Secure communication: public key infrastructure

Markulf Kohlweiss & Myrto Arapinis
School of Informatics
University of Edinburgh

February 10, 2021

Public keys

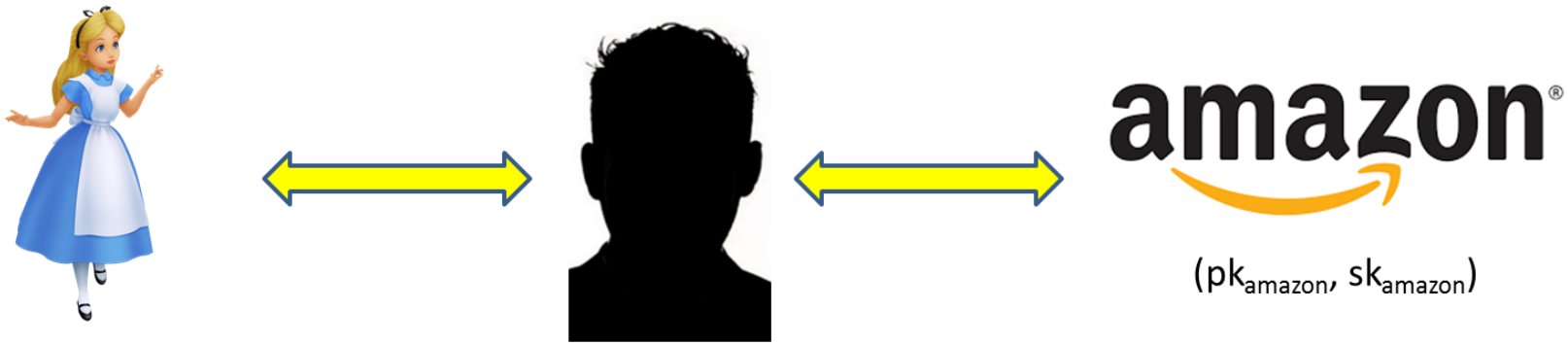


Figure: How does Alice trust that pk_{Amazon} is Amazon's public key?

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

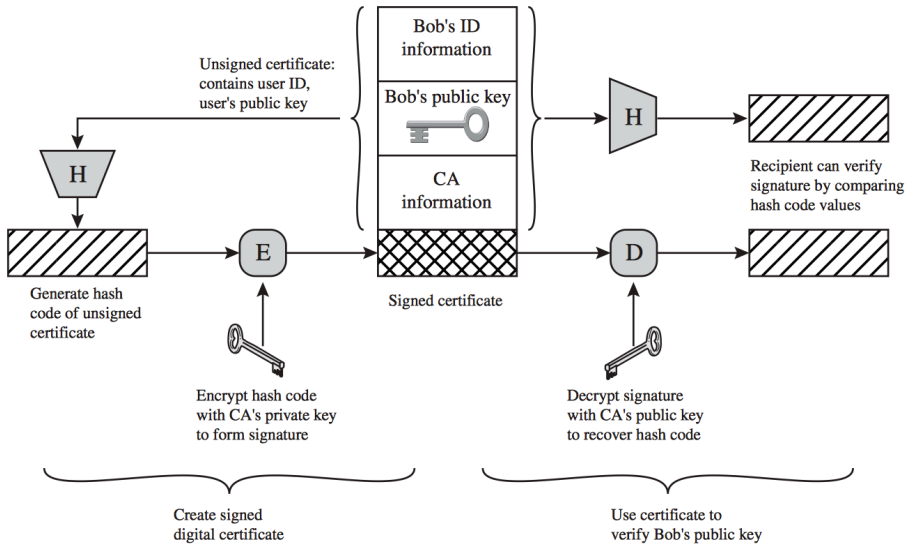


Figure: image from Cryptography and Network Security - Principles and Practice - William Stallings

