Internet Security

Public-Key Encryption and PKI

Public-Key Cryptography: History and Concept

1969 Jame Ellis — { No-secret key . encryption
secret key : decryption

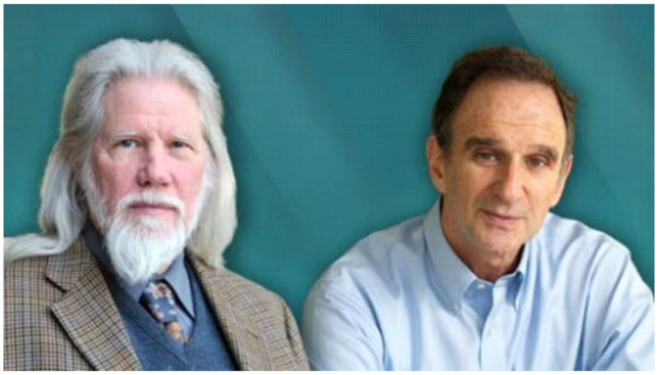
1976 { Whitfield Diffie
Martin Hellman (Stanford)

Diffie-Hellman
Key Exchange ✓

1976 { Rivest
Shamir
Adleman } (MIT) ⇒ RSA ✓

GCHQ Clifford Cocks 1973

Inventors of Public-Key Encryption



Whitfield Diffie Martin Hellman

2015 Turing Award Winner

Leonard Adleman

Ron Rivest

Adi Shamir

2002 Turing Award Winner

Clifford Cocks

RSA Algorithm

public key (e, n) $\quad 3 \quad 65537 = 2^{16}+1$

private key $(d \;\; n)$

Encryption. $M^e \bmod n \Longrightarrow C$

Decryption: $C^d \bmod n = M$

$$(M^e)^d \bmod n = \boxed{M^{e\cdot d} \bmod n = M}$$

Euler theorem

For any $M < p$ and q $\quad$ (p, q are prime #s)

$$\Rightarrow \; M^{(p-1)(q-1)+1} \bmod p\cdot q = 1 \cdot M$$

find p, q $\quad \boxed{n = p\cdot q}$, $\quad e = 65537$

$$\boxed{e\cdot d = 1(p-1)(q-1)+1}$$

$$e\cdot d = k(p-1)(q-1)+1$$

$$\Downarrow$$

$$\Rightarrow \; \boxed{e\cdot d \bmod (p-1)(q-1) = 1} \quad M$$

$$M^{e\cdot d} \bmod n$$

$$= M^{k(p-1)(q-1)} \cdot M \bmod n$$

$$= \left(M^{(p-1)(q-1)}\right)^{k} \cdot M \bmod n$$

$$= \underbrace{\cancel{\left(M^{(p-1)(q-1)} \bmod n\right)}^{\cancel{k}}}_{1} \cdot M \bmod n$$

find, p, q, $\boxed{n = p\cdot q}$,

find e

find d, s.t. $\boxed{e\cdot d \bmod (p-1)(q-1) = 1}$ $\Longrightarrow$ Extended Euclidian Algorithm

$a \cdot X \bmod n = 1$

$\underline{X = \boxed{a^{-1}}} \bmod n$

$n = 33$

$e = 17$

$\underline{M = 31}$

Exercise Related to RSA

Let n = 33 and e = 17.

1. Find the private key d.
2. Encrypt the message M = 31.

Assume RSA is used.

For 2, you don't need to get the final numeric results; showing the expression is sufficient. ~~You do need to find the numeric value of the private key, though~~.

$$n = 33 = 3 \times 11$$

$$e \cdot d \mod \underbrace{(3-1)(11-1)} = 1$$

$$e \cdot d \mod 20 = 1$$

$$17 \cdot \underset{13}{d} \mod 20 = 1$$

$$17 \cdot 13 = 221 \mod 20 = 1$$

$$\begin{cases} M^{17} \mod \overset{p.9}{33} = C \\ C^{13} \mod 33 = M \end{cases}$$

Computing Using Big Numbers

$$\underline{(31^{17} \bmod 33}$$

$$\downarrow$$

$$\cancel{\boxed{31^{17}}}$$

$$\underbrace{\underbrace{31 \cdot 31}_{\bmod n} \cdot 31}_{\bmod n} \cdot 31 \cdot 31 \cdots 31$$

$$\underline{(31^{2} \bmod 33)} \cdot \underline{31^{15}}$$

$$z = \underline{(\overbrace{1\,2\,3\,4\,5\,6\,7\,8\,9\,10\,11}^{1024 \text{ bit}} - - - - - - -)}$$

$$31$$

$$2^{1024} / 2^{5}$$

$$2^{1019}$$

$$\boxed{2^{1024}}$$

$$\boxed{\frac{1024}{2}}$$

$$(2^{2})^{2}$$

$$31^{z} = \left(\left(\left(\left(31^{32}\right)^{\cancel{z}/32}\right)^{2}\right)^{2}\right)^{2} \cdots$$

$$2^{2} \quad 2^{4} \quad 2^{8} \quad 2^{16} \quad 2 \cdots$$

$$e^{2^{1024}} = \left(\left(\left(\left(e^{\overset{2^{2}}{\cancel{2}}}\right)^{2}\right)^{2}\right)^{2}\right)$$

Digital Signature

$$[\text{Hash}(M)]^d$$

$$\cancel{M}^d \bmod n = C$$

Signature

(e, n)

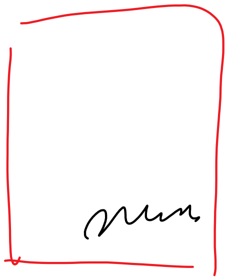
C^e

$M \rightarrow C$

$C^e \bmod n \Rightarrow M$

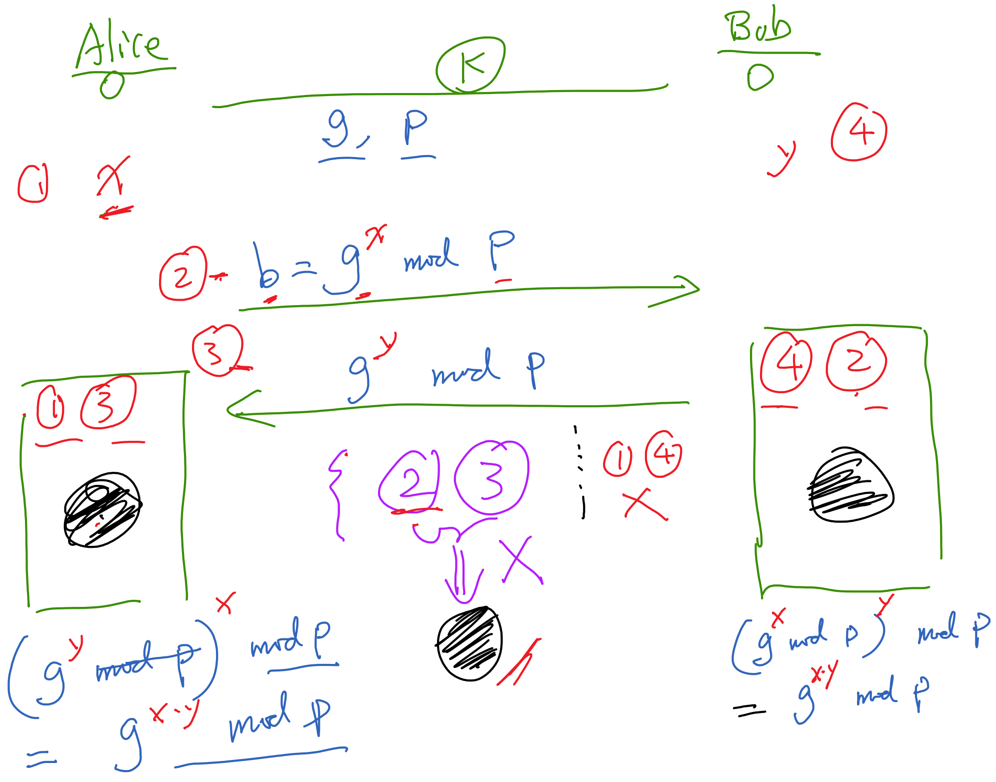
Signature verification

Letter : M



M, signature, (e, n)

Diffie-Hellman Key Exchange



$$g^x = b$$

$$\log_2 g^x = \log_2 b$$

$$x \log_2 g = \log_2 b$$

$$x = \frac{\log_2 b}{\log_2 g}$$

Discrete logarithm problem

Give $a^x \bmod n = b$
solve x

Turn DH to Public-Key Encryption

Alice - public key: $g^x \bmod p$ ✓ ?

private key: x ?

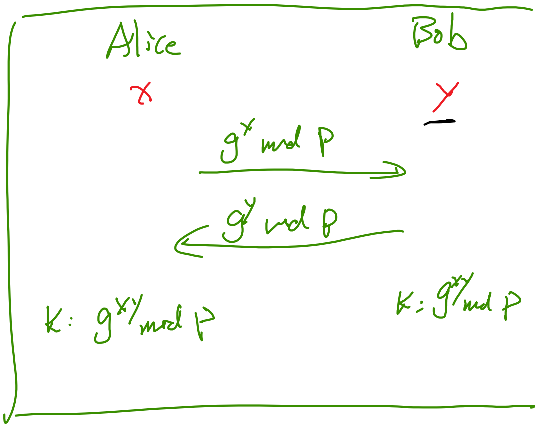
Bob.

Encryption (M): ~~AES~~$_K$(M) $K \cdot M \bmod p$ $K = g^{x \cdot y} \bmod p$; $g^y \bmod p$ ✓

Alice.

Decryption .

