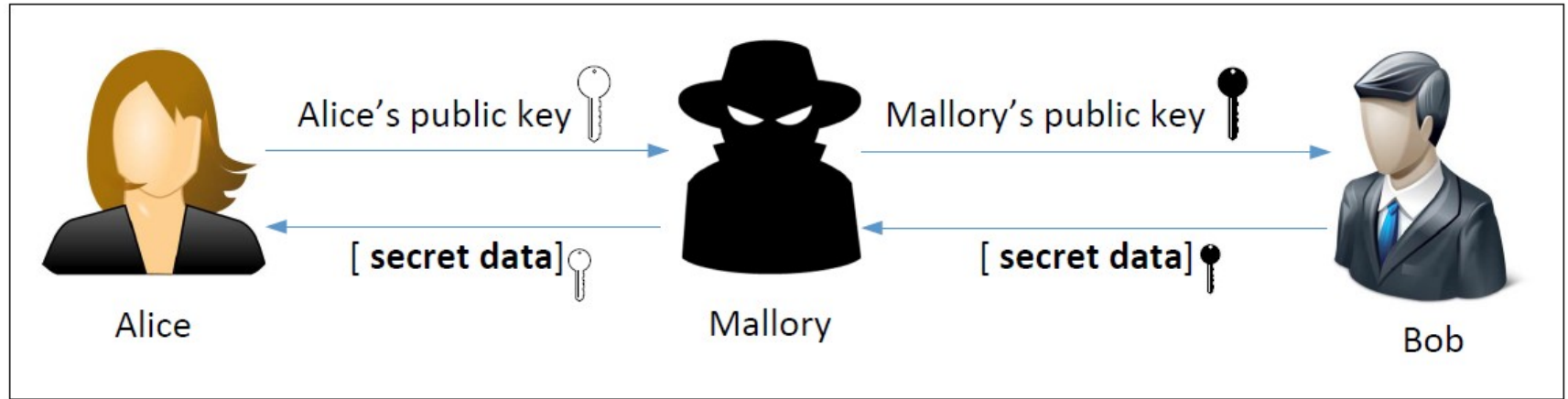


Public Key Infrastructure

Public Key Cryptography



Man-in-the-Middle (MITM) Attack



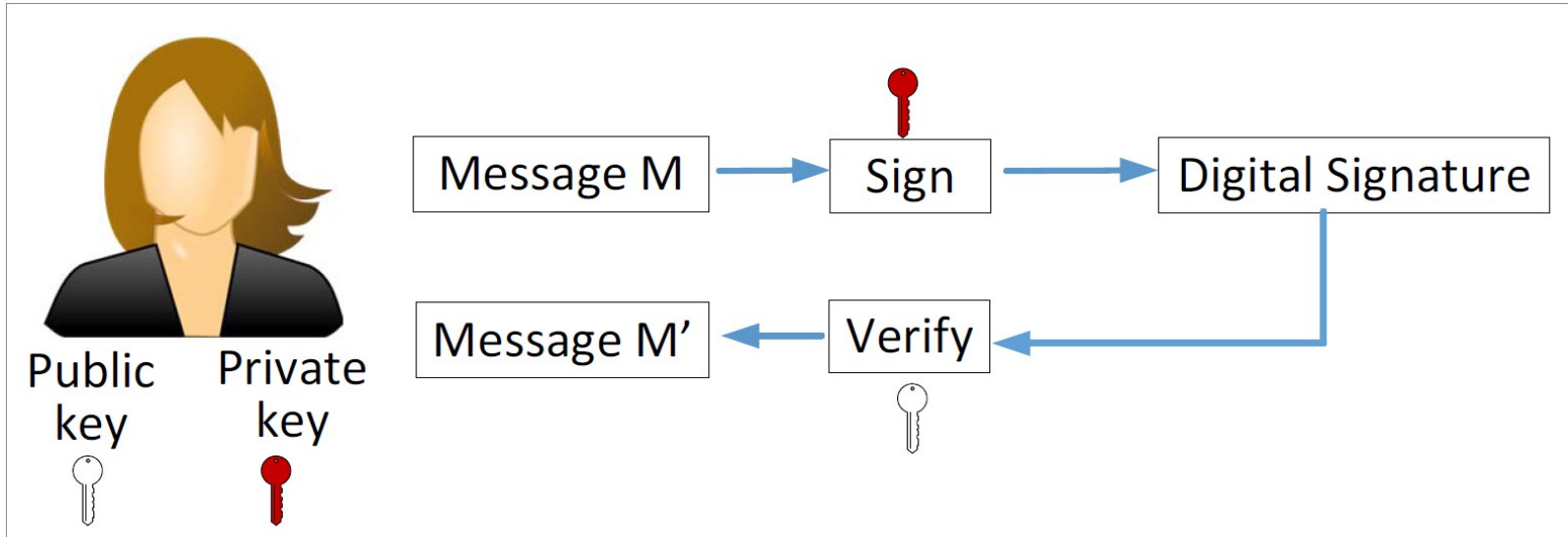
What Is the Fundamental Problem?

