State of SSL

InfoSec World 2011

v1.2

Ivan Ristic

Director of Engineering
iristic@qualys.com / @ivanristic

April 21st, 2011

INFOSEC WORLD CONFERENCE & EXPO 2011

QUALYS®

MIS TRAINING INSTITUTE

Agenda

1. State of SSL
2. Introduction to SSL Labs
3. SSL Configuration Survey
4. Future Work

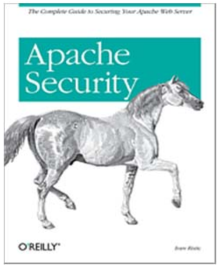
About Ivan Ristic

Ivan is a compulsive builder, usually attracted to problems no one else is working on

- *Apache Security*, O'Reilly (2005)
- **ModSecurity**, open source web application firewall
- **SSL Labs**, SSL, TLS, and PKI research
- *ModSecurity Handbook*, Feisty Duck (2010)
- **IronBee**, next-generation open source web application firewall

modsecurity

QUALYS® SSL LABS



MODSECURITY HANDBOOK
The Complete Guide to the Popular Open Source Web Application Firewall
Ivan Ristić
Feisty Duck

IRONBEE™
Open Source WAF

Part I:

State of SSL

Brief History

Protocol goal:

- Turn an insecure communication channel, no matter which protocol it is running, into a secure one
- Hide the complexity of secure communication from most developers
- Designed for HTTP, but can be used for pretty much anything

The original version designed at Netscape:

- Version 2 was released in 1994
- Found to have many issues, and quickly followed by v3
- Standardized under the name TLS (Transport Layer Security) in 1999
  - TLS v1.1 released in 2006
  - TLS v1.2 released in 2008

SSL Ecosystem

The SSL ecosystem includes many players:

- Basic cryptographic algorithms
- SSL and TLS encryption protocols
- IETF TLS Working Group
- Public Key Infrastructure (PKI) standards
- SSL library developers
- SSL Client vendors (esp. major browser vendors)
- SSL Server vendors
- Certificate Authorities and their resellers
- CA/Browser Forum
- System administrators
- Consumers

Major Challenges Today (1)

1. Fragility of the trust ecosystem
   - Validation often relies on DNS and email, which are not secure
   - Too many CAs and resellers—many weak links
   - Some CAs might be government-run
2. Bad SSL configuration is common
   - Few pay attention to SSL configuration
   - Easy to misconfigure, affecting security and performance
3. Slow adoption of modern standards
   - Most of the Internet runs yesterday's technologies
   - Interoperability issues slow down innovation

Major Challenges Today (2)

4. Lack of support for virtual SSL hosting
   - SSL site requires one exclusive IP address
   - This is expensive and slows everyone down
5. Mismatch between HTTP and SSL
   - Incorrectly developed web applications compromise SSL
   - Insecure session cookies
   - Mixed content
6. Performance and caching challenges
   - Protocols need to be changed to reduce latency
   - Cryptographic operation are generally not a problem
   - Most sites could improve performance by changing configuration

Part II:

SSL Labs

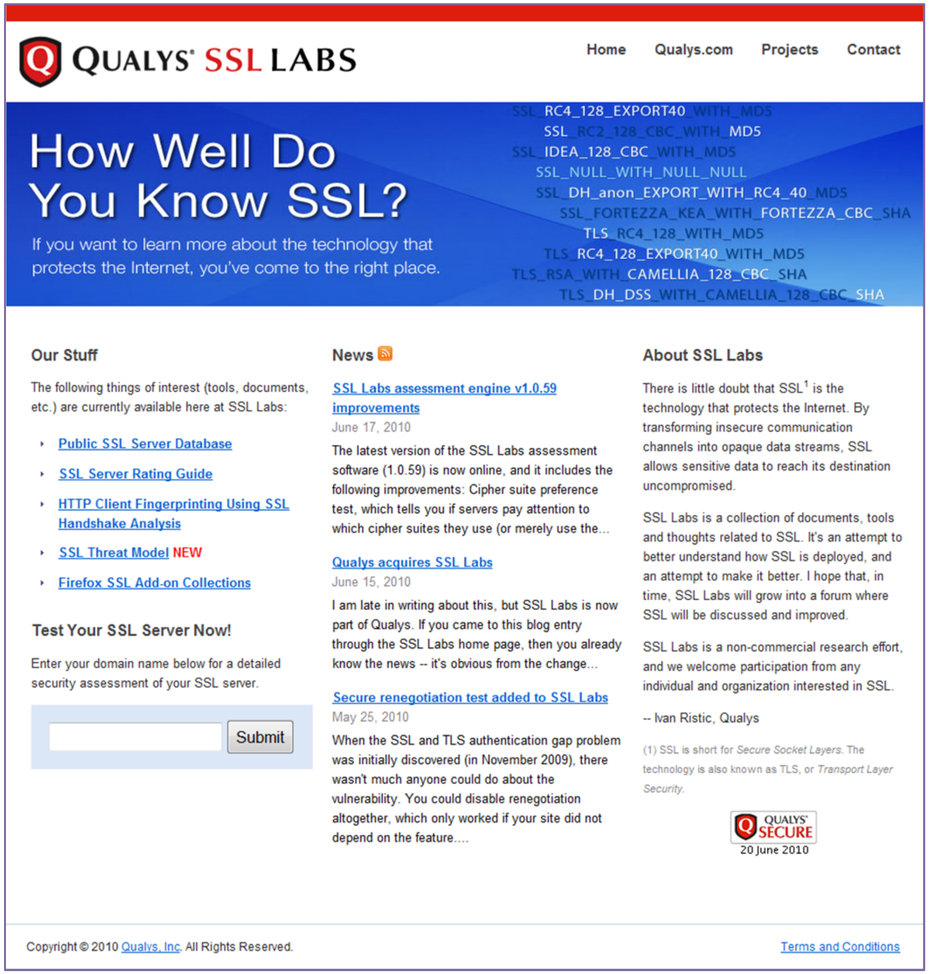
SSL Labs

SSL Labs:

- A non-commercial security research effort focused on SSL, TLS, and friends

Projects:

- Assessment tool
- SSL Rating Guide
- Passive SSL client fingerprinting tool
- SSL Threat Model
- **SSL Survey**


QUALYS SSL LABS
Home
Qualys.com
Projects
Contact
SSL_RC4_128_EXPORT40_WITH_MD5
SSL_RC2_128_CBC_WITH_MD5
SSL_IDEA_128_CBC_WITH_MD5
SSL_NULL_WITH_NULL_NULL
SSL_DH_anon_EXPORT_WITH_RC4_40_MD5
SSL_FORTEZZA_KEA_WITH_FORTEZZA_CBC_SHA
TLS_RC4_128_WITH_MD5
TLS_RC4_128_EXPORT40_WITH_MD5
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA
Submit
QUALYS SECURE
20 June 2010

How Well Do You Know SSL?

If you want to learn more about the technology that protects the Internet, you've come to the right place.

Our Stuff

The following things of interest (tools, documents, etc.) are currently available here at SSL Labs:

- Public SSL Server Database
- SSL Server Rating Guide
- HTTP Client Fingerprinting Using SSL Handshake Analysis
- SSL Threat Model NEW
- Firefox SSL Add-on Collections

Test Your SSL Server Now!

Enter your domain name below for a detailed security assessment of your SSL server.

News

SSL Labs assessment engine v1.0.59 improvements
June 17, 2010
The latest version of the SSL Labs assessment software (1.0.59) is now online, and it includes the following improvements: Cipher suite preference test, which tells you if servers pay attention to which cipher suites they use (or merely use the...