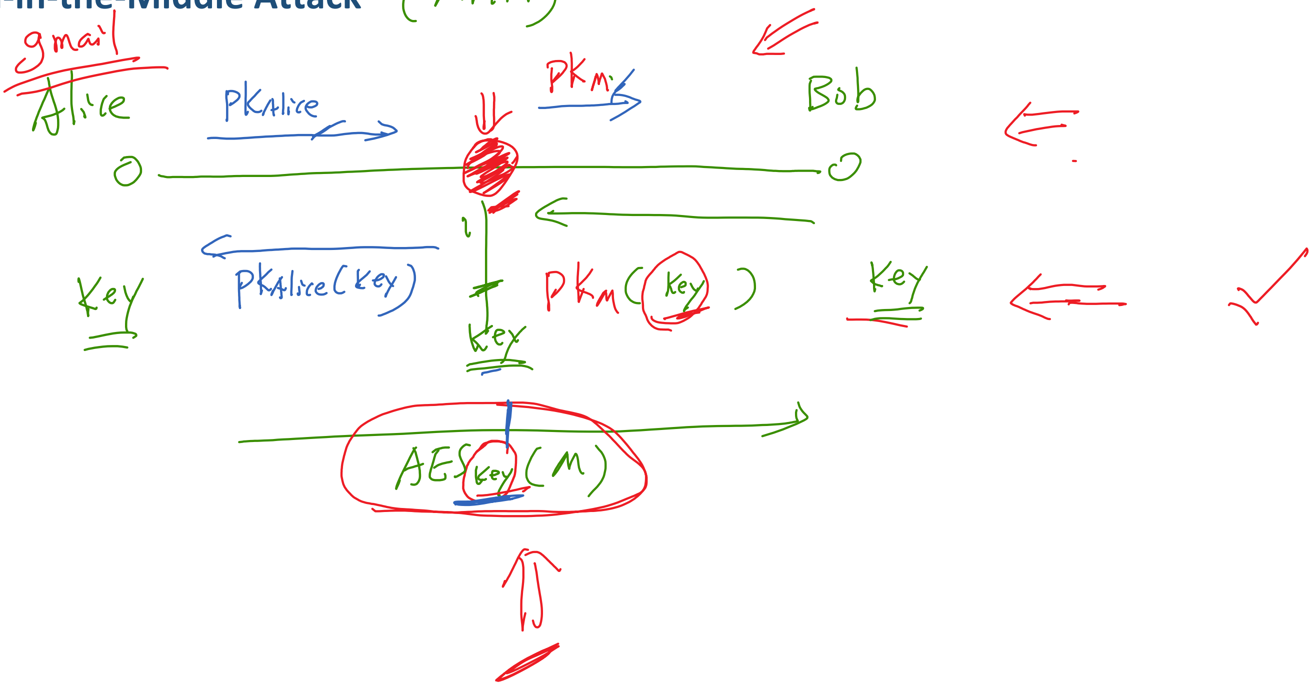
$$\left.\begin{matrix} g^x \bmod p \\ g^y \bmod p \end{matrix}\right\} \not\Rightarrow g^{x \cdot y} \bmod p$$



$$\underbrace{AES_K(M),\quad RSA(K)}$$

PUBLIC-KEY INFRASTRUCTURE (PKI)

Man-in-the-Middle Attack (MITM)



c key

K

Defeating the Man-in-the-Middle Attack Using Digital Signature

❖ Digital Signatures

Owner: $(M)_{sig}$

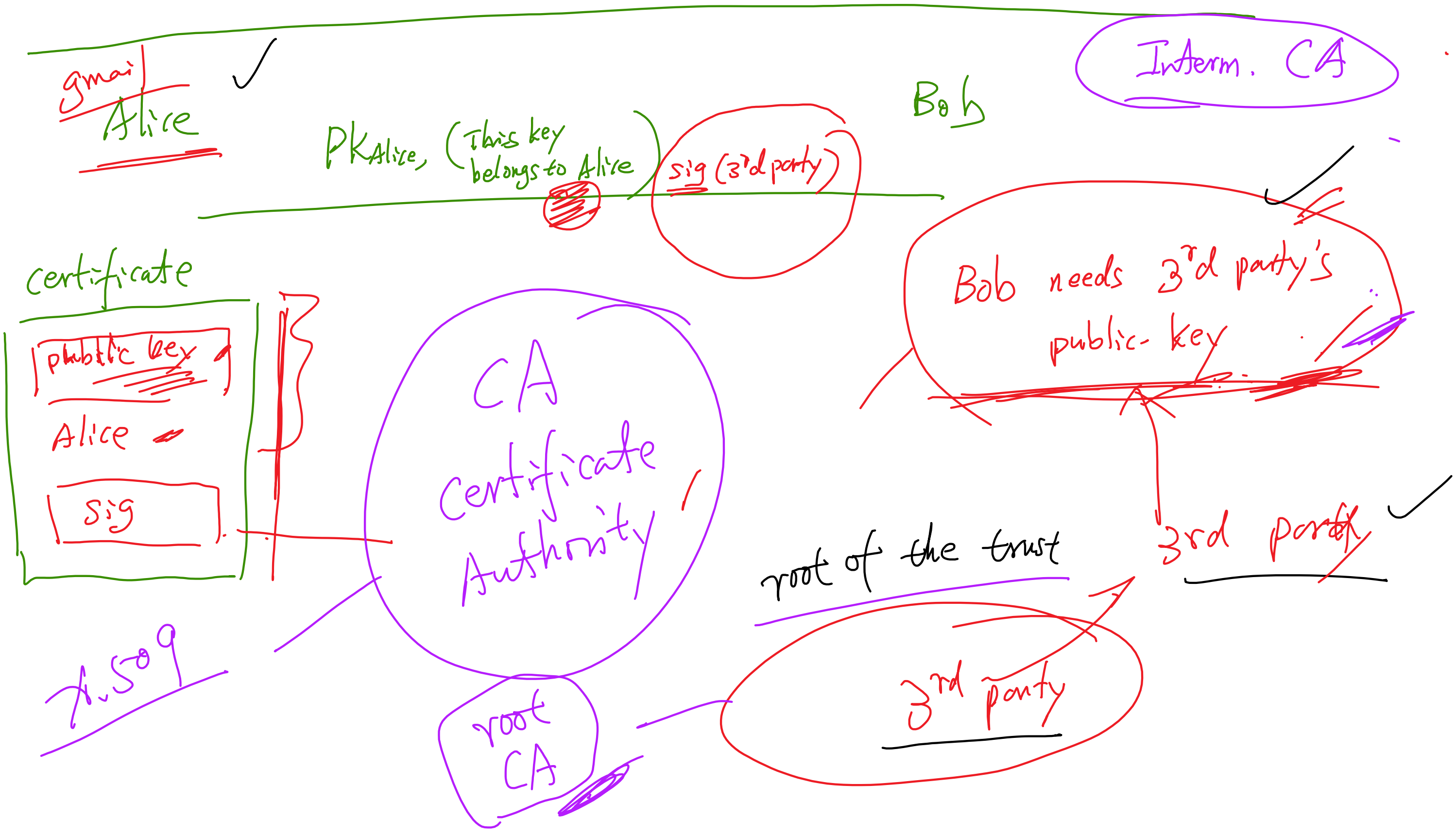
Anybody can verify

RSA

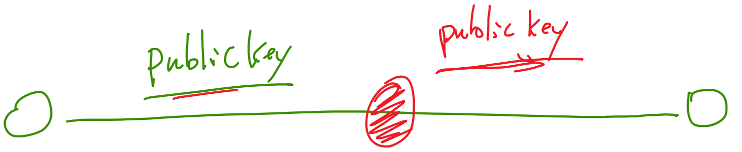
$M^e \bmod n \Rightarrow$ encryption $\Rightarrow$ { everybody can do it / owner can decrypt

Sig $M^d \bmod n \Rightarrow$ Signature. $\Rightarrow$ { only owner can do it / everbody can verify

(M, Sig) $H(M) \stackrel{?}{=} (Sig)^e \bmod n$

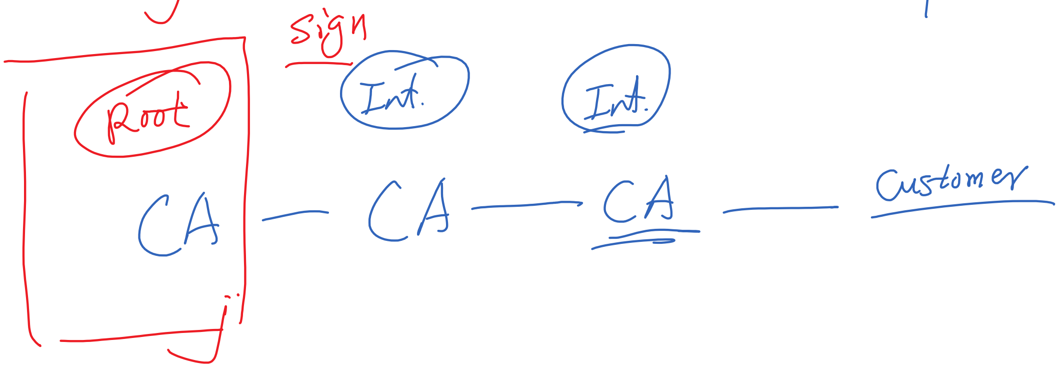


Review



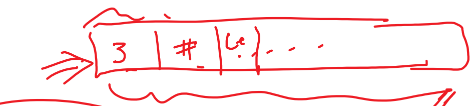
CA

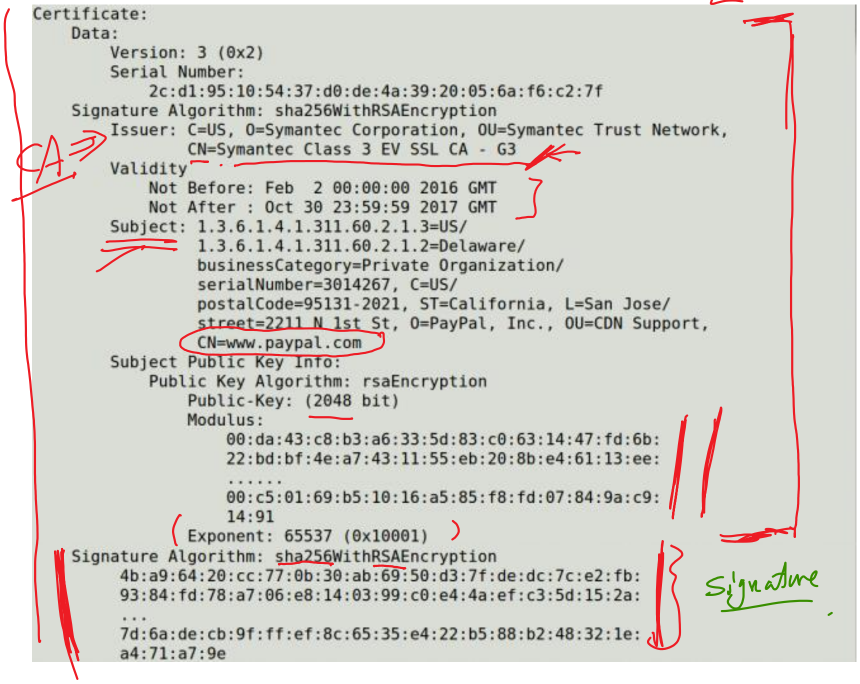
- prove you know the private key (owner of the key) ✓
- prove owner of the identity — domain
  - www.example.com/file
  - DNS
  - email



X.509 Certificate (paypal)

```
$ openssl x509 -in certificate.crt -text -noout
```