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

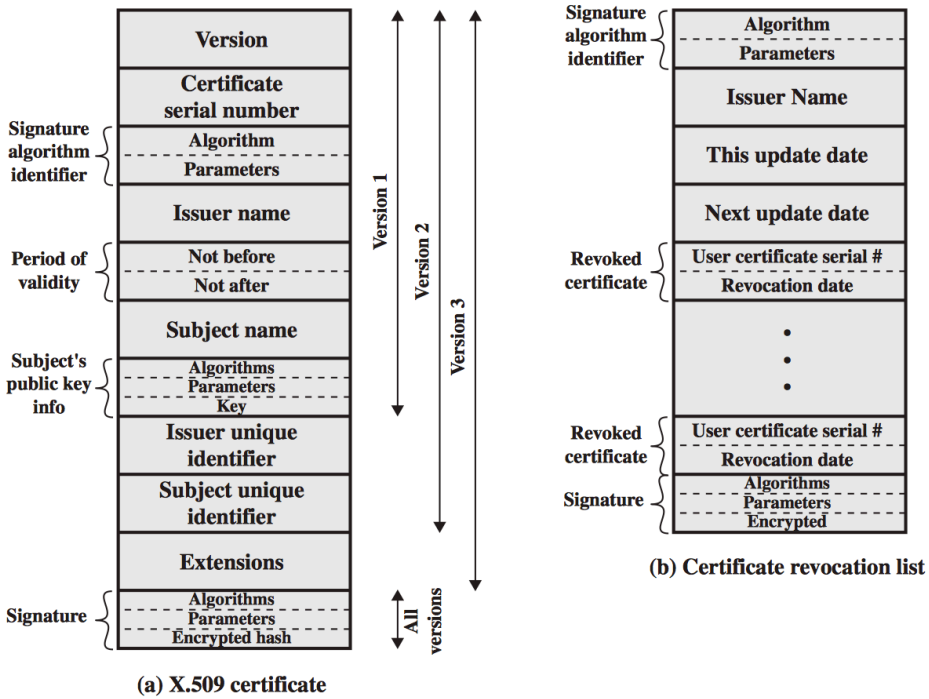


Figure: image from Cryptography and Network Security - Principles and Practice - William Stallings

