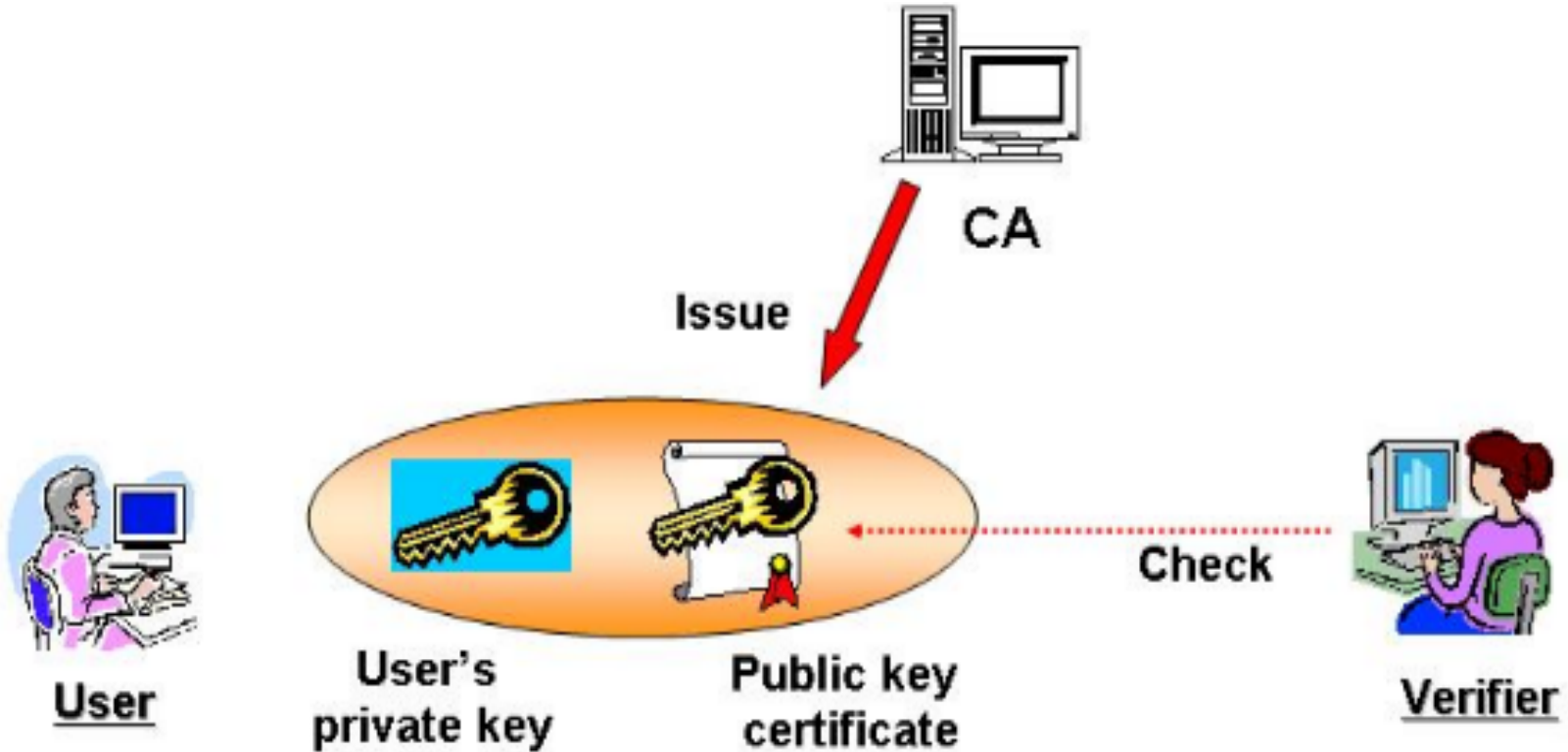




# Security in Internet: what is it now?

A presentation by Dmitry Belyavsky, TCI

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



\*) **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



• 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

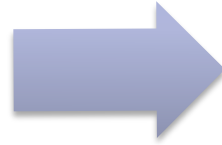
**Trustware**  
issued certificate for DLP-system

