

## CISCO RESPONSE TO DICTIONARY ATTACKS ON CISCO LEAP

Cisco® Aironet® products support a variety of IEEE 802.1X extensible authentication protocol (EAP) authentication types including Cisco LEAP, Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), EAP-Transport Layer Security (EAP-TLS), and Protected Extensible Authentication Protocol (PEAP). This document discusses offline dictionary attacks against Cisco LEAP in detail and provides mitigation strategies for securing wireless environments against possible dictionary attacks involving Cisco LEAP.

### OVERVIEW

Cisco LEAP is supported by a broad range of wireless LAN (WLAN) client adapters and devices, including Cisco Aironet Series products and Cisco Compatible Extensions client devices. Cisco LEAP is a mutual authentication algorithm that supports dynamic derivation of session keys. With Cisco LEAP, mutual authentication relies on a shared secret, the user's logon password—which is known by the client and the network, and is used to respond to challenges between the user and the Remote Authentication Dial-In User Service (RADIUS) server.

### ISSUE

At DEFCON, on August 1, 2003, a presentation explored mechanisms that could make it easier for someone to write a tool to launch an offline dictionary attack on password-based authentications that leverage Microsoft MS-CHAP, such as Cisco LEAP. The same tool was also demonstrated on October 1, 2003 at Unstrung's live event in New York. The source code of the dictionary attack tool called "asleep" was released on April 6, 2004.

During a dictionary attack, variations of passwords are used to compromise a user's authentication credentials. This is not a new attack or new vulnerability of Microsoft MS-CHAP or Cisco LEAP. Most password-based authentication algorithms are vulnerable to dictionary attacks in the absence of a strong password policy.

The most effective way to militate against dictionary attacks is to create a strong password policy. Since 2001, Cisco Systems® has recommended that its customers employ a strong password policy for protection from dictionary attacks. Cisco discussed Cisco LEAP's vulnerability to dictionary attacks in the [Cisco SAFE Wireless LAN Security White Paper](#), originally published in 2001. (Please refer to the "Standard EAP with TKIP WLAN Design" section, specifically Table 2.)

## DEFINING A DICTIONARY ATTACK

Most password-based authentication algorithms are susceptible to online (active) and offline (passive) dictionary attacks. During a dictionary attack, an attacker tries to guess a user's password and gain network access by using every "word" in a dictionary of common passwords or possible combinations of passwords. A dictionary attack relies on the fact that a password is often a common word, name, or concatenation of words or names with a minor modification such as a trailing digit or two. Longer passwords with a variety of characters (such as 4yosc10cP!) offer the greatest protection against dictionary attacks.

During an online dictionary attack, an attacker tries to actively gain network access by trying possible combinations of passwords for a specific user. Online dictionary attacks can be prevented using lockout mechanisms available on RADIUS servers to lock out the user after a certain number of invalid login attempts. Online attacks also provide some visibility (RADIUS server logs for failed login attempts, etc.) that a breach or compromise is being attempted, allowing for corrective measures to be taken.

An offline dictionary attack, such as the tool that was introduced at DEFCON and Unstrung's event, is carried out in two phases to uncover the user's password. In the first phase, the attacker captures the challenge-response messages between the user and the access network. In the second phase, the attacker looks for a password match by computing a list of possible challenge-response messages (using a pre-computed dictionary) and comparing these messages against the captured challenge-response message. The attacker uses known authentication protocol vulnerabilities to reduce the size of the user password dictionary. Using a strong password policy and periodically expiring user passwords significantly reduces an offline attack tool's success. Unlike online attacks, offline attacks are not easily detected.

### Offline Dictionary Attack Against MS-CHAP

With Cisco LEAP, users are authenticated to an access point via a password. This password is authenticated against a back-end RADIUS server. Below is the Cisco LEAP challenge-response protocol used during authentication.