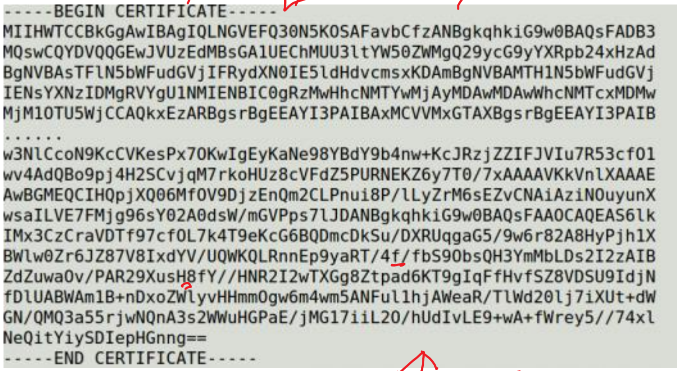




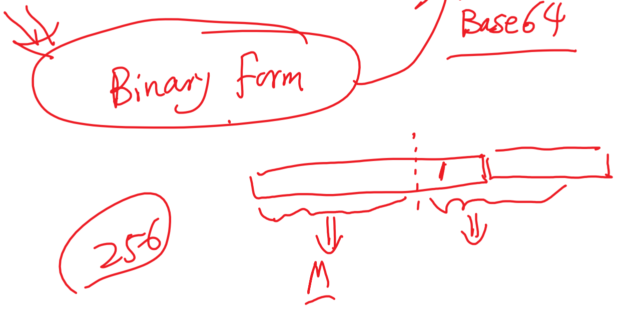
```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            2c:d1:95:10:54:37:d0:de:4a:39:20:05:6a:f6:c2:7f
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=Symantec Corporation, OU=Symantec Trust Network,
                CN=Symantec Class 3 EV SSL CA - 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
        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:
                    ......
                    00:c5:01:69:b5:10:16:a5:85:f8:fd:07:84:9a:c9:
                    14:91
                Exponent: 65537 (0x10001)
    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:
         ...
         7d:6a:de:cb:9f:ff:ef:8c:65:35:e4:22:b5:88:b2:48:32:1e:
         a4:71:a7:9e
```

CA

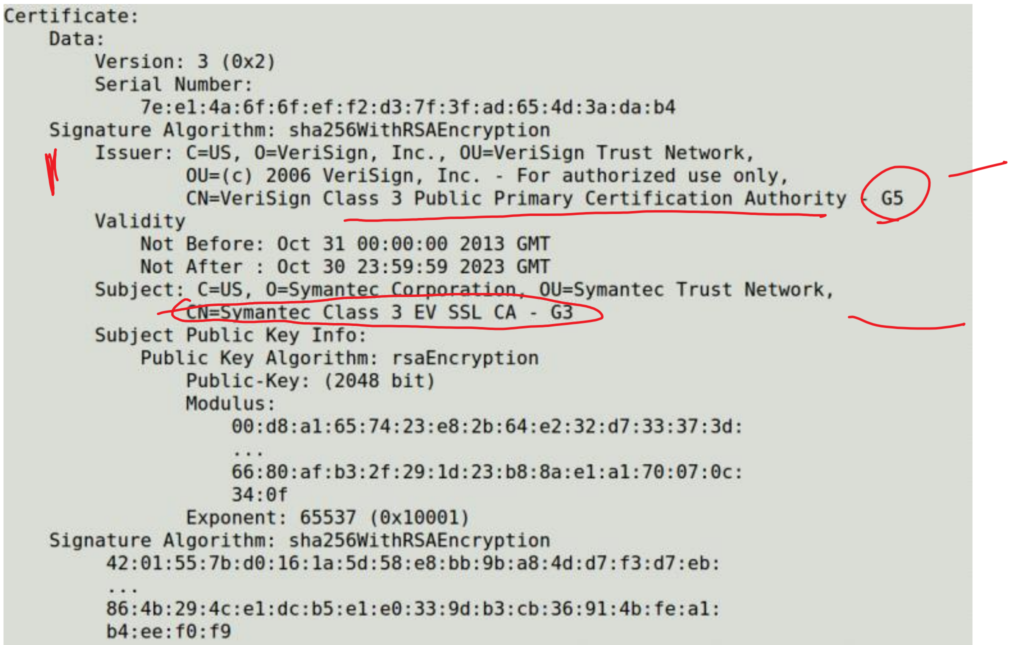
Signature



```
-----BEGIN CERTIFICATE-----
MIIHWTCCBkGgAwIBAgIQLNGVEFQ30N5KOSAFavbCfzANBgkqhkiG9w0BAQsFADB3
MQswCQYDVQQGEwJVUzEdMBsGA1UEChMUU3ltYW50ZWMgQ29ycG9yYXRpb24xHzAd
BgNVBAsTFlN5bWFudGVjIFRydXN0IE5ldHdvcmsxKDAmBgNVBAMTH1N5bWFudGVj
IENsYXNzIDMgRVYgU1NMIENBIC0gRzMwHhcNMTYwMjAyMDAwMDAwWhcNMTcxMDMw
MjM1OTU5WjCCAQkxEzARBgsrBgEEAYI3PAIBAxMCVVMxGTAXBgsrBgEEAYI3PAIB
......
w3NlCcoN9KcCVKesPx7OKwIgEyKaNe98YBdY9b4nw+KcJRzjZZIFJVIu7R53cfO1
wv4AdQBo9pj4H2SCvjqM7rkoHUz8cVFdZ5PURNEKZ6y7T0/7xAAAAVKkVnlXAAAE
AwBGMEQCIHQpjXQ06MfOV9DjzEnQm2CLPnui8P/lLyZrM6sEZvCNAiAziNOuyunX
wsaILVE7FMjg96sY02A0dsW/mGVPps7lJDANBgkqhkiG9w0BAQsFAAOCAQEAS6lk
IMx3CzCraVDTf97cfOL7k4T9eKcG6BQDmcDkSu/DXRUqgaG5/9w6r82A8HyPjh1X
BWlw0Zr6JZ87V8IxdYV/UQWKQLRnnEp9yaRT/4f/fbS9ObsQH3YmMbLDs2I2zAIB
ZdZuwaOv/PAR29XusH8fY//HNR2I2wTXGg8Ztpad6KT9gIqFfHvfSZ8VDSU9IdjN
fDlUABWAm1B+nDxoZWlyvHHmmOgw6m4wm5ANFul1hjAWeaR/TlWd20lj7iXUt+dW
GN/QMQ3a55rjwNQnA3s2WWuHGPaE/jMG17iiL2O/hUdIvLE9+wA+fWrey5//74xl
NeQitYiySDIepHGnng==
-----END CERTIFICATE-----
```



CA's X.509 Certificate

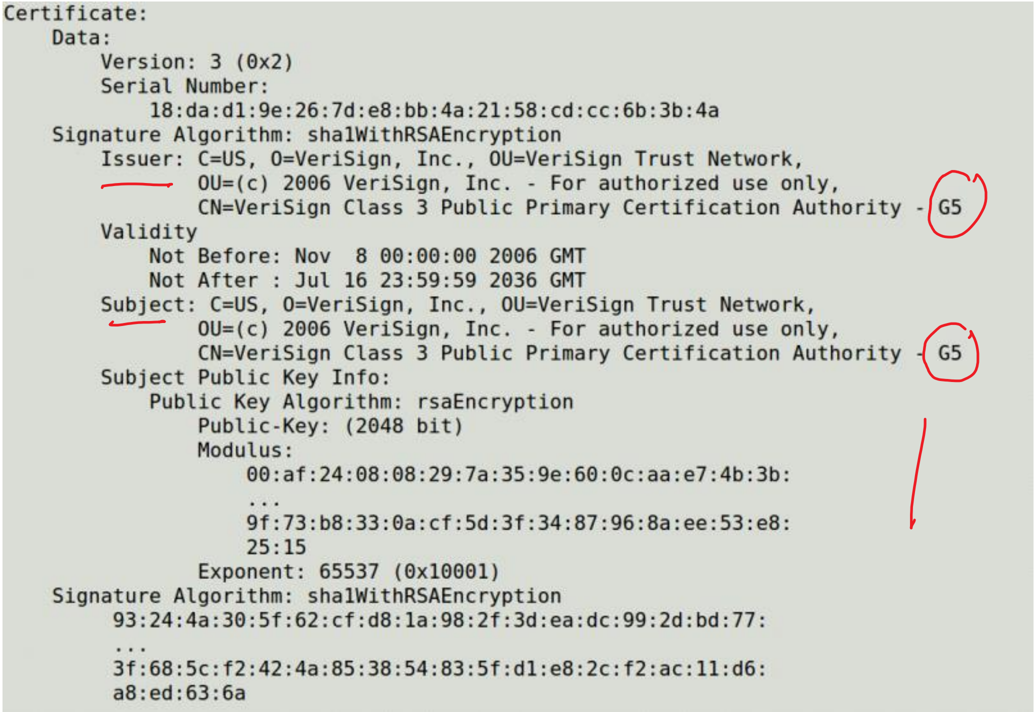


```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            7e:e1:4a:6f:6f:ef:f2:d3:7f:3f:ad:65:4d:3a:da:b4
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network,
                OU=(c) 2006 VeriSign, Inc. - For authorized use only,
                CN=VeriSign Class 3 Public Primary Certification Authority - G5
        Validity
            Not Before: Oct 31 00:00:00 2013 GMT
            Not After : Oct 30 23:59:59 2023 GMT
        Subject: C=US, O=Symantec Corporation, OU=Symantec Trust Network,
                CN=Symantec Class 3 EV SSL CA - G3
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:d8:a1:65:74:23:e8:2b:64:e2:32:d7:33:37:3d:
                    ...
                    66:80:af:b3:2f:29:1d:23:b8:8a:e1:a1:70:07:0c:
                    34:0f
                Exponent: 65537 (0x10001)
    Signature Algorithm: sha256WithRSAEncryption
         42:01:55:7b:d0:16:1a:5d:58:e8:bb:9b:a8:4d:d7:f3:d7:eb:
         ...
         86:4b:29:4c:e1:dc:b5:e1:e0:33:9d:b3:cb:36:91:4b:fe:a1:
         b4:ee:f0:f9
```

