Certificates

Martin Stanek

Department of Computer Science
Comenius University
stanek@dcs.fmph.uniba.sk

Cryptology 1 (2023/24)

Introduction

- certificate – binding an identity or multiple identities to a public key
  - identity: domain name, e-mail address, etc.
  - public key for asymmetric scheme (signature, encryption)
- certificate for different applications
  - TLS (SSL) connections, code signing, personal certificates for e-mail security, etc.
- certificate authorities: trusted third parties that provide these binds
  - subject and issuer
  - root and intermediary certificate authorities
  - certificate is a data structure signed by CA
  - signing certificate is only a fraction of services required from CA
- various assurance levels for TLS certificates:
  - DV – domain validated
  - OV – organization validated
  - EV – extended validation

Certificate chain

- what you get from a web server

```
Certificate chain
 0 s:C=SK, ST=Bratislavský kraj,
     O=Univerzita Komenského v Bratislave, CN=uniba.sk
   i:C=NL, O=GEANT Vereniging, CN=GEANT OV RSA CA 4
 1 s:C=NL, O=GEANT Vereniging, CN=GEANT OV RSA CA 4
   i:C=US, ST=New Jersey, L=Jersey City,
     O=The USERTRUST Network,
     CN=USERTrust RSA Certification Authority
 2 s:C=US, ST=New Jersey, L=Jersey City,
     O=The USERTRUST Network,
     CN=USERTrust RSA Certification Authority
   i:C=GB, ST=Greater Manchester, L=Salford,
     O=Comodo CA Limited, CN=AAA Certificate Services
```

Root CA

- certificate chain anchored in root CA
- self-signed certificate
- list of trusted certificates (not only root CAs) stored locally

```
Issuer: C=GB, ST=Greater Manchester, L=Salford,
  O=Comodo CA Limited, CN=AAA Certificate Services
Subject: C=GB, ST=Greater Manchester, L=Salford,
  O=Comodo CA Limited, CN=AAA Certificate Services
Validity
  Not Before: Jan  1 00:00:00 2004 GMT
  Not After : Dec 31 23:59:59 2028 GMT
X509v3 extensions:
  X509v3 Basic Constraints: critical
    CA:TRUE
```

Certificate – structure (1)

```
$ openssl s_client -showcerts -connect www.uniba.sk:443
  </dev/null 2>/dev/null|openssl x509 -outform PEM >uniba.pem
$ openssl x509 -in uniba.pem -text -nameopt utf8
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number:
        0d:73:0d:8b:36:f8:83:15:c4:89:60:4f:ee:33:ac:e8
    Signature Algorithm: sha384WithRSAEncryption
    Issuer: C=NL, O=GEANT Vereniging, CN=GEANT OV RSA CA 4
    Validity
        Not Before: Jun  5 00:00:00 2023 GMT
        Not After : Jun  4 23:59:59 2024 GMT
    Subject: C=SK, ST=Bratislavský kraj,
             O=Univerzita Komenského v Bratislave, CN=uniba.sk
```

Certificate – structure (2)

```
Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (2048 bit)
      Modulus:
          00:de:e9:b4:3c:ca:de:ce:94:1c:82:e9:66:8a:53:
          ...
          22:e7
      Exponent: 65537 (0x10001)
X509v3 extensions:
  X509v3 Authority Key Identifier:
          6F:1D:35:49:10:...:1F:95:BE:71:7A:0C
  X509v3 Subject Key Identifier:
          34:C0:7C:53:1B:...:86:31:4E:FF:43:15
  X509v3 Key Usage: critical
          Digital Signature, Key Encipherment
  X509v3 Basic Constraints: critical
          CA:FALSE
```

Certificate – structure (3)

```
X509v3 Extended Key Usage:
  TLS Web Server Authentication,
  TLS Web Client Authentication
X509v3 Certificate Policies:
  Policy: 1.3.6.1.4.1.6449.1.2.2.79
    CPS: https://sectigo.com/CPS
  Policy: 2.23.140.1.2.2
    X509v3 CRL Distribution Points:
      Full Name:
        URI:http://GEANT.crl.sectigo.com/GEANTOVRSACA4.crl
Authority Information Access:
  CA Issuers -
    URI:http://GEANT.crt.sectigo.com/GEANTOVRSACA4.crt
  OCSP - URI:http://GEANT.ocsp.sectigo.com
```

