MI-PB-17

Šifrované síťové protokoly a útoky proti nim, certifikáty identity.

SSL/TLS

Množina kryptografických protokolů, které poskytují bezpečnou komunikaci po internetu na úrovni trapsportní vrstvy.
SSL zastaralý, nahrazen TLS

Vrstvy: Nad protokolem transportní vrstvy (TCP/UDP) je nízkoúrovňový TLS Record, nad kterým jsou TLS protokoly vyšší úrovně

- Nižší:
  - **TLS Record Protocol:**
    - Rozklad a skládání paketů vyšší úrovně do rámců, volitelně komprese, šifrování (symetrická šifra), MAC (klíčovaný hash)
    - Komprese: volitelná, bezztrátová, výstupem je struktura `TLSCompressed`
    - Šifrování: `TLSCompressed` je vstupem do volitelné šifry/MAC -- výpočet MAC, následné šifrování.
      - Lze využít proudové šifry (RC4, ChaCha20), blokové šifry (AES CBC nebo AEAD -- Authenticated Encryption with Associated Data)
- Vyšší:
  - **Handshake Protocol:**
    - Zřízení session s parametry:
      - session ID: identifikace stavu aktivní nebo obnovitelné session
      - certifikát protistrany
      - kompresní algoritmus
      - specifikace šifry
      - master secret (sdílené mezi serverem a klientem)
      - resumable flag: lze sesison použít i pro nová připojení?
    - Zprávy:
      - **ClientHello:** první zpráva poslaná klientem, spuštění procesu domluvy (session ID, seznam kryptografických a kompresních možností klienta)
      - **ServerHello:** Server zvolí metody ze senamů v ClientHello, odpoví klientovi

        - **ServerCertificate:** Pokud zvolená metoda používá certifiáty, pošle server svůj certifikát
        - **ServerKeyExchange:** poslána, pokud ServerCertificate neobsahuje dost dat ke zřízení premaster secret
        - **Certificate Request:** Neanonymní server může požadovat certifikát od klienta
        - **Server Hello Done:** indikace dokončení všech "hello" zpráv od serveru
        - **Client Certificate:** Pokud server požádal, klient odešle certifikát
        - **Client Key Exchange:** Nastavení premaster secret
        - **Certificate Verify:** Ověření klientského certifikátu
        - **Finished:** Ověření, že zřízení klíče a autentizace byly úspěšně dokončeny
    - **Alert Protocol:**
        - Posílání informací o chybách a varováních v session
        - Každá zpráva má úroveň a číslo chyby:
            - "fatální": obě strany uzavřou spojení a zapomenou session ID, klíče a tajemství, session nelze obnovit
            - "varování": session může pokračovat, ale pokud si to příjemce nepřeje, může odeslat fatální chybu a session ukončit
    - **Change Cipher Spec Protocol:**
        - 1 typ zprávy - signalizace změny šifrování
        - Zpráva poslána klientem i serverem
    - **Application Data Protocol**

Typický scénář na webu: Server se serverovým certifikátem, anonymní klient
Serverový certifiát:

- self-signed: prohlížeč uživatele upozorní na nedůvěryhodnost
- vystaven důvěryhodnoou CA: dražší, šifrování+autentizace

Útoky na SSL/TLS

Útoky na protokol:

- Využití slabin v protokolu nebo jím používané kryptografii
- Prolomení vlastností, které by protokol měl zajišťovat
- Nezávislé na implementaci
- **Zranitelnost POODLE:**
    - Padding Oracle On Downgraded Legacy Encryption

    - Útok na zarovnání zpráv v CBC
- **Zranitelnost DROWN:**
    - Decrypting RSA with Obsolette and Weakened eNcryption
    - Využití Padding Oracle v kombinaci s RC2 a RC4 -- útok na RC4 pomocí padding oracle umožňuje postupně dešifrovat zprávu šifrovanou RSA
- **Zranitelnost SWEET:**
    - Útok na blokové šifry s 64b blokem
    - Využití narozeninového paradoxu -- pokud v ŠT vytvořeném CBC nalezneme 2 stejné bloky $\check{S}T_i, \check{S}T_j$, pak díky CBC platí $OT_i \oplus OT_j = \check{S}T_{i-1} \oplus \check{S}T_{j-1}$ -- oba OT lze dohledat statistickou analýzou

Útok na implemenaci protokolu:

