Project SweSSL

How and where is SSL (not) used in .SE?

Andreas Jonsson, andreas@romab.com
Tobias Norrbom, tobbe@romab.com
Robert Malmgren, rom@romab.com

ROMAB?

- IT and infosec consultants, 2/3 of company here today

- We don’t sell products
- We don’t sell certificates, nor make money from them

- *....but, we love the feeling of having a locked padlock in the URL bar*

Outline of talk

- Motivation
- Short intro to SSL/TLS
- (Classic) reasons for doing SSL
- Some relevant statistics
- New reasons for doing SSL
- Mythbusting
- Sum it all up

What this talk is ***NOT***....

- ... about to criticize
  - SSL bugs such as renegotiation
  - SSLstrip and attack methodologies
  - PKI, x509 and the technical stuff related to that
  - Browser vendors ***humongously*** large trust stores
  - CA vendors that gets hacked
  - CA's from rogue countries
  - CA vendors that leave their private keys on home page
  - .....
- *Because we all know that already, right?*

Ok, some about CA:s and trust stores

- Modern Browsers trust *a lot* of CA:s
- Some good reasons for this, some bad
  - *Good*: simple way to bootstrap a PKI
  - *Good*: breaks the Verisign monopoly
  - *Bad*: Can each of these CA:s be trusted?
  - *Bad*: can we trust that each CA, even the small ones, won't resell sub-CA:s or to keep their local security updated?

Of course they can!

- Currently 42 countries control a CA
    - ['AE', 'AT', 'AU', 'BE', 'BG', 'BM', 'BR', 'CA', 'CH', 'CL', 'CN', 'CO', 'CZ','DE', 'DK', 'EE', 'ES', 'EU', 'FI', 'FR', 'GB', 'HK', 'HU', 'IE', 'IL', 'IN','IS', 'IT', 'JP', 'KR', 'LT', 'LV', 'MK', 'MO', 'MX', 'MY', 'NL', 'NO', 'PL','PT', 'RO', 'RU', 'SE', 'SG', 'SI', 'SK', 'TN', 'TR', 'TW', 'UK', 'US', 'UY','WW', 'ZA']
- You can trust all of those countries

cn = china
ae = UAE
co = colombia
hk = hong kong
il = israel
ru = russia

sg = singapore
tn = tunisia
tr = turkey
tw = taiwain
uy = uruguay
za = south africa

Lack of name space?

Motivations

- New political landscape: Data retention act, IPRED, SIGINT, SSL MITM as a national/corporate security policy, etc
- New old threats: *firesheep*, etc

Internet is wireless these days, remember?

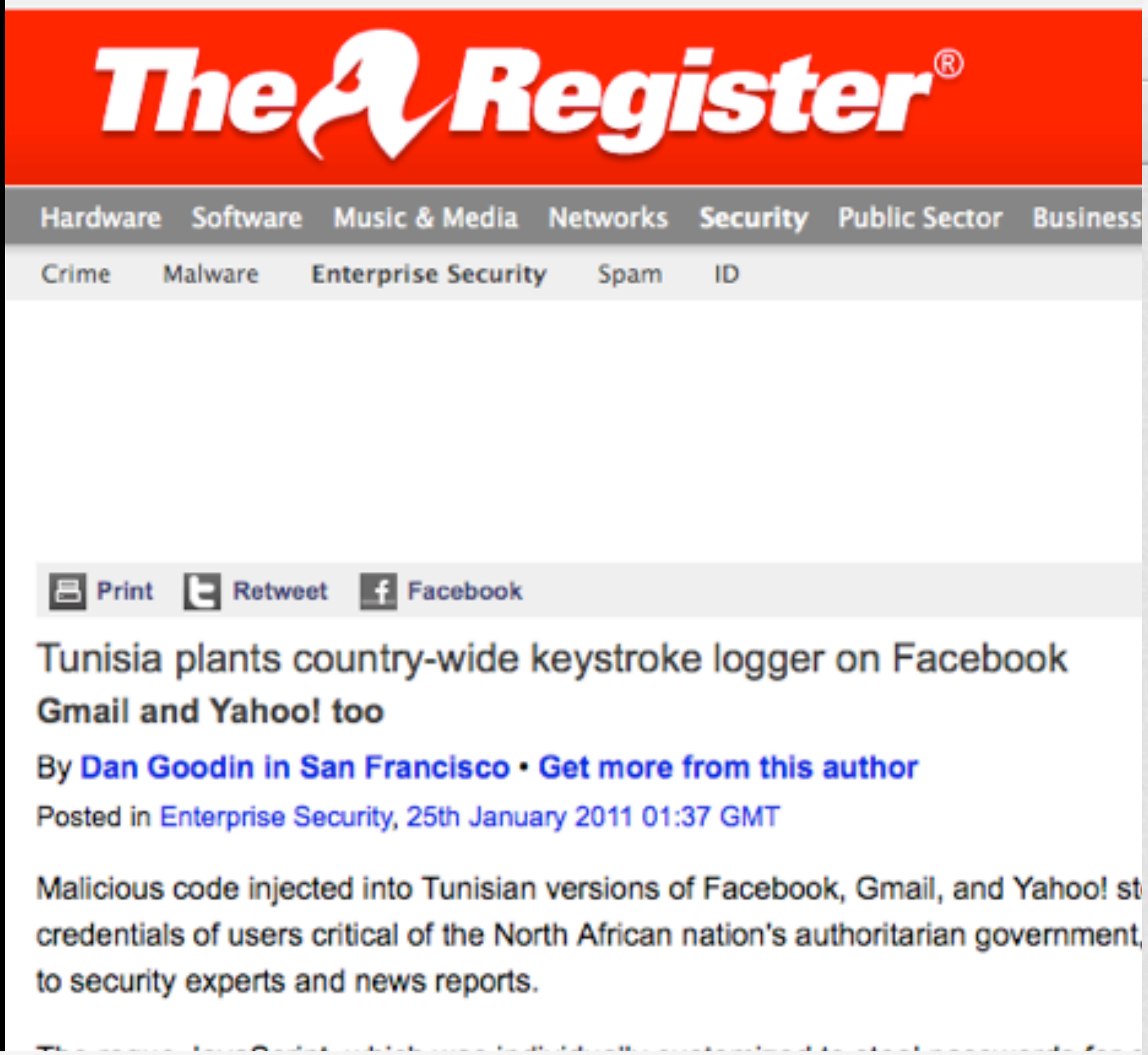
- We set out to gather info on real world SSL/TLS usage
- We wanted to know if info on 443/TCP where same as 80/TCP, not only SSL for subset of pages (login page)