Fundamental Problem: Bob has no way to tell whether the public key he has received belongs to Alice or not.

Solution:

- Find a trusted party to verify the identity
- Bind an identity to a public key in a certificate
- The certificate cannot be forged or tampered with (using digital signature)

Digital Signature



- If the signature is not tampered with, M' will be the same as M
- Only Alice can sign (she has the private key)
- Everybody can verify (public key is known publically)

Defeating MITM Attacks using Digital Signature

- Alice needs to go to a **trusted party** to get a certificate.
- After verifying Alice's identity, the trusted party issues a certificate with Alice's name and her public key.
- Alice sends the entire certificate to Bob.
- Bob verifies the certificate using the trusted party's public key.
- Bob now knows the **true owner** of a public key.

Public Key Infrastructure

- **Certificate Authority (CA):** a **trusted party**, responsible for verifying the identity of users, and then bind the verified identity to a public keys.
- **Digital Certificates:** A document certifying that the public key included inside does belong to the identity described in the document.
 - X.509 standard

Digital Certificate

- Let's get paypal's certificates

```
$ openssl s_client -showcerts -connect www.paypal.com:443 </dev/null
```

```
-----BEGIN CERTIFICATE-----  
MIIHWTCCBkGgAwIBAgIQLNQVEFQ30N5KOSAFavbCfzANBgkqhkiG9w0BAQsFADB3  
MQswCQYDVQQGEwJVUzEdMBsGA1UEChMUU3ltYW50ZWMgQ29ycG9yYXRpb24xHzAd  
... (omitted) ...  
GN/QMQ3a55rjwNQN3s2WWuHGPaE/jMG17iiL2O/hUdIvLE9+wA+fWrey5//74x1  
NeQitYiySDIepHGnng==  
-----END CERTIFICATE-----
```

- Save the above data to paypal.pem, and use the following command decode it (see next slide)

```
$ openssl x509 -in paypal.pem -text -noout
```


Example of X.509 Certificate (1st Part)

The CA's identity
(Symantec)

The owner of
the certificate
(paypal)

Certificate:

Data:

Serial Number:

2c:d1:95:10:54:37:d0:de:4a:39:20:05:6a:f6:c2:7f

Signature Algorithm: sha256WithRSAEncryption

Issuer: C=US, O=Symantec Corporation, OU=Symantec Trust Network,
CN=Symantec Class 3 EV SSL CA - G3

Validity

Not Before: Feb 2 00:00:00 2016 GMT

Not After : Oct 30 23:59:59 2017 GMT

Subject: 1.3.6.1.4.1.311.60.2.1.3=US/
1.3.6.1.4.1.311.60.2.1.2=Delaware/
businessCategory=Private Organization/
serialNumber=3014267, C=US/
postalCode=95131-2021, ST=California,
L=San Jose/street=2211 N 1st St,
O=PayPal, Inc., OU=CDN Support, CN=www.paypal.com

Example of X.509 Certificate (2nd Part)

Public key

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

Modulus:

00:da:43:c8:b3:a6:33:5d:83:c0:63:14:47:fd:6b:22:bd:
bf:4e:a7:43:11:55:eb:20:8b:e4:61:13:ee:de:fe:c6:e2:
... (omitted) ...

7a:15:00:c5:01:69:b5:10:16:a5:85:f8:fd:07:84:9a:c9:

Exponent: 65537 (0x10001)

CA's signature

Signature Algorithm: sha256WithRSAEncryption

4b:a9:64:20:cc:77:0b:30:ab:69:50:d3:7f:de:dc:7c:e2:fb:93:84:fd:
78:a7:06:e8:14:03:99:c0:e4:4a:ef:c3:5d:15:2a:81:a1:b9:ff:dc:3a:
... (omitted) ...

