Communication and Security Infrastructure

Przemysław Kubiak

October 2023

1 Public Key Infrastructure – X.509 Certificates

1.1 Introduction

- What is the relationship between Public key Infrastructure and certificates?
- How are the certificates structured?
- How was certificate flexibility (ability to use different algorithms) achieved?
- Certificate path validation algorithm.
- Are the X.509 certificates perfect?
- Other protocols and data structures used in certificate management.

1.2 What is the relationship between Public key Infrastructure and certificates?

- We focus on application of X.509 in authentication of communicating parties (TLS). Other applications:
  - signing documents,
  - signing and encryption of e-mails,
  - signing software packages.
- Application in authentication scenario is discussed in the handwritten notes from Lecture 1

1.3 How are the certificates structured?

- The X.509 certificate is composed of:
  - TbsCertificate,
  - description of SignatureAlgorithm,

  - SignatureValue.

- For details see Sect.4.1 of RFC5280 and the "Exercise Notes on PKI".
- In RFC we see ASN.1 encoding. To translate it to the binary form strict encoding rules (DER in case of X.509) are applied.
- Some fields of the X.509 certificate are rarely used – cf. Unique Identifiers.

1.4 How was certificate flexibility (e.g., ability to use different algorithms) achieved?

- `AlgorithmIdentifier` – see Sect.4.1.1.2 of RFC 5280
- OBJECT IDENTIFIER – cf. Annex A of X660 and the tree at the end of the handwritten notes from Lecture 1
- Examples of OID usage: Sect. 2.1 of RFC 4055 (for OID encoding rules click here, and its example you find on page 8 of the notes)
- Example of "parameters" field: RSASSA-PSS-params of the RSA-PSS encoding (see Fig.2 in RFC 3447)
- **ability to add custom extensions (and register them by OIDs)**

1.5 Certificate Extensions

See

- Name Constraints Extension
- handwritten notes from Lecture 2

1.6 Certificate path validation algorithm

See Sect.6 of RFC 5280 (for certificate policies see RFC 3647 and the paper)

1.7 Are the X.509 certificates perfect?

Definitely not.

Drawbacks:

- They are complex.
  - In the paper we read: "In practice, many libraries implementing X.509 have been shown to suffer from flaws that are due to noncompliance with the standard. Developing a compliant implementation is especially hindered by the design complexity, ambiguities, or underspecifications in the standard written in natural languages."

  - Exemplary security gaps in the implementations caused by complicated specification were discussed in handwritten notes from Lecture 2. More on certificate validation pitfals the reader will find on the webpage.

- (similar to the previous one) They are heavy – for constrained devices like eID documents a different certificate format is used: CVC (Card Verifiable Certificates) – see page 85 of BSI TR-03110 Part 3. The implementation of CVC is simpler and certificates are lighter.

- The trust hierarchy is well suited for organizations such as corporations, with a well-defined hierarchy:

  - Global trust philosophy can have global impact in case of a security incident:

    * in the paper we read that "In March 2011, news broke that Comodo - a security firm operating a certification authority - had been hacked. The intrusion resulted in the unwarranted issuance of 9 certificates for several high-profile domain names. A few months later, DigiNotar suffered a similar attack.".
    * Some kind of limitation of the trust hierarchy are: Name Constraints extension, Basic Constraint Extension:path length, DNS Certification Authority Authorization,
    * Other tools: Certificate Transparency (CT) framework – RFC 6962: "The intent is that eventually clients would refuse to honor certificates that do not appear in a log, effectively forcing CAs to add all issued certificates to the logs."

  - For more horizontal (not hierarchical) structure of trust other formats like PGP (local trust model), or experimental SPKI/SDSI (no glabal name space, but certificate chain discovery is not so obvious) were developed.

2 TLS protocol

TLS is placed between the transport protocol (TCP) nad the application protocol (HTTP, SMTP, FTP, IMAP, POP3, etc.). Most popular versions:

1. TLS 1.2: RFC 5246 (published in 2008)
2. TLS 1.3: RFC 8446 (published in 2008)

The idea for this chapter: look at the structure of the protocol, and then analyse exemplary attacks.