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

Public key certificates

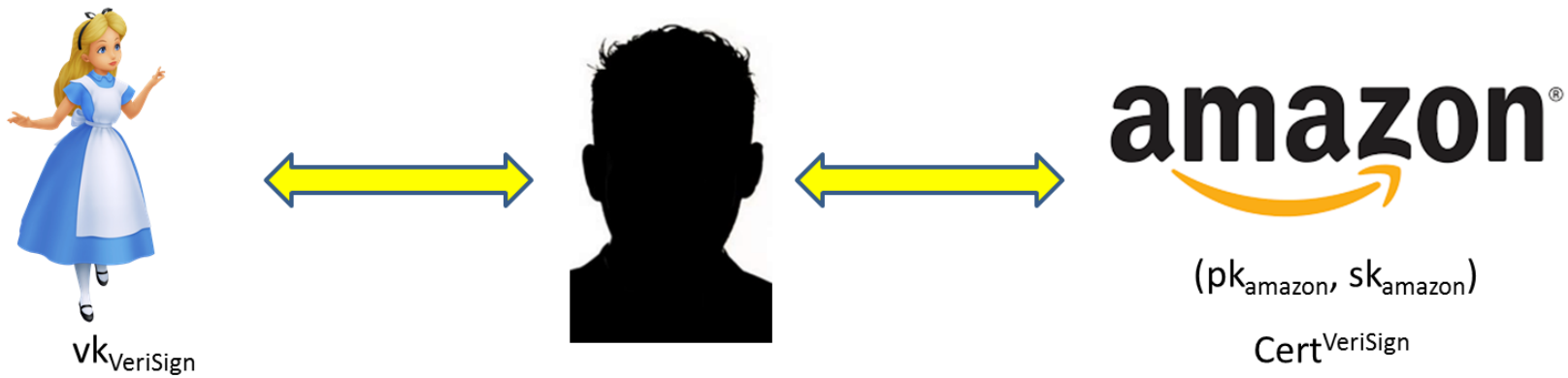
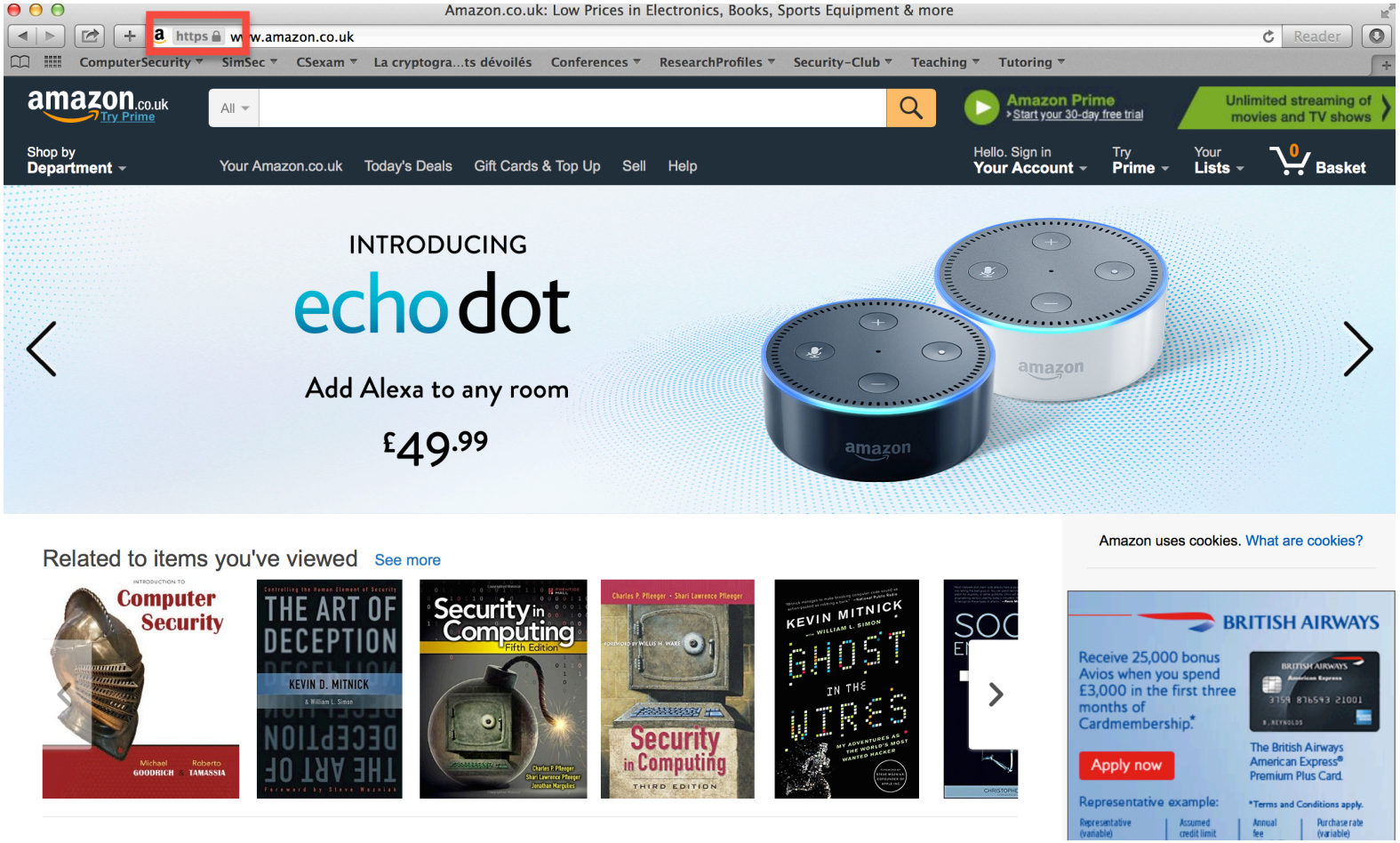


