Lecture 15: PKI and Certificates

COSC362 Data and Network Security

Book 1: Chapter 14 – Book 2: Chapters 21 and 23

Spring Semester, 2021

Motivation

- Public key infrastructures imply the use of public digital certificates.
- Digital signatures provide these certificates.
- X.509 certificates are standardised and used in most network security applications.

Outline

Outline

Definition

- NIST definition:
  - "A public key infrastructure is the key management environment for public key information of a public key cryptographic system."
- Key management concerned with *lifecycle* of cryptographic keys:
  - Generation, distribution, storage and destruction of keys.
- Various legal or business (trusted) entities may be involved:
  - Registration authorities (RAs): vouching for the identity of an user.
  - Validation authorities (VAs): verifying that identity.
  - Certification authorities (CAs): issuing digital certificates (certifying the public key of the user).

Outline

Digital Certificates

- How to be confident of the correct binding between a public key and its owner?
  - When using a public key to encrypt a message or to verify a digital signature.
- Achieved through the use of *digital certificates*:
  - They contain the public key and owner identity.
  - There is other information such as signature algorithm and validity period.
- Certificate digitally signed by a *certification authority* (CA):
  - CA should be trusted by the certificate verifier.
- Certificates play a central role in key management for PKIs.

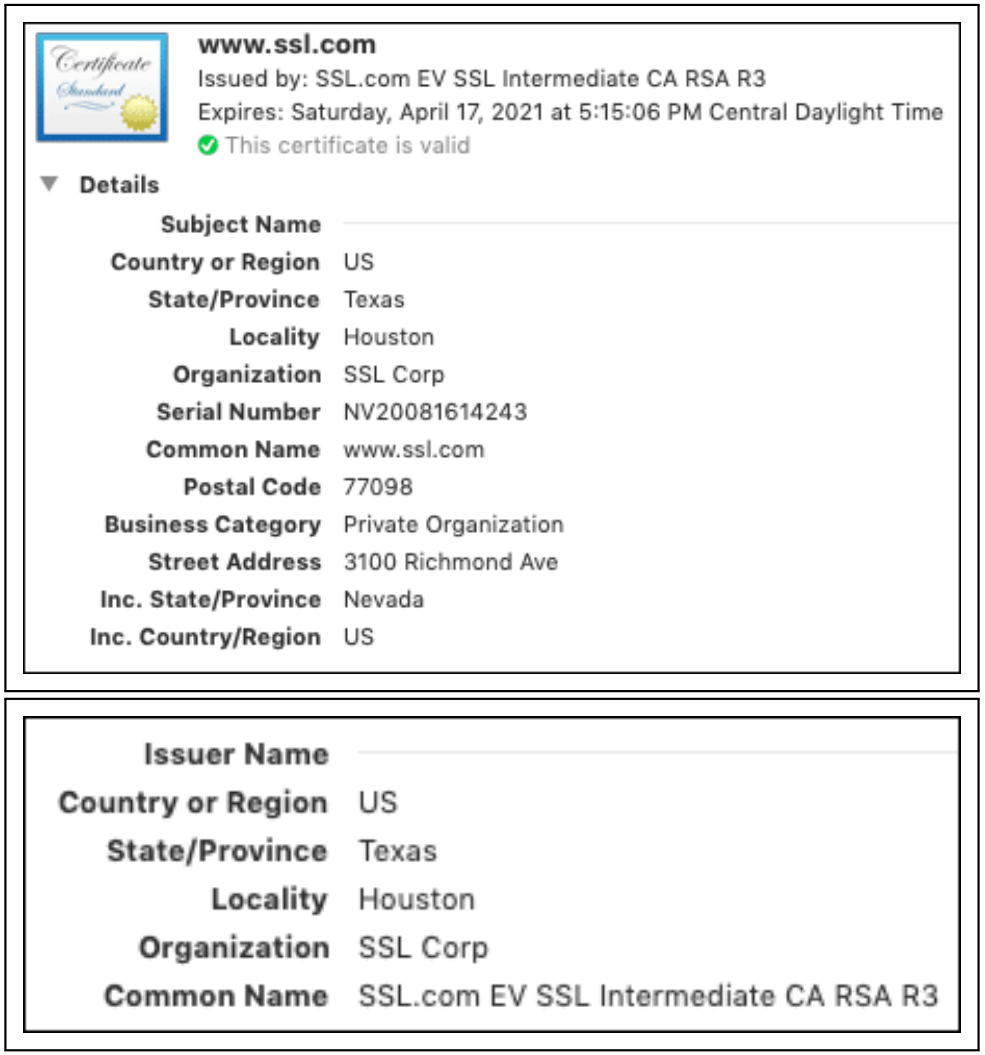
Certification Authority (CA)