2.1 TLS Structure

Each version is composed of two major components:

- The TLS Handshaking Protocols,
- The TLS Record Protocol.

2.2 TLS Handshake

Questions (TLS 1.2):

- How the server authenticates itself?
- How the client authenticates itself, if required by the server?
- How to "read" ciphersuites?
- How domain parameter are chosen in case of ECDH or in case of DH?
- How cipher suites are established?
- How session keys are derived? What function is used?

2.3 Cipher Suites

- the meaning, see e.g., An Introduction to Cipher Suites
- RFC 5246, Sect.A5
- RFC 8422
- RFC 8446, Sect.B4

2.4 Domain Parameters

See Server Key Exchange in RFC 8422.

2.5 Exemplary Attacks

- TLS renegotiation prefix injection vulnerability
- ALPACA attack

2.6 Exemplary Estensions

- ALPN
- SNI

2.7 TLS 1.3

Questions:

- How the handshake proceeds in this version? See Sect.2 of RFC8446
- How the client authenticates itself, if required by the server? See e.g., Post-Handshake Authentication
- How session keys are derived? See Sect.7.1 of RFC8446.

2.8 Lucky-13

See the handwritten notes from Lecture 5 and the paper.

3 eIDAS – negative impact of recent legislative proposal on website security ecosystem

3.1 Problem description

Art.45, paragraph 2: "Qualified certificates for website authentication referred to in paragraph 1 shall be recognised by web-browsers. For those purposes web-browsers shall ensure that the identity data provided using any of the methods is displayed in a user friendly manner. Web-browsers shall ensure support and interoperability with qualified certificates for website authentication referred to in paragraph 1 (...)"

Art.45a: "Web-browsers shall not take *any measures* contrary to their obligations set out in Art 45, notably the requirement to recognise Qualified Certificates for Web Authentication, and to display the identity data provided in a user friendly manner."

Remarks:

- It seems that the proposal is not officially available to the public (16.11.2023) – see the the website of Scott Helme.
- Members of cryptographic community express concerns about impact of the amendment.

Delegation of some responsibilities in response to the regulation (delegation according to the *trust, but verify* model) – see Lecture 6.

3.2 How the browser can find "redundant" certificates issued by malicious CAs

See

- the handwritten notes from Lecture 7

- The paper F-PKI: Enabling Innovation and Trust Flexibility in the HTTPS Public-Key Infrastructure

4 DNS – Introduction

See the

- handwritten notes from Lecture 8,
- handwritten notes from Lecture 9
- DNS header
- on reverse DNS lookup

5 DNSSEC

See the

- handwritten notes from Lecture 10,
- Turkey Hijacking IP addresses for popular Global DNS providers (2014)
- The DNSSEC Root Signing Ceremony
- A Longitudinal, End-to-End View of the DNSSEC Ecosystem (USENIX 2017), the authors write: "Our investigation reveals pervasive mismanagement of the DNSSEC infrastructure. For example, we found that 31% of domains that support DNSSEC fail to publish all relevant records required for validation; 39% of the domains use insufficiently strong key-signing keys; and although 82% of resolvers in our study request DNSSEC records, only 12% of them actually attempt to validate them. These results highlight systemic problems, which motivate improved automation and auditing of DNSSEC management.".
- Downgrading DNSSEC: How to Exploit Crypto Agility for Hijacking Signed Zones (USENIX 2023), the authors write "We validate the success of DNSSEC-downgrade attacks by poisoning the resolvers: we inject fake records, in signed domains, into the caches of validating resolvers. Our evaluations showed that during 2021 major DNS providers, such as Google Public DNS and Cloudflare, as well as 35% of DNS resolvers used by the web clients were vulnerable to our attacks. After coordinated disclosure with the affected operators, that number reduced to 5.03% in 2022.".
- Taking the DNS for a Walk; NSEC3 Prevalence and Recoverability, the author writes: "This paper presents a GPU-based attack on NSEC3 that recovered 44% of names for the internet's top 20,000 NSEC3-protected DNS zones, partially invalidating NSEC3's privacy and security goals". The python implementation of the NSEC(3) Walker is available on github.