CHAP (Challenge-Handshake Authentication Protocol)

CHAP je autentizační protokol, který pravidelně ověřuje identitu vzdáleného klienta pomocí „třícestného podání ruky“. Na rozdíl od staršího protokolu PAP (Password Authentication Protocol), který posílal heslo v čitelném textu, CHAP využívá kryptografické **hashování**.

Tento protokol je definován v normě RFC 1994 a je klíčový pro zabezpečení vytáčených spojení (dial-up), virtuálních soukromých sítí (VPN) a úložišť typu iSCSI.

Jak CHAP funguje (Třícestné podání ruky)

Proces ověření probíhá bezpečně díky tomu, že obě strany (klient i server) znají stejné heslo (tzv. „shared secret“), ale nikdy si ho navzájem nepošlou.

```
1. **Výzva (Challenge):** Server vygeneruje náhodný řetězec dat (tzv. nonce) a pošle ho klientovi.
2. **Odpověď (Response):** Klient vezme tuto výzvu, spojí ji se svým heslem a pomocí hashovací funkce (obvykle MD5) vypočítá výsledek (hash). Tento hash pošle zpět serveru.
3. **Ověření (Verification):** Server provede stejný výpočet (má k dispozici stejnou výzvu i heslo klienta). Pokud se výsledek serveru shoduje s hashem od klienta, potvrdí autentizaci.
```

Klíčové vlastnosti a výhody

- **Ochrana proti odposlechu:** Protože se po síti posílá pouze hash a náhodná výzva, útočník nemůže z těchto dat zpětně získat původní heslo.
- **Ochrana proti opakování útoku (Replay Attack):** Výzva je pokaždé jiná (náhodná). I kdyby útočník zachytil odpověď klienta, nemůže ji použít při příštím přihlášení, protože příští výzva bude vyžadovat jiný hash.
- **Průběžné ověřování:** Server může poslat výzvu klientovi kdykoliv během trvání spojení, aby se ujistil, že nebyl klient nahrazen útočníkem.

Srovnání: PAP vs. CHAP

Vlastnost	PAP	CHAP
Přenos hesla	Čitelný text (Plaintext).	Pouze hash (jednosměrný otisk).
Bezpečnost	Velmi nízká.	Vysoká (standard pro P2P).
Opakování výzvy	Pouze při navazování spojení.	Kdykoliv během spojení.
Nároky na CPU	Minimální.	Vyšší (kvůli výpočtům hashe).

MS-CHAP: Varianta od Microsoftu

Microsoft vyvinul vlastní verzi **MS-CHAP**, která se často používá v sítích Windows a VPN (PPTP).

- **MS-CHAP v2** je vylepšená verze, která umožňuje **vzájemnou autentizaci** – nejen server ověřuje klienta, ale i klient si ověří, že komunikuje se správným serverem.

Související pojmy: SSL/TLS, VPN, Hashování, MD5, Man-in-the-Middle, IP adresa, Autentizace.