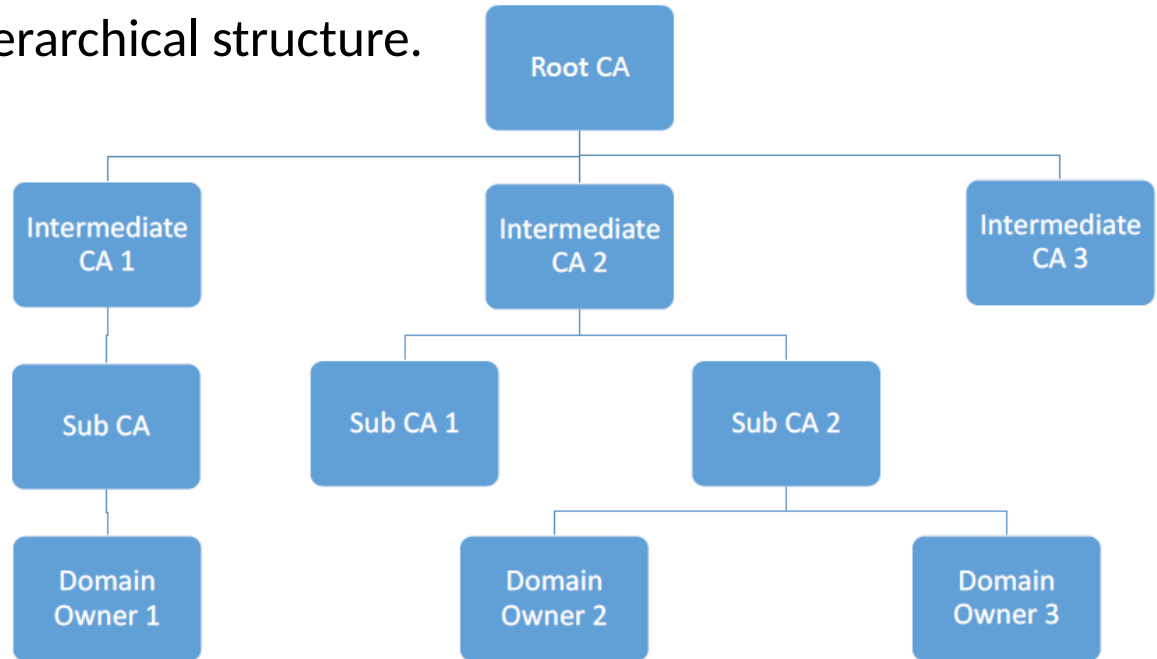
fb:00:3e:7d:6a:de:cb:9f:ff:ef:8c:65:35:e4:22:b5:88:b2:48:32:1e:

The Core Functionalities of CA

- **Verify the subject**
 - Ensure that the person applying for the certificate either owns or represents the identity in the subject field.
- **Signing digital certificates**
 - CA generates a digital signature for the certificate using its private key.
 - Once the signature is applied, the certificate cannot be modified.
 - Signatures can be verified by anyone with the CA's public key.

Root and Intermediate Certificate Authorities

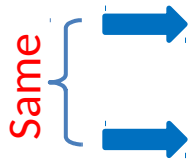
There are many CAs in the real world, and they are organized in a hierarchical structure.



Root CAs and Self-Signed Certificate

- A root CA's public key is also stored in an X.509 certificate. It is self-signed.
- Self-signed: the entries for the issuer and the subject are identical.

same



```
Issuer: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network,  
        OU=(c) 2006 VeriSign, Inc. - For authorized use only,  
        CN=VeriSign Class 3 Public Primary Certification Authority - G5  
Subject: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network,  
        OU=(c) 2006 VeriSign, Inc. - For authorized use only,  
        CN=VeriSign Class 3 Public Primary Certification Authority - G5
```

- How can they be trusted?
 - Public keys of root CAs are pre-installed in the OS, browsers and other software

Discussion Question

- **Question:** If the root CA's certificate is self-signed, how do we verify it?
- **Answer:** There is no way to verify it. We just make sure that the certificate is obtained in a trusted way
 - Come with the operating system (if we trust OS, we trust the cert.)
 - Come with the software (if we trust the software, we trust the cert.)
 - Manually added (if we trust our own decision, we trust the cert.)
 - Sent to us by somebody whom we don't trust (don't trust the cert.)