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



# The significant case: DigiNotar

2011, June



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



Browsers excluded  
DigiNotar certificates for  
good  
The company went  
bankrupt



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

# More about “DigiNotar case”

Certificate

General Details Certification Path

### Certificate Information

This certificate is intended for the following purposes:

- Ensures the identity of a remote computer
- Proves your identity to a remote computer
- Protects e-mail messages
- Ensures software came from software publisher
- Protects software from alteration after publication
- Allows data to be signed with the current time

\* Refer to the certification authority's statement for more information.

**Issued to:** \*.google.com

**Issued by:** DigiNotar Public CA 2025

**Valid from:** 7/10/2011 to 7/9/2013

Learn more about [certificates](#)

Security Error

https://www.google.com/accounts/ServiceLogin?service=mail&passive=true&rm=false&continue=https%3A%2F%2Fmail.google.com%2Fmail%2F%3Fui%3Dhtml%26zy%31

FUEL - A simple, flex... FUEL CMS: A Rapid... فرومگاه بین المللی شه... کتابتیک بقیه و کاغذ وز... iMacros

## Invalid Server Certificate

You attempted to reach [www.google.com](https://www.google.com), but the server presented an invalid certificate.

[Back](#)

[Help me understand](#)

When you connect to a secure website, the server hosting that site presents your browser with something called a certificate. This certificate contains identity information, such as the address of the website, which is verified by a third party. By checking that the address in the certificate matches the address of the website, it is possible to verify that you are connecting to the website you intended, and not a third party (such as an attacker on your network).

In this case, the server certificate or an intermediate CA certificate presented to your browser is invalid. This certificate is malformed, contains invalid fields, or is not supported.

Certificate

General Details Certification Path

Certification path

- DigiNotar Root CA
- DigiNotar Public CA 2025
- \*.google.com

[View Certificate](#)

Certificate status:  
This certificate is OK.

Learn more about [certification paths](#)