Certificate – structure (4)

- three SCTs in the certificate (just one example presented)
- this particular Log ID corresponds to the CT log *Google Xenon 2024*

```
CT Precertificate SCTs:
  Signed Certificate Timestamp:
    Version   : v1 (0x0)
    Log ID    : 76:FF:88:...:CC:F5:87:BA:34:
                B4:A4:CD:...:67:4C:5A:3A:74
    Timestamp : Jun  5 09:17:59.922 2023 GMT
    Extensions: none
    Signature : ecdsa-with-SHA256
      30:45:02:21:00:B0:EA:76:09:55:55:0B:DB:A2:96:07:
      ...
      6A:9B:A7:3E:6B:89:90
```

Certificate – structure (5)

```
  X509v3 Subject Alternative Name:
    DNS:uniba.sk, DNS:cdv.uniba.sk, ... DNS:zona.uniba.sk
Signature Algorithm: sha384WithRSAEncryption
Signature Value:
    8a:9a:dd:8f:0c:...:a8:3f:9b:b6:bb:92:f9:
    ...
    56:5d:57:a5:9f:c5:7e:9d
```

Certificate authority

- identity validation, certificate issuance, certificate renewal, re-key, modification, validation of revocation request, revocation, certificate status services, etc.
- Certificate Policies and Certification Practices Statements
  - often separate policy and CPS for web PKI, S/MIME (mail), document signing, etc.
  - publicly available (identifier/URI embedded in a certificate)
  - defines how CA performs its duties
  - structure follows RFC 3647
- Trust
  - CA/Browser Forum – various requirements for CAs: baseline, network security etc.
  - web browsers have policies for CA inclusion, e.g., Mozilla (Mozilla Root Store Policy), Chrome (Chrome Root Program Policy)

Certificate – issuing and revoking

- CSR (Certificate signing request)
  - subject, public key info (algorithm and public key), signature
- CRL (Certificate revocation list) – signed list of revoked serial numbers

```
Certificate Revocation List (CRL):
  Version 2 (0x1)
  Signature Algorithm: sha384WithRSAEncryption
  Issuer: C = NL, O = GEANT Vereniging, CN = GEANT OV RSA CA 4
  Last Update: Dec  6 20:40:23 2023 GMT
  Next Update: Dec 13 20:40:23 2023 GMT
  CRL extensions:
    X509v3 Authority Key Identifier:
      6F:1D:35:49:10:6C:...:E8:1F:95:BE:71:7A:0C
    X509v3 CRL Number:
      1425
```

Certificate – issuing and revoking (2)

- CRL – sometimes there is a reason for revocation

```
Serial Number: 1A126E9D41E0816D734AF372ABE143F0
  Revocation Date: Jan 16 10:43:35 2023 GMT
    CRL entry extensions:
      X509v3 CRL Reason Code: Key Compromise
Serial Number: C5F46C65A85EF19AAC6C8E47F1BBE4B8
  Revocation Date: Jan 16 11:00:04 2023 GMT
Serial Number: 21F1F04ACACFD8022AEBAA8D0FC84E4C
  Revocation Date: Jan 16 11:22:25 2023 GMT
    CRL entry extensions:
      X509v3 CRL Reason Code: Superseded
```

Checking certificate's validity – OCSP

- OCSP – Online Certificate Status Protocol, RFC 6960
- OCSP reponder published in a certificate (if CA supports OCSP):
  - Authority Information Access
  - usually over HTTP
  - `http://GEANT.ocsp.sectigo.com`
- request: serial number of the certificate, hash of the issuer's DN, hash of the issuer's public key, some extensions (such as OCSP nonce)
- response: signed status (good/revoked/unknown), produced at, this update, next update