Handshake (Informatika a Sítě)

Handshake (v doslovném překladu „potřesení rukou“) je v informatice a telekomunikacích automatizovaný proces vyjednávání, ke kterému dochází mezi dvěma zařízeními nebo programy těsně předtím, než mezi nimi začne probíhat plnohodnotná komunikace.

Cílem tohoto procesu je stanovit pravidla, podle kterých bude přenos dat probíhat. Zařízení si během „potřesení rukou“ vzájemně sdělí, jakou rychlostí dokážou komunikovat, jaké protokoly podporují, jakou formu šifrování použijí a vzájemně se synchronizují. Bez úspěšného dokončení tohoto procesu nemůže být spojení navázáno.

TCP Three-Way Handshake

Nejznámějším příkladem tohoto procesu je tzv. trojcestný handshake (Three-way handshake), který je absolutním základem protokolu TCP (Transmission Control Protocol). Tento protokol pohání drtivou většinu dnešního internetu (načítání webových stránek, stahování souborů, e-maily).

Aby se zabránilo ztrátě dat v chaotickém prostředí sítě, musí se klient (např. váš webový prohlížeč) a server (např. webová stránka) nejprve synchronizovat pomocí tří kroků:

1. Krok: SYN (Synchronize) Klient odešle serveru paket s nastaveným příznakem SYN. Tímto krokem klient žádá o navázání spojení a sděluje serveru své počáteční sekvenční číslo, které bude používat pro sledování pořadí odeslaných dat.

2. Krok: SYN-ACK (Synchronize-Acknowledge) Server přijme požadavek a odpoví paketem, který má nastavené oba příznaky (SYN i ACK). Server tímto krokem potvrzuje přijetí klientova požadavku (ACK) a zároveň posílá klientovi své vlastní počáteční sekvenční číslo (SYN), aby byla komunikace obousměrná.

3. Krok: ACK (Acknowledge) Klient obdrží odpověď od serveru a odešle zpět finální potvrzovací paket (ACK). Tím serveru potvrzuje, že obdržel jeho sekvenční číslo. Spojení je v tuto chvíli plně navázáno (ESTABLISHED) a může začít samotný a spolehlivý přenos užitečných dat.

TLS / SSL Cryptographic Handshake

Zatímco TCP handshake řeší pouze spolehlivost spojení, v moderním internetu je nutné komunikaci také zabezpečit. K tomu slouží TLS (Transport Layer Security) handshake, který následuje bezprostředně po dokončení TCP handshake a tvoří základ zabezpečeného protokolu HTTPS.

Během TLS handshake probíhá komplexní kryptografické vyjednávání. Klient zašle zprávu „ClientHello“, ve které nabídne seznam šifrovacích algoritmů (Cipher Suites), které podporuje. Server z nich vybere ten nejbezpečnější, odpoví zprávou „ServerHello“ a zašle klientovi svůj digitální certifikát (obsahující veřejný klíč) k ověření identity.

Následně obě strany pomocí složité matematiky (např. Diffie-Hellmanovy výměny klíčů) vygenerují

sdílený symetrický klíč. Tento klíč se pak používá k rychlému a bezpečnému šifrování veškerých dat, která si klient a server následně vyměňují. Tím je zajištěno, že ani případný útočník odposlouchávající síť nepřečte přenášená data.

Hardwarový Handshake

Ačkoliv je dnes pojem spojován primárně se sítěmi a softwarem, historicky (a v průmyslu dodnes) existuje i hardwarový handshake. Tento koncept se používá například u sériových linek (rozhraní RS-232) nebo starých modemů.

V hardwarovém pojetí se používají fyzické vodiče, kterými si zařízení posílají elektrické signály jako RTS (Request to Send - Žádost o odeslání) a CTS (Clear to Send - Připraveno k příjmu). Tím starší a pomalejší zařízení (např. tiskárna) signalizovalo počítači, aby dočasně zastavil tok dat, dokud tiskárna nezpracuje plný buffer (paměť).

Související pojmy: TCP/IP, TLS/SSL, HTTPS, SYN paket, Paket, Kryptografie, Síťový protokol, Šifrování, RS-232.