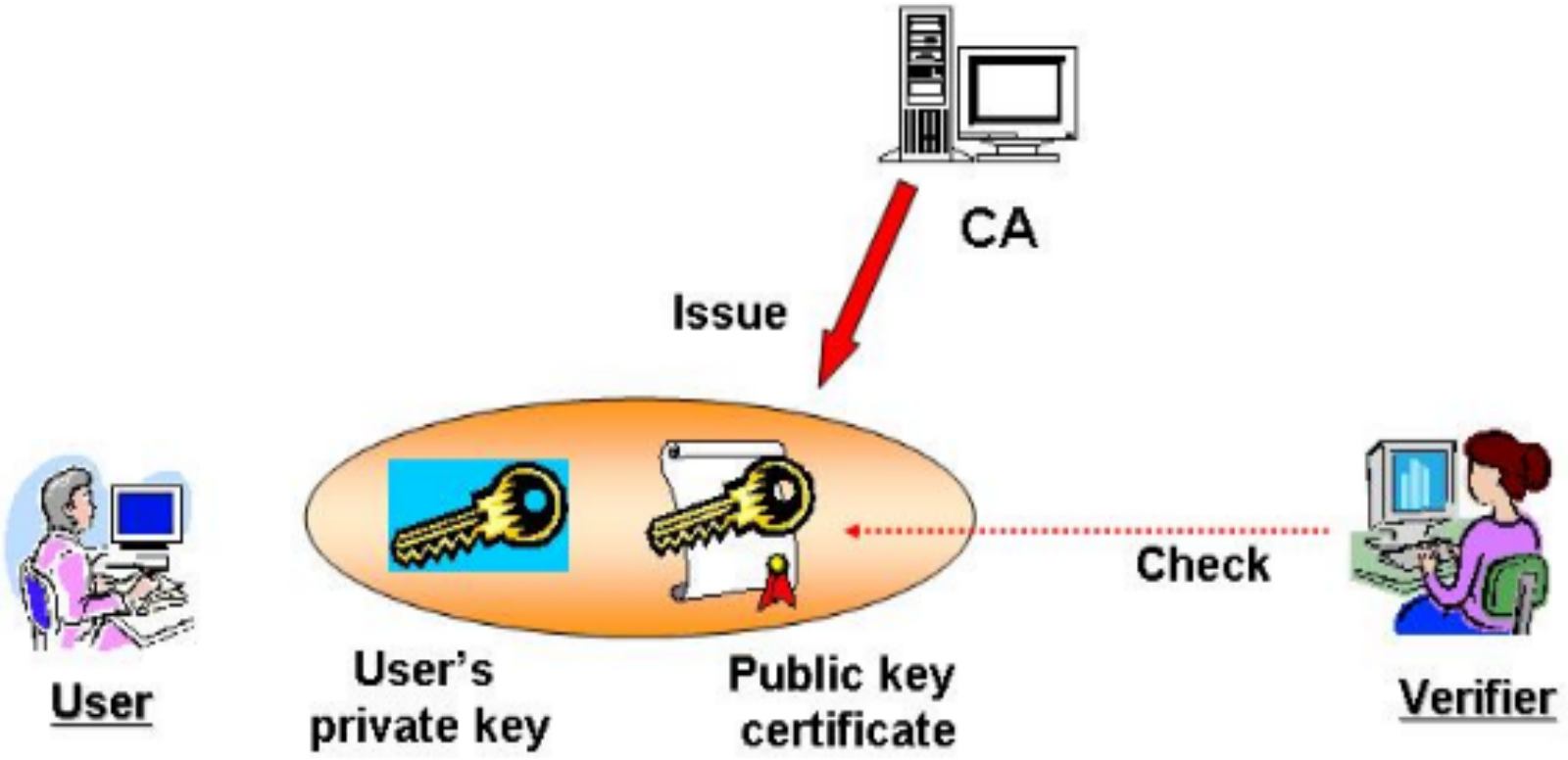
Security in Internet: what is it now?