Figure: Alice can now verify Amazon's certificate

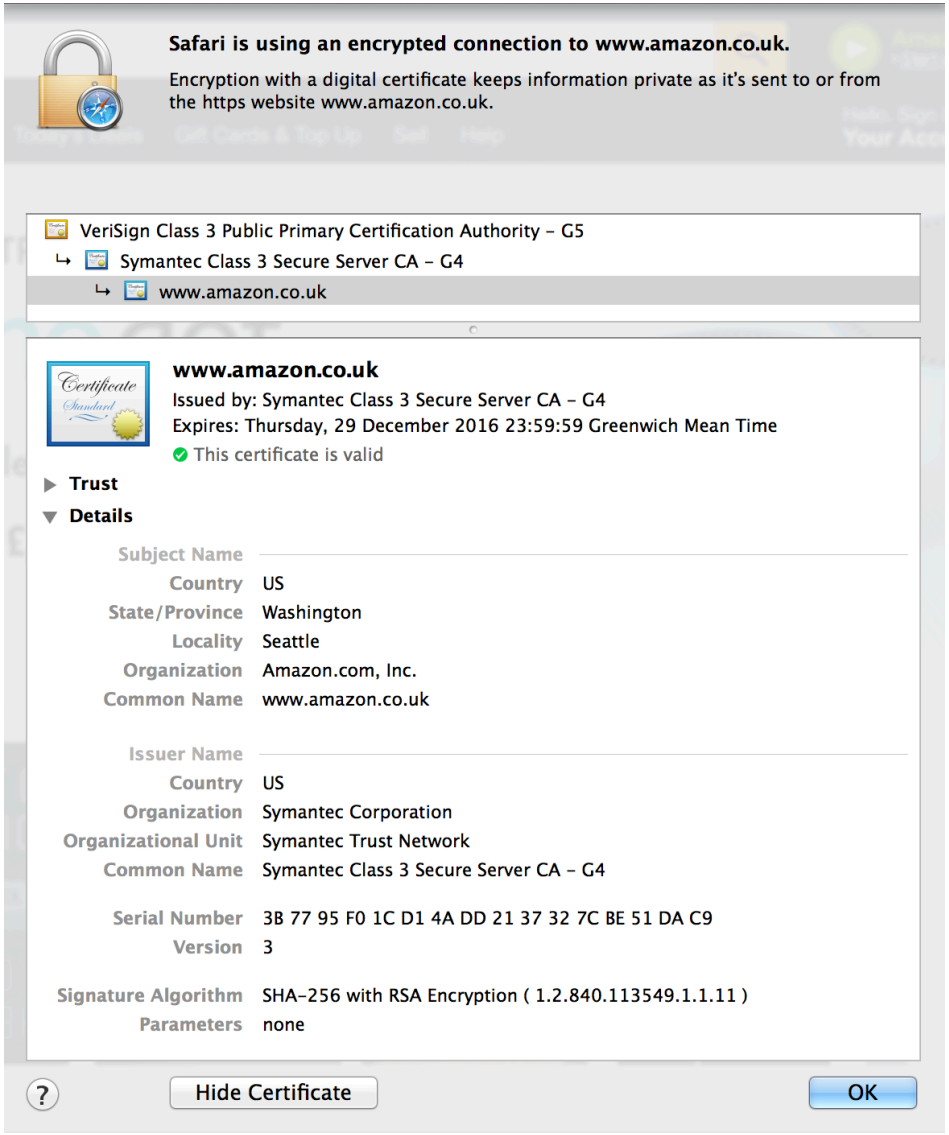
Using public key certificates to secure the Internet