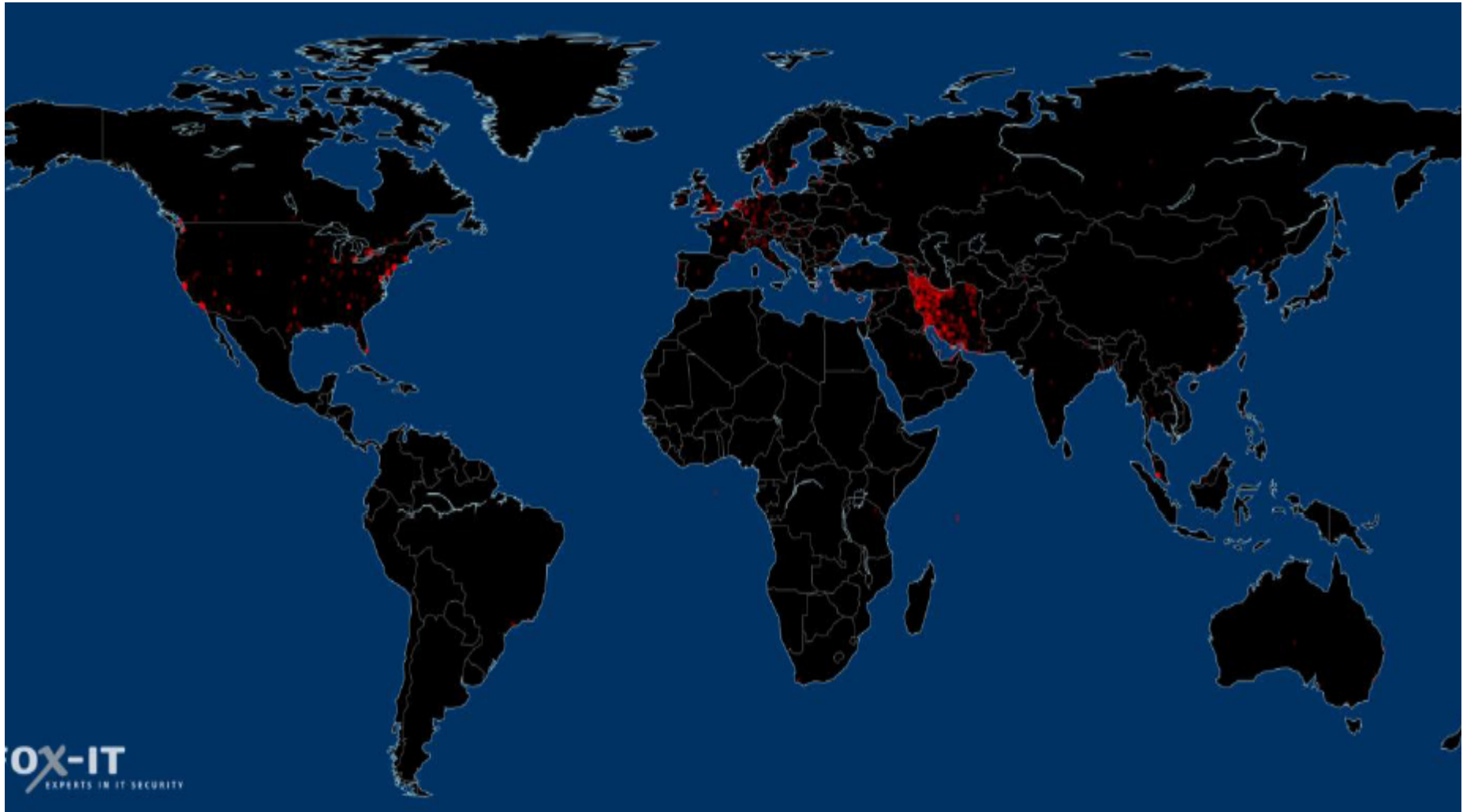
OK

EN 4:06 PM 8/27/2011





# More about “DigiNotar case”