A presentation by Dmitry Belyavsky, TCI

ENOG 6 / RIPE NCC Regional Meeting
Kiev, Ukraine, October 2013

About PKI *)



*) **PKI (public-key infrastructure)** is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates

Technical Centre of Internet

Some minor incidents

- 2011

One of COMODO partners issued certificates: Addons.mozilla.org, Login.live.com, Mail.google.com, www.google.com, Login.yahoo.com (x3), Login.skype.com

- 2012

Trustware

issued certificate for DLP-system

TurkTrust

incorrect (???) issued certificate with sign rights except common

Technical Centre of Internet

The significant case: DigiNotar

2011, June

Certification Authority DigiNotar issued certificates for more than 20 sites, Google among them

DigiNotar inactivity

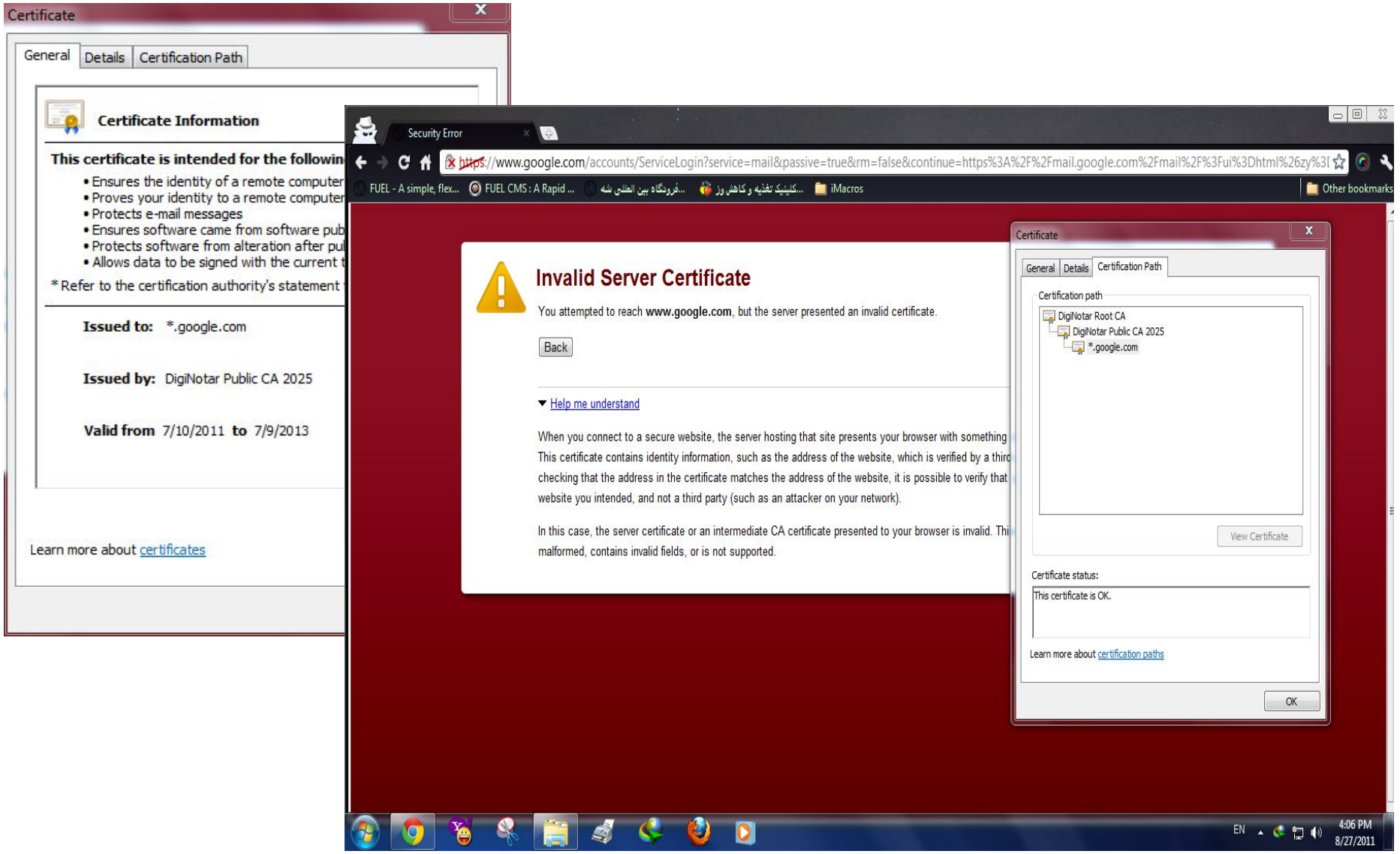
Fisrt complaint appeared on Google forum (Chrome browser contains the list of real Google sites certificates)

