Public Key Infrastructure (PKI)

Myrto Arapinis
School of Informatics
University of Edinburgh

October 16, 2017
Public keys

Figure: How does Alice trust that $pk_{Amazon}$ is Amazon’s public key?

Public-key encryption schemes are secure only if the authenticity of the public key is assured.
Distribution of public keys

1. **Public announcements** - participants broadcast their public key
   😞 does not defend against forgeries

2. **Publicly available directories** - participants publish their public key on public directories
   😞 does not defend against forgeries

3. **Public-key authority** - participants contact the authority for each public key it needs
   😞 bottleneck in the system

4. **Public-key certificates** - CAs issue certificates to participants on their public key
   😊 as reliable as public-key authority but avoiding the bottleneck
Public key certificates

A certificate consists mainly of:

- a public key
- a subject identifying the owner of the key
- a signature by the CA on the key and the subject binding them together

the CA is trusted
X.509 certificates

Figure: image from Cryptography and Network Security - Principles and Practice - William Stallings

- X.509 defines a framework for the provision of authentication services
- Used by many applications such as TLS
Public key certificates

Figure: Alice can now verify Amazon's certificate
Using public key certificates to secure the Internet

A very important implicit assumption
The browser is trusted to be “secure”
Amazon’s certificate

Safari is using an encrypted connection to www.amazon.co.uk.

Encryption with a digital certificate keeps information private as it's sent to or from the https website www.amazon.co.uk.

VeriSign Class 3 Public Primary Certification Authority – G5
Symantec Class 3 Secure Server CA – G4
www.amazon.co.uk

www.amazon.co.uk
Issued by: Symantec Class 3 Secure Server CA – G4
Expires: Thursday, 29 December 2016 23:59:59 Greenwich Mean Time
This certificate is valid

Trust
Details

Subject Name
Country: US
State/Province: Washington
Locality: Seattle
Organization: Amazon.com, Inc.
Common Name: www.amazon.co.uk

Issuer Name
Country: US
Organization: Symantec Corporation
Organizational Unit: Symantec Trust Network
Common Name: Symantec Class 3 Secure Server CA – G4

Serial Number: 38 77 95 F0 1C D1 4A DD 21 37 32 7C 8E 51 DA C9
Version: 3
Signature Algorithm: SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters: none

Hide Certificate
OK
Browser root certificates
Having a single CA sign all certificates is not practical

Instead a root CA signs certificates for level 1 CAs, level 1 CAs sign certificates for level 2 CAs, etc
Self-signed certificates

Safari can't verify the identity of the website “lists.gno.org”.
The certificate for this website was signed by an unknown certifying authority. You might be connecting to a website that is pretending to be “lists.gno.org”, which could put your confidential information at risk. Would you like to connect to the website anyway?

- Always trust “lists.gno.org” when connecting to “lists.gno.org”

lists.gno.org

Self-signed root certificate
Expires: Saturday, December 6, 2014 2:26:42 PM MT (CA)

This root certificate is not trusted

- When using this certificate: Always Trust
- Secure Sockets Layer (SSL): Always Trust
- X.509 Basic Policy: Always Trust

Details

Hide Certificate  Cancel  Continue
Lenovo's Superfish security snafu blows up in its face

The preloaded Superfish adware does more than hijack website ads in a browser. It also exposes Lenovo owners to a simple but dangerous hack that could spell disaster.

Removing software that comes with your brand-new Windows computer can be frustrating, but recently discovered software on new Lenovo laptops -- the top-selling laptop brand in 2014 -- can put your entire digital life at risk.

The preloaded software, called Superfish, alters your search results to show you different ads than you would otherwise see. But it also tampers with your computer's security so that attackers can snoop on your browser traffic -- no matter which browser you're using.

*Attackers are able to see all the communication
And more recently (September 2016)

Security

Mozilla wants woeful WoSign certs off the list

Backdating SHA-1 certs is just not on

27 Sep 2016 at 03:58, Richard Chirgwin

Mozilla wants to kick Chinese certificate authority (CA) WoSign out of its trust program.