CA

Int. CA

Root CA's X.509 Certificate



```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            18:da:d1:9e:26:7d:e8:bb:4a:21:58:cd:cc:6b:3b:4a
    Signature Algorithm: sha1WithRSAEncryption
        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
        Validity
            Not Before: Nov  8 00:00:00 2006 GMT
            Not After : Jul 16 23:59:59 2036 GMT
        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
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:af:24:08:08:29:7a:35:9e:60:0c:aa:e7:4b:3b:
                    ...
                    9f:73:b8:33:0a:cf:5d:3f:34:87:96:8a:ee:53:e8:
                    25:15
                Exponent: 65537 (0x10001)
    Signature Algorithm: sha1WithRSAEncryption
         93:24:4a:30:5f:62:cf:d8:1a:98:2f:3d:ea:dc:99:2d:bd:77:
         ...
         3f:68:5c:f2:42:4a:85:38:54:83:5f:d1:e8:2c:f2:ac:11:d6:
         a8:ed:63:6a
```

self-signed

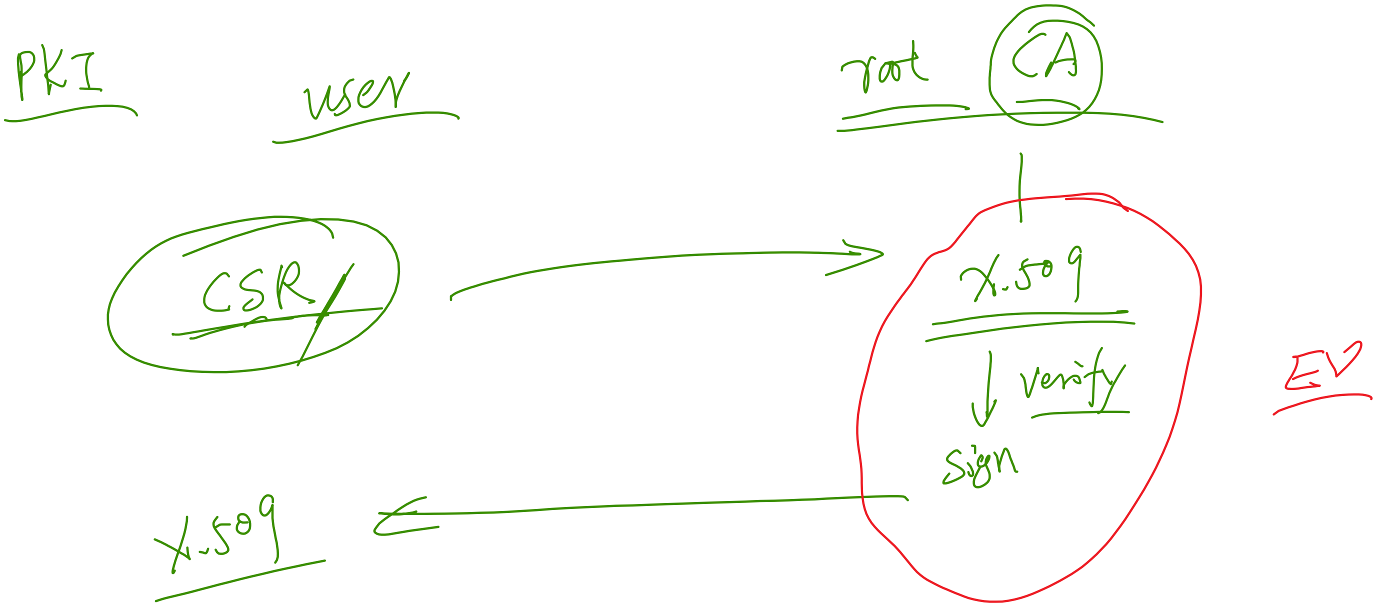
root - CA

Root Certificate Authority (CA)

Survey result on April 2016:

- Comodo Group: 40.6%
- Symantec: 26.0% market share
- GoDaddy: 11.8%
- GlobalSign: 9.7%

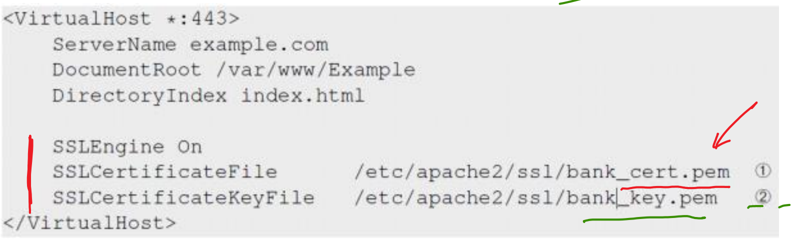
Getting X.509 Certificate from CA



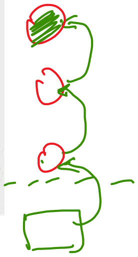
Set up HTTPS Web Server using X.509 Certificate

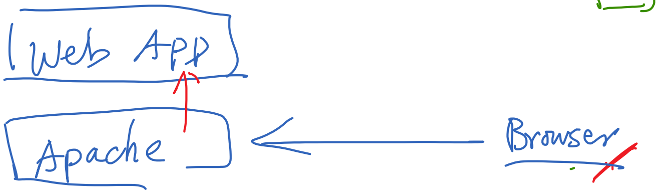
❖ Apache configuration file

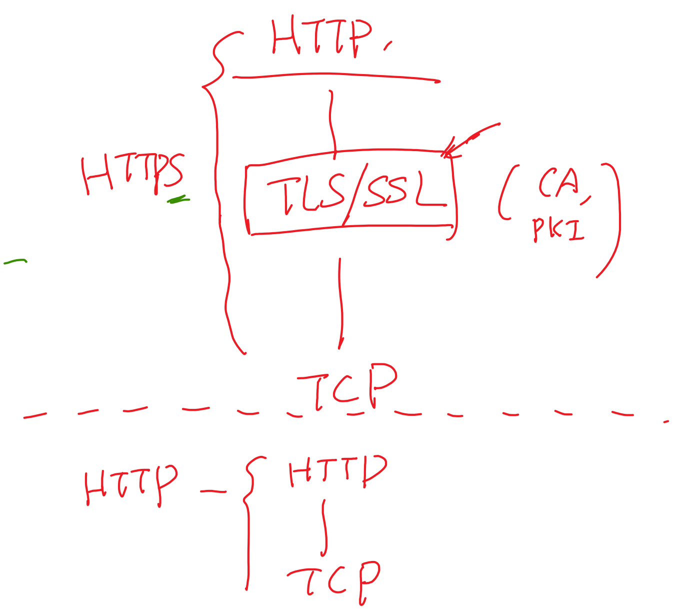
12.04



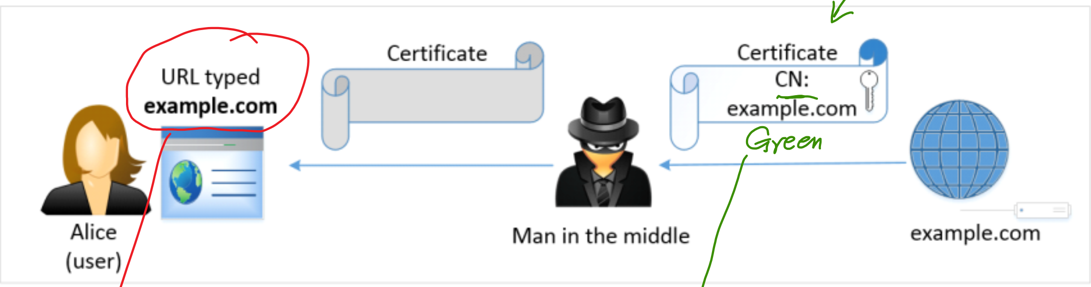
```
<VirtualHost *:443>
    ServerName example.com
    DocumentRoot /var/www/Example
    DirectoryIndex index.html

    SSLEngine On
    SSLCertificateFile      /etc/apache2/ssl/bank_cert.pem   ①
    SSLCertificateKeyFile   /etc/apache2/ssl/bank_key.pem    ②
</VirtualHost>
```