Browsers excluded DidiNotar certificates for good

The company went bankrupt

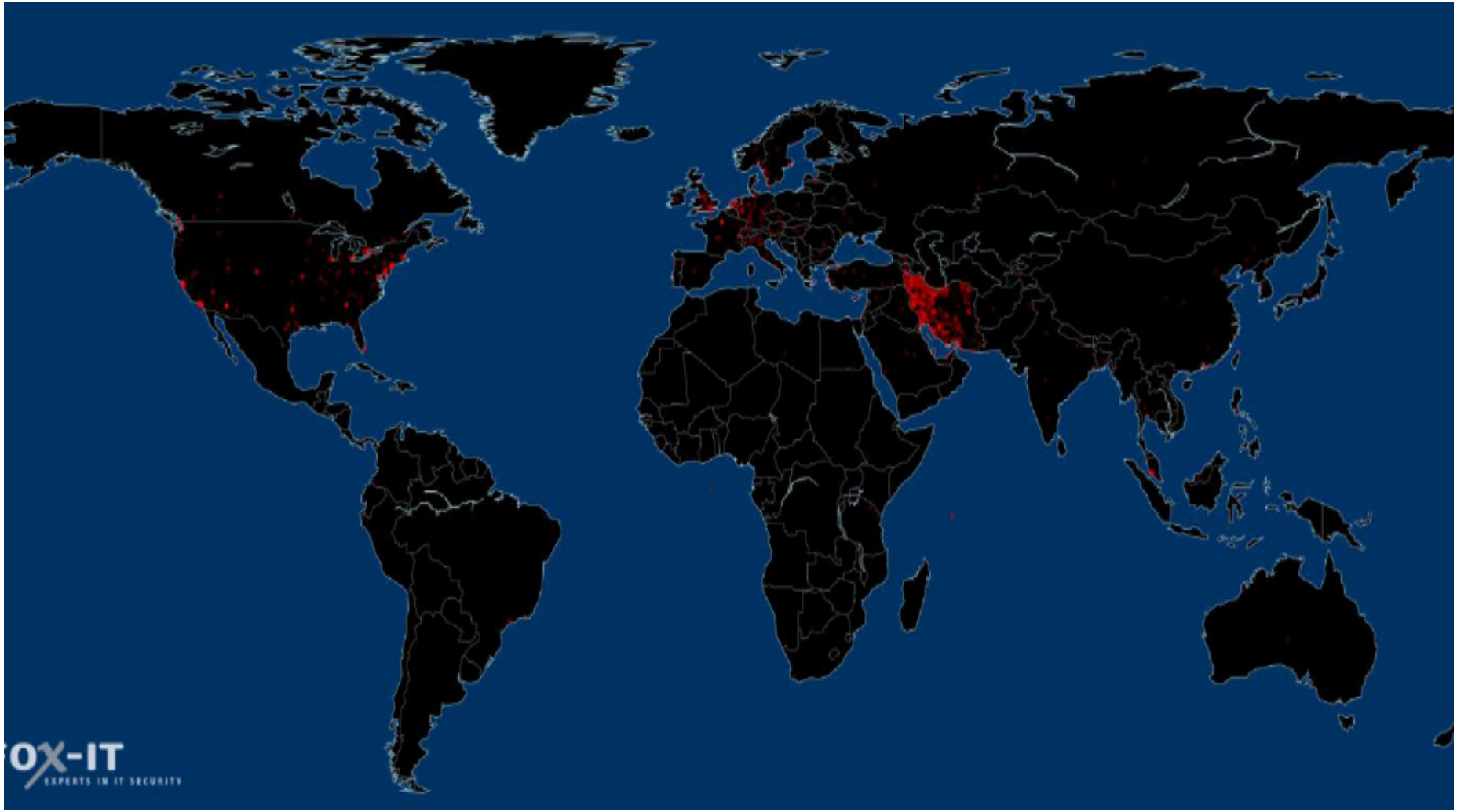
Technical Centre of Internet

More about “DigiNotar case”