- A CA creates, issues and revokes certificates for subscribers and other CAs.
- A CA has a *certification practice statement* (CPS).
- A CPS covers issues such as:
  - Checks performed before certificate issue
  - Physical, personnel and procedural security controls for the CA
  - Technical and key pair protection and management controls
  - Certificate revocation management procedures
  - Accreditation information
  - Legal and privacy issues and liability limitations

X.509 Standard

- Most widely used standard:
  - Originally ITU standard.
  - Now RFC 5280.
  - Current version (number 3) allows flexible extensions.
- Important fields in X.509 certificates:
  - Version number
  - Serial number (set by the CA)
  - Signature algorithm identifier (algorithm used to digitally sign)
  - Issuer name (of the CA)
  - Subject name (of the user to which the certificate is issued)
  - Public key information
  - Validity period
  - Digital signature (of the certificate, generated by the CA)

Example



www.ssl.com
Issued by: SSL.com EV SSL Intermediate CA RSA R3
Expires: Saturday, April 17, 2021 at 5:15:06 PM Central Daylight Time
This certificate is valid

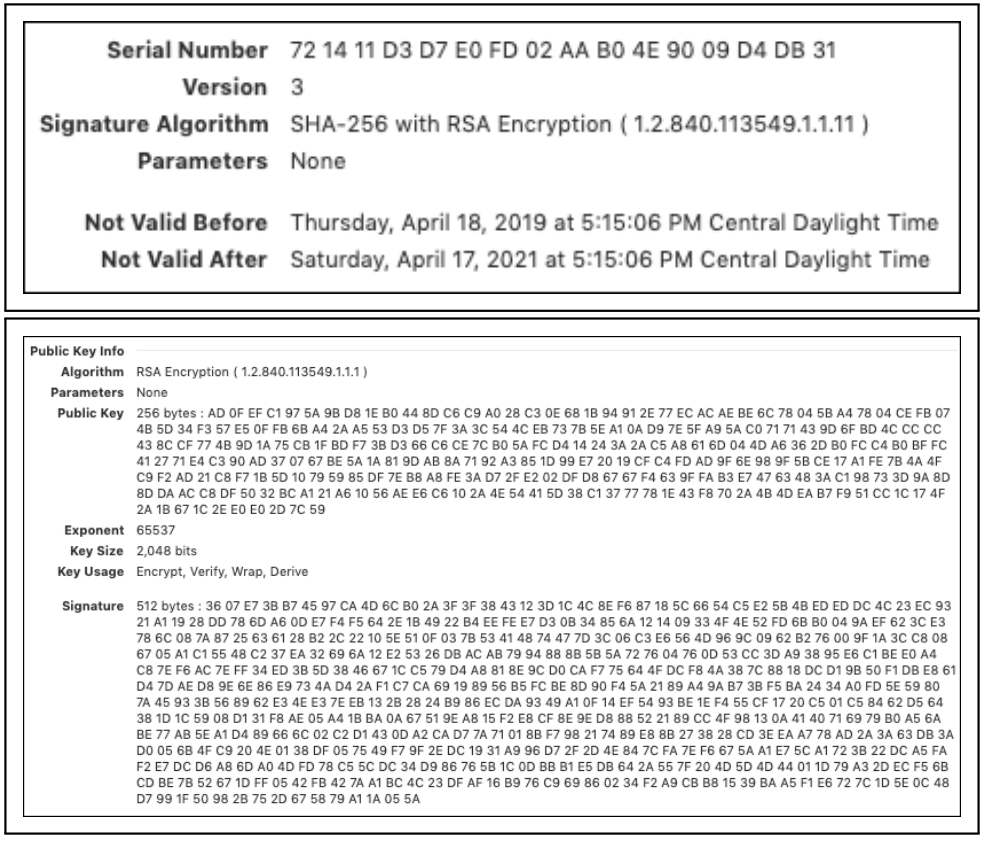
Details

Subject Name	
Country or Region	US
State/Province	Texas
Locality	Houston
Organization	SSL Corp
Serial Number	NV20081614243
Common Name	www.ssl.com
Postal Code	77098
Business Category	Private Organization
Street Address	3100 Richmond Ave
Inc. State/Province	Nevada
Inc. Country/Region	US