Intermediate CAs and Chain of Trust

```
$ openssl s_client -showcerts -connect www.paypal.com:443
```

```
Certificate chain
```

```
0 s: ... /CN=www.paypal.com
```

```
i: ... /CN=Symantec Class 3 EV SSL CA - G3
```

Paypal's certificate

```
-----BEGIN CERTIFICATE-----
```

```
MIIHWTCCBkGgAwIBAgIQLNQVEFQ30N5KOSAFavbCfzANBgkqhkiG9w0BAQsFADB3
```

```
...
```

```
-----END CERTIFICATE-----
```

```
1 s: ... /CN=Symantec Class 3 EV SSL CA - G3
```

```
i: ... /CN=VeriSign Class 3 Public Primary Certification
```

```
Authority - G5
```

Intermediate CA's certificate

```
-----BEGIN CERTIFICATE-----
```

```
MIIFKzCCBBOgAwIBAgIQfuFKb2/v8tN/P61lTTratDANBgkqhkiG9w0BAQsFADCB
```

```
...
```

```
-----END CERTIFICATE-----
```

A is
used to
verify B

A

Something else is need to verify A (certificate from
another intermediate CA or root CA)

Manually Verifying a Certificate Chain

- Paypal.pem: Save Paypal's certificate to a file called
- Symatec-g3.pem: Save certificate from "Symantec Class 3 EV SSL CA – G3"
- VeriSign-G5.pem: Save the VeriSign-G5's certificate from the browser

Root CA's certificate



```
$ openssl verify -verbose -CAfile VeriSign-G5.pem  
-untrusted Symantec-G3.pem Paypal.pem  
Paypal.pem: OK
```



Chain of certificates

Trusted CAs in the Real World

- Not all of the trusted CAs are present in all browsers.
- According to W3Techs in April 2017, Comodo takes most of the market share followed by IdenTrust, Symantec Group, GoDaddy Group, GlobalSign and DigiCert.
- The list of trusted CAs supported by browser can be found:
 - **For the Chrome browser:**
 - Settings -> Show advanced settings -> Manage Certificates
 - **For the Firefox browser:**
 - Edit -> Preferences -> Advanced -> Certificates -> View Certificates -> Certificate Manager -> Authorities

How PKI Defeats the MITM Attack

- Assume that Alice wants to visit `https://example.com`
- When the server sends its public key to Alice, an attacker intercepts the communication. The attacker can do the following things:
 - Attacker forwards the authentic certificate from example.com
 - Attacker creates a fake certificate
 - Attacker sends his/her own certificate to Alice

Attacker Forwards the Authentic Certificate

- Attacker (Mike) forwards the authentic certificate
- Alice sends to the server a **secret**, encrypted using the public key.
- The **secret** is used for establishing an encrypted channel between Alice and server
- Mike doesn't know the corresponding private key, so he cannot find the **secret**.
- Mike can't do much to the communication, except for DoS.
- **MITM attack fails.**