Qualys acquires SSL Labs
June 15, 2010
I am late in writing about this, but SSL Labs is now part of Qualys. If you came to this blog entry through the SSL Labs home page, then you already know the news -- it's obvious from the change...

Secure renegotiation test added to SSL Labs
May 25, 2010
When the SSL and TLS authentication gap problem was initially discovered (in November 2009), there wasn't much anyone could do about the vulnerability. You could disable renegotiation altogether, which only worked if your site did not depend on the feature....

About SSL Labs

There is little doubt that SSL[1] is the technology that protects the Internet. By transforming insecure communication channels into opaque data streams, SSL allows sensitive data to reach its destination uncompromised.

SSL Labs is a collection of documents, tools and thoughts related to SSL. It's an attempt to better understand how SSL is deployed, and an attempt to make it better. I hope that, in time, SSL Labs will grow into a forum where SSL will be discussed and improved.

SSL Labs is a non-commercial research effort, and we welcome participation from any individual and organization interested in SSL.

-- Ivan Ristic, Qualys

(1) SSL is short for *Secure Socket Layers*. The technology is also known as TLS, or *Transport Layer Security*.

Terms and Conditions

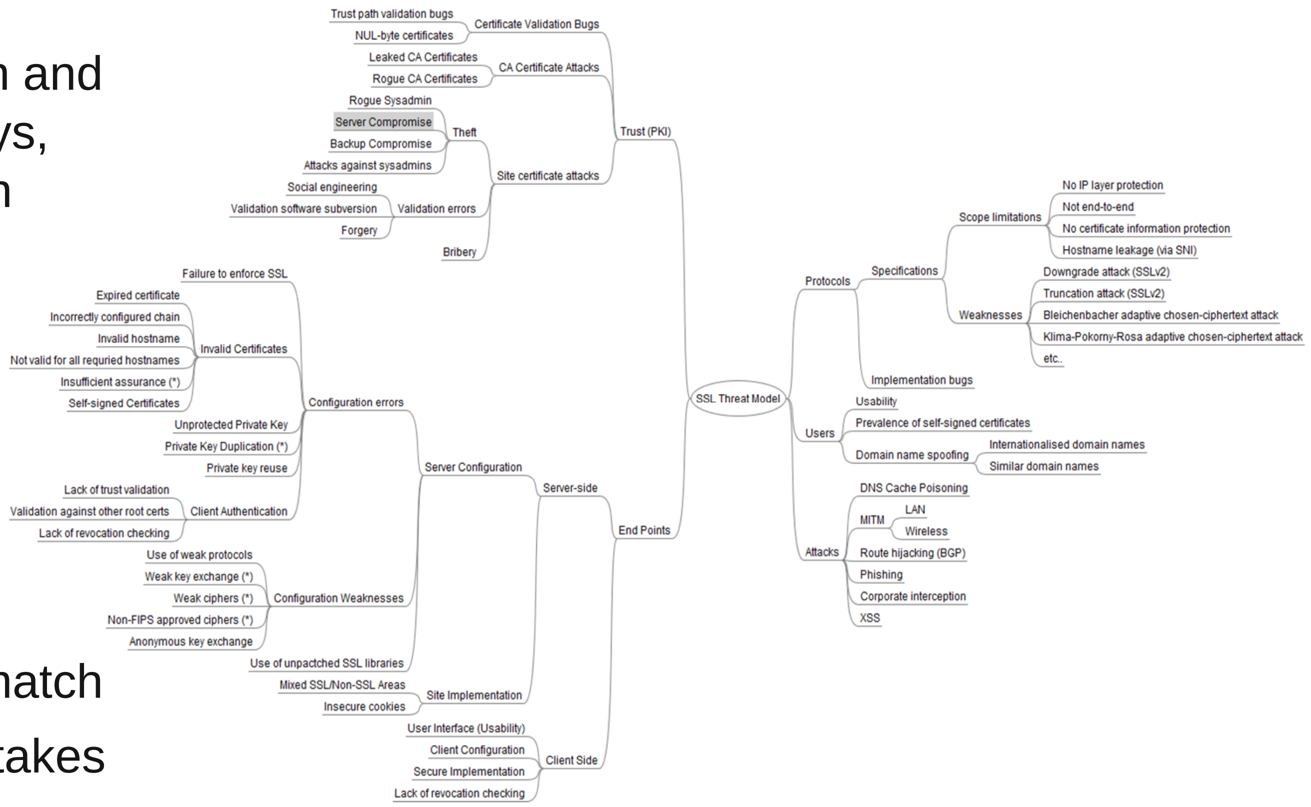
SSL ~~Threat~~ Fail Model

How can SSL fail?

- In about a million and one different ways, some worse than others.

Principal issues:

- Implementation flaws
- MITM
- Usability issues
- Impedance mismatch
- Deployment mistakes
- PKI trust challenges



SSL Rating Guide

What is the purpose of the guide?

- Sum up a server’s SSL configuration, and explain how scores are assigned
- Make it possible for non-experts to understand how serious flaws are
- Enable us to quickly say if one server
  is better configured than another
- Give configuration guidance

QUALYS SSL LABS

How Well Do
You Know SS

If you want to learn more about the te
protects the Internet, you've come to

Our Stuff

The following things of interest (tools, documents, etc.) are currently available here at SSL Labs:

- Public SSL Server Database
- SSL Server Rating Guide
- HTTP Client Fingerprinting Using SSL Handshake Analysis
- SSL Threat Model NEW
- Firefox SSL Add-on Collections

Test Your SSL Server Now!

Enter your domain name below for a detaile
security assessment of your SSL server.

Sub

Copyright © 2010 Qualys, Inc. All Rights

SSL Survey HTTP Rating Guide

version 1.0 (5 July 2010)

Copyright © 2010 Qualys SSL Labs (www.ssllabs.com)

Abstract

The Secure Sockets Layer (SSL) protocol is a standard for encrypted network communication. We feel that there is surprisingly little attention paid to how SSL is configured, given its widespread usage. SSL is relatively easy to use, but it does have its traps. This guide aims to establish a straightforward assessment methodology, allowing administrators to assess SSL server configuration confidently without the need to become SSL experts.