How PKI Defeats MITM Attacks



Hostname ≟ CN

certificate check

Attacker's public key

CN: attacker.com

Sig

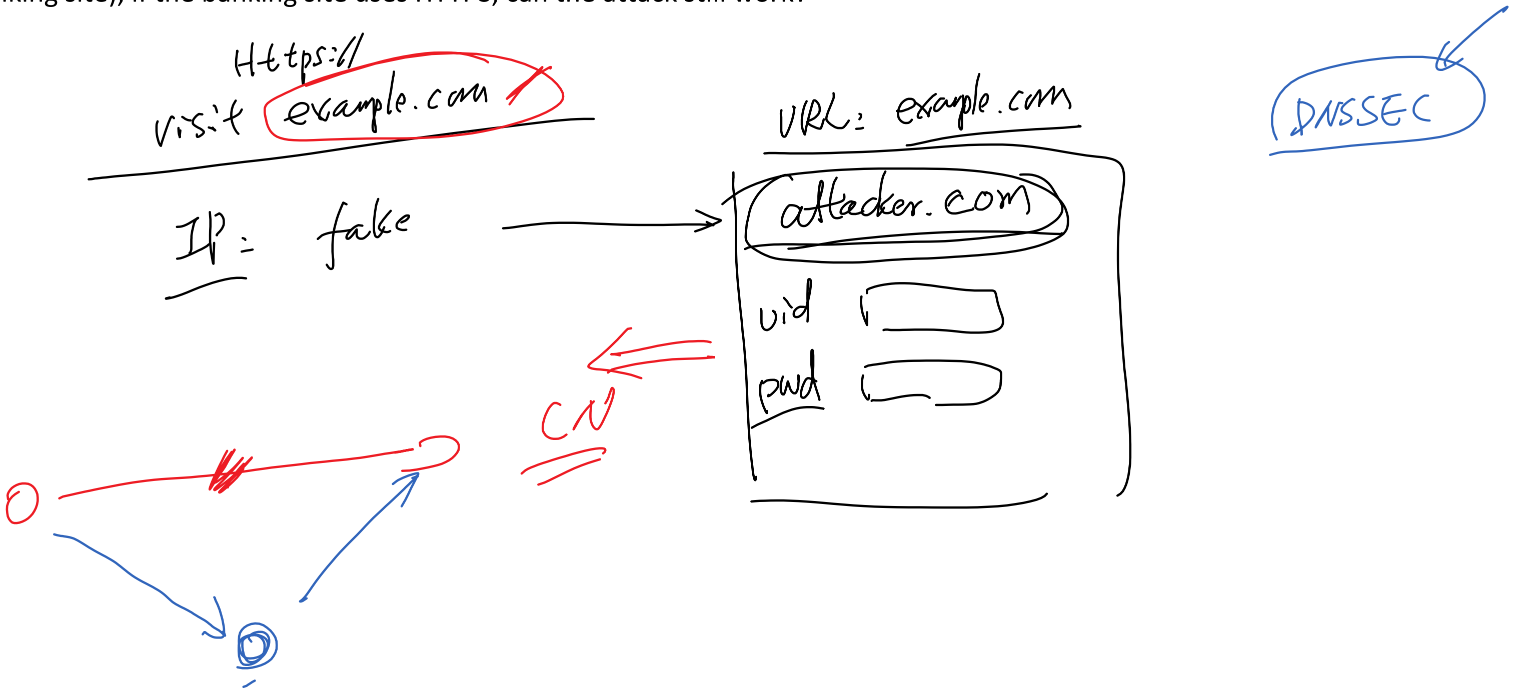
SV

VPN

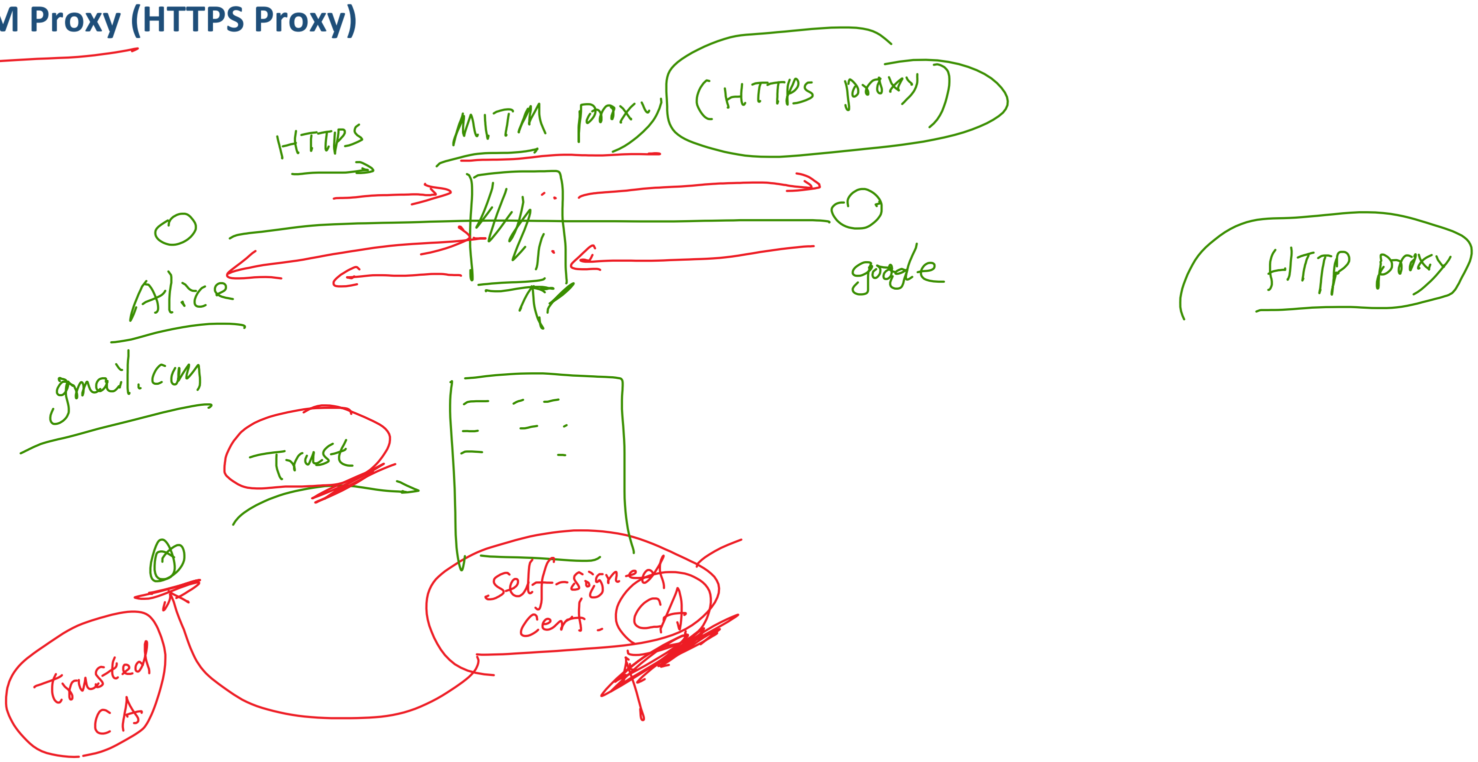
cert.

Question: DNS

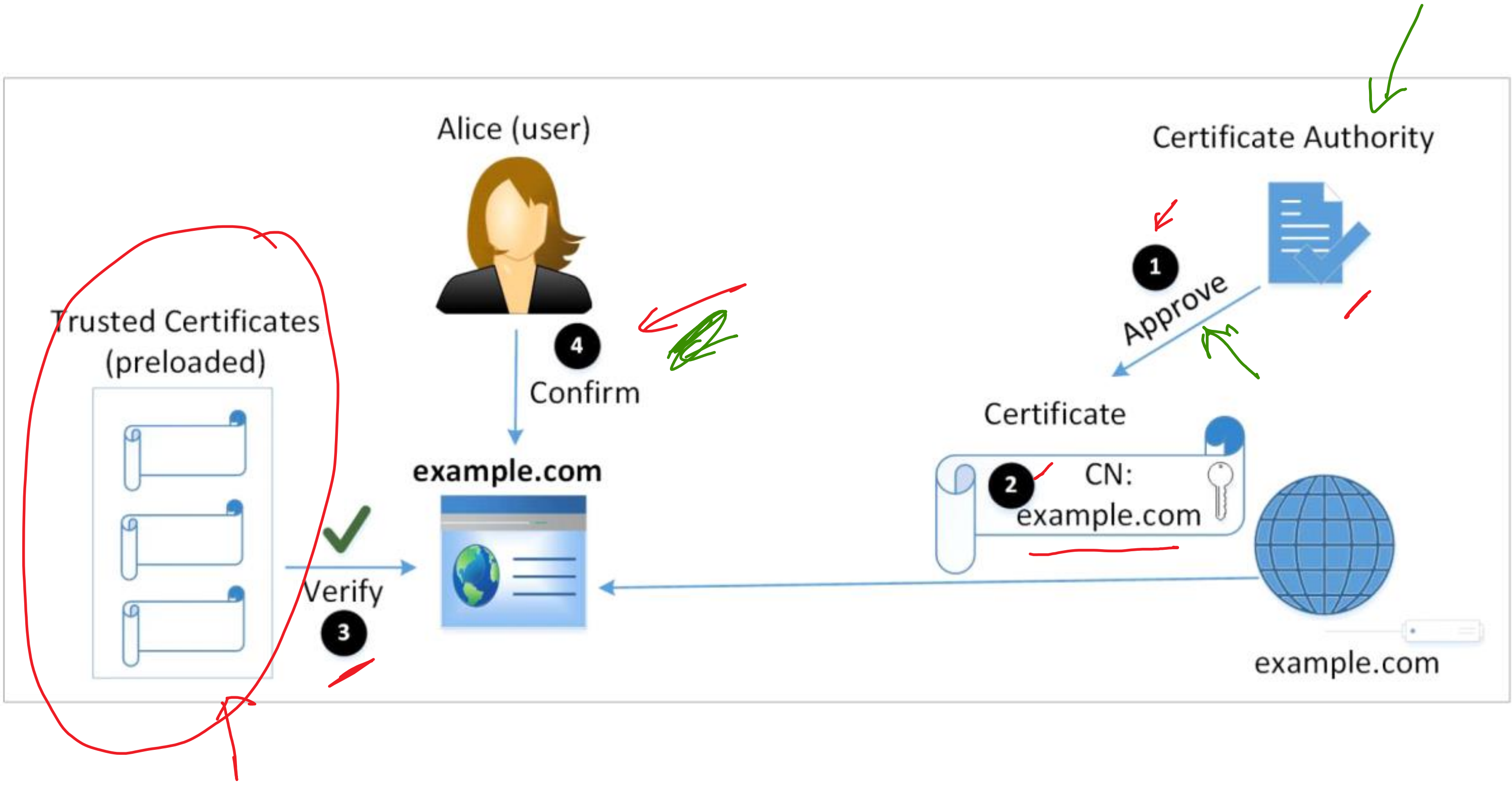
For the DNS cache-poisoning attack (i.e., provide a fake IP address for a banking site), if the banking site uses HTTPS, can the attack still work?



MITM Proxy (HTTPS Proxy)

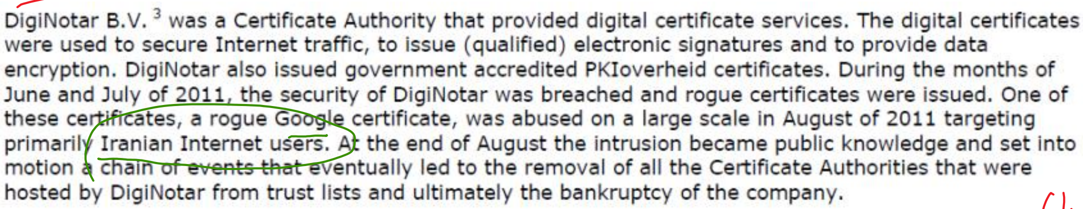


Attacks on PKI ❶❷❸❹

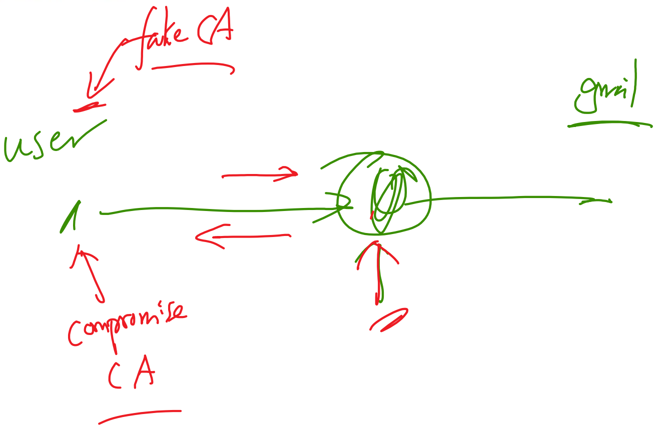


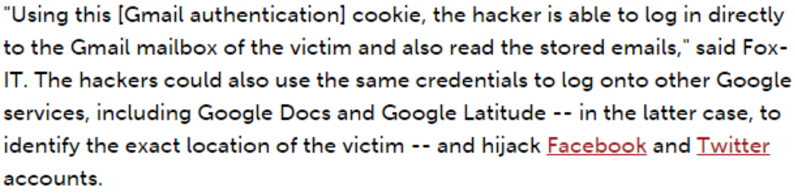
Attack on CA ❶

DigiNotar Case Study

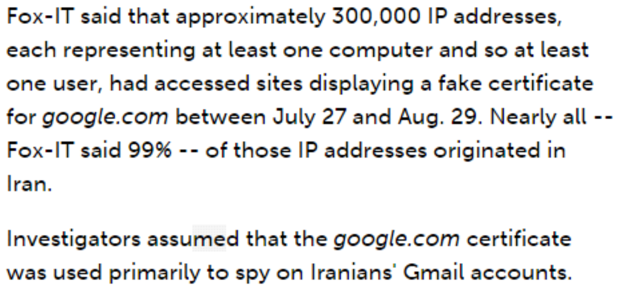


DigiNotar B.V. [3] was a Certificate Authority that provided digital certificate services. The digital certificates were used to secure Internet traffic, to issue (qualified) electronic signatures and to provide data encryption. DigiNotar also issued government accredited PKIoverheid certificates. During the months of June and July of 2011, the security of DigiNotar was breached and rogue certificates were issued. One of these certificates, a rogue Google certificate, was abused on a large scale in August of 2011 targeting primarily Iranian Internet users. At the end of August the intrusion became public knowledge and set into motion a chain of events that eventually led to the removal of all the Certificate Authorities that were hosted by DigiNotar from trust lists and ultimately the bankruptcy of the company.