Problem statement

- In a world where everyone uses unencrypted http traffic, there is no empiri on just how much *monitoring, intercept, hijacking, redirection, cookie stealing* going on

- *Without SSL*, the monitoring of citizens during the arabic spring would have gone unnoticed

- If they controlled - and used - their own root CA, the rules of the game would have been different



Tunisia plants country-wide keystroke logger on Facebook

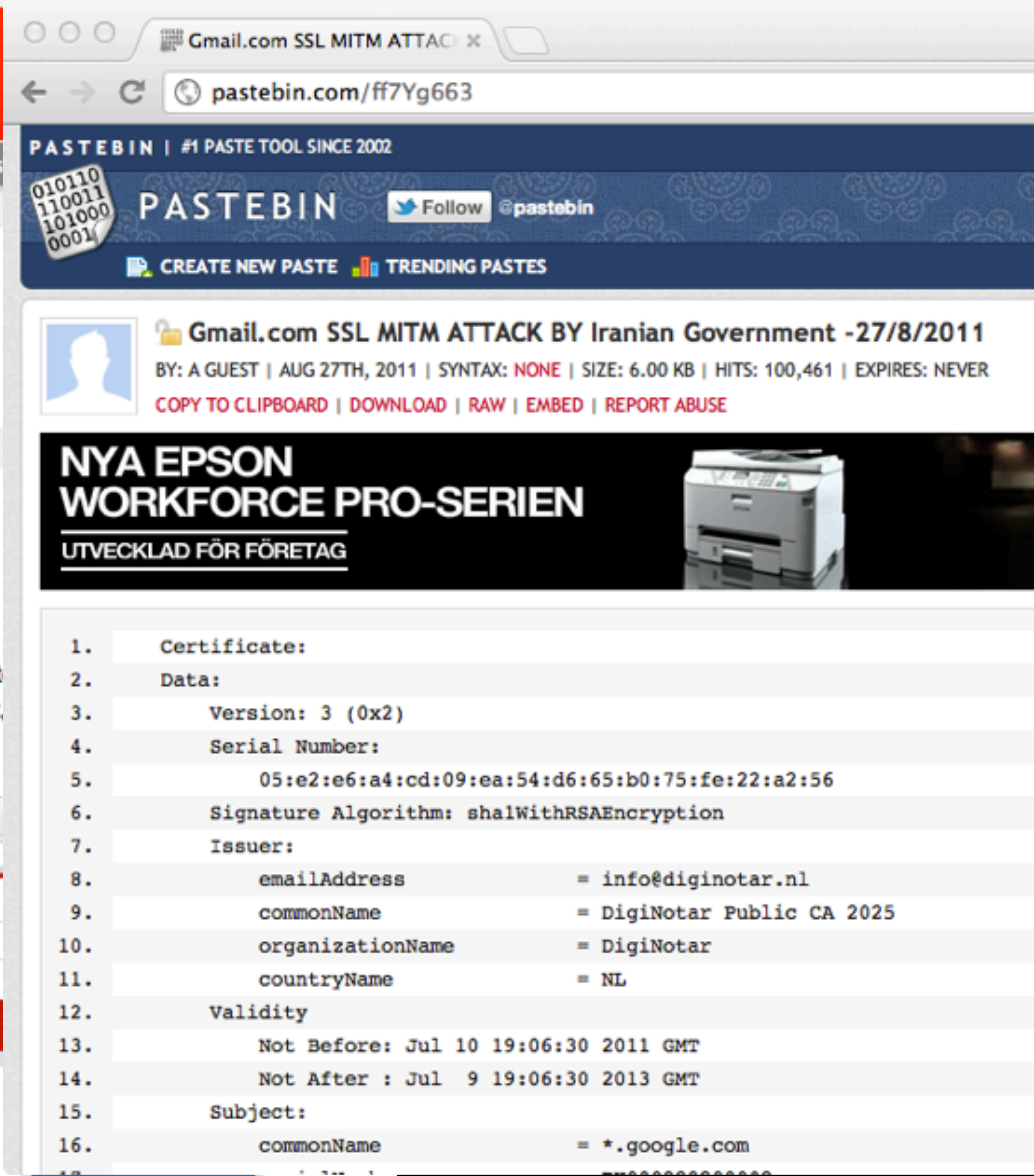
Gmail and Yahoo! too

By Dan Goodin in San Francisco • Get more from this author

Posted in Enterprise Security, 25th January 2011 01:37 GMT

Malicious code injected into Tunisian versions of Facebook, Gmail, and Yahoo! st
credentials of users critical of the North African nation's authoritarian government,
to security experts and news reports.

