

CHAP or ARAP With TACACS+: Interoperability Problems With One–Time Password Systems

Document ID: 13880

Introduction

Prerequisites

Requirements

Authentication Method

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

There is a fundamental conflict between the crypto challenge authentication technology that Challenge Handshake Authentication Protocol (CHAP) and AppleTalk Remote Access Protocol (ARAP) use and the one–time token technology that Security Dynamics and other firms use.

Prerequisites

Requirements

There are no specific requirements for this document.

Authentication Method

Under normal circumstances (fixed passwords located either on the local router database or on a Terminal Access Controller Access Control System (TACACS+) server), the authentication method is as this list shows:

1. The Network Access Server (NAS) generates a challenge, which is a large random number, and sends it to the client who dials in.
2. The client takes the challenge and appends the secret (the password) to the challenge.
3. The client hashes the resulting string with Message Digest Algorithm 5 (MD5).

The result is a 128–bit hash that is sent back to the NAS. It is computationally unfeasible to find a second input that maps to the same output or to deduce the original message from just the digest and challenge.

4. The NAS uses the challenge that it sends the client to look up the secret for this particular user. The NAS can find the secret locally or it can query the TACACS+ server using the SENDPASS message. Either way, the cleartext version of this password must be transferred to the NAS. In order to generate the correct response, the NAS then takes the challenge, appends the secret, and hashes the resulting string using MD5. It compares the response from the client to the correct response and allows or denies access to the client.

The main point in this description of the authentication process is that the NAS must have access to the cleartext version of the secret. This is where the one–time password (OTP) technology used by Security Dynamics and other vendors interferes. There is no way for the server to produce the particular token which

is, in effect, at any given time. Thus, the Security Dynamics Incorporated (SDI) server cannot answer the SENDPASS message from the NAS, and the NAS cannot proceed with the CHAP or ARAP verification of the client's response. Generally, an OTP server cannot provide the secret because, in an effort to eliminate the lack of time synchronization between the OTP server and the token, an entire list of allowable tokens exists at any given point in time.

There is no resolution to the conflict between crypto challenge authentication technology and OTP. A fundamental change is necessary to the authentication protocol to accommodate OTPs, and this change is beyond Cisco's control.

Workarounds to resolve the conflict are possible. The most obvious one is incorporated in the NAS and referred to as the single-line workaround. It includes both the username and the OTP in the username field of the response. Since the username is passed in cleartext (only the challenge response is encrypted), it can be parsed into two parts: the username and the OTP. If the NAS can parse the input and then issue a login authentication, as opposed to a SENDPASS, the response can be taken from the server, and client access can be denied or allowed. This works because the only answer that is expected with a login is a yes or a no. The server does not need to send us the secret because we do not need to verify the CHAP or ARAP response. This workaround used to be available in XTACACS, but when Authentication, Authorization, and Accounting (AAA) was introduced with TACACS, this functionality was not carried over.

Another workaround is to implement the intelligence into the SDI server. When the SDI server gets an ARAP authentication request, it can parse the username into the two components and verify or deny the user. SDI has not implemented this workaround.

The last workaround is to upgrade both the OTP server and the NAS to support the new revision of the TACACS+ protocol specification. The new revision incorporates the SENDAUTH message type. The SENDAUTH request includes the entire challenge and response from the client so that it is now the responsibility of the OTP server to verify the client's response. By eliminating SENDPASS, the OTP server no longer needs to send the cleartext version of the password; therefore, bypassing the inherent limitations of OTP technology. The OTP server can compare the client's response to the list of allowable responses and tell the NAS whether the authentication should be allowed or denied.

Cisco IOS® Software Release 11.2 implements the SENDAUTH functionality. SDI does not have a daemon that supports the new revision of the TACACS+ protocol specification.

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

Related Information

- **Terminal Access Controller Access Control System (TACACS+)**
 - **Technical Support & Documentation – Cisco Systems**
-

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Jul 24, 2007

Document ID: 13880