Technical Centre of Internet

More about “DigiNotar case”



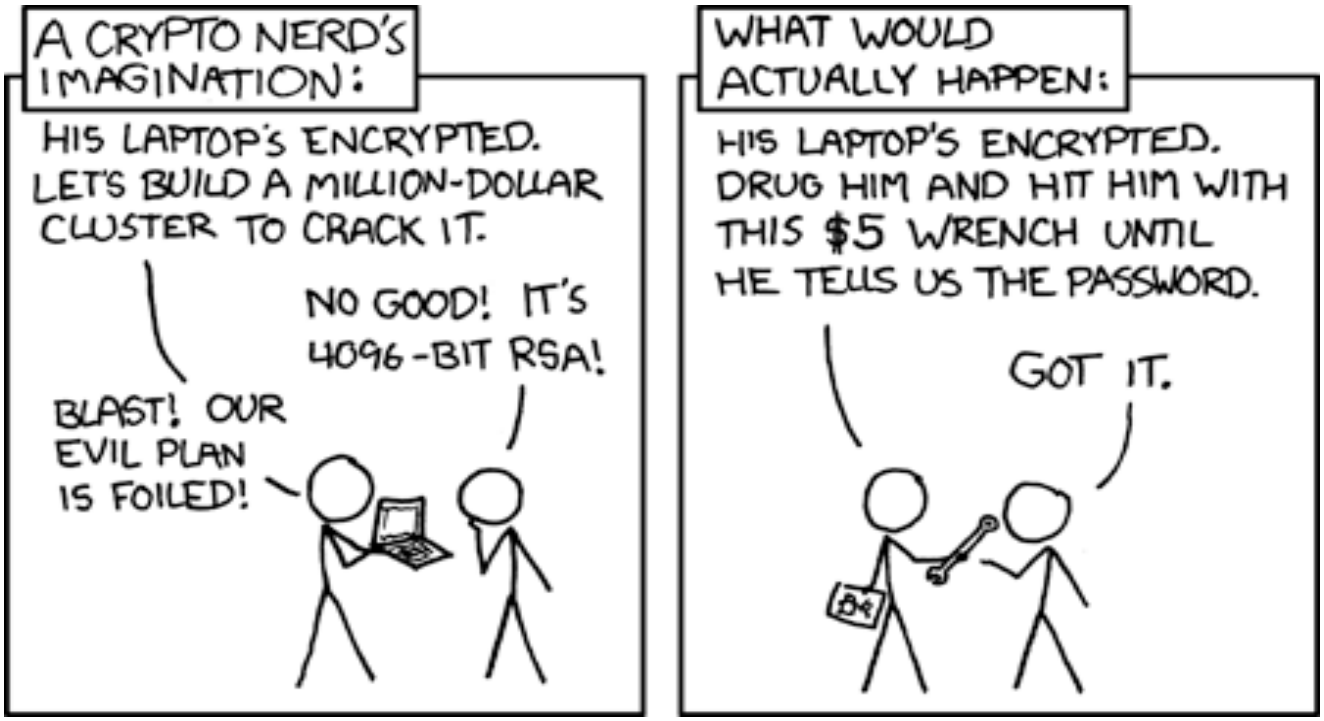
OCSP requests for the fake *.google.com certificate

