

Síťová bezpečnost a TLS

Síťová bezpečnost je soubor opatření, technologií a pravidel určených k ochraně integrity, důvěrnosti a dostupnosti dat při jejich přenosu počítačovou sítí. V dnešním otevřeném prostředí internetu je základním předpokladem bezpečnosti protokol **TLS** (Transport Layer Security).

1. Protokol TLS (Transport Layer Security)

TLS je nástupcem staršího protokolu SSL (Secure Sockets Layer). Jeho úkolem je vytvořit šifrovaný „tunel“ mezi klientem (prohlížečem) a serverem.

Protokol zajišťuje tři základní věci:

- **Šifrování:** Data jsou pro útočníka na síti nečitelná.
- **Autentizace:** Pomocí certifikátů máte jistotu, že komunikujete se skutečným serverem (např. vaší bankou), a ne s podvodníkem.
- **Integrita:** Kontrola, zda data nebyla během cesty záměrně či náhodou modifikována.

2. Jak funguje TLS Handshake

Navázání bezpečného spojení (Handshake) probíhá v několika krocích:

1. ****Client Hello:**** Prohlížeč pošle serveru seznam podporovaných šifer.
2. ****Server Hello + Certifikát:**** Server pošle svůj digitální certifikát (obsahující jeho veřejný klíč).
3. ****Ověření:**** Prohlížeč ověří u certifikační autority (CA), zda je certifikát platný.
4. ****Výměna klíče:**** Strany si pomocí `[[it:sec:cryptography|asymetrické kryptografie]]` vymění dočasný ****symetrický klíč****.
5. ****Šifrovaný přenos:**** Veškerá další data se již šifrují rychlejší symetrickou šifrou (např. AES).

3. Vrstvy síťové bezpečnosti

Síťová bezpečnost se neomezuje jen na šifrování, ale využívá několik obranných prvků:

- **Firewall:** Brána, která filtruje příchozí a odchozí provoz na základě definovaných pravidel.
- **IDS/IPS (Intrusion Detection/Prevention System):** Systémy, které analyzují síťový provoz a hledají známky útoku (např. skenování portů).
- **VPN (Virtual Private Network):** Vytváří bezpečné šifrované spojení i v rámci nedůvěryhodných sítí (veřejné Wi-Fi).

4. Digitální certifikáty a CA

Aby asymetrická kryptografie fungovala, musíme věřit, že veřejný klíč patří danému webu. K tomu slouží:

- **Certifikační autorita (CA):** Důvěryhodné instituce (např. Let's Encrypt, DigiCert), které podepisují certifikáty webů.
- **HTTPS:** Kombinace protokolu HTTP a TLS. Symbol zámku v prohlížeči značí, že spojení je zabezpečeno platným certifikátem.

5. Nejčastější útoky na síťové vrstvě

- **Man-in-the-Middle (MitM):** Útočník se vklíní mezi klienta a server a odposlouchává komunikaci. TLS tomuto útoku brání pomocí autentizace.
- **DDoS (Distributed Denial of Service):** Zahltí síť nebo server obrovským množstvím požadavků, čímž ho vyřadí z provozu.
- **Sniffing:** Pasivní odposlech nešifrovaných dat (např. v protokolech HTTP, FTP, Telnet).

Související články:

- [Kryptografie a šifrování](#)
- [Model OSI a síťové vrstvy](#)
- [Správa hesel a MFA](#)

Tagy: security network tls ssl https firewall ddos encryption

From:
<https://serviceit.cz/> - IT ENCYKLOPEDIE

Permanent link:
https://serviceit.cz/doku.php?id=it:sec:network_security

Last update: **2026/01/02 13:28**