The rogue JavaScript, which was individually customized to steal passwords for a



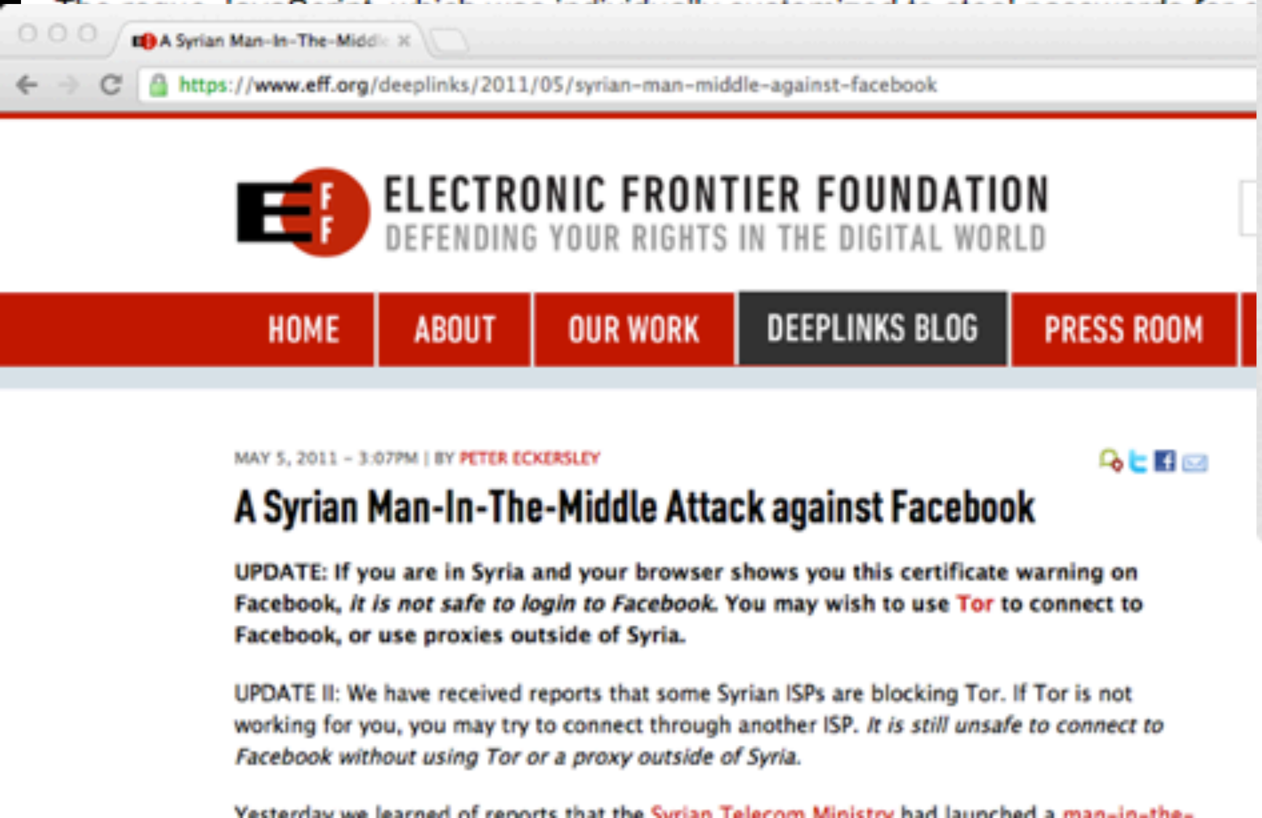
Gmail.com SSL MITM ATTAC ×
pastebin.com/ff7Yg663
PASTEBIN | #1 PASTE TOOL SINCE 2002
PASTEBIN
Follow @pastebin
CREATE NEW PASTE
TRENDING PASTES

Gmail.com SSL MITM ATTACK BY Iranian Government -27/8/2011

BY: A GUEST | AUG 27TH, 2011 | SYNTAX: NONE | SIZE: 6.00 KB | HITS: 100,461 | EXPIRES: NEVER

COPY TO CLIPBOARD | DOWNLOAD | RAW | EMBED | REPORT ABUSE

```
Certificate:
Data:
    Version: 3 (0x2)
    Serial Number:
        05:e2:e6:a4:cd:09:ea:54:d6:65:b0:75:fe:22:a2:56
    Signature Algorithm: sha1WithRSAEncryption
    Issuer:
        emailAddress                = info@diginotar.nl
        commonName                  = DigiNotar Public CA 2025
        organizationName            = DigiNotar
        countryName                 = NL
    Validity
        Not Before: Jul 10 19:06:30 2011 GMT
        Not After : Jul  9 19:06:30 2013 GMT
    Subject:
        commonName                  = *.google.com
```



A Syrian Man-In-The-Middl ×
https://www.eff.org/deeplinks/2011/05/syrian-man-middle-against-facebook
ELECTRONIC FRONTIER FOUNDATION
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD
HOME
ABOUT
OUR WORK
DEEPLINKS BLOG
PRESS ROOM

MAY 5, 2011 - 3:07PM | BY PETER ECKERSLEY

A Syrian Man-In-The-Middle Attack against Facebook

UPDATE: If you are in Syria and your browser shows you this certificate warning on Facebook, *it is not safe to login to Facebook*. You may wish to use Tor to connect to Facebook, or use proxies outside of Syria.

UPDATE II: We have received reports that some Syrian ISPs are blocking Tor. If Tor is not working for you, you may try to connect through another ISP. *It is still unsafe to connect to Facebook without using Tor or a proxy outside of Syria.*

Yesterday we learned of reports that the Syrian Telecom Ministry had launched a man-in-the-