Source: FOX-IT, Interim Report, http://cryptome.org/0005/diginotar-insec.pdf

Technical Centre of Internet

NSA interference in security

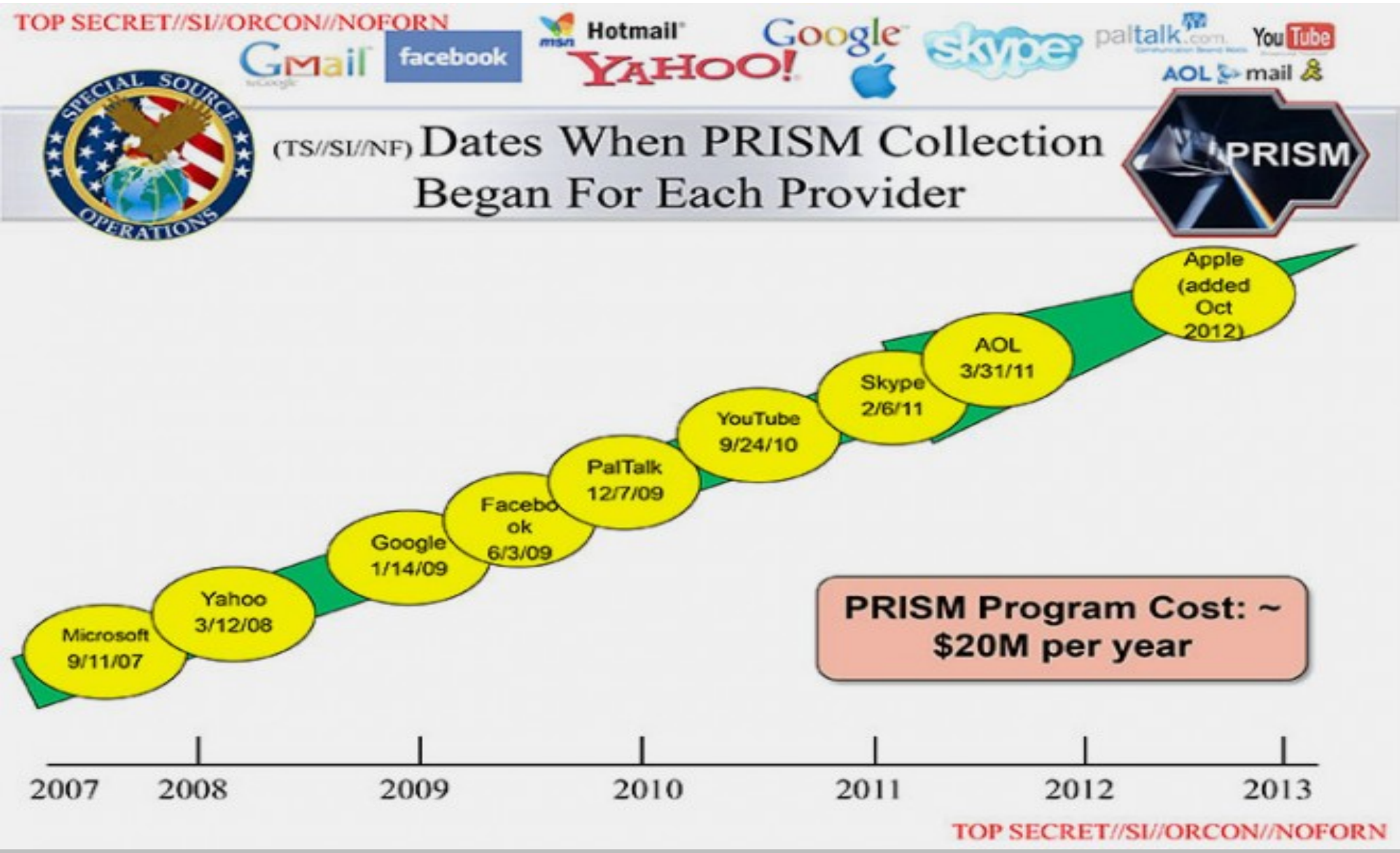
2013



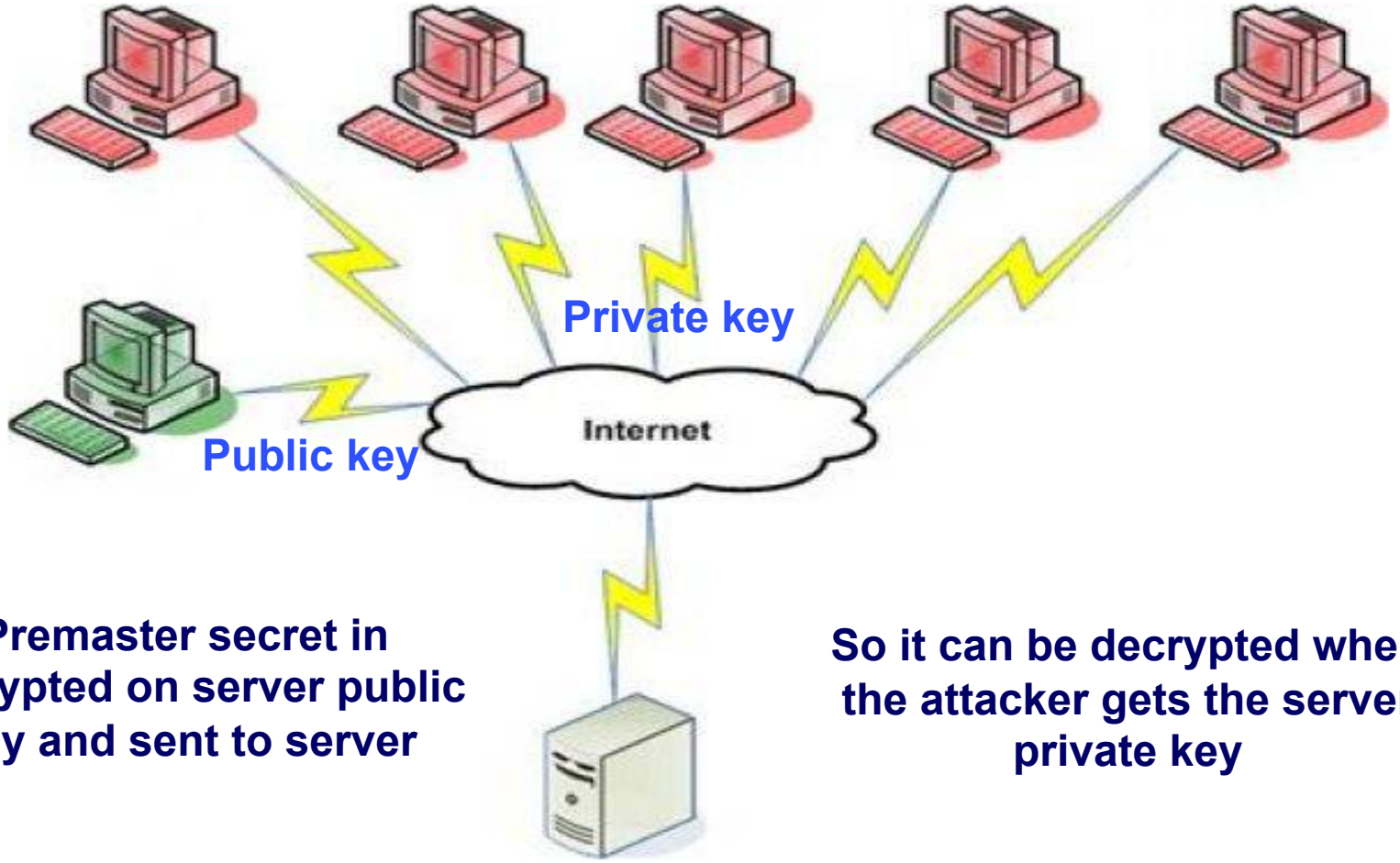
Source:http://xkcd.com/538/

Technical Centre of Internet

RRISM timeline



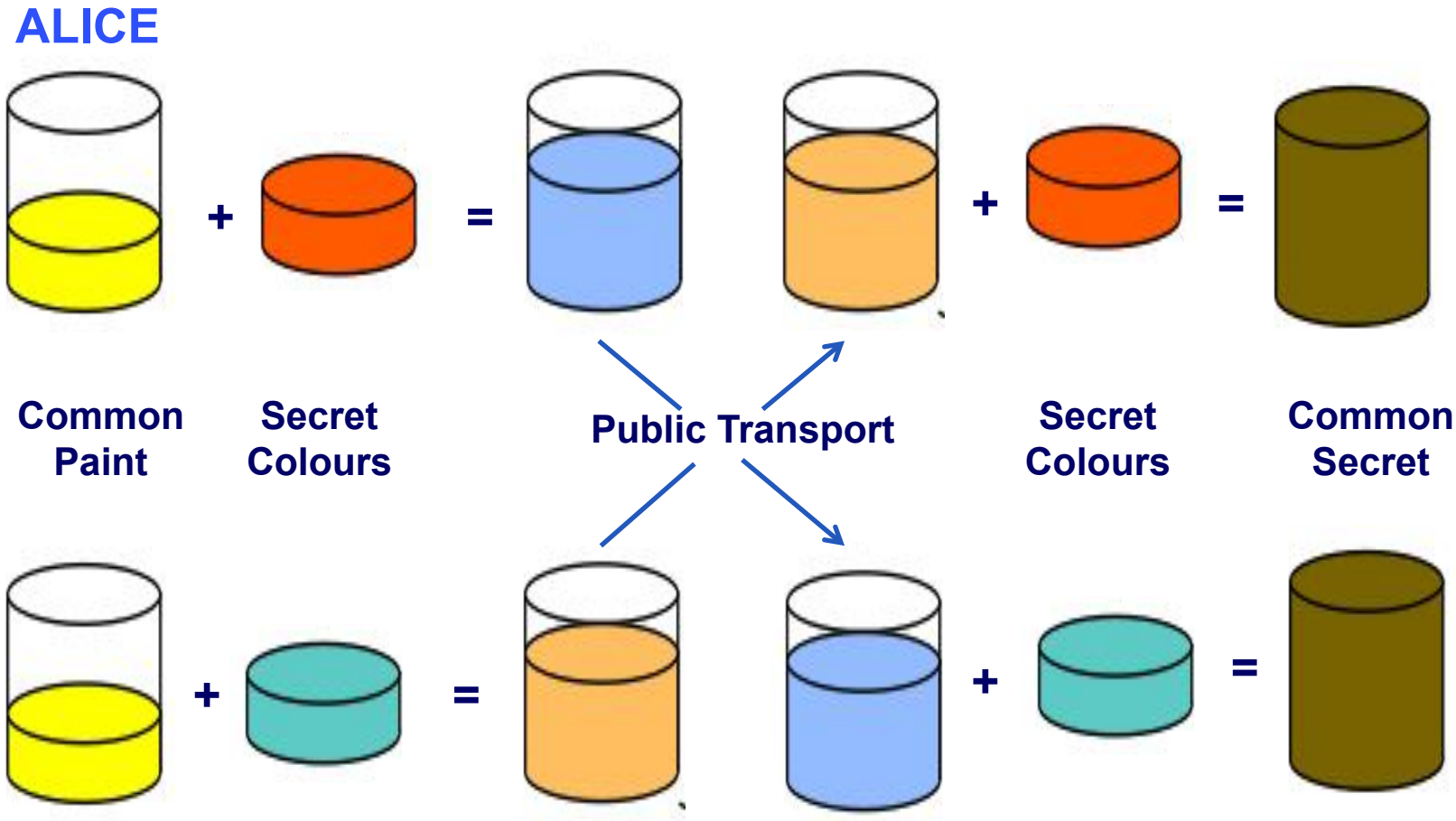
RSA key exchange



Premaster secret in encrypted on server public key and sent to server

So it can be decrypted when the attacker gets the server private key

Perfect Forward Secrecy



SSL Best Practices

https://www.ssllabs.com/projects/best-practices/

Technical Centre of Internet

If you are an end-user…

Five pieces of advice:

- ✓ **Hide in the network**
- ✓ **Encrypt your communications**
- ✓ **Assume that while your computer can be compromised, it would take work and risk on the part of the NSA – so it probably isn't**
- ✓ **Be suspicious of commercial encryption software, especially from large vendors**
- ✓ **Try to use public-domain encryption that has to be compatible with other implementations**

Bruce Schneier:

“I understand that most of this is impossible for the typical internet user”

PKI: extra trust

DANE (RFC 6698)