QUALYS SSL LABS

www.ssllabs.com

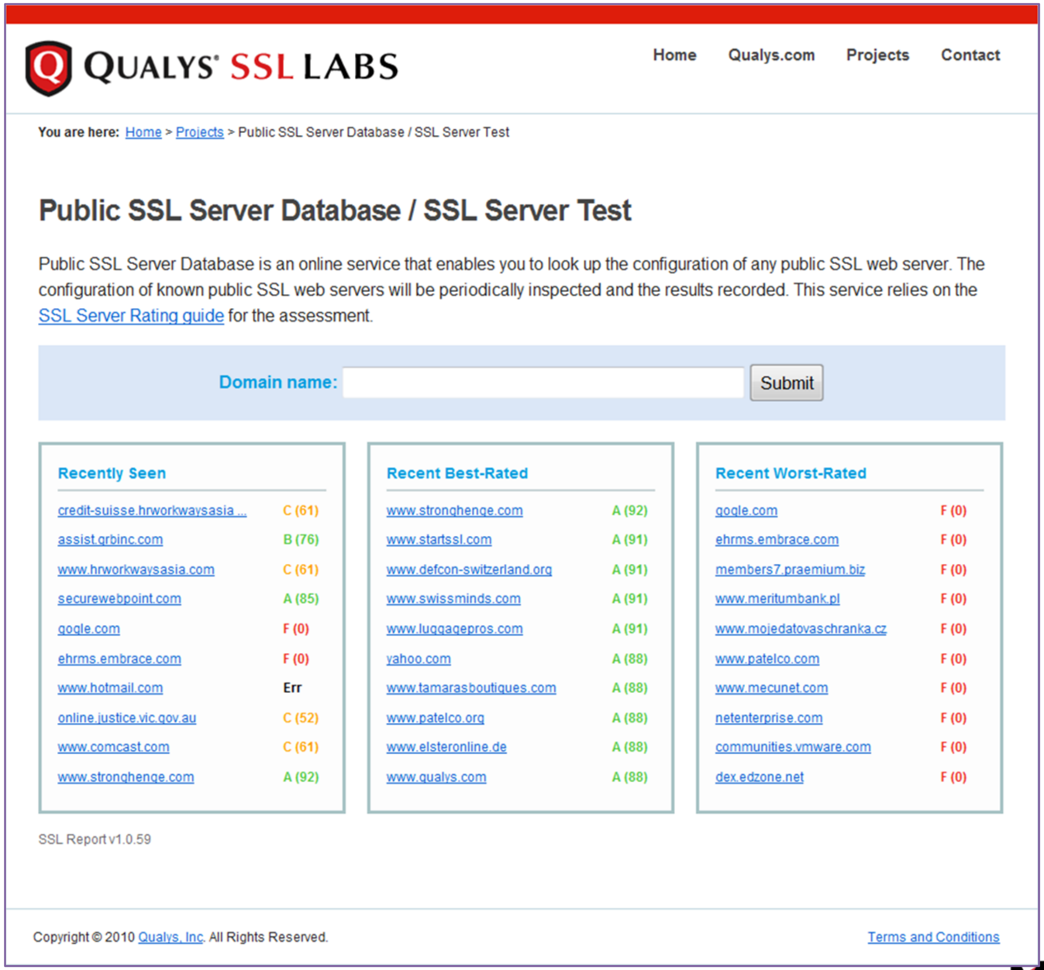
Online SSL Assessment Overview

Main features:

- Free online SSL test
- Comprehensive, yet easy on CPU
- Results easy to understand

What we analyze:

- Configuration
- Certificate chain
- Protocol and cipher suite support
- Enabled Features
- Weaknesses



You are here: Home > Projects > Public SSL Server Database / SSL Server Test

Public SSL Server Database / SSL Server Test

Public SSL Server Database is an online service that enables you to look up the configuration of any public SSL web server. The configuration of known public SSL web servers will be periodically inspected and the results recorded. This service relies on the SSL Server Rating guide for the assessment.

Domain name:

Recently Seen	
credit-suisse.hrworkwaysasia ...	C (61)
assist.grbinc.com	B (76)
www.hrworkwaysasia.com	C (61)
securewebpoint.com	A (85)
gogle.com	F (0)
ehrms.embrace.com	F (0)
www.hotmail.com	Err
online.justice.vic.gov.au	C (52)
www.comcast.com	C (61)
www.stronghenge.com	A (92)

Recent Best-Rated	
www.stronghenge.com	A (92)
www.startssl.com	A (91)
www.defcon-switzerland.org	A (91)
www.swissminds.com	A (91)
www.luggagepros.com	A (91)
yahoo.com	A (88)
www.tamarasboutiques.com	A (88)
www.patelco.org	A (88)
www.elsteronline.de	A (88)
www.qualys.com	A (88)

Recent Worst-Rated	
gogle.com	F (0)
ehrms.embrace.com	F (0)
members7.praemium.biz	F (0)
www.meritumbank.pl	F (0)
www.mojedatovaschranka.cz	F (0)
www.patelco.com	F (0)
www.mecunet.com	F (0)
netenterprise.com	F (0)
communities.vmware.com	F (0)
dex.edzone.net	F (0)

SSL Report v1.0.59

Copyright © 2010 Qualys, Inc. All Rights Reserved.

Terms and Conditions

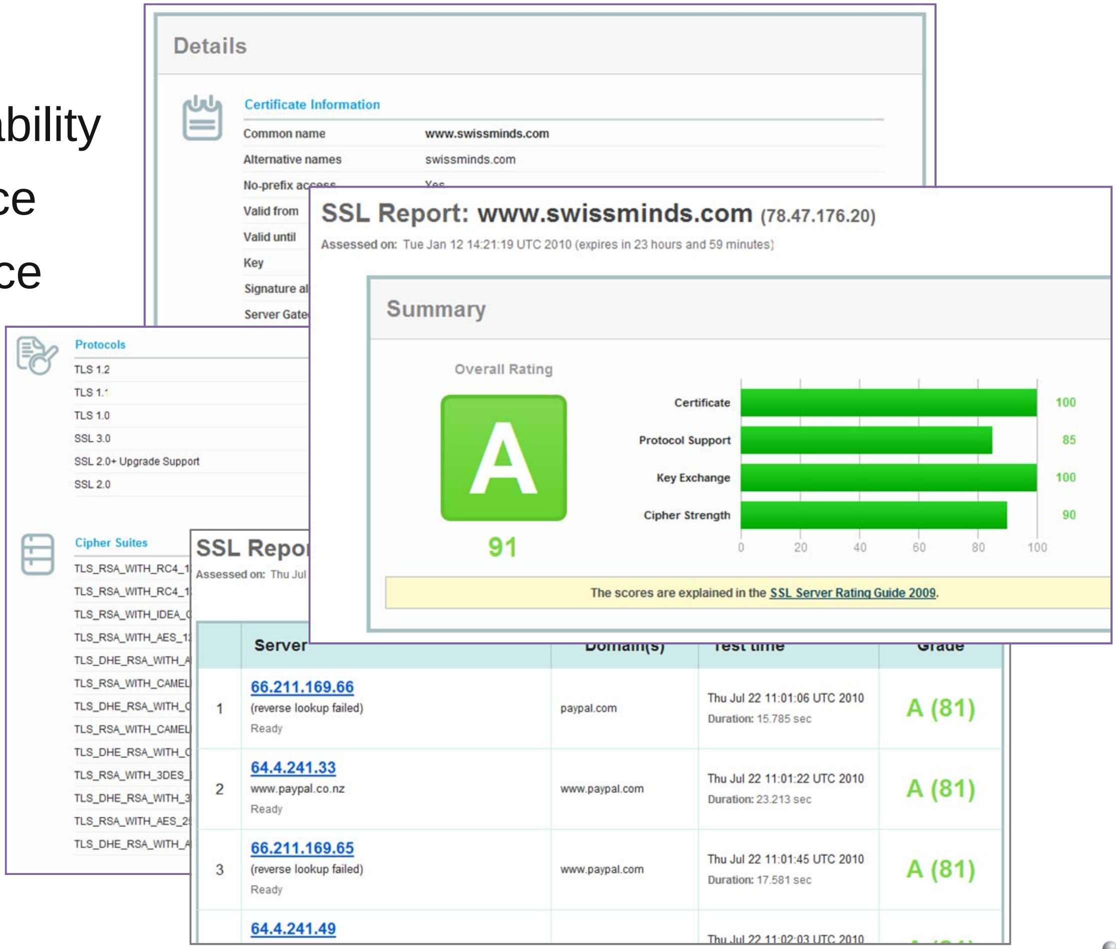
SSL Assessment Details

Highlights:

- Renegotiation vulnerability
- Cipher suite preference
- TLS version intolerance
- Session resumption
- Firefox 3.6 trust base

Every assessment consists of about:

- 2000 packets
- 200 connections
- 250 KB data



Details

Certificate Information

Common name	www.swissminds.com
Alternative names	swissminds.com
No-prefix access	Yes
Valid from	
Valid until	
Key	
Signature al	
Server Gate	

Protocols

- TLS 1.2
- TLS 1.1
- TLS 1.0
- SSL 3.0
- SSL 2.0+ Upgrade Support
- SSL 2.0

Cipher Suites

- TLS_RSA_WITH_RC4_1
- TLS_RSA_WITH_RC4_1
- TLS_RSA_WITH_IDEA_C
- TLS_RSA_WITH_AES_1
- TLS_DHE_RSA_WITH_A
- TLS_RSA_WITH_CAMEL
- TLS_DHE_RSA_WITH_C
- TLS_RSA_WITH_CAMEL
- TLS_DHE_RSA_WITH_C
- TLS_RSA_WITH_3DES_
- TLS_DHE_RSA_WITH_3
- TLS_RSA_WITH_AES_2
- TLS_DHE_RSA_WITH_A

SSL Report: www.swissminds.com (78.47.176.20)

Assessed on: Tue Jan 12 14:21:19 UTC 2010 (expires in 23 hours and 59 minutes)

Summary

Overall Rating

A

91

The scores are explained in the SSL Server Rating Guide 2009.