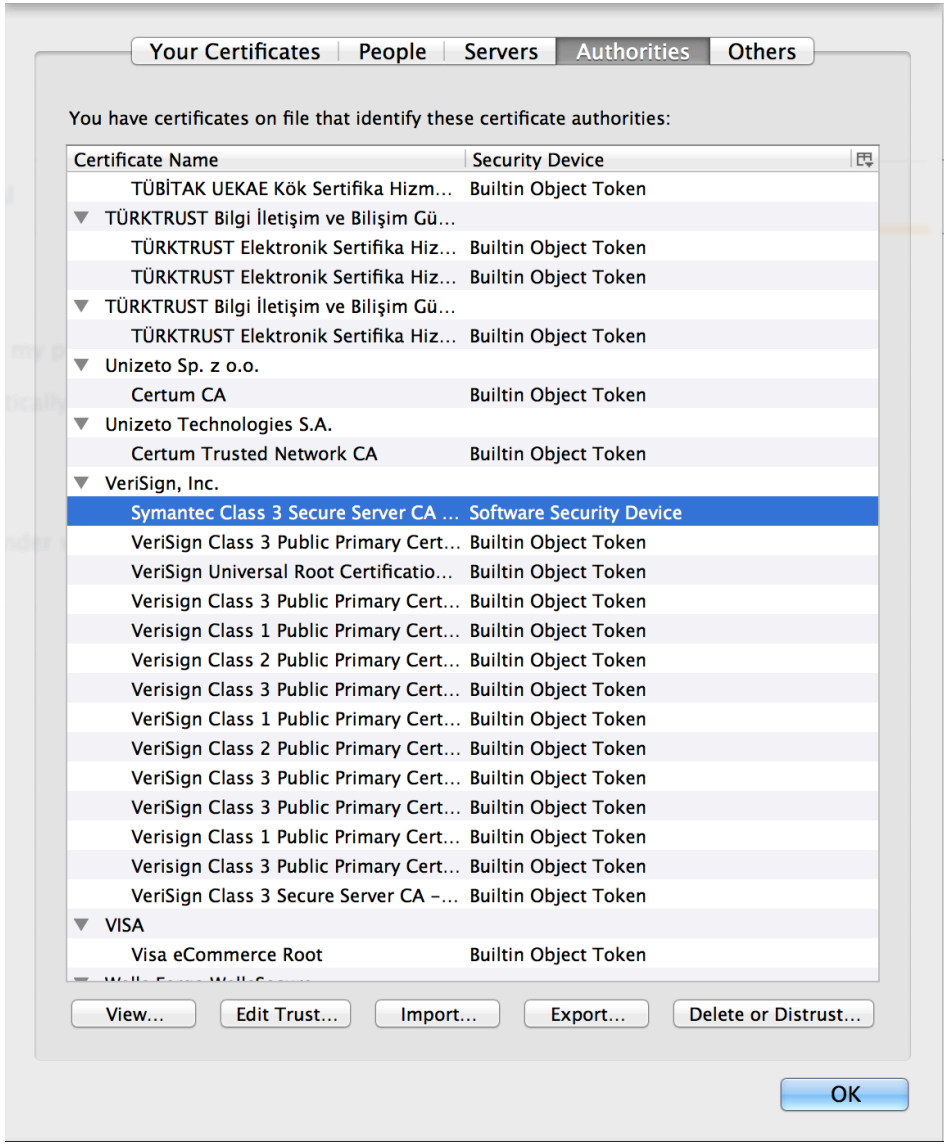
A very important implicit assumption

The browser is trusted to be "secure"