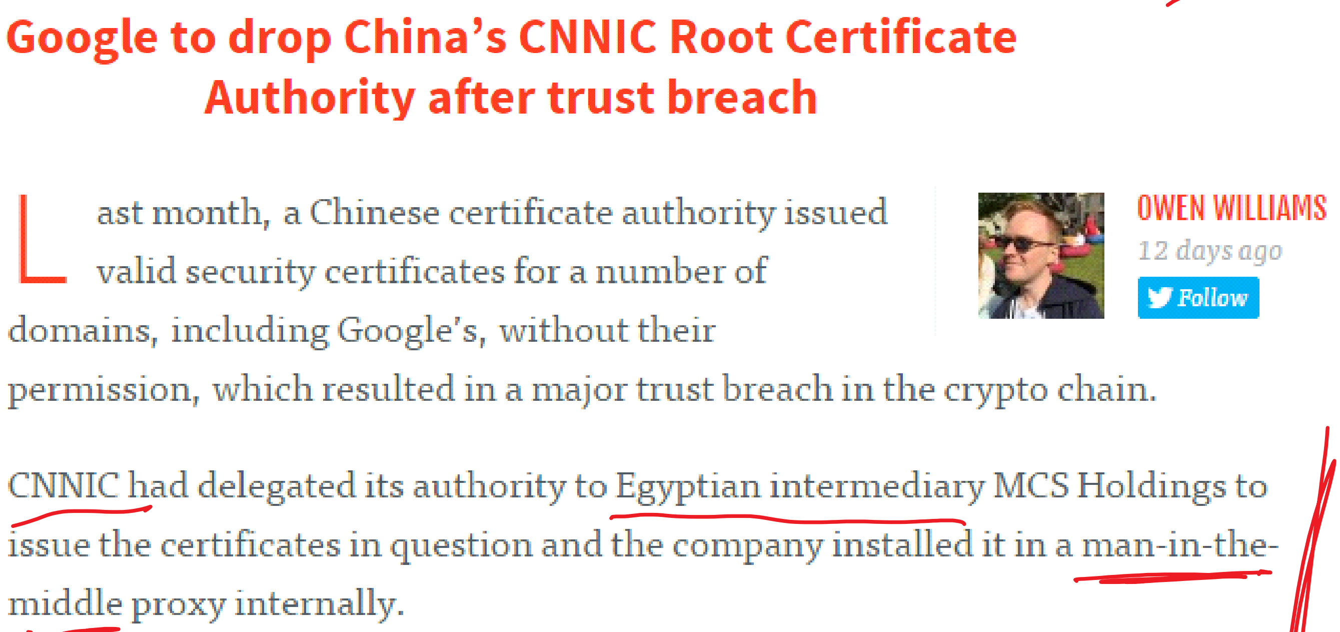
"Using this [Gmail authentication] cookie, the hacker is able to log in directly to the Gmail mailbox of the victim and also read the stored emails," said Fox-IT. The hackers could also use the same credentials to log onto other Google services, including Google Docs and Google Latitude -- in the latter case, to identify the exact location of the victim -- and hijack Facebook and Twitter accounts.



Fox-IT said that approximately 300,000 IP addresses, each representing at least one computer and so at least one user, had accessed sites displaying a fake certificate for *google.com* between July 27 and Aug. 29. Nearly all -- Fox-IT said 99% -- of those IP addresses originated in Iran.

Investigators assumed that the *google.com* certificate was used primarily to spy on Iranians' Gmail accounts.

CNNIC Case Study



Google to drop China's CNNIC Root Certificate Authority after trust breach

OWEN WILLIAMS

12 days ago

Last month, a Chinese certificate authority issued valid security certificates for a number of domains, including Google's, without their permission, which resulted in a major trust breach in the crypto chain.

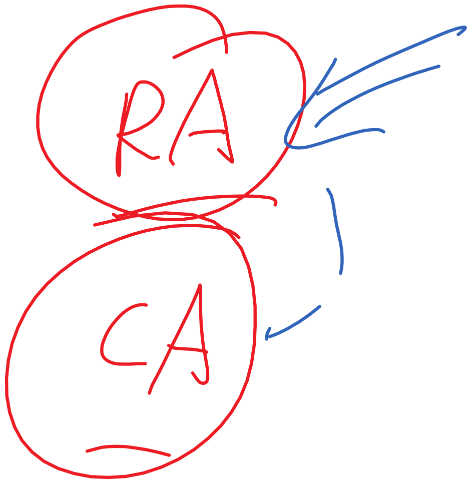
CNNIC had delegated its authority to Egyptian intermediary MCS Holdings to issue the certificates in question and the company installed it in a man-in-the-middle proxy internally.

Protecting CA

Comodo Case Study (March 2011)

Verification

Signing



Countermeasure: Certificate Pinning

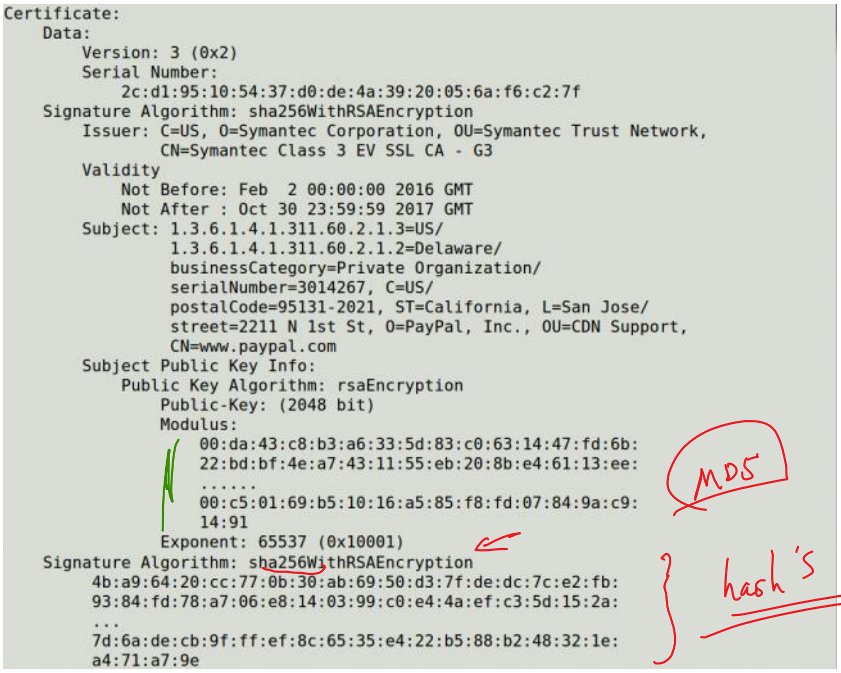
Chrome

App (chase.com)

pin { cert of chase.com
public key

Attack on Algorithm ❷

The Imporance of Collision Resistance



```
Certificate:
    Data:
        Version: 3 (0x2)
        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
        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:
                    ......
                    00:c5:01:69:b5:10:16:a5:85:f8:fd:07:84:9a:c9:
                    14:91
                Exponent: 65537 (0x10001)
    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:
         ...
         7d:6a:de:cb:9f:ff:ef:8c:65:35:e4:22:b5:88:b2:48:32:1e:
         a4:71:a7:9e
```

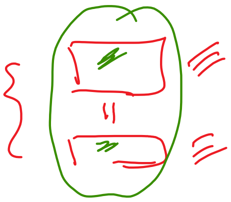
MD5

hash's signature

R1 : example.com

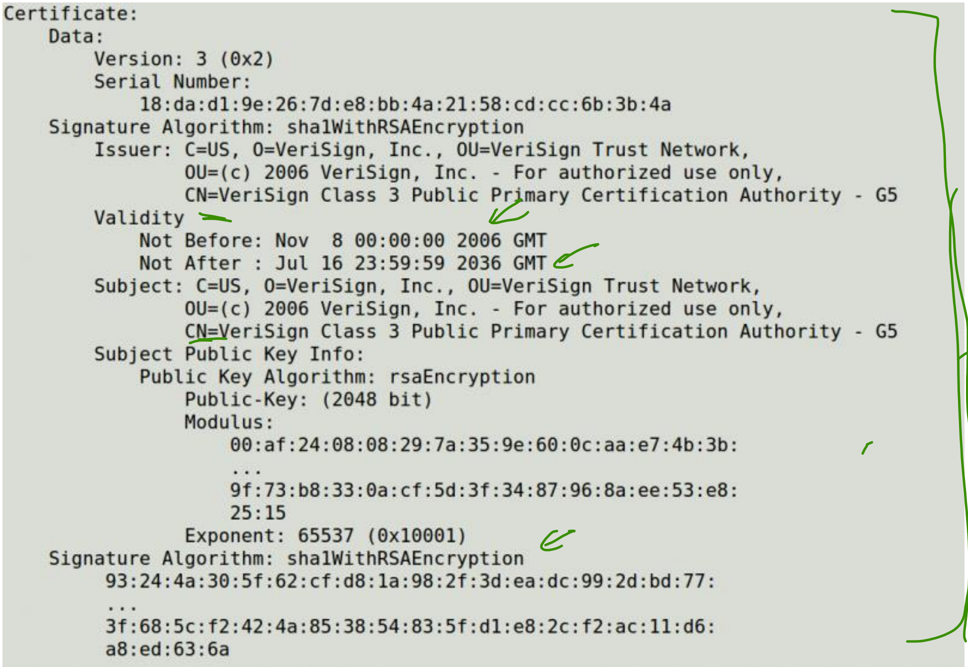
R2 : microsoft.com

same hash



Question: Root CA's certificate and SHA1

Question: I notice that VeriSign's G5 certificate (self-signed) uses sha1, which is proven not to be collision resistant in February 2017, should VeriSign immediately revoke this certificate? Why or Why not?