SSL Repor

Assessed on: Thu Jul

	Server	Domain(s)	Test time	Grade
1	66.211.169.66 (reverse lookup failed) Ready	paypal.com	Thu Jul 22 11:01:06 UTC 2010 Duration: 15.785 sec	A (81)
2	64.4.241.33 www.paypal.co.nz Ready	www.paypal.com	Thu Jul 22 11:01:22 UTC 2010 Duration: 23.213 sec	A (81)
3	66.211.169.65 (reverse lookup failed) Ready	www.paypal.com	Thu Jul 22 11:01:45 UTC 2010 Duration: 17.581 sec	A (81)
	64.4.241.49		Thu Jul 22 11:02:03 UTC 2010	

INFOSEC WORLD CONFERENCE & EXPO 2011

MIS TRAINING INSTITUTE

Part IV:

SSL Survey

Finding Servers to Assess

In our first survey, in 2010:

- We looked at 119 million domain name registrations
- Also examined the Alexa's top 1m domain names
- Arrived to about 900,000 server to assess
- About **600,000 were valid** and were used in the survey

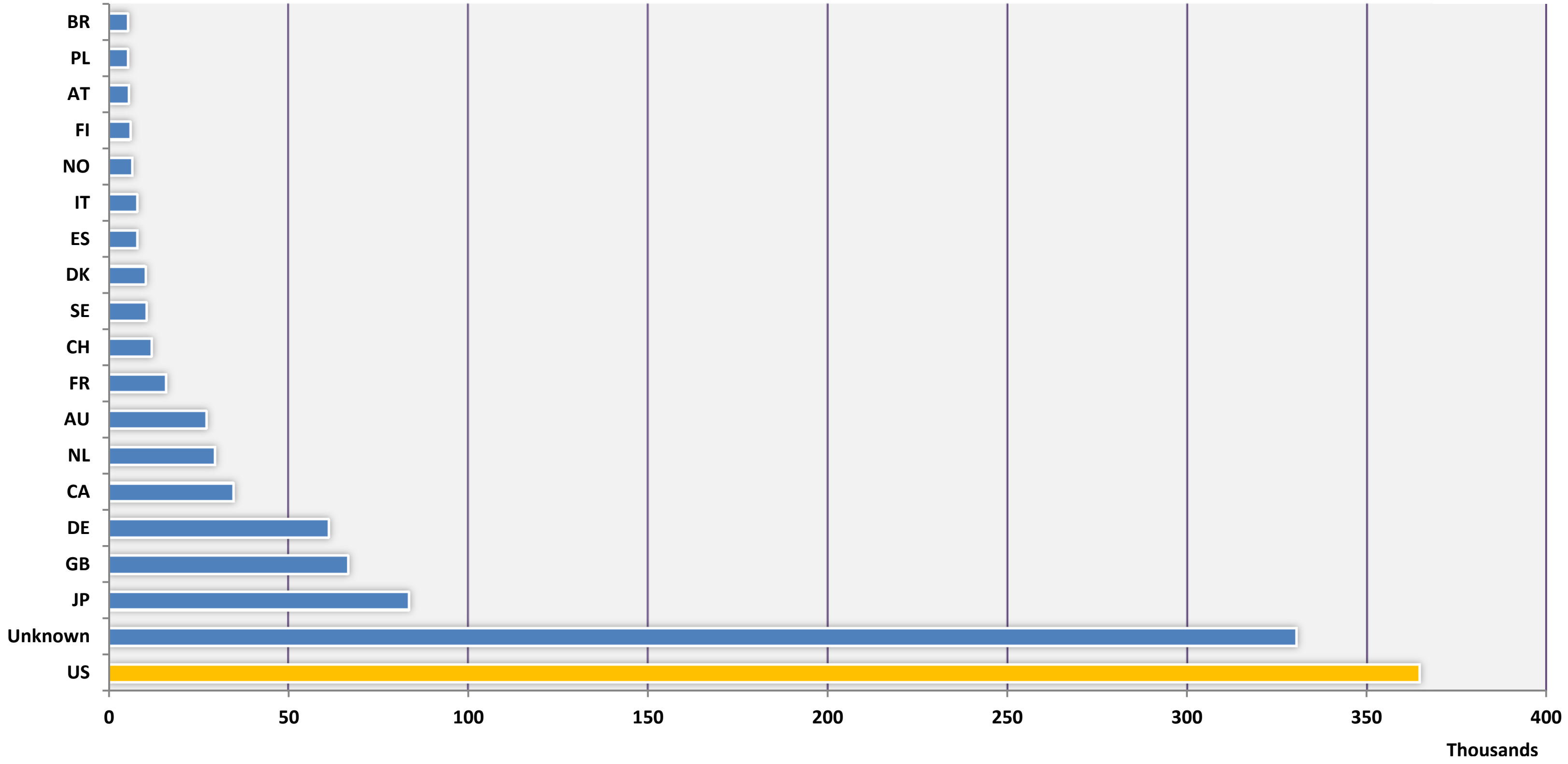
This time around (second pass):

- We used the data from **EFF's SSL Observatory**
- Almost doubled the number of valid certificates, to about **1.2m**

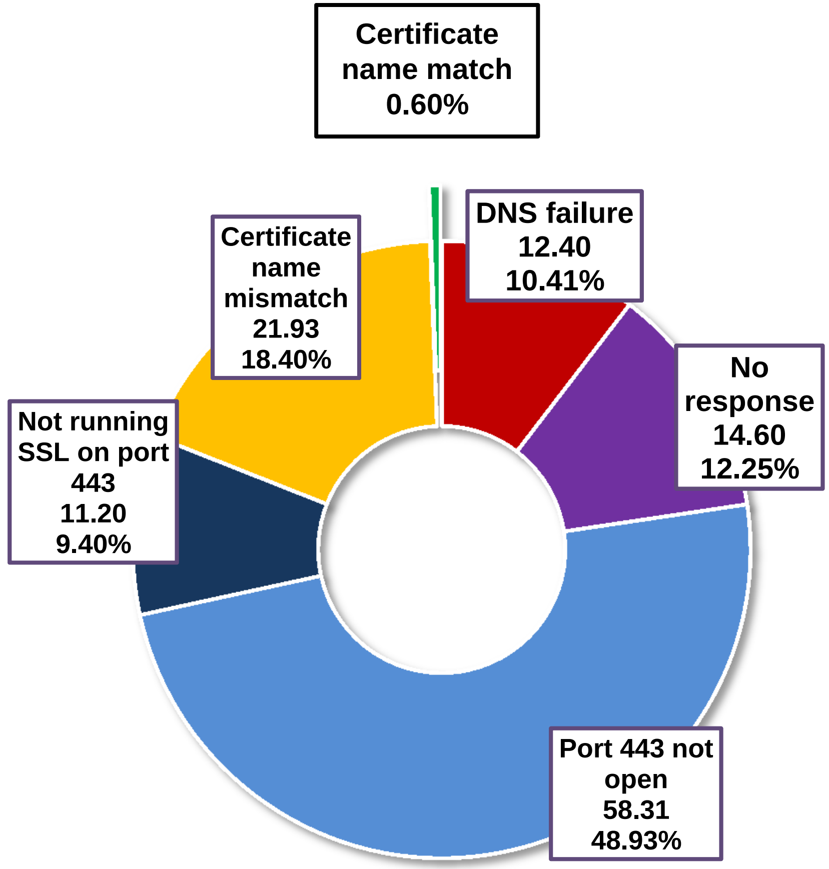
EFF ELECTRONIC FRONTIER FOUNDATION

Countries Overview

Countries with over 5,000 certificates:



High Level View

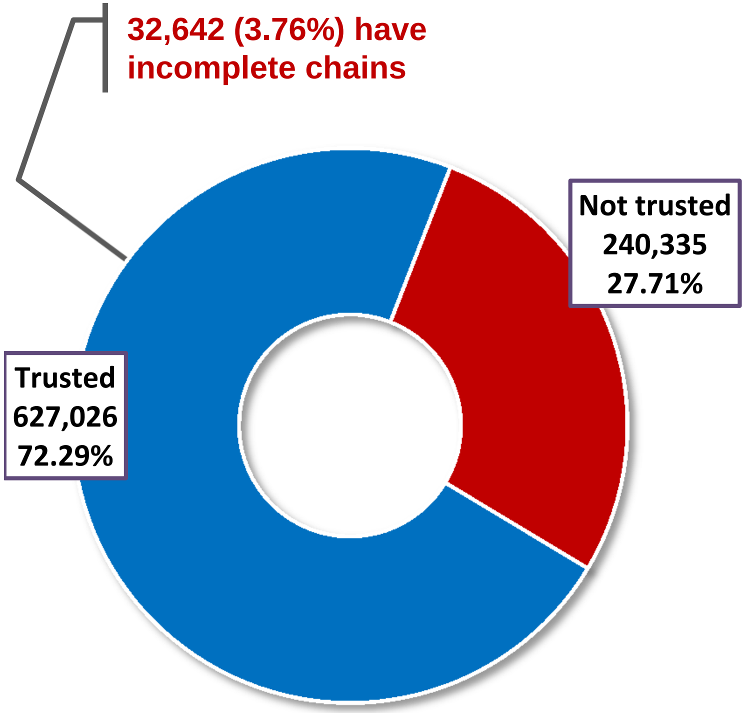


In **2010**, we looked at 119 million domain names (60% of all registrations):

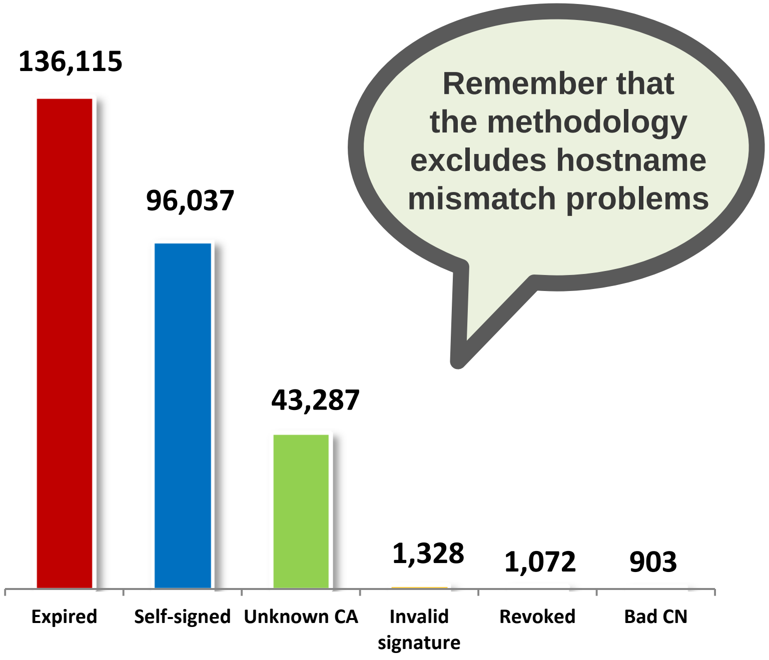
- 22.66% not operational
- 48.03% does not listen on port 443
- 9.40% runs something else on port 443
- 18.40% certificate name mismatches
- 0.60% certificate name matches (and not even those are all valid)

- Virtual web hosting hugely popular
  - 119m domain names represented by about 5.3m IP addresses
  - 22.65m domain names with SSL represented by about 2m IP addresses
- Issues:
  - **No virtual SSL web hosting**
  - **No way for a browser to know if a site uses SSL**

How Many Certs Failed Validation and Why?



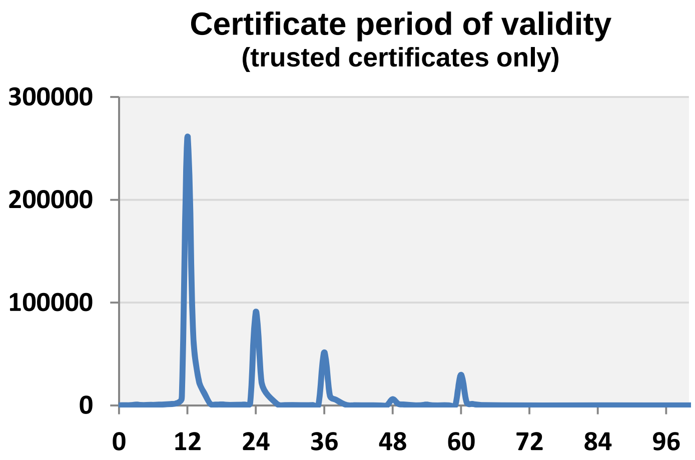
Trusted versus untrusted certificates

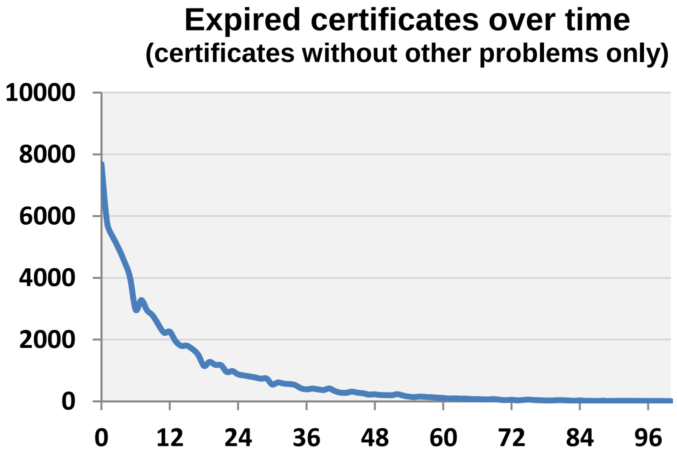


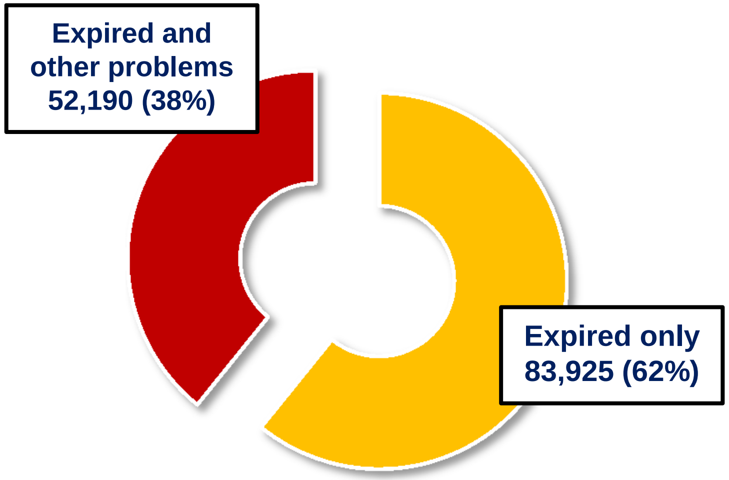
Remember that the methodology excludes hostname mismatch problems