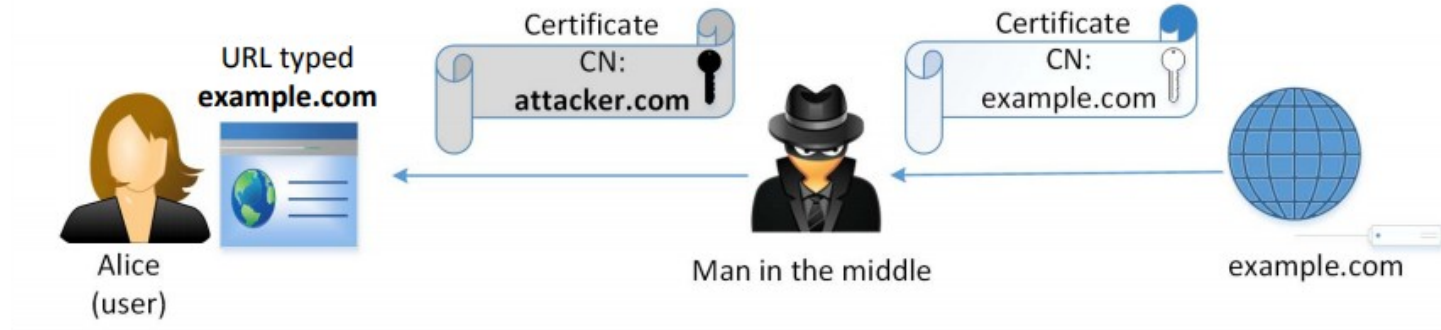
Attacker Creates a Fake Certificate

- Attacker (Mike) creates fraudulent certificate for the example.com domain.
- Mike replaces the server's public with his own public key.
- Trusted CAs will not sign Mike's certificate request as he does not own example.com.
- Mike can sign the fraudulent certificate by himself and create a self-signed certificate.
- Alice's browser will not find any trusted certificate to verify the received certificate and will give the following warning:

```
example.com uses an invalid security certificate.  
The certificate is not trusted because it is self-signed.
```

- **MITM attack fails** if the user decide to terminate the connection

Attacker Sends His/Her Own Certificate

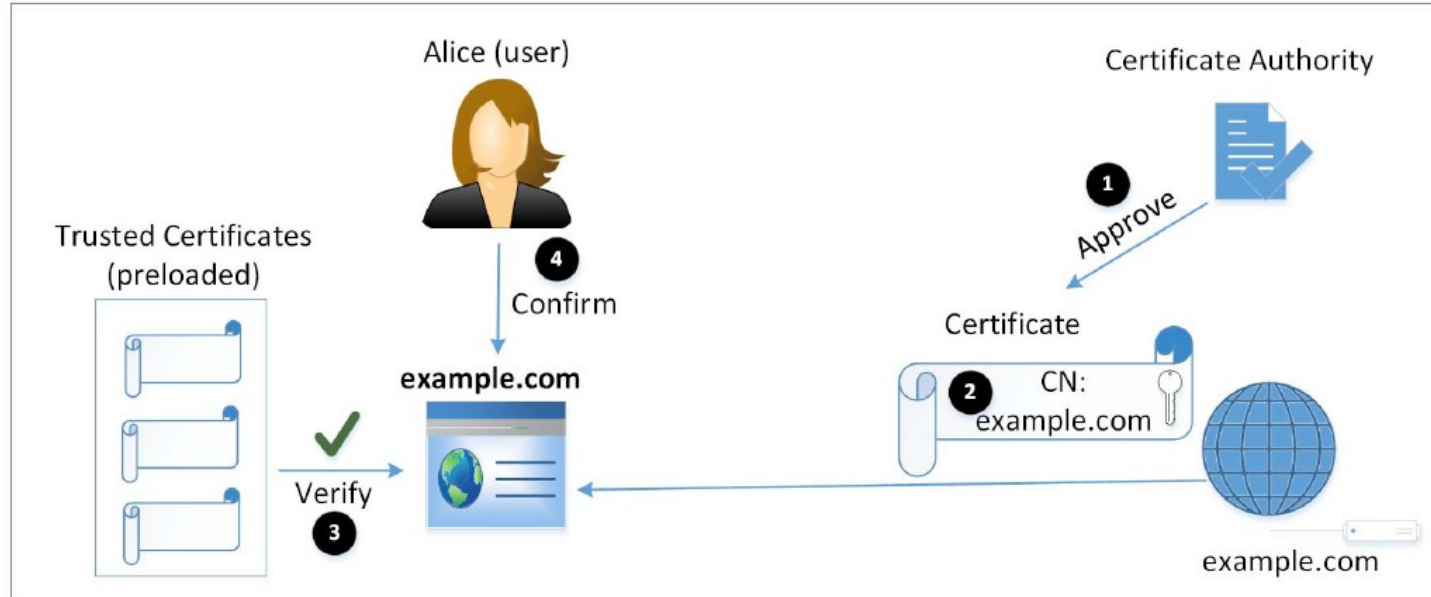


- Attacker's certificate is valid.
- Browser checks if the identity specified in the subject field of the certificate matches the Alice's intent.
 - There is a mismatch: **attacker.com** \neq **example.com**
- Browser terminates handshake protocol: **MITM fails**

The Importance of Verifying Common Name

- During TLS/SSL handshake browsers conduct two important validations
 - 1) Checks whether the received certificate is valid or not.
 - 2) Verifies whether the subject (Common Names) in the certificate is the same as the hostname of the server.
- Not verifying the common name is a common mistake in software