1. The wireless client sends an authentication request.
2. The access point relays the authentication request to the RADIUS server.
3. The RADIUS server acknowledges the client's request and sends an 8-byte challenge.
4. The wireless client computes a response:
  - a. The password is hashed with MD4. A 16-byte hash is produced.
  - b. The hash is padded with 5 nulls. 21 bytes are produced.
  - c. The resulting 21 bytes are split into 7-byte units.
5. DES encrypts the challenge as plain-text with the 7-byte unit as the key.
6. The resulting cipher text is concatenated producing 24 bytes.
7. The resulting 24 bytes are sent from the wireless client to the server as the challenge-response.
8. The RADIUS server MD4 hashes the stored NT hash for the user (user's password is MD4 hashed twice) and repeats steps 4-7 to calculate the expected client response.
9. If the client and RADIUS responses match authentication is complete.

The optimization used by the dictionary attack tool focuses on step 4b above. The last 2 bytes of the hash are padded with nulls. This means that there are only 2 characters to brute force in the last 7 bytes. This radically reduces the number of DES encryptions that must be performed. Each character is 1 byte or 256 bits, so the maximum number of DES encryptions that have to be performed is 65,536.

In order for this dictionary attack tool to work, the word must be in the dictionary and the MD4 hash precomputed. If the user has a non-dictionary word for passwords, the likelihood of the tool being able to crack the password is greatly reduced.

By including a special character in the password (especially if this special character is not the first or last character), the overhead of the attack is greatly increased, requiring the attacker to precompute the dictionary to conform to the password policy and then create the MD4 hashes for these generated dictionaries.

Another description of an offline dictionary attack is in this [DEFCON Presentation](#).

Another perspective on offline dictionary attacks can be found in the SecurityFocus BugTraq e-mail [Cisco LEAP Insecurities + POC](#) dated October 3, 2003.

## DICTIONARY ATTACK MITIGATION

To help our customers respond to the possibility of dictionary attacks, Cisco strongly recommends that all of our customers to review their security policies and institute the previously published best practices that are outlined below and in the [Cisco SAFE White Papers](#).

- Use a strong password policy (as detailed below) and periodically expire user passwords (recommended at least every three months) giving users advanced warning to change passwords before they expire.
- If unable to implement a strong password policy, consider migrating to another EAP type like EAP-FAST, PEAP or EAP-TLS whose authentication methods are not susceptible to dictionary attacks:
  - EAP-FAST is an authentication protocol that creates a secure tunnel without using certificates.
  - PEAP is a hybrid authentication protocol that creates a secured TLS tunnel between the WLAN user and the RADIUS server to authenticate the user to the network.
  - EAP-TLS uses pre-issued digital certificates to authenticate a user to the network.

**Note:** PEAP and EAP-TLS require certificate and public key infrastructure (PKI) management on both RADIUS servers and WLAN clients. Migration to these EAP types from Cisco LEAP requires careful planning, testing, and execution.

Additional information about implementation requirements for EAP-FAST and PEAP is provided later in this document.

## KEEPING YOUR WIRELESS NETWORK SECURE

Cisco LEAP is a secure 802.1X EAP authentication solution when used in conjunction with a strong password policy. Our customers can confidently deploy and continue to use Cisco LEAP which provides robust, enterprise-class, wireless LAN security services that closely parallel the security available in a wired LAN, by implementing a strong password policy. Cisco LEAP advantages over other 802.1X types include:

- Minimal requirements on the client device, or host system (critical for PDAs and several handheld devices)
- Support for a broad range of operating systems including Windows, Mac OS, Windows CE, MS-DOS, and Linux
- Deployment and operational simplicity

## IMPLEMENTING STRONG PASSWORD POLICIES

Instructing users to select strong passwords is one of the most effective means to mitigate the possibility of a successful dictionary attack. On a Windows host, it is possible to implement password complexity rules to force users to choose strong passwords, which are more difficult for hackers to determine. Some characteristics of strong passwords include:

- A minimum of 10 characters
- A mixture of uppercase and lowercase letters
- At least one numeric character (0-9) or non-alphanumeric characters (example: !#@&)
- Use at least one special character within the password—not at the beginning or end
- No form of the user's name or user ID
- A word that is not found in the dictionary (domestic or foreign)
- Randomly generated passwords

Here are some examples of strong passwords:

- 4yosc10cP!, from “for your own safety choose ten character Password!”
- cnw84Fri\*YAD, from “cannot wait for Friday”

Additional information about creating and managing strong passwords can be found in [Appendix A](#).