Validation failures

Certificate Validity and Expiry Distribution





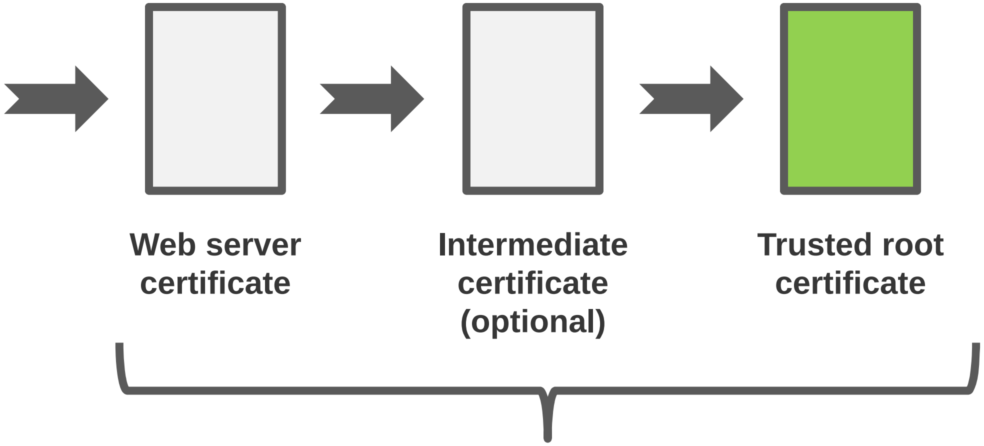


How many certificates are only expired, and how many have other problems too?

Trusted Issuers and Chain Length

We saw 618 ultimately-trusted certificate issuers

- They led to 95 trust anchors

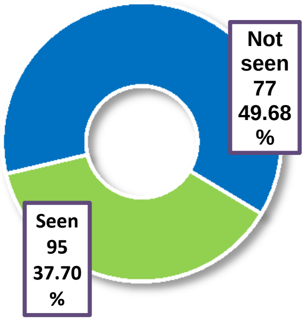


Web server certificate

Intermediate certificate (optional)

Trusted root certificate

This path is 2 levels deep in 19% of cases, and 3 levels deep in 48% of cases.

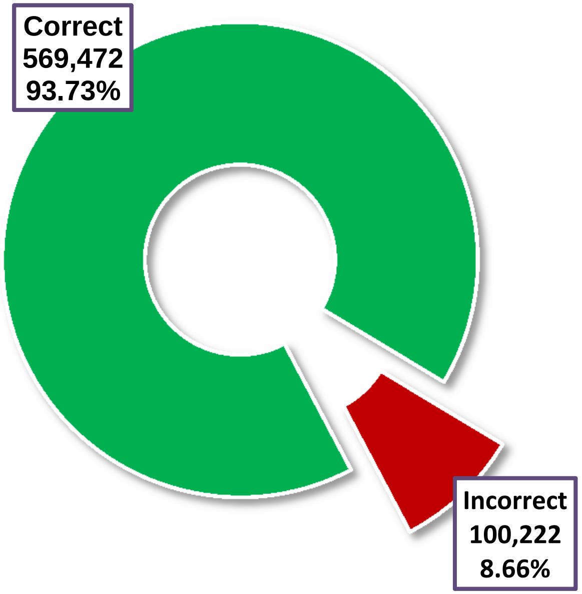


157 trusted CA certificates (from Firefox 3.6.13)

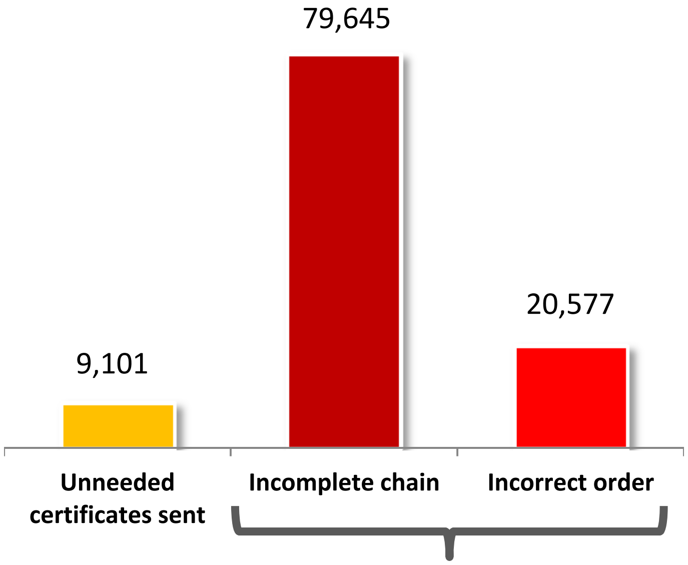
Chain length	Certificates seen
2	224,972
3	552,130
4	335,272
5	41,785
6	3,314
7	10

Recommended length

Certificate Chain Correctness



Correct versus incorrect certificate chains



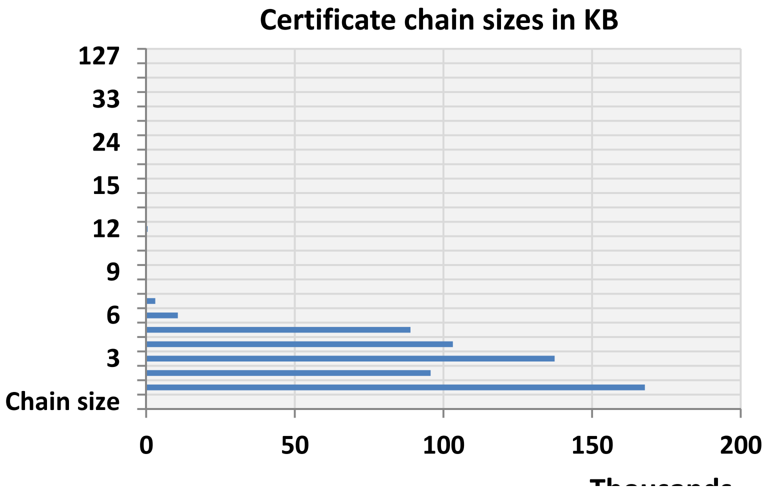
Could invalidate chains, depending on client

Issues with certificate chains

Certificate Chain Size and Length

In **43.65%** of all cases, there's more certificates sent than needed

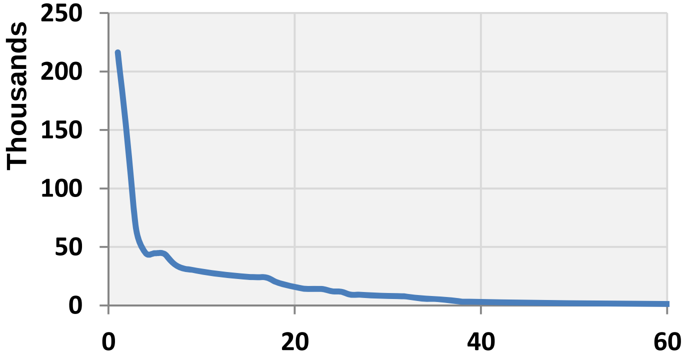
- When latency between client and server is high, the unneeded certificates waste the precious initial bandwidth
- Important when you need to want the performance to be as good as possible