Attacks Surfaces on PKI



Attack on CA's Verification Process

- CA's job has two parts:
 - Verify the relationship between certificate applicant and the subject information inside the certificate
 - Put a digital signature on the certificate
- **Case study: Comodo Breach [March 2011]**
 - Popular root CA.
 - The approval process in Southern Europe was compromised.
 - Nine certificates were issued to seven domains and hence the attacker could provide false attestation.
 - One of the affected domain (a key domain for the Firefox browser):
`addons.mozilla.org`

Attack on CA's Signing Process

- If the CA's private key is compromised, attackers can sign a certificate with any arbitrary data in the subject field.
- **Case Study: the DigiNotar Breach [June-July 2011]**
 - A top commercial CA
 - Attacker got DigiNotar's private key
 - 531 rogue certificates were issued.
 - Traffic intended for Google subdomains was intercepted: MITM attack.
- **How CAs Protect Their Private Key**
 - Hardware Security Model (HSM)

Attacks on Algorithms

- Digital Certificates depend on two types of algorithms
 - one-way hash function and digital signature
- **Case Study: the Collision-Resistant Property of One-Way Hash**
 - At CRYPTO2004, Xiaoyun Wang demonstrated collision attack against MD5.
 - In February 2017, Google Research announced SHAttered attack
 - Attack broke the collision-resistant property of SHA-1
 - Two different PDF files with the same SHA-1 has was created.
- Countermeasures: use stronger algorithm, e.g. SHA256.

Attacks on User Confirmation

- After verifying the certificate from the server, client software is sure that the certificate is valid and authentic
- In addition, the software needs to confirm that the server is what the user intends to interact with.
- Confirmation involves two pieces of information
 - Information provided or approved by user
 - The common name field inside the server's certificate
 - Some software does not compare these two pieces of information: **security flaw**

Attacks on Confirmation: Case Study

Phishing Attack on Common Name with Unicode

- Zheng found out several browsers do not display the domain name correctly if name contains Unicode.
- xn-80ak6aa92e . com is encoded using Cyrillic characters. But domain name displayed by browser likes like apple . com
- Attack:
 - Get a certificate for xn-80ak6aa92e . com
 - Get user to visit xn-80ak6aa92e . com, so the common name is matched
 - User's browser shows that the website is apple.com. **User can be fooled.**
- Had the browser told the user that the actual domain is not the real apple.com, the user would stop.

Types of Digital Certificate

- Domain Validated Certificates (DV)
- Organizational Validated Certificates (OV)
- Extended Validated Certificates (EV)

Domain Validated Certificates (DV)

- Most popular type of certificate.
- The CA verifies the domain records to check if the domain belongs to applicant.
- Domain Control Validation (DCV) is performed on domain name in the certificate request.
- DCV uses information in the WHOIS database
- DCV is conducted via
 - Email
 - HTTP
 - DNS

Organizational Validated Certificates (OV)

- Not very popular type of certificate.
- CAs verify the following before issuing OV certificates:
 - Domain control validation.
 - Applicant's identity and address.
 - Applicant's link to organization.
 - Organization's address.
 - Organization's WHOIS record.
 - Callback on organization's verified telephone number.

Extended Validated Certificates (EV)

- CAs issuing EV certificates require documents that are legally signed from registration authorities.
- EV CA validate the following information:
 - Domain control validation.
 - Verify the identity, authority, signature and link of the individual.
 - Verify the organization's physical address and telephone number.
 - Verify the operational existence.
 - Verify the legal and proper standings of the organization.
- EV certificate, hence, costs higher but is trustworthy.

How Browsers Display Certificate Types

Chrome browser

DV/OV Certificate

 Secure | <https://www.microsoft.com/en-us/>

EV Certificate

 PayPal, Inc. [US] | <https://www.paypal.com/us/home>

Firefox browser

DV/OV Certificate

 <https://www.microsoft.com/en-us/>

EV Certificate

 PayPal, Inc. (US) | <https://www.paypal.com/us/home>

Summary

- MITM attacks on public key cryptography
- Public-Key Infrastructure
- X.509 digital certificate
- Certificate Authority and how CA signs certificate
- How PKI defeats MITM attacks
- Attacks on PKI
- Different types of digital certificate