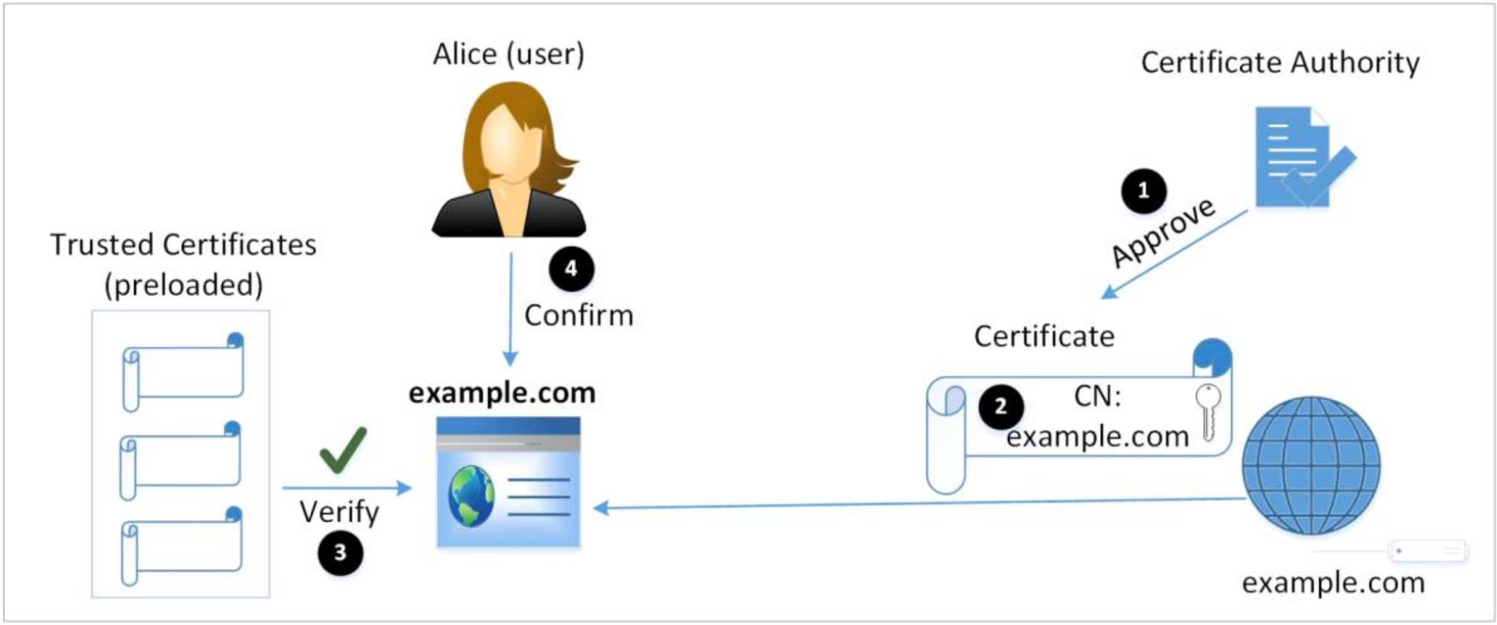


```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            18:da:d1:9e:26:7d:e8:bb:4a:21:58:cd:cc:6b:3b:4a
    Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, O=VeriSign, Inc., OU=VeriSign Trust Network,
                OU=(c) 2006 VeriSign, Inc. - For authorized use only,
                CN=VeriSign Class 3 Public Primary Certification Authority - G5
        Validity
            Not Before: Nov  8 00:00:00 2006 GMT
            Not After : Jul 16 23:59:59 2036 GMT
        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
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:af:24:08:08:29:7a:35:9e:60:0c:aa:e7:4b:3b:
                    ...
                    9f:73:b8:33:0a:cf:5d:3f:34:87:96:8a:ee:53:e8:
                    25:15
                Exponent: 65537 (0x10001)
    Signature Algorithm: sha1WithRSAEncryption
         93:24:4a:30:5f:62:cf:d8:1a:98:2f:3d:ea:dc:99:2d:bd:77:
         ...
         3f:68:5c:f2:42:4a:85:38:54:83:5f:d1:e8:2c:f2:ac:11:d6:
         a8:ed:63:6a
```

C1

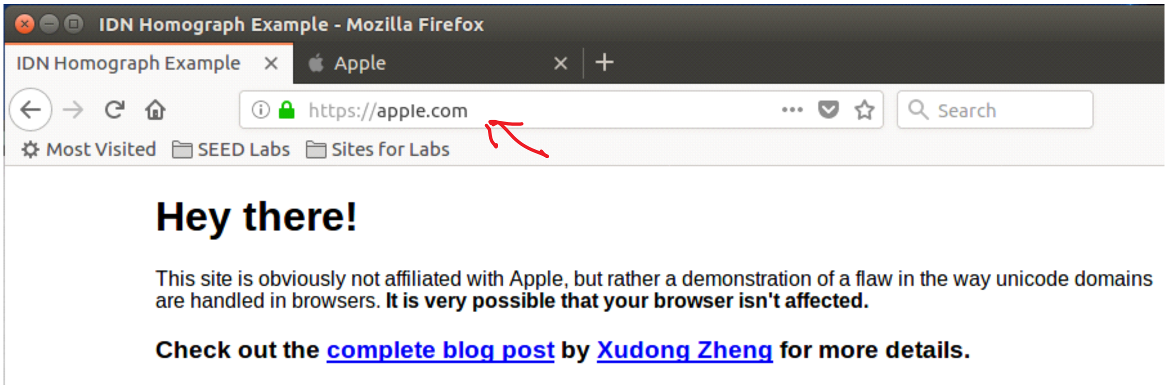
Attack on Trusted Certificates ❸

Attack on User Confirmation ❹



IDN Homograph Attack

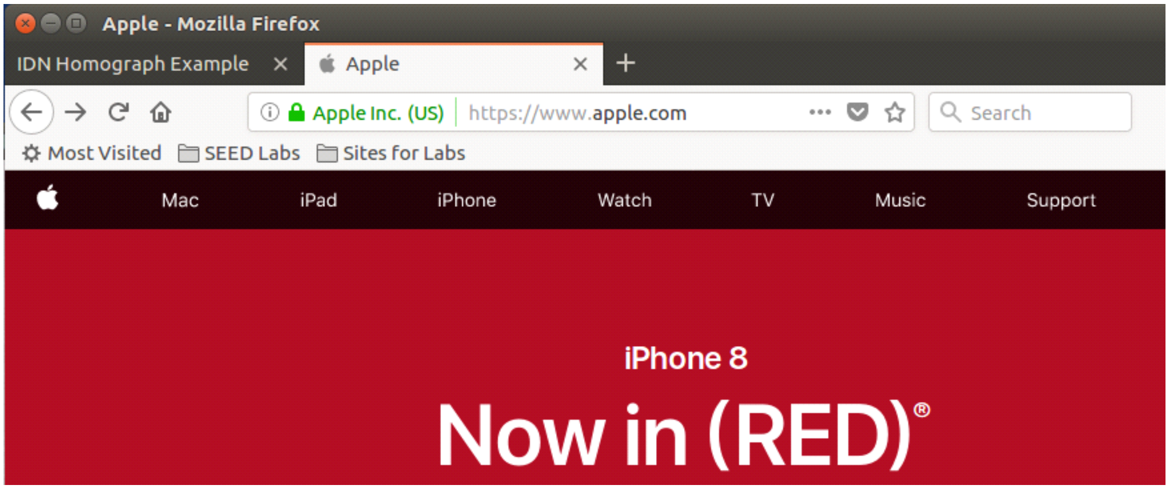
❖ What you see (from Firefox)



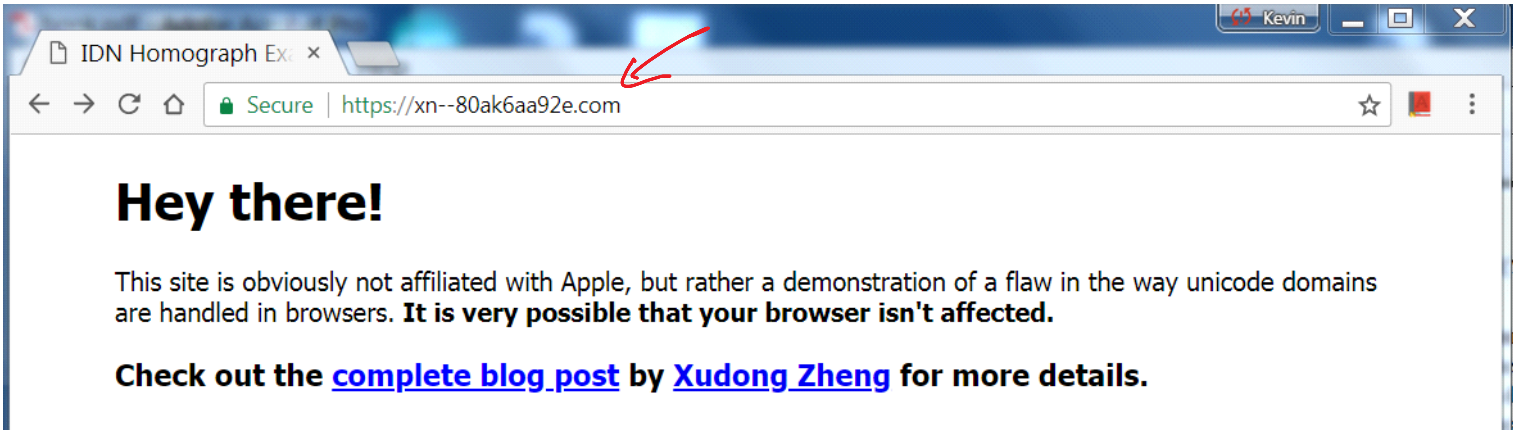
Hey there!

This site is obviously not affiliated with Apple, but rather a demonstration of a flaw in the way unicode domains are handled in browsers. **It is very possible that your browser isn't affected.**

Check out the complete blog post by Xudong Zheng for more details.