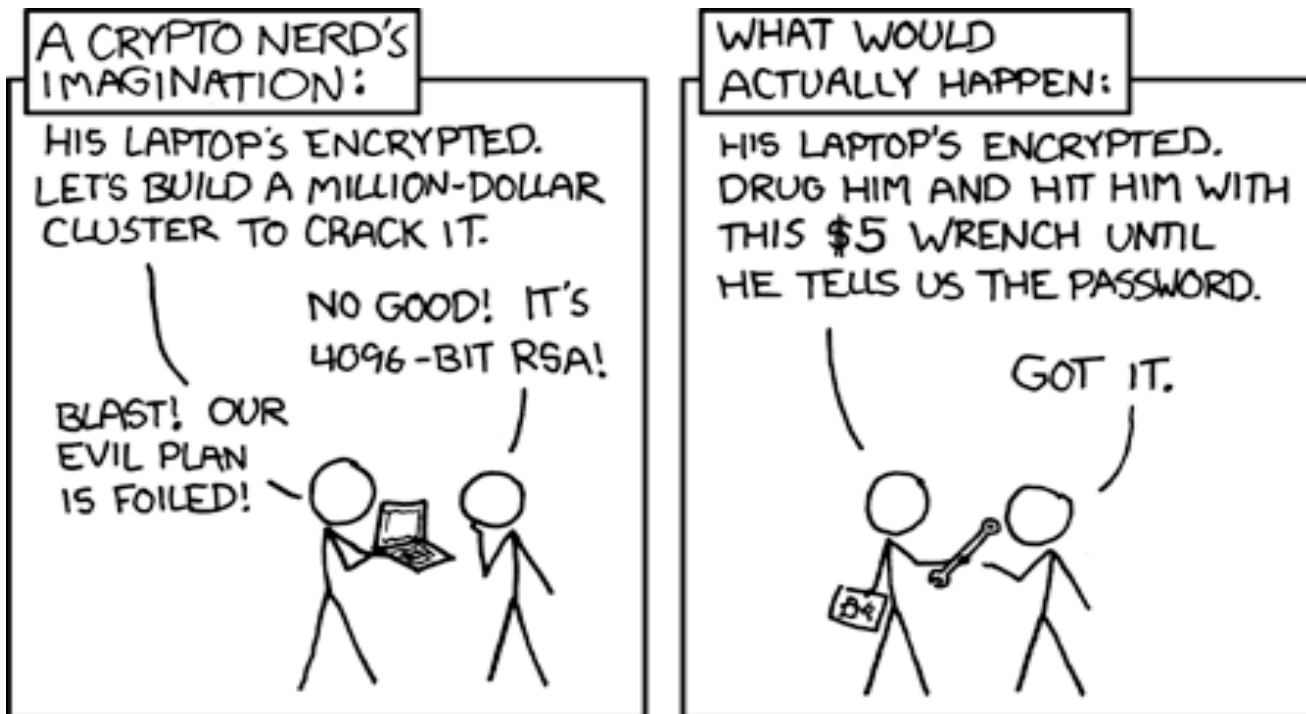
**OCSF requests for the fake \*.google.com certificate**