Issuer Name	
Country or Region	US
State/Province	Texas
Locality	Houston
Organization	SSL Corp
Common Name	SSL.com EV SSL Intermediate CA RSA R3

- Information about the subject (the user to which the certificate is issued)
- Information about the issuer (the CA)

Example



Serial Number	72 14 11 D3 D7 E0 FD 02 AA B0 4E 90 09 D4 DB 31
Version	3
Signature Algorithm	SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters	None
Not Valid Before	Thursday, April 18, 2019 at 5:15:06 PM Central Daylight Time
Not Valid After	Saturday, April 17, 2021 at 5:15:06 PM Central Daylight Time

Public Key Info

Algorithm	RSA Encryption (1.2.840.113549.1.1.1)
Parameters	None
Public Key	256 bytes : AD 0F EF C1 97 5A 9B D8 1E B0 44 8D C6 C9 A0 28 C3 0E 68 1B 94 91 2E 77 EC AC AE BE 6C 78 04 5B A4 78 04 CE FB 07 4B 5D 34 F3 57 E5 0F FB 6B A4 2A A5 53 D3 D5 7F 3A 3C 54 4C EB 73 7B 5E A1 0A D9 7E 5F A9 5A C0 71 71 43 9D 6F BD 4C CC CC 43 8C CF 77 4B 9D 1A 75 CB 1F BD F7 3B D3 66 C6 CE 7C B0 5A FC D4 14 24 3A 2A C5 A8 61 6D 04 4D A6 36 2D B0 FC C4 B0 BF FC 41 27 71 E4 C3 90 AD 37 07 67 BE 5A 1A 81 9D AB 8A 71 92 A3 85 1D 99 E7 20 19 CF C4 FD AD 9F 6E 98 9F 5B CE 17 A1 FE 7B 4A 4F C9 F2 AD 21 C8 F7 1B 5D 10 79 59 85 DF 7E B8 A8 FE 3A D7 2F E2 02 DF D8 67 67 F4 63 9F FA B3 E7 47 63 48 3A C1 98 73 3D 9A 8D 8D DA AC C8 DF 50 32 BC A1 21 A6 10 56 AE E6 C6 10 2A 4E 54 41 5D 38 C1 37 77 78 1E 43 F8 70 2A 4B 4D EA B7 F9 51 CC 1C 17 4F 2A 1B 67 1C 2E E0 E0 2D 7C 59
Exponent	65537
Key Size	2,048 bits
Key Usage	Encrypt, Verify, Wrap, Derive
Signature	512 bytes : 36 07 E7 3B B7 45 97 CA 4D 6C B0 2A 3F 3F 38 43 12 3D 1C 4C 8E F6 87 18 5C 66 54 C5 E2 5B 4B ED ED DC 4C 23 EC 93 21 A1 19 28 DD 78 6D A6 0D E7 F4 F5 64 2E 1B 49 22 B4 EE FE E7 D3 0B 34 85 6A 12 14 09 33 4F 4E 52 FD 6B B0 04 9A EF 62 3C E3 78 6C 08 7A 87 25 63 61 28 B2 2C 22 10 5E 51 0F 03 7B 53 41 48 74 47 7D 3C 06 C3 E6 56 4D 96 9C 09 62 B2 76 00 9F 1A 3C C8 08 67 05 A1 C1 55 48 C2 37 EA 32 69 6A 12 E2 53 26 DB AC AB 79 94 88 8B 5B 5A 72 76 04 76 0D 53 CC 3D A9 38 95 E6 C1 BE E0 A4 C8 7E F6 AC 7E FF 34 ED 3B 5D 38 46 67 1C C5 79 D4 A8 81 8E 9C D0 CA F7 75 64 4F DC F8 4A 38 7C 88 18 DC D1 9B 50 F1 DB E8 61 D4 7D AE D8 9E 6E 86 E9 73 4A D4 2A F1 C7 CA 69 19 89 56 B5 FC BE 8D 90 F4 5A 21 89 A4 9A B7 3B F5 BA 24 34 A0 FD 5E 59 80 7A 45 93 3B 56 89 62 E3 4E E3 7E EB 13 2B 28 24 B9 86 EC DA 93 49 A1 0F 14 EF 54 93 BE 1E F4 55 CF 17 20 C5 01 C5 84 62 D5 64 38 1D 1C 59 08 D1 31 F8 AE 05 A4 1B BA 0A 67 51 9E A8 15 F2 E8 CF 8E 9E D8 88 52 21 89 CC 4F 98 13 0A 41 40 71 69 79 B0 A5 6A BE 77 AB 5E A1 D4 89 66 6C 02 C2 D1 43 0D A2 CA D7 7A 71 01 8B F7 98 21 74 89 E8 8B 27 38 28 CD 3E EA A7 78 AD 2A 3A 63 DB 3A D0 05 6B 4F C9 20 4E 01 38 DF 05 75 49 F7 9F 2E DC 19 31 A9 96 D7 2F 2D 4E 84 7C FA 7E F6 67 5A A1 E7 5C A1 72 3B 22 DC A5 FA F2 E7 DC D6 A8 6D A0 4D FD 78 C5 5C DC 34 D9 86 76 5B 1C 0D BB B1 E5 DB 64 2A 55 7F 20 4D 5D 4D 44 01 1D 79 A3 2D EC F5 6B CD BE 7B 52 67 1D FF 05 42 FB 42 7A A1 BC 4C 23 DF AF 16 B9 76 C9 69 86 02 34 F2 A9 CB B8 15 39 BA A5 F1 E6 72 7C 1D 5E 0C 48 D7 99 1F 50 98 2B 75 2D 67 58 79 A1 1A 05 5A