❖ The actual name (from Chrome)



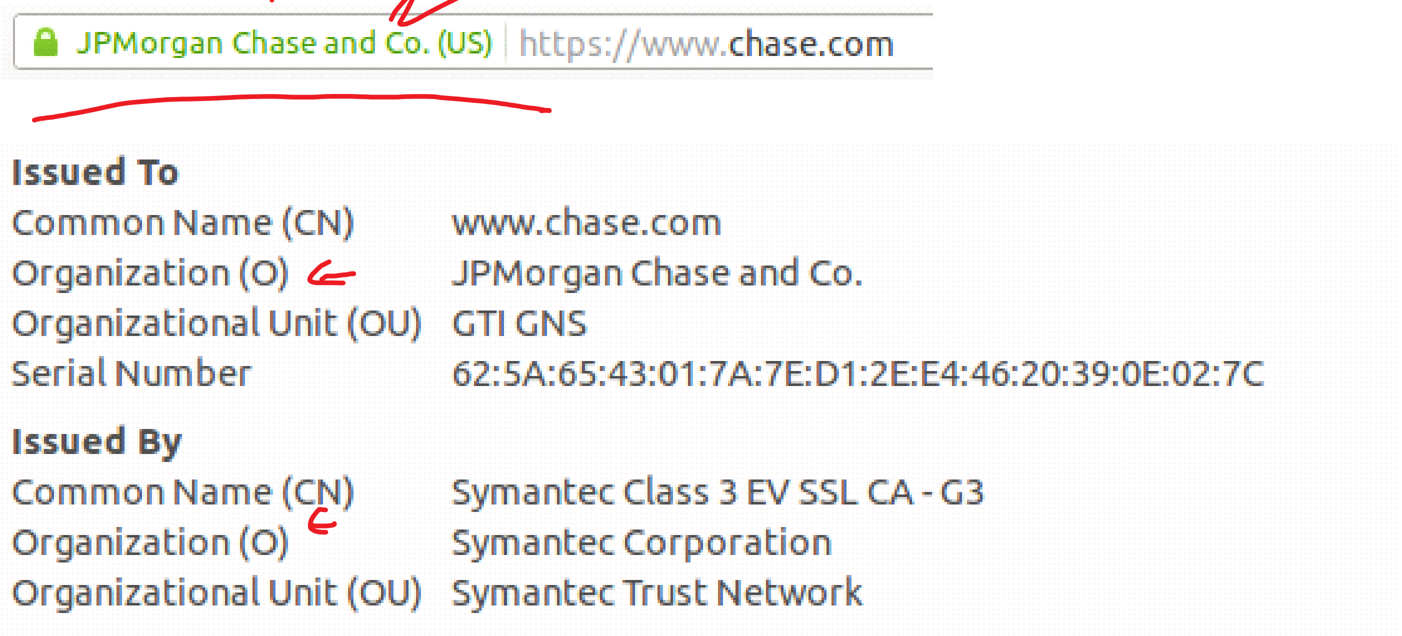
Hey there!

This site is obviously not affiliated with Apple, but rather a demonstration of a flaw in the way unicode domains are handled in browsers. **It is very possible that your browser isn't affected.**

Check out the complete blog post by Xudong Zheng for more details.

Types of X.509 Certificate

- DV: Domain Validated
- OV: Organization Validated
- EV: Extended Validated



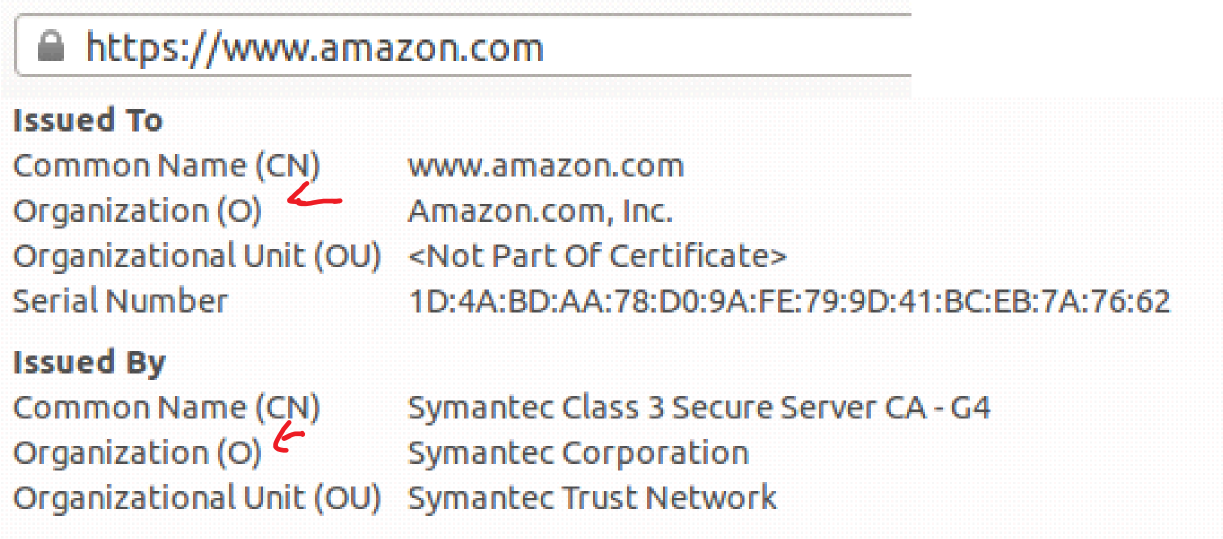
JPMorgan Chase and Co. (US) | https://www.chase.com

Issued To

Common Name (CN)	www.chase.com
Organization (O)	JPMorgan Chase and Co.
Organizational Unit (OU)	GTI GNS
Serial Number	62:5A:65:43:01:7A:7E:D1:2E:E4:46:20:39:0E:02:7C

Issued By

Common Name (CN)	Symantec Class 3 EV SSL CA - G3
Organization (O)	Symantec Corporation
Organizational Unit (OU)	Symantec Trust Network



https://www.amazon.com

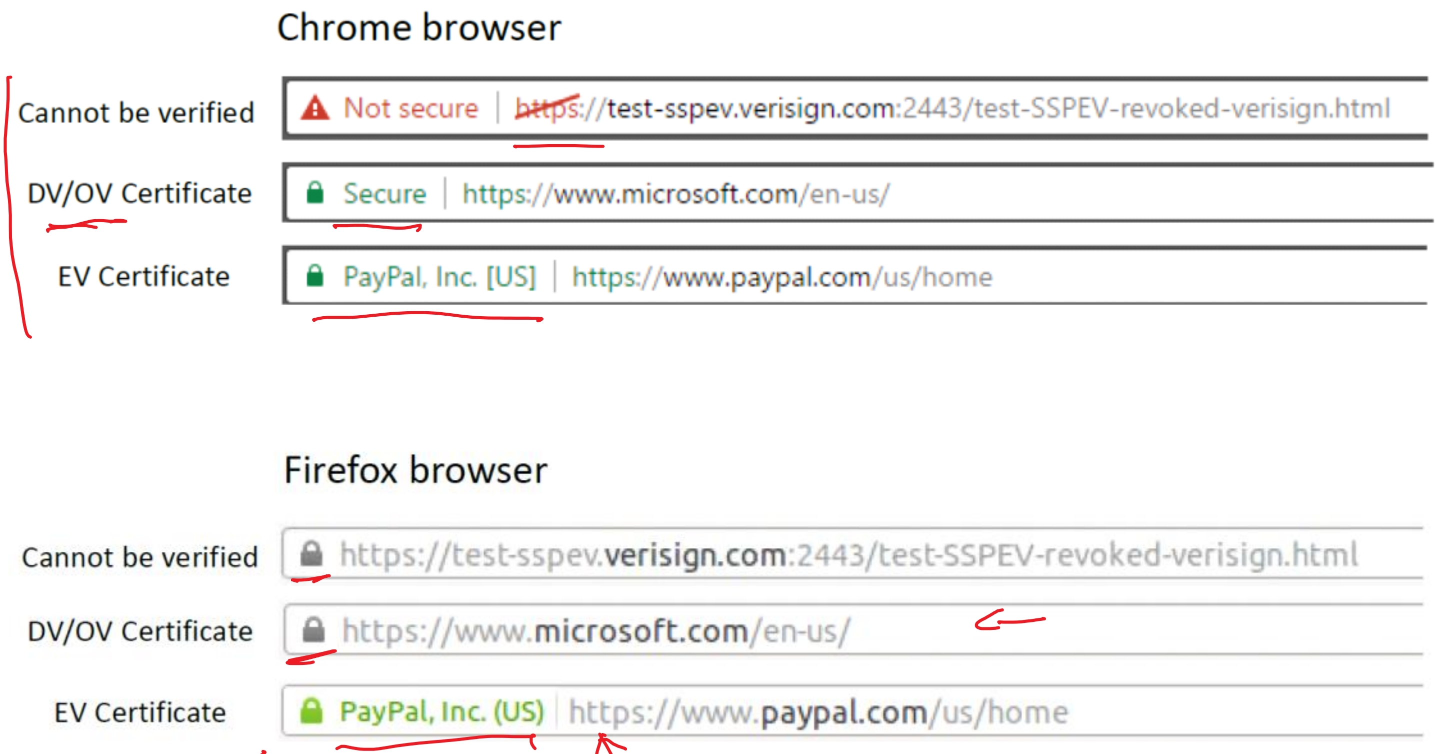
Issued To

Common Name (CN)	www.amazon.com
Organization (O)	Amazon.com, Inc.
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	1D:4A:BD:AA:78:D0:9A:FE:79:9D:41:BC:EB:7A:76:62

Issued By

Common Name (CN)	Symantec Class 3 Secure Server CA - G4
Organization (O)	Symantec Corporation
Organizational Unit (OU)	Symantec Trust Network

Types of X.509 Certificates



Chrome browser

Cannot be verified	⚠ Not secure | ~~https~~://test-sspev.verisign.com:2443/test-SSPEV-revoked-verisign.html
DV/OV Certificate	🔒 Secure | https://www.microsoft.com/en-us/
EV Certificate	🔒 PayPal, Inc. [US] | https://www.paypal.com/us/home

Firefox browser

Cannot be verified	🔒 https://test-sspev.verisign.com:2443/test-SSPEV-revoked-verisign.html
DV/OV Certificate	🔒 https://www.microsoft.com/en-us/
EV Certificate	🔒 PayPal, Inc. (US) | https://www.paypal.com/us/home

Certificate Revocation List (CRL)

Summary

- Public key encryption concept
- Diffie-Hellman key exchange protocol
- RSA algorithm
- Man-in-the-middle attack
- Digital signature, X.509 certificate, and CA
- How PKI defeats MITM
- Attacks on PKI