David Simma, Sebastian Rimml

CHAP (Challange Handshake Authentication Protocol)

Kurz zusammengefasst wurde Chap dazu entwickelt, um die Sicherheitsrisiken seinen vorgängers PAP zu verringern. CHAP ist ein Authentifizierungsverfahren, das auf das PPP (Point-to-Point) Protocol basiert. Grundsätzlich wird CHAP verwendet, um sich in ein Computernetzwerk einzuwählen und sich zu authentifizieren.

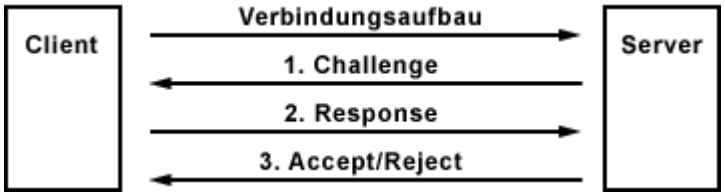
PPP

PPP basiert auf dem HDLC (High-Level Data Link Control) und ist der Nachfolger des SLIP (Seriel Line Internet) Protocol. Es wird verwendet, um den Verbindungsaufbau über Wählleitungen zu ermöglichen.

PAP

Im Unterschied zu CHAP wird bei PAP das Passwort für die Authentifizierung nicht verschlüsselt, sondern zusammen mit der Benutzerkennung übertragen. Dadurch können die mitgeschickten Daten von einer *man-in-the-middle-attack* ausgelesen werden.

Ablauf der Authentifizierung



Verbindungsaufbau

Bevor eine Authentifizierung des Clients gestartet werden kann, muss eine Verbindung mit diesem eröffnet werden.

1. Challenge

Der Server überträgt an den Client einen zufälligen Wert (Challenge). Mit der Grundlage dieses Wertes muss sich der Client in folgenden Schritten authentifizieren.

2. Response

Aufgrund der erhaltenen Challenge setzt der Client jetzt seine Response zusammen. Nach dem Passwort selbst wird die Challenge hinzugefügt. Die neue Zeichenkette wird mittels einer Einweg-HASH-Funktion verschlüsselt und im Anschluss an den Server gesendet.

3. Accept / Reject

Der Server errechnet sich aus dem im Klartext gespeicherten Passwort und der Challenge ebenfalls die Zeichenkette und verschlüsselt diese mit der gleichen Methode. Sollte der erhaltene Hash mit dem selbst berechneten übereinstimmen, so ist die Authentifizierung erfolgreich. Andernfalls wird die Verbindung mit dem Client abgelehnt.

Worin besteht die Sicherheit?
Ein Angreifer, welcher die Kommunikation zwischen Client und Server mithört erhält lediglich die Challenge selbst und die endgültig gehashte Zeichenkette. Das Passwort wird nie in Klartext übertragen.

Sollte jedoch ein Man-In-The-Middle-Angriff gestartet werden, kann das Passwort unter bestimmten Umständen in Erfahrung gebracht werden. Sollte der Client sowohl PAP als auch CHAP anbieten, könnte der Angreifer dem Client vorspielen, es handle sich um eine PAP-Verbindung anstelle einer CHAP-Verbindung. Dieser sendet nun das Passwort mit angehängter Challenge unverschlüsselt an den Angreifer. Dieser muss also im Folgeschluss nur noch die Verschlüsselungsmethode erraten und kann somit den gesamten Datenverkehr zwischen Server und Client mithören.

Lösung:
Der Client sollte auf einem aktuellen Stand der Technik gehalten werden. Bei neueren Clients wird die PAP-Verbindung nicht mehr unterstützt, da diese als Unsicher gilt. Bei älteren Geräten kann unter Umständen die Verbindungsmöglichkeit deaktiviert werden.