Basics of SSL/TLS protocols and certificates

PV219
Adam Venclovský

Agenda

- What is SSL/TLS
- History
- Functions
- Encryption
- Handshake protocol
- PKI
- Certificate lifecycle
- Chain of trust
- TLS certificate types
- Cyber attacks
- Future of the TLS

What is SSL/TLS

- Secuse sockets layer (SSL), Transport layer security (TLS)
- These are protocols used to secure communication between two computers through internet or other network
- SSL was original protocol developed by Netscape corporation in 1995 and TLS is its modern and more secure version.
- Today, SSL protocol is not used anymore

Why is SSL not used anymore

- Security shorcomings and errors
  - POODLE (Padding Oracle On Downgraded Legacy Encryption),BEAST (Browser Exploit Against SSL/TLS
- New versions support
- Support of modern cryptographic algorithms (AES, SHA-256)
- Development organization recommendations (IETF, NIST)

Main functions of SSL/TLS

- Encription of the data
- Ensure of secure connection (handshake)
- Authentication
- Data integrity

Handshake

- The client and server agree on the encryption parameters, exchange the necessary information and create a common key for data encryption
- ClientHello
- ServerHello
- Server authentization
- Premaster secret
- Master secret
- Cryptoghraphic algorithm agreement
- finish

Public X Private key

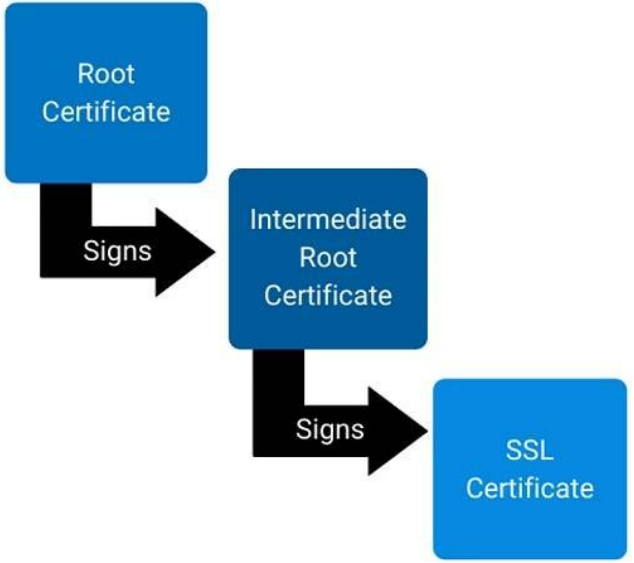
- Private key
  - Kept in privacy
  - Data decryption
  - Signing of the messages
- Public key
  - Publicly available
  - Data encryption
  - Verify of digital signature

What is certificate and how it works

- Digital identification document confirming identity
- Certificate lifecycle:
  - Creation of certificate
  - Digital signature
  - Certificate distribution
  - Certificate verification

Chain of trust (certificate verification process)

- Concept that describes hierarchistic system of trust between certificate authorities and certificates
- Trust in certificate authority (CA)
- Creating the chain of trust
- Certificate verification
- Certificate revocation list (CRL)



Let's Encrypt

TLS Certificate types

- Domain validated (DV) certificates
- Organization validated (OV) certificates
- Extended validation (EV) certificates
- Wildcard certificates
- Multi-domain certificates

Cyber attacks

- Man-in-the-middle
  - Logjam
  - Spoofing
- Phishing
- Abuse of CA

Man-in-the-middle (MITM)

- While ongoing typical handshake, attacker catch the communication (vulnerability of network devices,DNS hijacking)
- Than he „stands between client and server“
- Spoofing
  - Passive access to information distribted between client and server
- Manipulation
- Pretend identity
- Logjam attack
  - Attacker in this position can reduce size of Diffie-Hellman encryption algorithm parameters so it can be breakable

Consequences of successful attacks

- Leak of private information such as login info, banking information, personal identifiers, etc.
- Dezinformation, lost of integtity of data
- Attack on user‘s devices
- Affects credibility of CA
- DoS (denial of Service)
- Financial theft

Future of the TLS

- today‘s threads – quantum PC that can brute force everything
- New cryptoghraphic algorithms
- Support of new, quicker protocols like QUIC (quick UPD internet connections)
- Standardization
- Adaptation for AI and AR

Thank you for attention