REAL Motivations

Kill *plaintext* communication for a major protocol

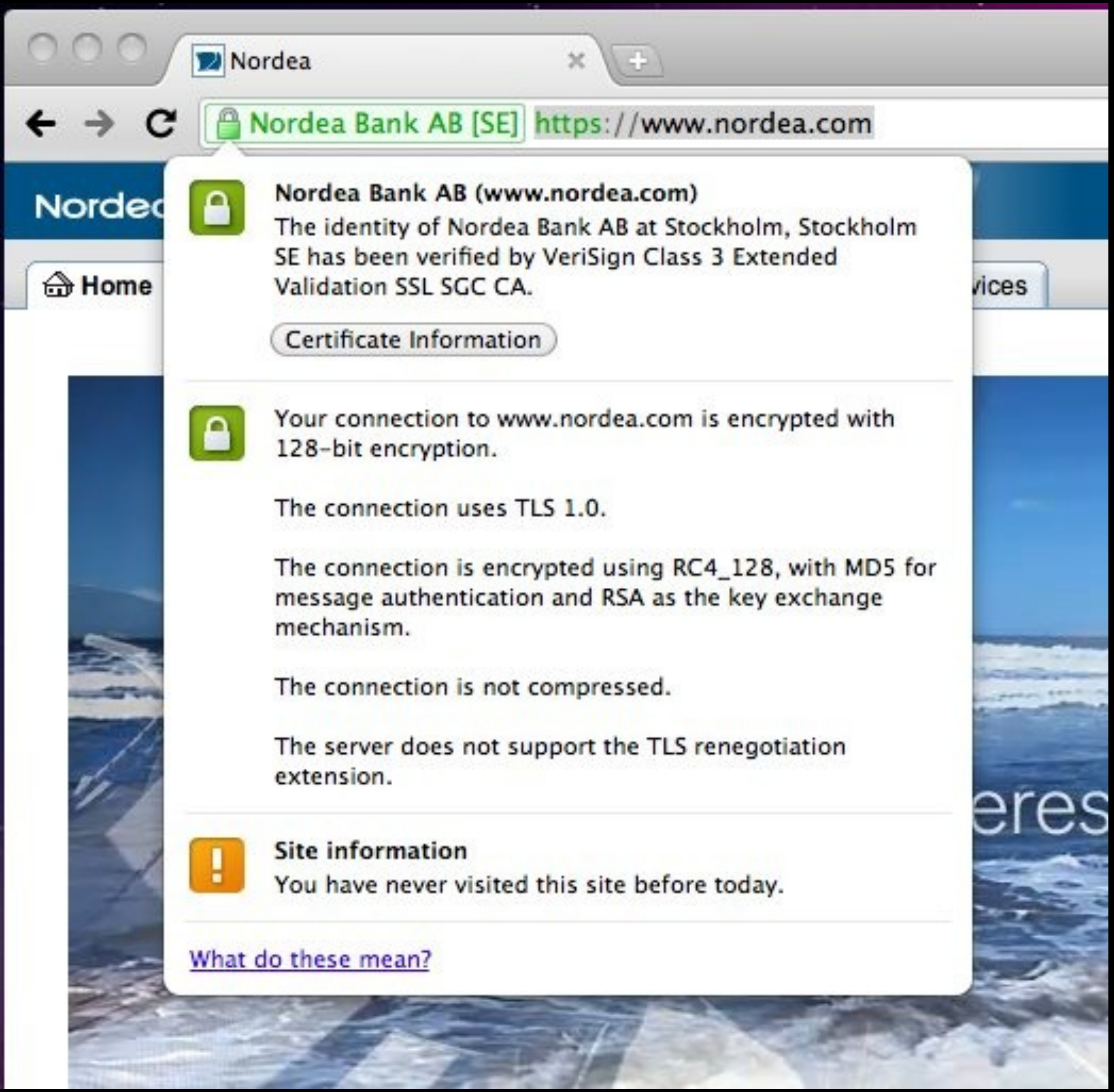
Only exchange data encrypted

SSL in 3 bullets

- Used to protect communication against eavesdropping that would be bad for the site owner / company services provided by site

- Require X.509 certificates and PKI. Commercial CA providing certs after "some" validation

- Developed by Netscape in mid 90's (SSLv2), matures (SSLv3) and embraced by IETF (TLS, latest 1.2)



Nordea Bank AB (www.nordea.com)
The identity of Nordea Bank AB at Stockholm, Stockholm SE has been verified by VeriSign Class 3 Extended Validation SSL SGC CA.

Certificate Information

Your connection to www.nordea.com is encrypted with 128-bit encryption.

The connection uses TLS 1.0.

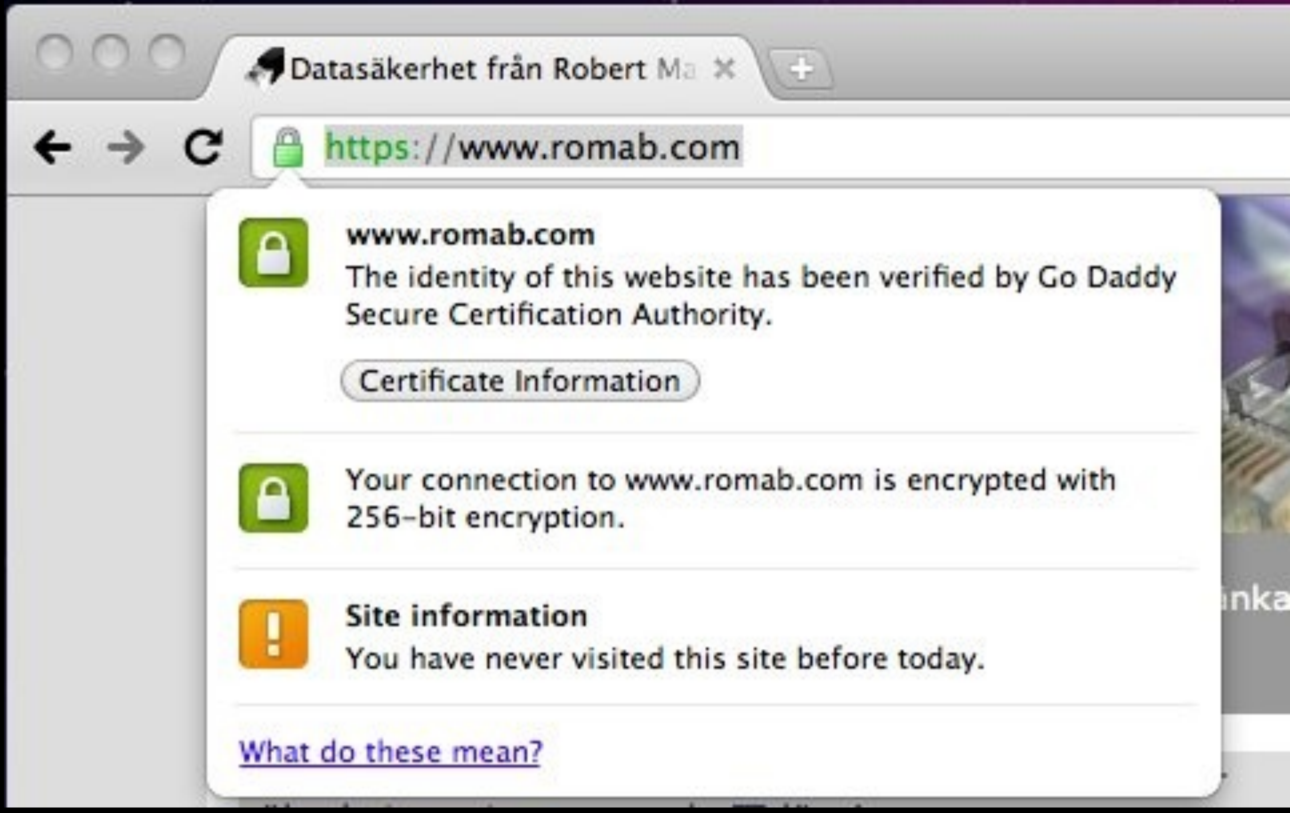
The connection is encrypted using RC4_128, with MD5 for message authentication and RSA as the key exchange mechanism.