- Serial number
- X.509 version (3)
- Signature algorithm
- Period validity
- Information about the public key
- Information about the signature

Using a Certificate

- Verifying a certificate:
  - By checking that the CA's signature is valid.
  - By checking that any conditions set in the certificate are correct.
- In order to verify a certificate:
  - The user of the certificate must have the correct public key of the CA.
- It does not matter how the user obtains the certificate.
- Public directories may store certificates:
  - Often, the owner of the public key sends the certificate to the user.

Certification Paths

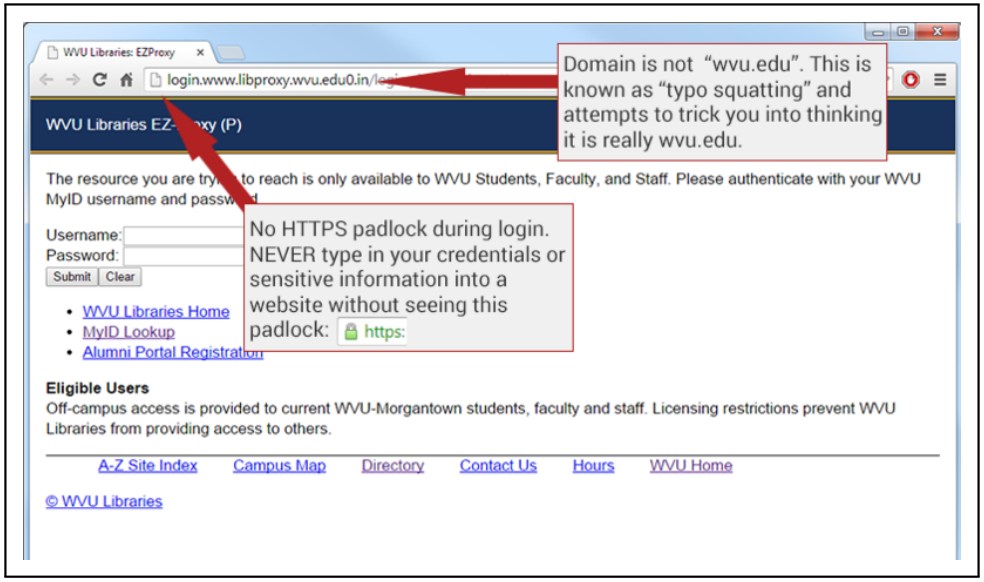
- Suppose that the public key of the CA ca_0 is not already known and trusted.
- Then, ca_0's public key can be certified by another CA ca_1.
- In turn, ca_1's public key can be certified by another CA ca_2.
- Thus, a *chain of trust* is set up, known as a *certification path*:

$$ca_n \rightarrow \cdots \rightarrow ca_2 \rightarrow ca_1 \rightarrow ca_0$$

- Suppose that an entity has a trusted copy of ca_n's public key.
- The chain of trust is used with certificates for all the *intermediate* CAs to obtain a trusted copy of ca_0's public key.