## CISCO SECURE ACCESS CONTROL SERVER PASSWORD ENFORCEMENT

Cisco Secure Access Control Server (ACS) has built-in mechanisms designed to enforce password complexity, similar to the Windows mechanisms. Most users who use Cisco LEAP will need to make these changes on their Windows servers, but if you are storing Cisco LEAP passwords in Cisco Secure ACS, apply the precautions as noted in the [Cisco Secure Access Control Server for Windows System Configuration: Basic User Guide](#) to help ensure that your users are selecting better passwords.

## EAP-FAST IMPLEMENTATION

EAP-FAST is a nonproprietary EAP type that offers flexible, easy deployment and management. It supports a variety of user and password database types, supports server-initiated password expiration and change, and does not require digital certificates. Implementing EAP-FAST does not require infrastructure changes.

Cisco submitted an informational draft to the Internet Engineering Task Force (IETF) for EAP-FAST on February 8, 2004. Cisco developed EAP-FAST for customers who want to deploy an 802.1X EAP type that does not use certificates and provides protection from dictionary attacks. For example, a customer using Cisco LEAP who cannot enforce a strong password policy and does not want to use certificates can migrate to EAP-FAST for protection from dictionary attacks. For more information about EAP-FAST, read the [EAP-FAST Q&A](#).

Migration from Cisco LEAP to EAP-FAST is simple because EAP-FAST does not require client or server certificates:

- Client devices—Easy migration from Cisco LEAP to EAP-FAST for Cisco Aironet client adapters is aided by the Cisco Aironet Configuration Administration Tool or the Cisco Aironet Client Administration Utility where IT administrators can define a new profile for EAP-FAST and bundle client configuration, firmware, driver, and Cisco Aironet Client Utility together or use the Cisco Aironet Installation Wizard files. EAP-FAST is available for Cisco Aironet 350 Series and Cisco Aironet 5 GHz 54 Mbps Series (Cisco Aironet CB20A) client adapters on computers running Windows 2000 or Windows XP with Cisco Aironet Windows Installation Wizard Software Release 1.3. EAP-FAST is also available for Cisco Aironet 350 Series client adapters on computers running Windows CE 3.0 (PPC 2002 or PPC 2003) or Windows CE .NET 4.2 with Cisco Aironet Software Release 2.50 for Windows CE.
- Access points—Cisco Aironet Series access points running Cisco IOS® Software version 12.2(11)JA or later have native support for EAP-FAST built in.
- AAA server—Customers using the Cisco Secure ACS need to upgrade to version 3.2.3 to support EAP-FAST.

### PEAP IMPLEMENTATION

PEAP is a form of EAP that uses TLS tunnels to protect the authentication challenge and response messages between the WLAN user and the RADIUS server. Migrating to PEAP requires the use of a PKI and may require more administration than Cisco LEAP installations. PEAP is described in more detail in the [Cisco SAFE: Wireless LAN Security in Depth](#) white paper.

Migration from Cisco LEAP to PEAP requires the following planning, testing, and deployment procedures:

- Define the solution components involved:
  - WLAN clients and client operating system (PEAP supplicant support)
  - Infrastructure support (RADIUS infrastructure with PEAP support)
- Identify migration scope and migration goals:
  - Decide if only PEAP user authentication will be implemented or if both PEAP user and PEAP machine authentication will be implemented
- Identify changes to existing client management, EAP deployment, troubleshooting tools and procedures.

Table 1 outlines the client operating system and RADIUS support requirements for different PEAP implementations.