The connection is not compressed.

The server does not support the TLS renegotiation extension.

Site information
You have never visited this site before today.

What do these mean?



www.romab.com
The identity of this website has been verified by Go Daddy Secure Certification Authority.

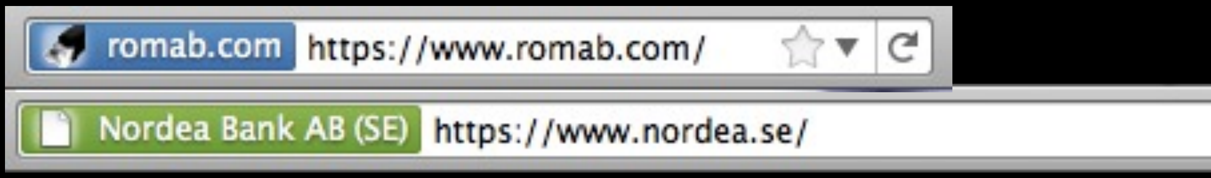
Certificate Information

Your connection to www.romab.com is encrypted with 256-bit encryption.

Site information
You have never visited this site before today.

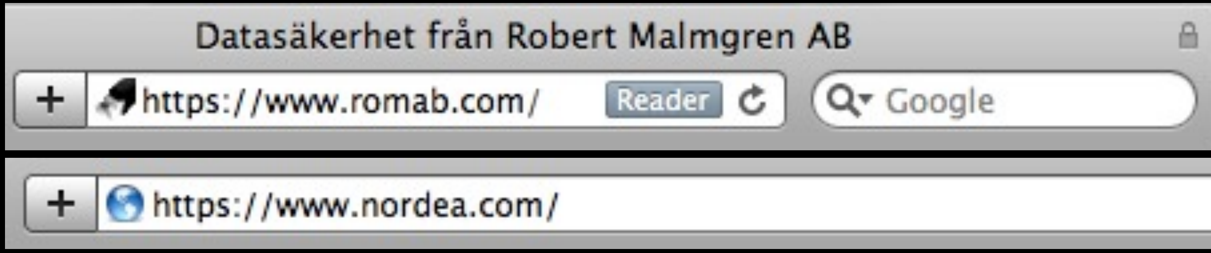
What do these mean?