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

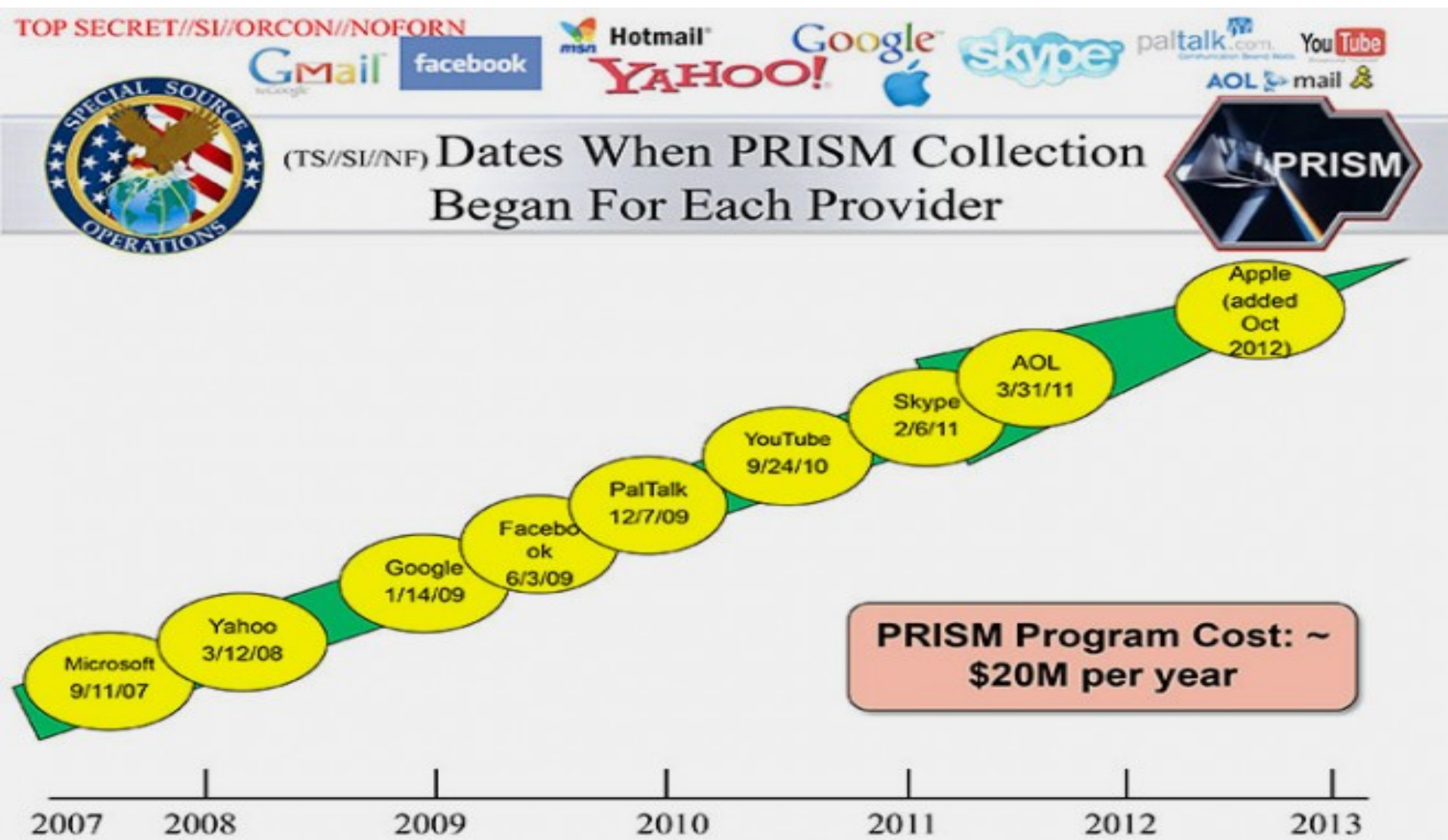


# NSA interference in security

2013



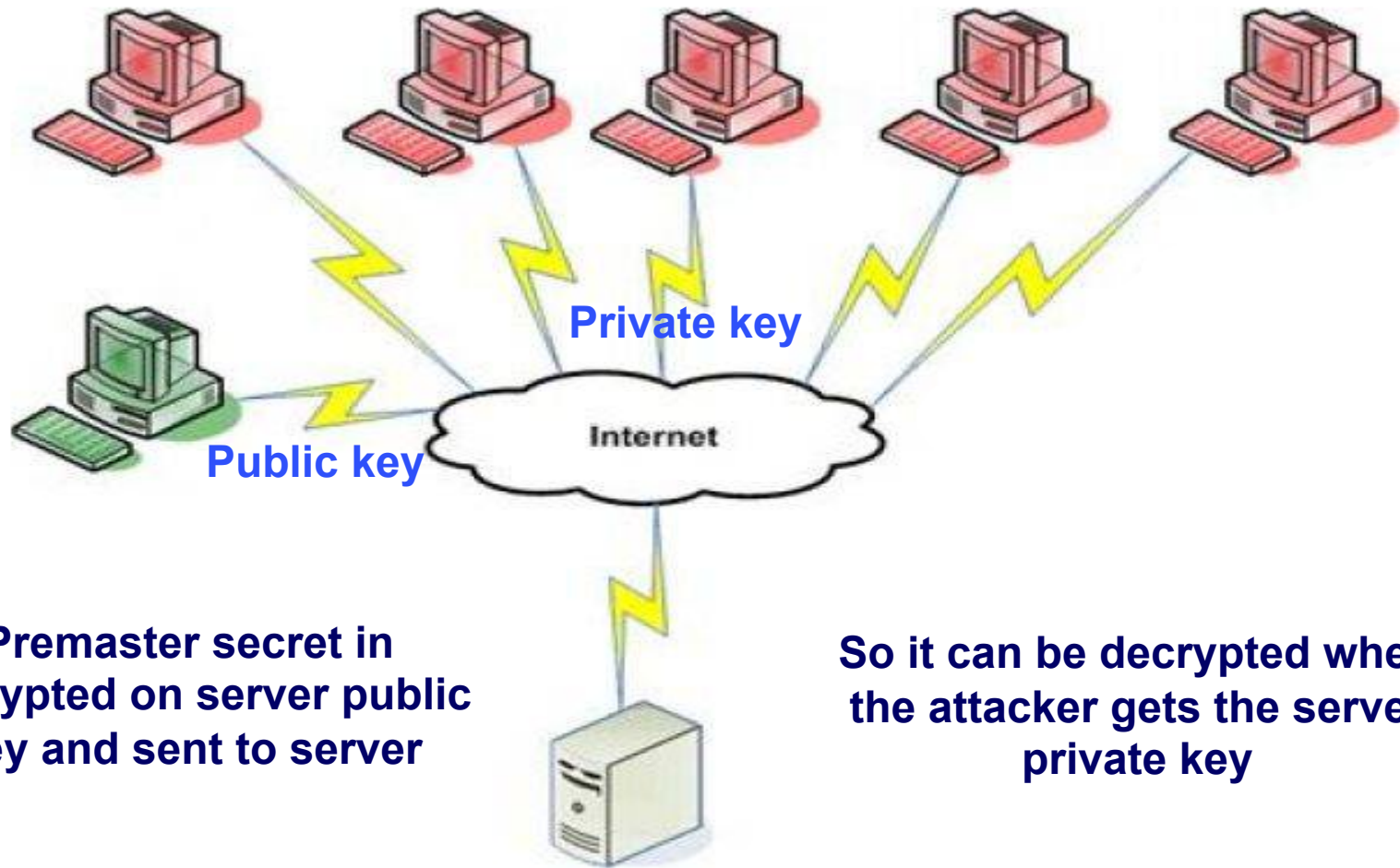
Source: <http://xkcd.com/538/>





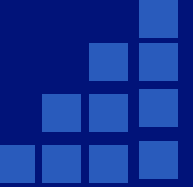


# RSA key exchange

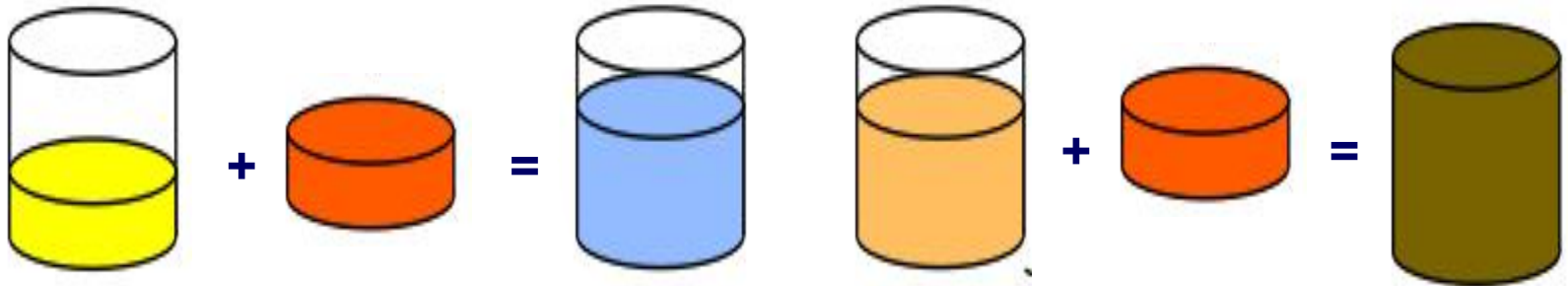




# Perfect Forward Secrecy



**ALICE**



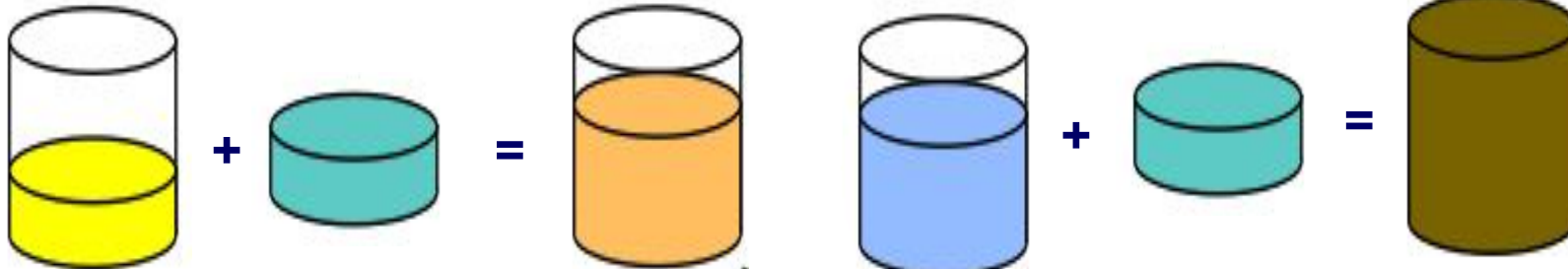
Common  
Paint

Secret  
Colours

Public Transport

Secret  
Colours

Common  
Secret



**BOB**

**SSL Best Practices**

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