**Table 1** PEAP Implementation Requirements

PEAP Supplicant	Client Operating Systems Supported	RADIUS Servers Supported
Microsoft PEAP supplicant (PEAP/MS-CHAPv2)	Windows 2000, XP, PPC 2002, and Windows CE 4.1/4.2	Cisco Secure ACS 3.2, Funk Odyssey Server, and Interlink RADIUS server
Cisco PEAP supplicant (PEAP/GTC)	Windows 2000, XP, and PPC 2002	Cisco Secure ACS 3.2, Funk Odyssey Server, and Interlink RADIUS server
Meetinghouse supplicant (both PEAP/GTC and PEAP/MS-CHAPv2)	Windows 98 SE, ME, NT4, 2000, XP, PPC 2002, CE.NET 4.1/4.2, MAC OS X, and Linux (Red-Hat 8 and 9)	Cisco Secure ACS 3.2, Funk Odyssey Server, and Interlink RADIUS server
Funk supplicant (PEAP/MS-CHAPv2)	Windows 98, ME, 2000, XP, and PPC platforms	Cisco Secure ACS 3.2, Funk Odyssey Server, and Interlink RADIUS server

PEAP migration procedure:

- Phase 1: Lab testing of functionality and solution verification
- Phase 2: Implement changes to management, deployment, and troubleshooting tools/procedures (for Cisco LEAP to PEAP migration and PEAP support)
- Phase 3: Limited migration (deploy to subset of user community to identify and address unanticipated deployment issues)
- Phase 4: Wide-scale migration from Cisco LEAP to PEAP

#### **ADDITIONAL INFORMATION**

Cisco Systems is continuously working to enhance wired and wireless LAN security in conjunction with our partners and standards bodies.

To learn more about dictionary attacks on Cisco LEAP read the [Cisco Security Notice: Dictionary Attack on Cisco LEAP](#) from Cisco TAC.

For further guidance on wireless LAN security best practices, refer to section 5.2.2 of the [802.11 Wireless LAN Security White Paper](#).

For more information on EAP authentication types such as Cisco LEAP, EAP-FAST, PEAP, and EAP-TLS and additional deployment information, please refer to [Cisco Aironet Technical References](#).

#### **APPENDIX A: PASSWORD CREATION AND MANAGEMENT INFORMATION**

##### **Reviewing The Strength Of User Passwords**

The most common way to check for weak passwords is to use a password recovery and auditing tool such as LC4 or John the Ripper (<http://www.openwall.com/john/>). Password strength should be checked regularly, even with password complexity enabled. User accounts with weak passwords should be expired and the users notified when their weak passwords are cracked.

##### **LC4**

New password auditors will find the LC4 password recovery and auditing tool easy to use. An optional Wizard helps users navigate through the process of configuring and running a password audit, letting them choose from preconfigured quick, common, strong, or custom configurations. Extensive documentation explains potential complications to keep password audits from becoming frustrating.

## PASSWORD-GENERATION UTILITIES AND TOOLS

To help create stronger passwords, many companies and individuals have released tools that help administrators and users generate strong passwords. These tools can be used by individuals who cannot select a strong password on their own or by companies as standard policy. In general, it is better if a user can select a strong password using sound guidelines such as those outlined within this document. When users generate their own passwords, they're less likely to write the password down or document it anywhere but in their memory.

If the guidelines detailed in this document to create strong passwords do not reflect your current password policy, you can either use password-generation utilities to create passwords that reflect the policy or update the policy.

### Selecting a Password Generator Tool

Select a password generator tool that provides an effective source of entropy, or the amount of bits that are used for seeding functions. For example, a password generator that uses the timer as a source of entropy, such as a low-quality random number generator, is not suitable for generating hard-to-guess passwords. The dictionary attack on this type of password is based on guessing the time of password generation rather than a particular word. This type of password is not suitable for secure environments. The source of entropy should also be clearly defined. A tool that does not include its source of entropy may have unknown security weaknesses. You must be able to examine how the entropy functions to verify its quality.

The tool should provide passwords that are not sent in the clear or unencrypted. Unencrypted passwords are no longer secret by the time they are received. The tool should also support all the parameters necessary to make the generated passwords compliant with your password policy (minimum length, special characters, and a mixture of upper- and lowercase characters).