Firefox

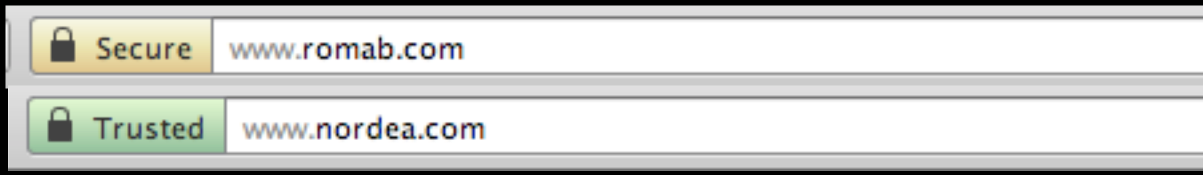


romab.com https://www.romab.com/
Nordea Bank AB (SE) https://www.nordea.se/

Safari



Opera



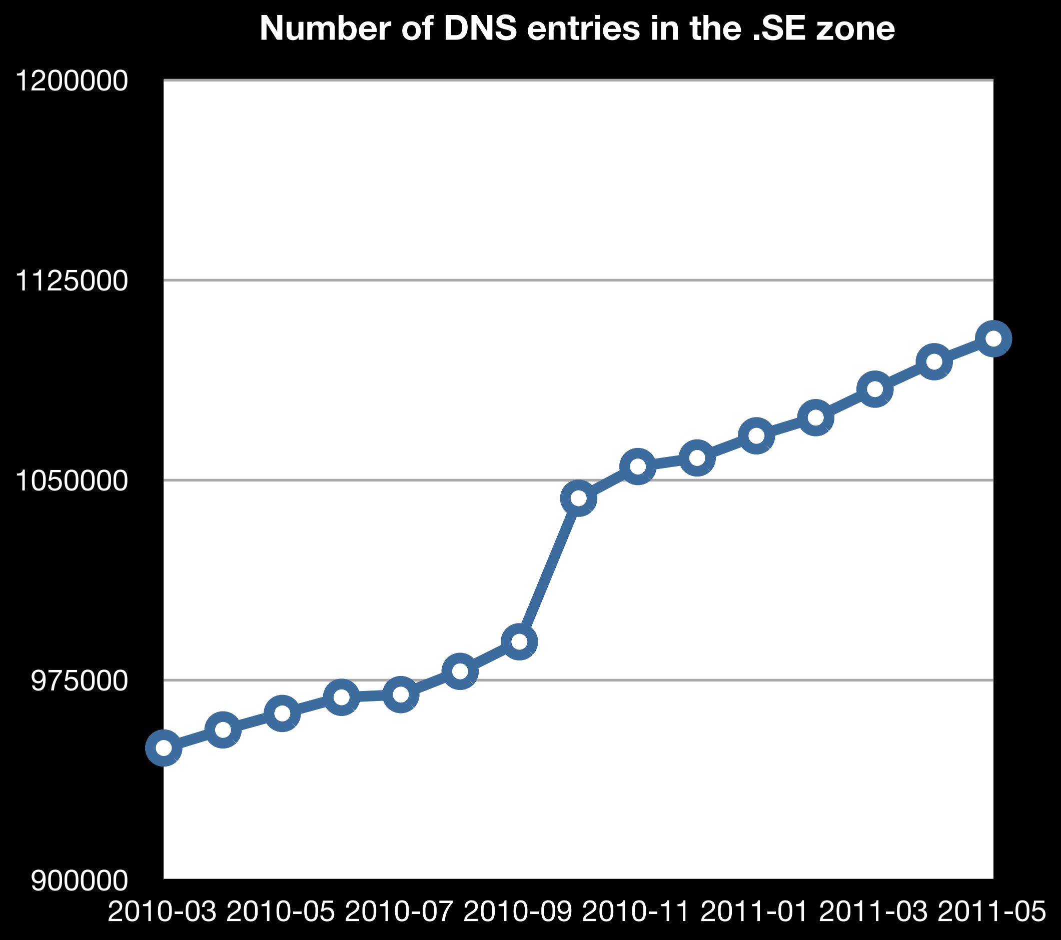
SQL observeratory data related to yesterdays $crypto

```
+-------------------------+----------+
| Signature Algorithm     | count(*) |
+-------------------------+----------+
|  sha512WithRSAEncryption |        1 |
|  sha1WithRSA             |        1 |
|  md2WithRSAEncryption    |        4 |
|  sha256WithRSAEncryption |       62 |
|  md5WithRSAEncryption    |    29958 |
|  sha1WithRSAEncryption   |  1503333 |
+-------------------------+----------+
```

```
+-----------------+----------+
| RSA_Modulus_Bits | count(*) |
+-----------------+----------+
| NULL            |       25 |
| 511             |        3 |
| 512             |     4165 |
| 730             |        1 |
| 767             |        1 |
| 768             |       38 |
| 1023            |      977 |
| 1024            |   869402 |
.......
| 2047            |      145 |
| 2048            |   564514 |
| 3333            |        1 |
| 3584            |        3 |
| 3889            |        1 |
| 4000            |        2 |
| 4028            |        1 |
| 4069            |       18 |
| 4092            |        2 |
| 4096            |    15574 |
| 4192            |        1 |
| 4196            |        2 |
| 5120            |        2 |
| 6095            |        2 |
| 8192            |       38 |
| 16384           |        1 |
+-----------------+----------+
```

1024 bit (~60%), 2048 bit (~39%) and 4096 bit (~1%)

Some statistics on SSL usage



Today ~1,1 million domains in .SE

- Approximately 13300 sites with 443/TCP (~1%)
- Broken chain of trust, revoked, selfsigned, bad name, etc ~2300
- Hard redirects to 80/TCP ~5915
- Webmail + citrix ~936

- *Thus we have ~**4137** (< 0.5%) hosts using SSL left in the .SE zone*

- Browsing demo

(new) reasons to do SSL

An eavesdropper could by watching your behaviour on:

- news sites and blogs, easily determine *your political preferences*
- porn sites/erotica and forums, easily determine *your sexual prefences*
- traffic sites easily determine *your traveling patterns*
- communities, such as facebook, easily determine *who your friends are*
- search engines, easily *determine what's on your mind this second*
- communities, such as facebook, easily determine *who you are*
- what you buy, such as commercial sites, determine *your income class*
- what you sell and buy on auction sites, determine *what your hobbies are*
- *ETC, ETC*

SweSSL

- Painstakinly manually check

    1. *Is 443/TCP reachable and SSL enabled*
    2. *That the SSL setup is correct*
    3. *That the same content is served via HTTPS as in HTTP*
    4. *The page does not contain mixed content*

Sites we have sampled

- Swedish alexa top 100
- Swedish media sites
- Alexa top 100 international media
- Swedish labour unions
- Swedish political parties

If you actually use SSL, *use it properly*

- No self-signed
- No mixed mode, e.g. dont include content via http
- Don’t redirect to plaintext http on port 80. Bad for security. Bad for page rank
- No wildcard cert for web hosting company
- Should you include google analytics on ssl page, or not?
- Have ALT NAMES for your other known identities (e.g. sverigesradio.se AND sr.se)

If you actually set it up, *govern it properly*

- Don't have expired cert. Beside losing service, you look incompetent
- Follow trend, be prepared to act. What to do if your CA is revoked?
- This adds another dimension if you use certificate pining or HSTS.

Mythbusting: awkward & expensive

- Hard to setup in web server

  ✓ No, its not (*The megaLOL: StartSSL service to generate private key and distribute you a bundle for your setup*)

