Password Authentication Protocol

Password Authentication Protocol (**PAP**) is a password-based authentication protocol used by Point-to-Point Protocol (PPP) to validate users.[1] PAP is specified in RFC 1334 (https://datatracker.ietf.org/doc/html/rfc1334) .

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

As the Point-to-Point Protocol (PPP) sends data unencrypted and "in the clear", PAP is vulnerable to any attacker who can observe the PPP session. An attacker can see the users name, password, and any other information associated with the PPP session. Some additional security can be gained on the PPP link by using CHAP or EAP. However, there are always tradeoffs when choosing an authentication method, and there is no single answer for which is more secure.

When PAP is used in PPP, it is considered a weak authentication scheme. Weak schemes are simpler and have lighter computational overhead than more complex schemes such as Transport Layer Security (TLS), but they are much more vulnerable to attack. While weak schemes are used where the transport layer is expected to be physically secure, such as a home

DSL link. Where the transport layer is not physically secure a system such as Transport Layer Security (TLS) or Internet Protocol Security (IPsec) is used instead.

Other uses of PAP

PAP is also used to describe password authentication in other protocols such as RADIUS and Diameter. However, those protocols provide for transport or network layer security, and therefore that usage of PAP does not have the security issues seen when PAP is used with PPP.

Benefits of PAP

When the client sends a clear-text password, the authentication server will receive it, and compare it to a "known good" password. Since the authentication server has received the password in clear-text, the format of the stored password can be chosen to be secure "at rest". If an attacker were to steal the entire database of passwords, it is computationally infeasible to reverse the function to recover a plaintext password.

As a result, while PAP passwords are less secure when sent over a PPP link, they allow for more secure storage "at rest" than with other methods such as CHAP.

Working cycle

PAP authentication is only done at the time of the initial link establishment, and verifies the identity of the client using a two-way handshake.

1. Client sends username and password. This is sent repeatedly until a response is received from the server.
2. Server sends authentication-ack (if credentials are OK) or authentication-nak (otherwise)[2]

PAP packets

Description	1 byte	1 byte	2 bytes	1 byte	Variable	1 byte	Variable
Authentication-request	Code = 1	ID	Length	Username length	Username	Password length	Password
Authentication-ack	Code = 2	ID	Length	Message length	Message		
Authentication-nak	Code = 3	ID	Length	Message length	Message		

PAP packet embedded in a PPP frame. The protocol field has a value of C023 (hex).

Flag	Address	Control	Protocol (C023 (hex))	Payload (table above)	FCS	Flag

See also

- SAP – Service Access Point

Notes

1. *"Password Authentication Protocol (PAP)" (https://www.geeksforgeeks.org/password-authentication-protocol-pap/) . GeeksforGeeks. 2018-07-17. Retrieved 2020-11-08.*
2. *Forouzan (2007). Data Commn & 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.*

References

- Lloyd, Brian; Simpson, William Allen (1992). "Password Authentication Protocol" (https://datatracker.ietf.org/doc/html/rfc1334#page-2) . *PPP Authentication Protocols* (https://datatracker.ietf.org/doc/html/rfc1334) . IETF. p. 2. doi:10.17487/RFC1334 (https://doi.org/10.17487%2FRFC1334) . RFC 1334 (https://datatracker.ietf.org/doc/html/rfc1334) . Retrieved 16 July 2015.

This computer networking article is a stub. You can help Wikipedia by expanding it (https://en.wikipedia.org/w/index.php?title=Password_Authentication_Protocol&action=edit) .