## ADDITIONAL TOOLS TO ENFORCE STRONG PASSWORD POLICIES

Other tools are available to assist administrators in enforcing password policies and password complexity. Below are links to tools that were found using a simple Google search. Cisco does not endorse these tools, but is providing these links as examples of technology to enforce strong passwords.

- LCZ Password Defender  
<http://www.littlecatz.com/password.html>
- Anixis Password Policy Enforcer  
<http://www.anixis.com/products/ppe/default.htm?anixispid=0A1004>

## ADDITIONAL INFORMATION ON PASSWORD COMPLEXITY

The following links address the importance of password complexity:

- Sans Institut Password Policy

[http://www.sans.org/resources/policies/Password\\_Policy.pdf](http://www.sans.org/resources/policies/Password_Policy.pdf)

- Atomic Quilogy: Password Strength Matters

<http://atomic.quilogy.com/default.aspx?storyId=pwd>

- Microsoft TechNet: Best Practice Guide for Securing Active Directory Installations and Day-to-Day Operations: Part I

<http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/activedirectory/maintain/bpguide/part1/adsecp1.msp>

#### **ADDITIONAL INFORMATION ON CHOOSING STRONG PASSWORDS**

Below is a list of Websites that discuss how to choose strong passwords.

- Microsoft: How to Create Stronger Passwords

<http://www.microsoft.com/security/articles/password.asp>

- Folder Password Expert: Creating a Strong Password

<http://www.folder-password-expert.com/h-4-strong-password.html>

#### **OTHER REFERENCES**

- United States Military Academy: An overview of wireless attacks

[http://www.itoc.usma.edu/Documents/ITOC\\_TR-2003-101\\_\(G6\).pdf](http://www.itoc.usma.edu/Documents/ITOC_TR-2003-101_(G6).pdf)

- University of Freiburg: A critical look at MSCHAPv2 and associated vulnerabilities

[http://mopo.informatik.uni-freiburg.de/pptp\\_mschapv2/](http://mopo.informatik.uni-freiburg.de/pptp_mschapv2/)

- Kismet: Wireless war driving utilities to help locate rogue access points

<http://kismetwireless.net/>

- Wellenreiter: A war driving utility to help locate rogue access points

<http://www.wellenreiter.net/>

- Hewlett Packard Labs: Wireless tools for Linux

[http://www.hpl.hp.com/personal/Jean\\_Tourrilhes/Linux/Tools.html](http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html)

- The Unofficial 802.11 Security Web Page

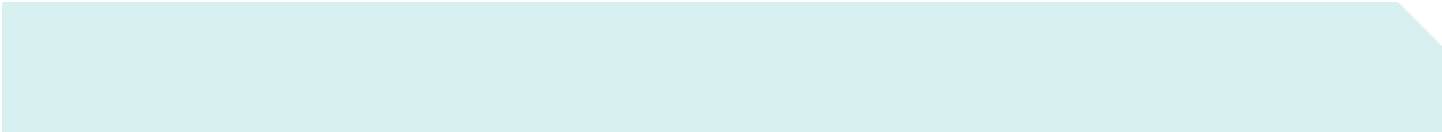
<http://www.drizzle.com/~aboba/IEEE/>

- DEFCON Presentation

<http://home.jwu.edu/jwright/presentations/asleap-defcon.pdf>

- Center for Password Sanity: Paper on the password dilemma

<http://www.smat.us/sanity/pwdilemma.html>





Corporate 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: 408 526-4100

European Headquarters  
Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
www-europe.cisco.com  
Tel: 31 0 20 357 1000  
Fax: 31 0 20 357 1100

Americas Headquarters  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-7660  
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

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the  
**Cisco Web site at [www.cisco.com/go/offices](http://www.cisco.com/go/offices)**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus  
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland  
Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland  
Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden  
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

All contents are Copyright © 1992–2004 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, the Cisco Systems logo, and Aironet are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.  
(0403R) 204113\_ETMG\_LS\_12.04