..

HTTPS a TLS (Detailní pohled)

HTTPS (Hypertext Transfer Protocol Secure) je bezpečným rozšířením protokolu HTTP. Šifrování, které HTTPS využívá, je zajištěno protokolem **TLS** (Transport Layer Security).

Ačkoliv se stále běžně používá zkratka **SSL**, jde o označení historického předchůdce, který je dnes již z bezpečnostních důvodů zakázán.

Architektura TLS

Protokol TLS se skládá ze dvou hlavních vrstev:

- **TLS Handshake Protocol:** Umožňuje serveru a klientovi se navzájem autentizovat a dohodnout se na šifrovacích algoritmech a klíčích dříve, než jsou odeslána jakákoliv data.
- **TLS Record Protocol:** Zajišťuje samotný bezpečný přenos dat a kontrolu jejich integrity pomocí dohodnutých klíčů.

Evoluce: TLS 1.2 vs. TLS 1.3

Přechod na verzi 1.3 (standardizovanou v roce 2018) přinesl největší revoluci v bezpečnosti webu za 20 let.

Klíčové změny v TLS 1.3:

- **Odstranění slabých šifer:** Byly odstraněny algoritmy jako MD5, SHA-1, RC4 nebo DES.
- **Perfect Forward Secrecy (PFS):** V TLS 1.3 je PFS povinné. To znamená, že i když útočník v budoucnu získá soukromý klíč serveru, nemůže zpětně dešifrovat dříve zachycenou komunikaci.
- **Zrychlení (1-RTT):** Odstraněním nadbytečných zpráv se zkrátila doba navazování spojení na polovinu.

Digitální certifikáty a PKI

Základem důvěry v HTTPS je **PKI** (Public Key Infrastructure). Server prokazuje svou identitu pomocí certifikátu.

Typy certifikátů podle ověření:

- **DV (Domain Validation):** Nejběžnější (např. Let's Encrypt). Ověřuje se pouze kontrola nad doménou.
- **OV (Organization Validation):** Autorita ověřuje i existenci firmy.

- **EV (Extended Validation):** Nejpřísnější ověření. V minulosti zobrazovaly prohlížeče zelený pruh s názvem firmy.

Co obsahuje certifikát:

- **Subject:** Název domény (Common Name).
- **Public Key:** Veřejný klíč serveru použitý pro výměnu klíčů.
- **Issuer:** Název autority, která certifikát podepsala.
- **Validity:** Datum, odkdy dokdy certifikát platí.

Zabezpečení hlavičkami (HSTS)

Samotné HTTPS nestačí, pokud se útočník pokusí uživatele „shodit“ na nešifrované HTTP (tzv. Downgrade attack). K tomu slouží:

> **HSTS (HTTP Strict Transport Security):** Speciální hlavička, kterou server říká prohlížeči: „Příští rok se ke mně připojuj výhradně přes HTTPS. Ignoruj jakékoliv pokusy o HTTP spojení.“

— **Viz také:** 1-RTT, QUIC, HTTP/3, Digitální podpis