Challenge-Handshake Authentication Protocol

In computing, the **Challenge-Handshake Authentication Protocol** (**CHAP**) is an authentication protocol originally used by Point-to-Point Protocol (PPP) to validate users. CHAP is also carried in other authentication protocols such as RADIUS and Diameter.

Almost all network operating systems support PPP with CHAP, as do most network access servers. CHAP is also used in PPPoE, for authenticating DSL users.

As the PPP sends data unencrypted and "in the clear", CHAP is vulnerable to any attacker who can observe the PPP session. An attacker can see the user's name, CHAP challenge, CHAP response, and any other information associated with the PPP session. The attacker can then mount an offline dictionary attack in order to obtain the original password. When used in PPP, CHAP also provides protection against replay attacks by the peer through the use of a challenge which is generated by the authenticator, which is typically a network access server.

Where CHAP is used in other protocols, it may be sent in the clear, or it may be protected by a security layer such as Transport Layer Security (TLS). For example, when CHAP is sent over RADIUS using User Datagram Protocol (UDP), any attacker who can see the RADIUS packets can mount an offline dictionary attack, as with PPP.

CHAP requires that both the client and server know the clear-text version of the password, although the password itself is never sent over the network. Thus when used in PPP, CHAP provides better security as compared to Password Authentication Protocol (PAP) which is vulnerable for both these reasons.

Benefits of CHAP

When the peer sends CHAP, the authentication server will receive it, and obtain the "known good" password from a database, and perform the CHAP calculations. If the resulting hashes match, then the user is deemed to be authenticated. If the hashes do not match, then the users authentication attempt is rejected.

Since the authentication server has to store the password in clear-text, it is impossible to use different formats for the stored password. If an attacker were to steal the entire database of passwords, all of those passwords would be visible "in the clear" in the database.

As a result, while CHAP can be more secure than PAP when used over a PPP link, it prevents more secure storage "at rest" than with other methods such as PAP.

Variants

MS-CHAP is similar to CHAP but uses a different hash algorithm, and allows for each party to authenticate the other.

Working cycle

CHAP is an authentication scheme originally used by Point-to-Point Protocol (PPP) servers to validate the identity of remote clients. CHAP periodically verifies the identity of the client by using a three-way handshake. This happens at the time of establishing the initial link (LCP), and may happen again at any time afterwards. The verification is based on a shared secret (such as the client's password).[1]

1. After the completion of the link establishment phase, the authenticator sends a "challenge" message to the peer.
2. The peer responds with a value calculated using a one-way hash function on the challenge and the secret combined.
3. The authenticator checks the response against its own calculation of the expected hash value. If the values match, the authenticator acknowledges the authentication; otherwise it should terminate the connection.
4. In PPP, the authenticator may send a new challenge at random intervals to the peer and repeats steps 1 through 3. However, when CHAP is used in most situations (e.g. RADIUS), this step is not performed.

CHAP packets

Description	1 byte	1 byte	2 bytes	1 byte	Variable	Variable
Challenge	Code = 1	ID	Length	Challenge length	Challenge value	Name
Response	Code = 2	ID	Length	Response length	Response value	Name
Success	Code = 3	ID	Length		Message	
Failure	Code = 4	ID	Length		Message	

The ID chosen for the random challenge is also used in the corresponding response, success, and failure packets. A new challenge with a new ID must be different from the last challenge with another ID. If the success or failure is lost, the same response can be sent again, and it triggers the same success or failure indication. For MD5 as hash the response value is `MD5(ID||secret||challenge)`, the MD5 for the concatenation of ID, secret, and challenge.[2]

See also

Wikibooks has a book on the topic of: ***Network Plus Certification/Security/User Authentication***

- List of authentication protocols
- Password Authentication Protocol
- Challenge–response authentication

- Cryptographic hash function

References

1. *Forouzan (2007). Data Communications & Networking 4E Sie (https://books.google.com/books?id=6HaNKmfBK1oC&pg=PA352) . McGraw-Hill Education (India) Pvt Limited. pp. 352–. ISBN 978-0-07-063414-5. Retrieved 24 November 2012.*
2. *"Understanding and Configuring PPP CHAP Authentication" (http://www.cisco.com/en/US/tech/tk713/tk507/technologies_tech_note09186a00800b4131.shtml) . Cisco tech note. 2005. Retrieved 2011-08-14.*

External links

- RFC 1994 (https://datatracker.ietf.org/doc/html/rfc1994) PPP Challenge Handshake Authentication Protocol (CHAP)
- RFC 2865 (https://datatracker.ietf.org/doc/html/rfc2865) Remote Authentication Dial In User Service (RADIUS): *uses PAP or CHAP*
- RFC 3748 (https://datatracker.ietf.org/doc/html/rfc3748) Extensible Authentication Protocol (EAP): *discusses CHAP*

WIKIPEDIA