- Mnoho implementací neúplných nebo nesprávných
- **Zranitelnost FREAK:**
    - Factoring RSA Export Asymmetric Keys
    - Omezená délka klíče exportní RSA (512 b)
    - *(exportní šifra -- šifra dost slabá na to, aby mohla být v devadesátých letech exportována z USA)*
    - Vynucení exportních šifer při MITM -- servery stále podporují nepoužívané exportní šifry

Útok na služby nad protokolem:

- **Zranitelnost Heartbleed:**
    - Heartbeat: mechanismus ověření, zda je spojení stále funkční
    - Nesprávná kontrola vstupů: knihovna odeslala požadovaný počet bytů nezávisle na tom, kolik přijala -- nadbytečné byty obsahovaly hodnoty z paměti

Útok na uživatele:

- Nesprávné používání dostupných technologií
- Man-in-the-middle
- SSL Strip
- StripTLS: SSL Strip u emailů

Man-in-the-middle a šifrovaný provoz

SSL Stripping: I když stránka podporuje HTTPS, přinutí se ke komunikaci přes HTTP

Certificate Pinning: Injekce vlastního certifikátu do systému oběti

TLS Protocol Downgrade: Vynucení staršího (slabšího) algoritmu

Virtual Private Network

Zaručuje CIA

Druhy:

- Podle vrstvy:
  - **L3:**
    - IP paket:

      `dest IP (PC2) | src IP (PC1) | data | CRC`
    - Nový IP paket:

      `dest IP (R2) | src IP (R1) | zašifrovaný paket | CRC`
    - `R1` a `R2` : VPN terminator nebo VPN concentrator
  - **L2:**
    - Rámec:

      `dest MAC (PC2) | src MAC (PC1) | dest IP (PC2) | src IP (PC1) | data | CRC`
    - Nový rámec:

      `dest IP (R2) | src IP (R1) | zašifrovaný rámec | CRC`
- Tunnel vs. transport:
  - **Tunnel:** šifrován celý paket, použije se jako data

    `dest IP (R2) | src IP (R1) | zašifrovaný paket | CRC`
  - **Transport:** šifrují se pouze data

    `dest IP (R2) | src IP (R1) | dest IP(PC2) | dest IP (PC1) | zašifrovaná data | CRC`
- **Site-to-site:** vliv na celou síť
- **Remote Access VPN:** jednotliví uživatelé mají přístup do sítě
- **Split Tunnel:** Při remote access zaměstnance z domova jde přes firmu jenom firemní provoz, ostatní jde do internetu přímo

IPsec

Na začátku key agreement protocol -- **HAGLE:**

- hash (MD5/SHA1)
- authentication (RSA podpisy)
- gruoup (Diffie-Hellmann group)
- length (délka trvání)
- encryption method (AES/DES/3DES)

Authentication Header: autentizace paketů pomocí klíčované MAC funkce

Encapsulated Security Protocol: Autentizace a šifrování paketů pomocí klíčované MAC a šifrovací funkce

Otevření tunelu:

- **IKE Phase 1** (ISAKMP, Internet Security Association and Key Management)
  1. **asymetrický tunel:** dohoda symetrického klíče
  2. **symetrický tunel:** autentizace
- **IKE Phase 2** (IPSec)
  3. **asymetrický tunel:** dohoda symetrického klíče
  4. **symetrický tunel:** data

RADIUS

Jedna databáze pro AAA funkcionalitu na celé síti
(Authentication, Authorization, Accounting)

Certifikáty

Distribuce veřejných klíčů bez kontaktu s třetím důvěryhodným subjektem

Certifikát: Struktura obsahující:

- Veřejný klíč držitele
- Identifikační údaje držitele
- Dobu platnosti certifikátu
- Další údaje vytvořené certifikační autoritou

Certifikát **podepsán soukromým klíčem CA** -- každý účastník komunikace může ověřit veřejným

klíčem CA

Certifikční autorita: Důvěryhodná třetí strana, která na základě žádostí vydává a aktualizuje certifikáty

Certifikační strom: Struktura vzájemně propojených CA, reprezentován kořenovou CA s kořenovým certifikátem

- **Řetězec certifikátů:** Posloupnost certifikátů od certifikátu uživatele ke kořenovému certifikátu
- Certifikát platný ⇔ platné všechny certifikáty v řetězci certifikátů
- Kořenový certifikát ověřen jinou bezpečnou cestou, např. křížovou certifikací (2 kořenové CA si vzájemně ověří certifikáty)
- Komunikace mezi A a B v různých stromech: A pošle B certifikát A podepsaný CA1, certifikát CA1 podepsaný CA1, certifikát CA1 podepsaný CA2