Certificate chain sizes in KB

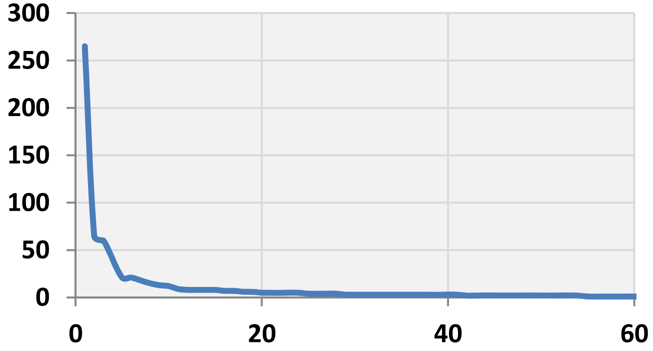
Certs sent	Actual	Should be
1	227,520	270,779
2	181,996	334,248
3	113,672	2,368
4	78,931	186
5	3,320	8
6	1,491	0
7	48	0
8	28	0
9	49	0
10	489	0
11	4	0
12	10	0
13	24	0
15	1	0
16	1	0
17	2	0
61	1	0
70	1	0
116	1	0

Trusted Anchors

Certificates per issuer
(618 issuers in total)



Certificates per trust anchor
(95 anchors in total)



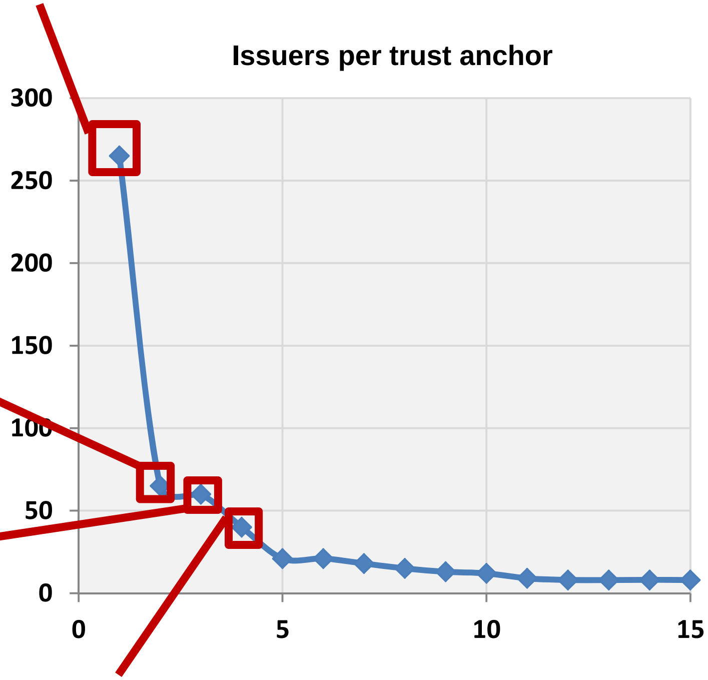
Issuer	Certificates
Go Daddy Class 2 Certification Authority	216,388
Equifax Secure Certificate Authority	144,050
UTN-USERFirst-Hardware	63,647
VeriSign Class 3 Secure Server CA - G2	44676
www.verisign.com/CPS	44643
GeoTrust DV SSL CA	44047
Thawte Premium Server CA	35735
Thawte SSL CA	31703
Thawte Server CA	30445
PositiveSSL CA	28990
DigiCert High Assurance CA-3	27821
VeriSign Class 3 Secure Server CA - G3	26538
Thawte DV SSL CA	26057
GlobalSign Domain Validation CA	24902
Network Solutions Certificate Authority	24320
RapidSSL CA	24121
Starfield Secure Certification Authority	23813
Entrust Certification Authority - L1C	20016

18 issuers on this page account for 881,912 (76.19%) certificates

Trusted Anchors and Trust Delegation

On average, there will be **6.5** issuers for every trust anchor

- Top 10 anchors have more than 10 issuers each
- They account for a total of 530 issuers, or 86% of all
- Deutsche Telekom alone accounts for 43% of all issuers we saw



Deutsche Telekom Root CA 2 (265)

GTE CyberTrust Global Root (65)

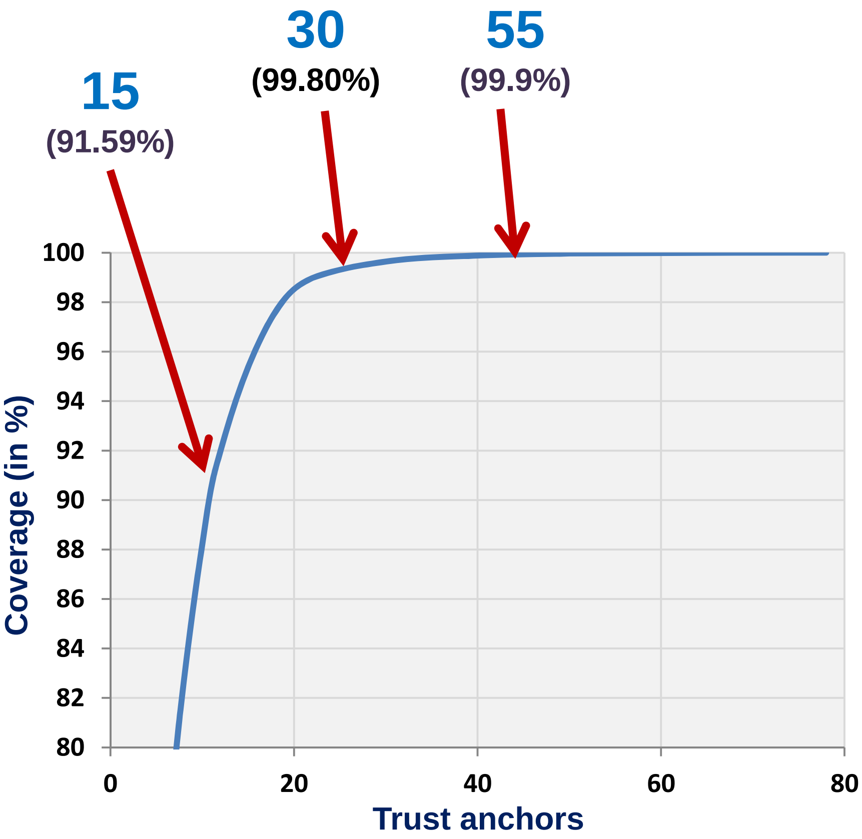
AddTrust (60)

UTN-USERFirst-Hardware (40)

How Many Trust Anchors Do We Need?

Let's try to figure the minimum number of trust anchors!