## 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”**



## **DANE (RFC 6698)**

Limited browsers support

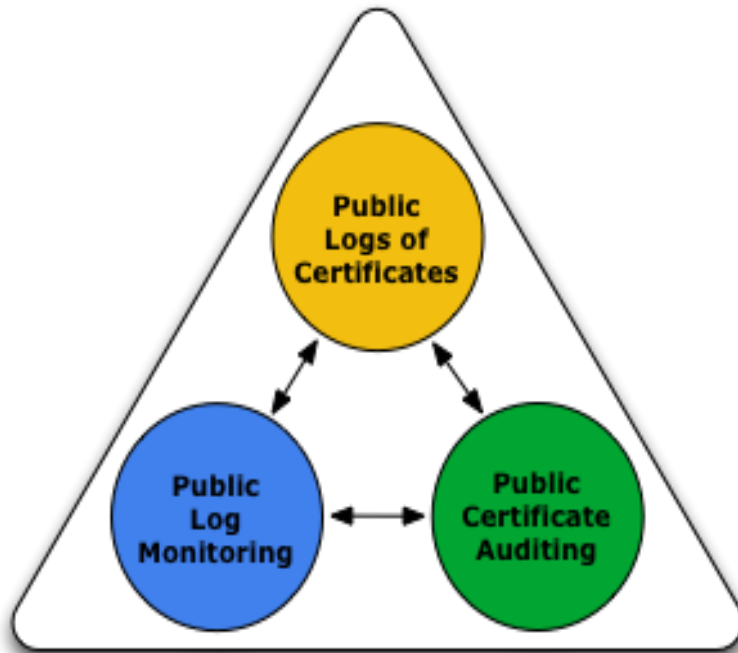
## **Certificate pinning:**

Mozilla Certificate Patrol,  
Chrome cache for Google certificates

## **Certificate transparency (RFC 6962)**



# Certificate Transparency: how it works



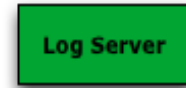
Current TLS/SSL System



Cert issuance (SSL cert)

TLS handshake (SSL cert)

TLS/SSL System with Certificate Transparency (X.509v3 Extension)



CA submission (Precertificate) ①  
Log response (SCT) ②

③ Cert issuance (SSL cert w/SCT)

TLS handshake (SSL cert w/ SCT)

- Existing TLS/SSL system
- Supplemental CT components
- One-time operations
- Synchronous operations





**Inspired by Google**  
(Support in Chrome announced)

**One of the authors - Ben Laurie**  
(OpenSSL Founder)

**CA support – Comodo**



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



## The weakest element in the system of safety provision is

# HUMAN FACTOR!



**Questions?**

**Drop 'em at:**

**[beldmit@tcinet.ru](mailto:beldmit@tcinet.ru)**