Amazon's certificate



Browser root certificates



Chain of trust

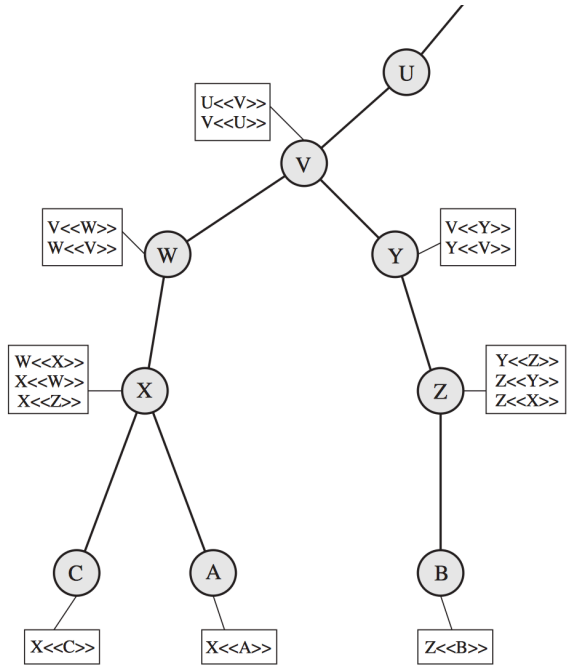
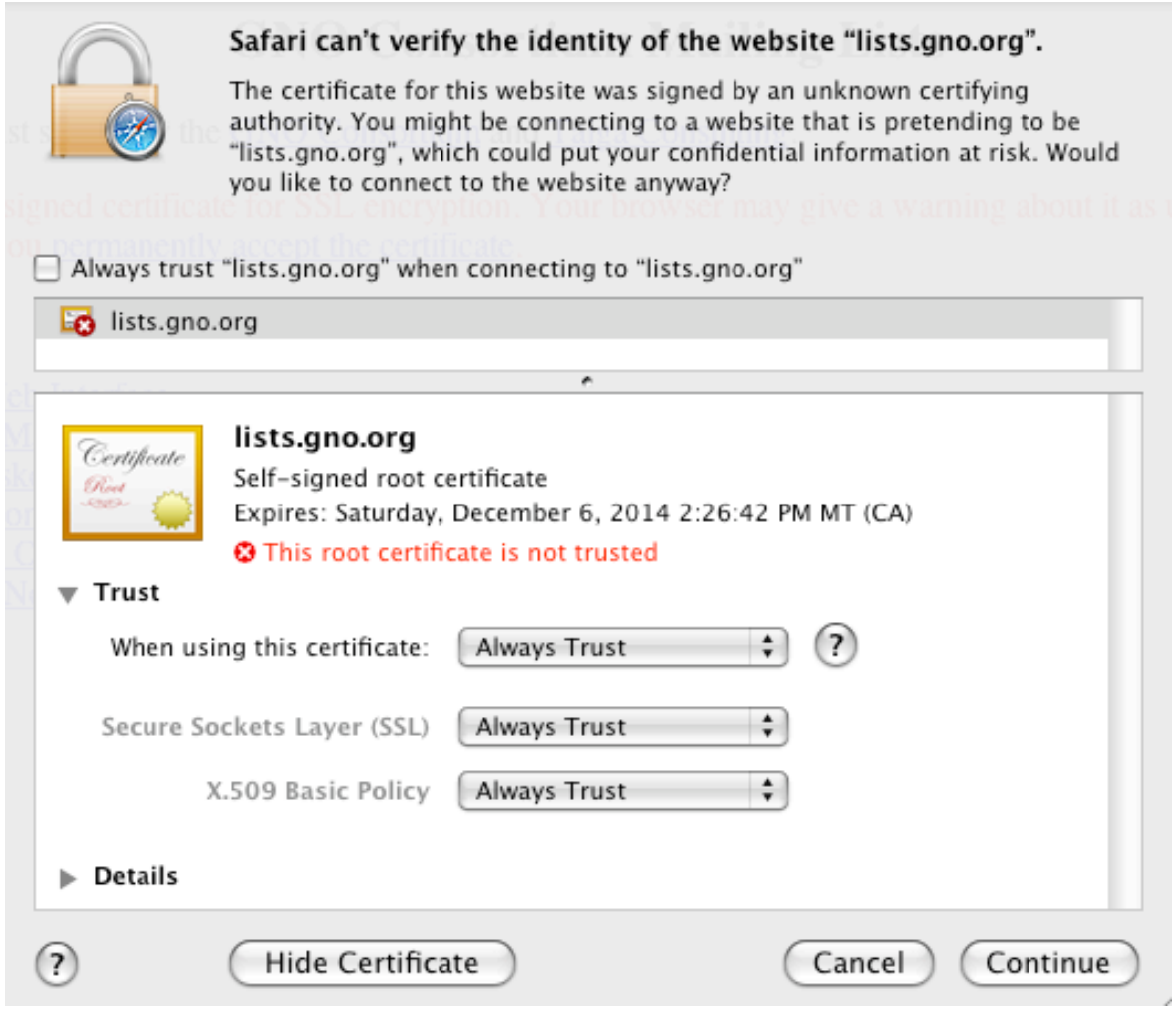


Figure: X.509 Hierarchy - image from Cryptography and Network Security - Principles and Practice - William Stallings

- 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



The Lenovo Superfish scandal (February 2015)

c|net Search Reviews News Video How To Smart Home Cars Deals Dow

CNET › Security › Lenovo's Superfish security snafu blows up in its face

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.

Security

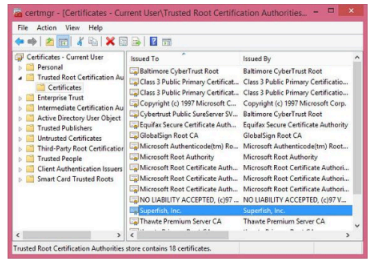
February 20, 2015
5:00 AM PST

by Seth Rosenblatt
@sethr

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



Superfish code hides in hard-to-reach places on your new Lenovo laptop, making it difficult to remove.

Screenshot by Robert Graham/Errata Security

And more recently (September 2016)

The Register®
Biting the hand that feeds IT

DATA CENTRE SOFTWARE NETWORKS SECURITY TRANSFORMATION DEVOPS BUSINESS HARDWARE SCIENCE

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 42

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

More

Mozil

IT
So
Tick
Mgr
Serv
freshs

Revocation

- A certificate needs to be revoked if the corresponding private key has been compromised.
- Certificate Revocation Lists (CRLs) are the solution adopted in X.509.
- Online Certificate Status Protocol (OCSP) stapling is the modern solution to this problem.