Limited browsers support

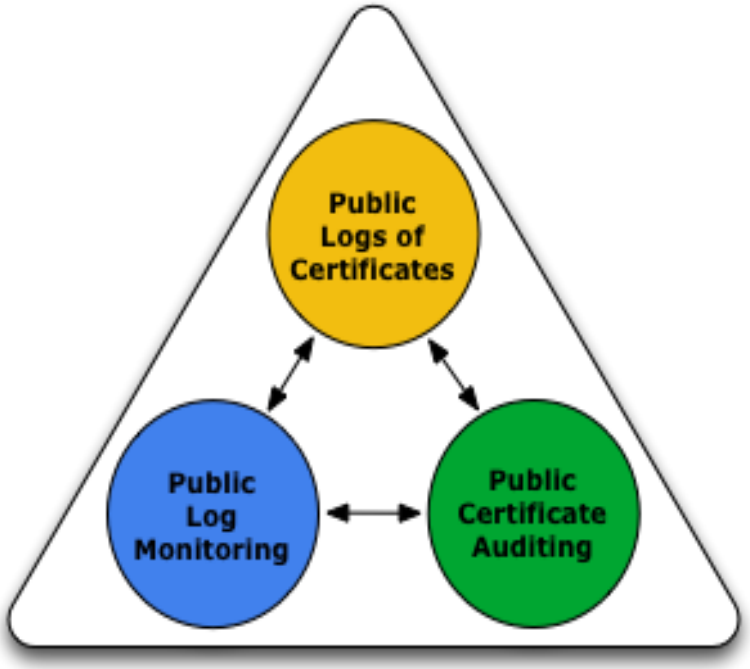
Certificate pinning:

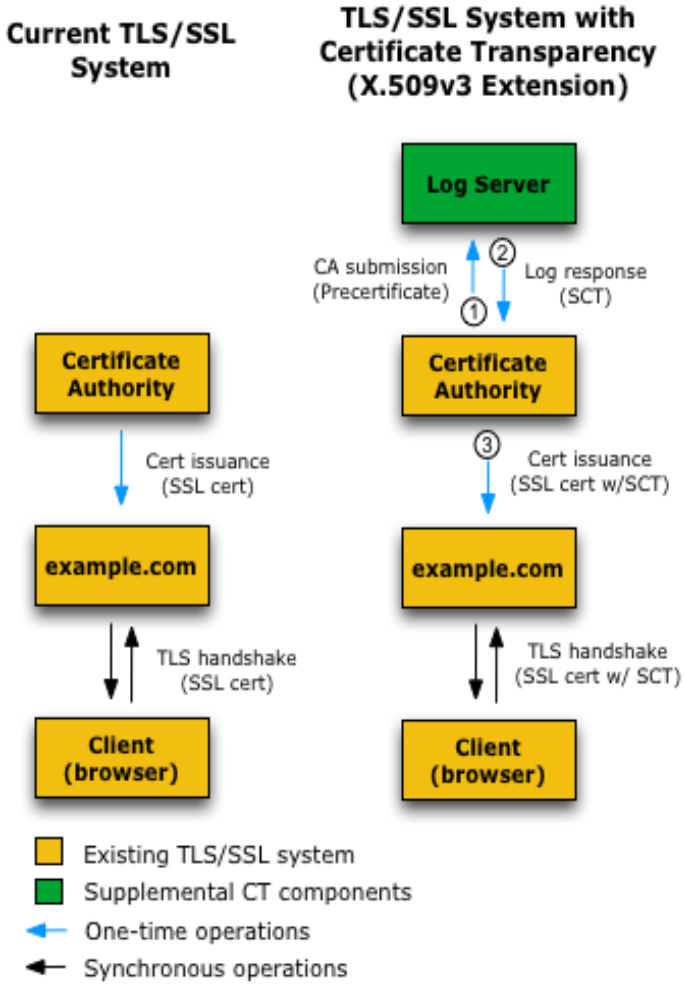
Mozilla Certificate Patrol,
Chrome cache for Google certificates

Certificate transparency (RFC 6962)

Technical Centre of Internet

Certificate Transparency: how it works





Source: http://www.certificate-transparency.org

& Two other options

Certificate Transparency Deployment

Inspired by Google
(Support in Chrome announced)

One of the authors - Ben Laurie
(OpenSSL Founder)

CA support – Comodo

Technical Centre of Internet

Summary

For today the cryptographic mechanism https is not a guarantee of safety

The weakest element in the system of safety provision is

HUMAN FACTOR!

Q&A

Questions?

Drop ‘em at:

beldmit@tcinet.ru