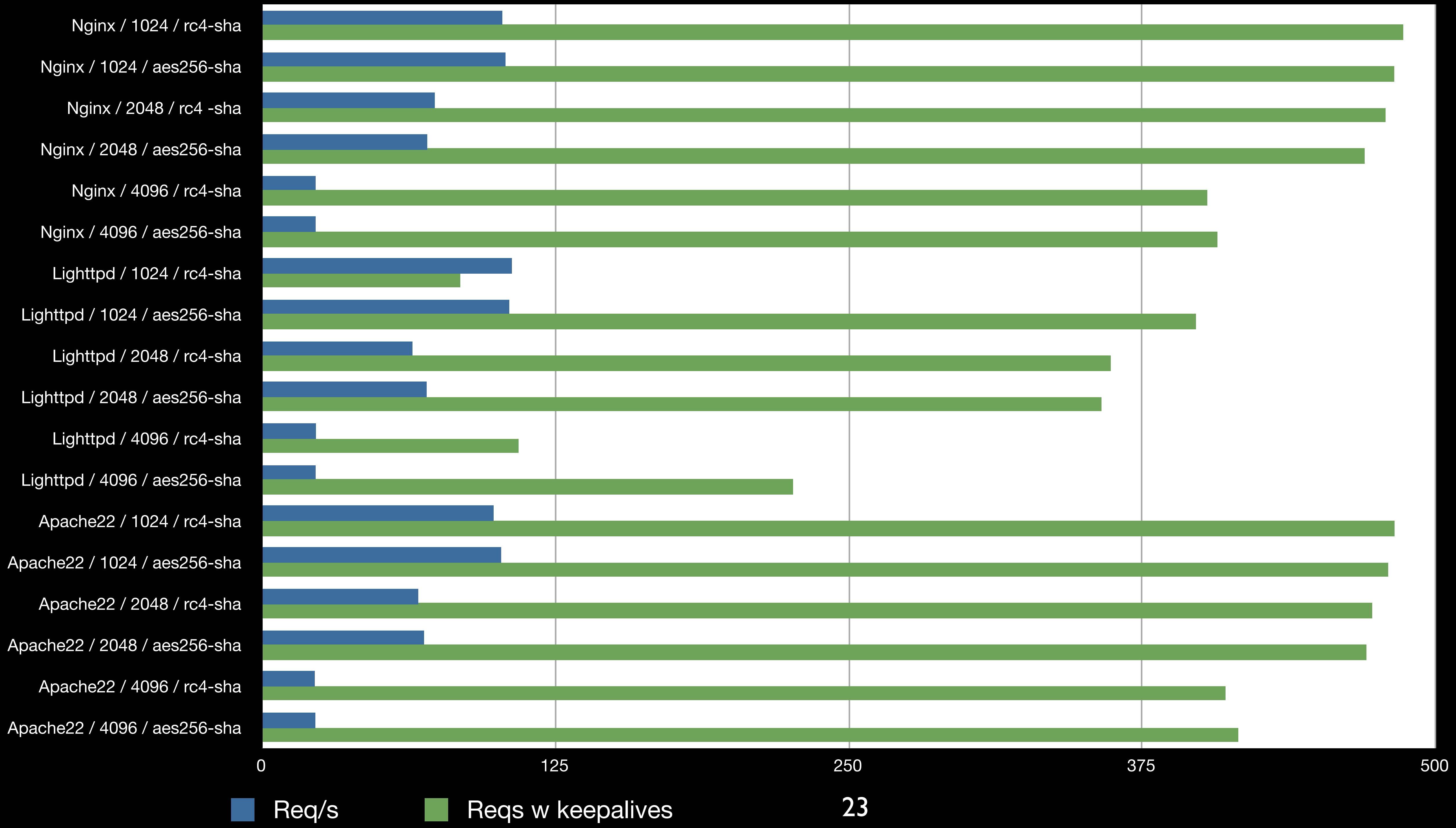
- Certificates are expensive

  ✓ From ~$50, is not expensive. Free alternative exists

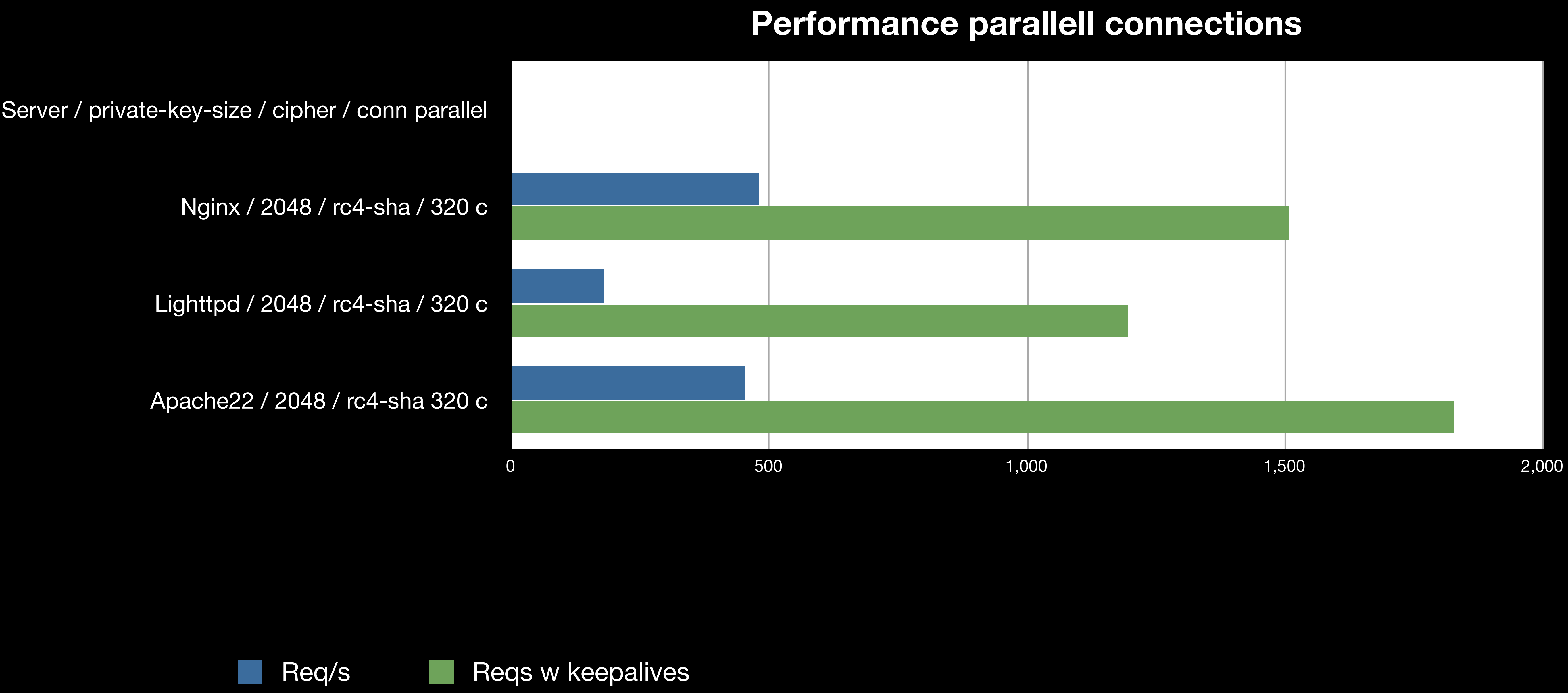
- My business model is based on advertisments, it wont work with SSL