Phishing Attack

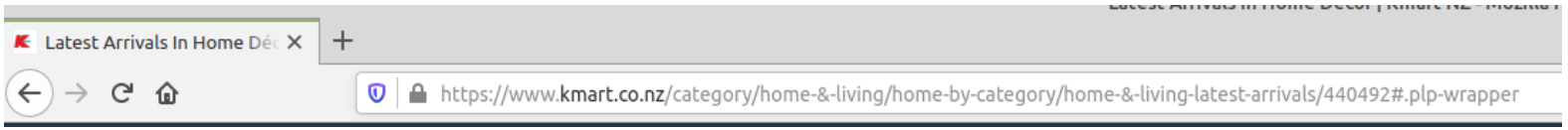
- The victim connects securely to a bogus site with the wrong certificate.
- The attacker makes the URL similar and the interface identical to a genuine site.



- If the website uses a certificate, then the *padlock* indicator still shows:
  - But the secure connection is to the attacker's site.

- Not always easy to tell if a certificate is one for a genuine site.

Extended Validation Certificates



- Browser indication:
  - A color in the address bar to indicate that the certificate has been issued at a specified level.
- Agreement between browser developers and CAs:
  - No technical difference in the certificate.
  - Just signed by a specific intermediate CA.
- Surveys have shown that extended validation certificates are mostly ignored by users.

Revocation

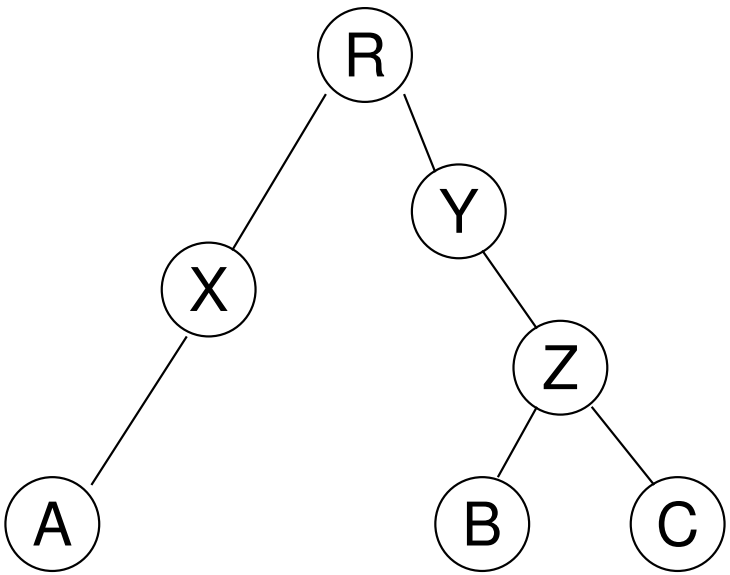
- Declaring a certificate invalid even though its validity period is current.
- The user must check which certificates have been revoked.
- Certificate revocation list (CRL):
  - Each CA periodically issues a list of revoked certificates which can be downloaded and then checked by clients before using a certificate.
- Online certificate status protocol (OCSP):
  - A server maintains a current list of revoked certificates and responds to requests about specific certificates.

Public Key Pinning

- Allowing browsers to fix for a certain time the public key used to verify certificates for certain sites.
- Preventing attacks due to compromised CAs.
- Supported by Firefox and other browsers.
- Previously supported by Chrome, but Google announced to remove it (Oct. 2017).

Outline

Hierarchical PKI



Root CA

Intermediate CAs

Users

- A CA certifies the public key of the entity below.
- In a non-hierarchical PKI, certification done between any CAs:
  - *X* can certify *Y*'s public key, or *Z* can certify *Y*'s public key.

Browser PKI

- Multiple hierarchies with preloaded public keys as root CAs.
- Intermediate CAs can be added.
- Users can also add their own certificates.
- Most servers send their public key and certificate to the browser at the start of a secure communication using TLS protocol.

OpenPGP PKI

- Used in PGP email security.
- Certificate includes ID, public key, validity period and *self-signature*.
- There is NO certification authorities:
  - Keys signed by anyone.
- Various key servers store keys:
  - Example: `http://pgp.mit.edu`
- Often known as *web of trust*.

Do we have some time left?

Yes, then let's start Lecture 16!