell NDS, LDAP password; OTP or token Server: Digital certificate	Windows password	Windows password, LDAP user ID/password (manual provisioning required for Pac provisioning)	Windows password****	Digital certificate
Single Sign-On Using Windows Login	No	Yes	Yes	Yes	Yes

	PEAP with Generic Token Card (GTC)	PEAP with Microsoft Challenge Authentication Protocol (MS-CHAP) Version 2	EAP-FAST	Cisco LEAP	EAP-TLS
Password Expiration and Change	No	Yes	Yes	No	–
Works with Fast Secure Roaming	No	No	Yes	Yes	No
Works with WPA and WPA2	Yes	Yes	Yes	Yes	Yes

* PEAP/GTC is supported on Cisco Compatible Version 2 clients and above.

** Greater operating system coverage is available with Meetinghouse and Funk supplicants.

*** Cisco Aironet 350 Series WLAN client devices and Cisco Aironet 5 GHz 54 Mbps Wireless LAN Client Adapters (CB20A) support EAP-FAST on Windows XP, Windows 2000, and Windows CE operating systems.

**** Requires strong passwords. Read more at: Cisco Response to Dictionary Attacks on Cisco LEAP.

FOR MORE INFORMATION

For more information about the Cisco Unified Wireless Network, visit: http://www.cisco.com/go/unifiedwireless

For more information about Cisco Aironet products, visit: http://www.cisco.com/go/aironet

Read the Cisco Wireless LAN Security brochure at:
http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps430/ps4076/prod_brochure09186a00801f7d0b.html

For more information about EAP-FAST, visit:
http://www.cisco.com/en/US/products/hw/wireless/ps430/products_qanda_item09186a00802030dc.shtml

For more information about Cisco LEAP, visit:
http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps430/prod_qas0900aecd801764f1.shtml

For more information about 802.11i, WPA and WPA2, visit:
http://www.cisco.com/en/US/prod/collateral/wireless/ps5678/ps430/prod_qas0900aecd801e3e59.shtml

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.