  ✓ Most banner networks are SSL capable

Mythbusting: performance

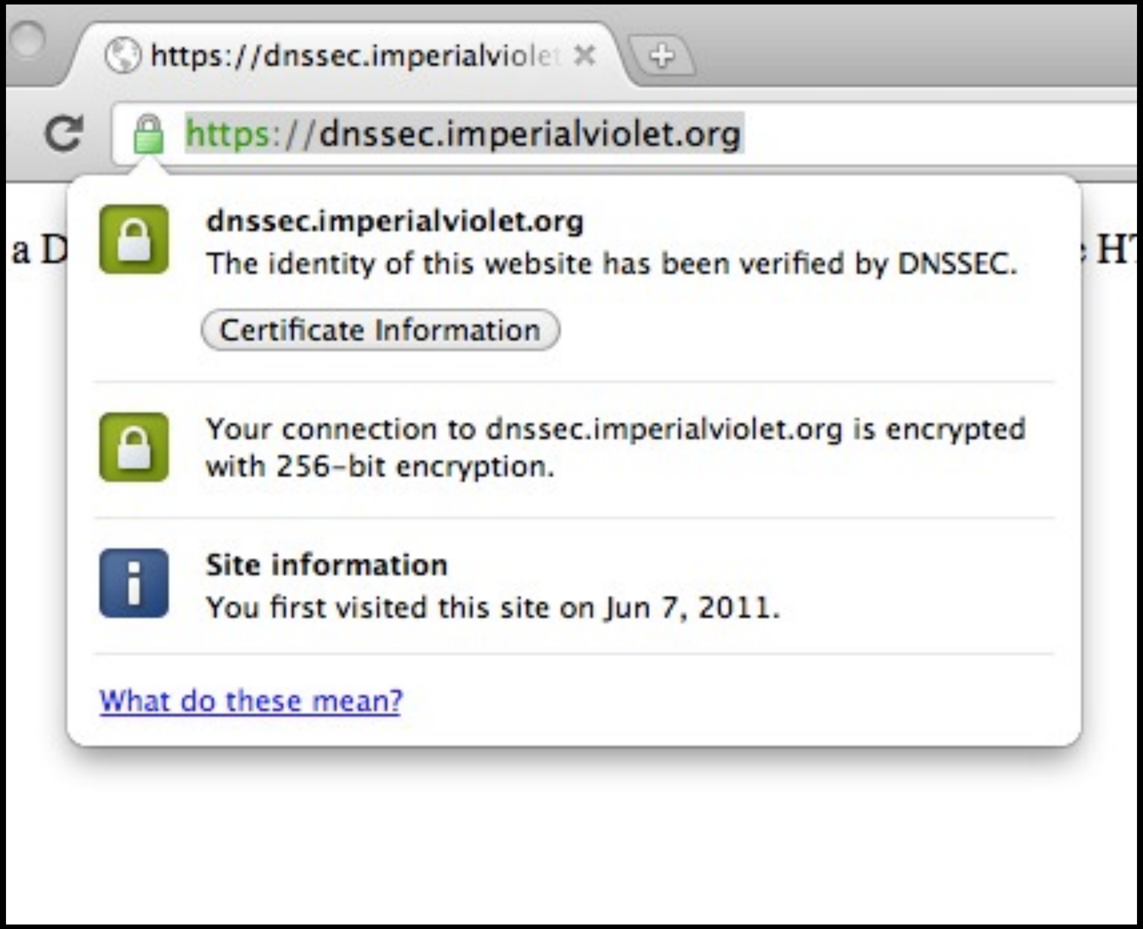


Mythbusting: performance



New techbologies: HSTS, DANE, DNSSec, etc

- HSTS - HTTP Strict Transport Security - Force HTTPS reconnections
- FalseStart - faster HTTPS initiation
- SPDY
- Certificate pinning


https://dnssec.imperialviolet.org

dnssec.imperialviolet.org
The identity of this website has been verified by DNSSEC.

Your connection to dnssec.imperialviolet.org is encrypted with 256-bit encryption.

Site information
You first visited this site on Jun 7, 2011.

http://www.imperialviolet.org/2011/06/16/dnssecchrome.html

HTTPS-everywhere

- Plugin for firefox + chrome, developed by the EFF
- Pre-made ruleset for sites that partially or completely supports SSL
- Stable ruleset ~1000 rules
- Current ruleset >1200 rules
- Many rules in the repo is **a result of SweSSL!**

Server recommendations

- Ensure keep alives
- Enable HSTS to protect users
- Cache like you mean it
- Cache-type: public allows for libnss based browsers to cache to disk
- CDNs can be a real pain: only 2 services: plain or PCIDSS. Remember this when evaluating suppliers. *AKAMAI, i am looking at you.*

Client recommendations

- Use useful add-ons
  - Noscript
  - HTTPS-everywhere
  - Certificate patrol
  - SSLpersonas
  - Expiry canary
  - Cipherfox
  - Cert viewer plus

- Be ware of trust stores
  - Especially at work
  - Tampering can introduce unintended side effects

Summary

- TLS is not used as well as it should, especially for *privacy enhancements*
  - SSL used by e-banking, e-shop, remote access, but not much more...
  - How much MITM today? Not known since we only use HTTP.....
- Lots of technical and business model advances makes going all in on HTTPS possible, even simple

https://www.romab.com/swessl