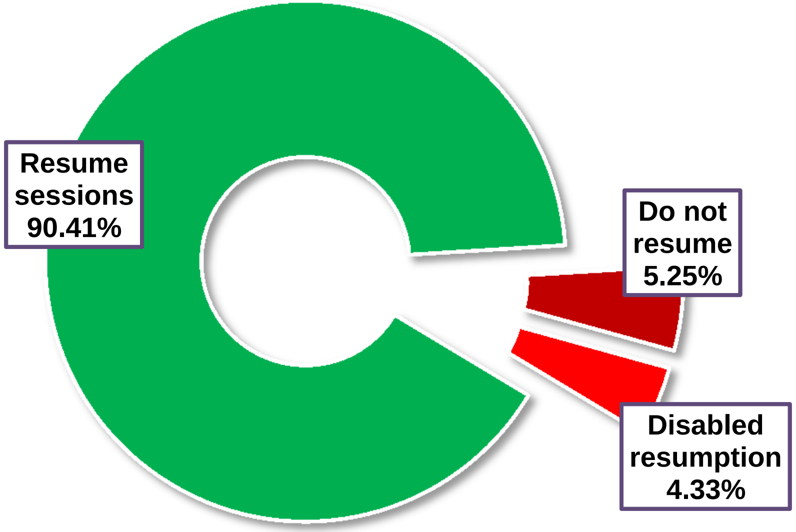
- With only 15 trust anchors you can access almost 92% of all SSL web sites
- You can access virtually all sites with anywhere from 30 to 55 trust anchors
- Which means that you can pretty much safely remove about 100 trust anchors (2/3rd) from Firefox
- We didn't even see about 60 of those in our scan



Session Resumption

Session resumption is a very important performance optimization

- It avoids the expensive handshake operations on all but first connection
- Most sites support it, but almost 10% (110k) don’t
- Session resumption may be challenging to deploy when load balancing is used

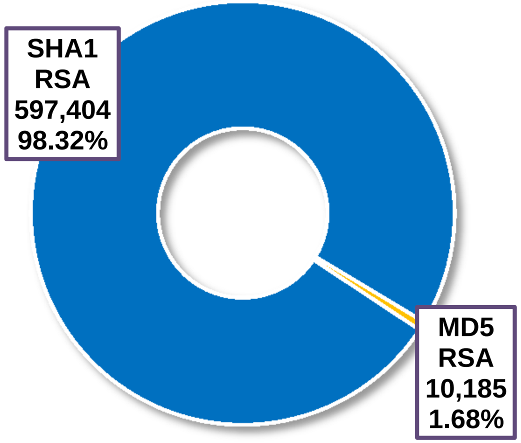


Session resumption support

Certificate Keys and Signatures

Virtually all trusted certificates use **RSA** keys; **only 17 DSA** keys

- SHA1 with RSA is the most popular choice for the signature algorithm
- We are starting to see SHA256, but on a very small number of certificates:
  - SHA256 with RSA: 81
- Virtually all keys 1024 or 2048 bits long
- Still 111 weak RNG keys from Debian



Signature algorithm

Key length	Certificates seen
512	2,358
1024	583,120
2048	557,322
4096	14,233
8192	29

Support for Multiple Domain Names

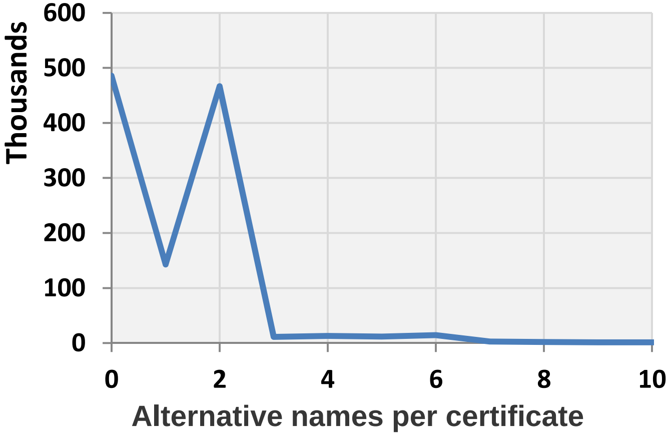
Most sites support 0, 1, or 2 alternative domain names

- Some CAs will automatically add 2 alternative domain names (“example.com” and “www.example.com”)
- Untrusted 3o.hu has 354 (8.2 KB cert)!
- Untrusted www.epi.es has 287 and they are all wildcards (7.5 KB cert)!

About **4.40%** certificates use wildcards

- 2.34% as the common name
- 2.06% in the alternative name

About **38.60%** certificates support access with and without the “www” part.

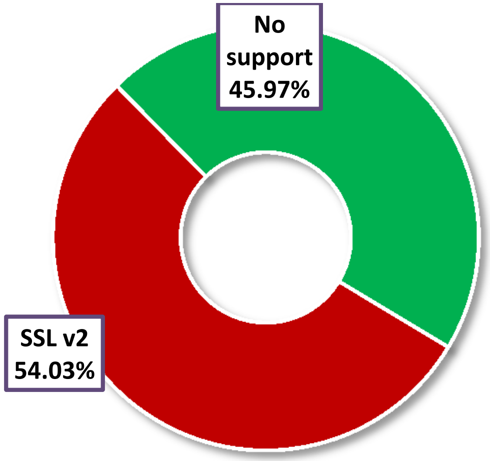


Alternative names	Name
299	portal.uni-freiburg.de
268	www.hu-berlin.de
239	prd.icr-corp.com
233	www.uni-wuerzburg.de
221	sl1web.byu.edu

Protocol Support

Half of all trusted servers support the insecure SSL v2 protocol

- Modern browsers won't use it, but wide support for SSL v2 demonstrates how we neglect to give any attention to SSL configuration
- Virtually all servers support SSLv3 and TLS v1.0
- Virtually no support for TLS v1.1 (released in 2006) or TLS v1.2 (released in 2008)
- At least 18,111 servers will accept SSLv2 but only deliver a user-friendly error message over HTTP



Protocol	Support	Best protocol
SSL v2.0	625,484	-
SSL v3.0	1,156,033	13,471
TLS v1.0	1,143,673	1,141,458
TLS v1.1	2,191	2,007
TLS v1.2	211	211

Ciphers, Key Exchange and Hash Functions

Triple DES and **RC4** rule in the cipher space

- There is also good support for AES, DES and RC2

Key exchange	Servers	Percentage
RSA	1,157,434	99.99%
RSA_EXPORT	623,914	53.90%
DHE_RSA	478,694	41.35%
RSA_EXPORT_1024	418,707	36.17%
DHE_RSA_EXPORT	250,337	21.62%

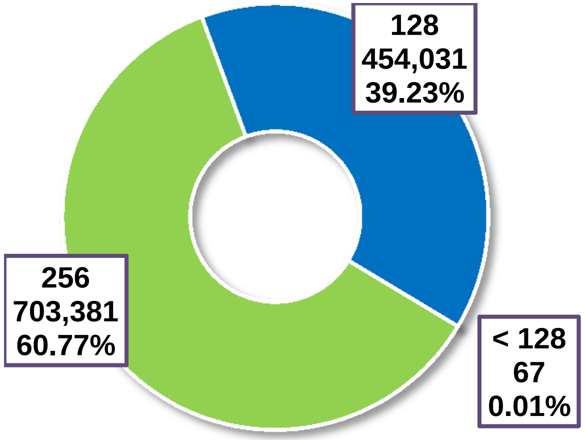
Hash	Servers	Percentage
SHA	1,154,171	99.71%
MD5	1,103,240	95.31%
SHA256	77	-
SHA384	423	-

Cipher	Servers	Percentage
3DES_EDE_CBC	1,139,215	98.42%
RC4_128	1,129,315	97.56%
AES_128_CBC	713,188	61.61%
AES_256_CBC	703,320	60.76%
DES_CBC	666,185	57.55%
RC4_40	624,294	53.93%
RC2_CBC_40	600,048	51.84%
RC2_128_CBC	518,803	44.82%
RC4_56	414,396	35.80%
DES_CBC_40	297,783	25.72%
IDEA_CBC	80,405	6.94%
RC2_CBC_56	73,491	6.34%
CAMELLIA_256_CBC	33,287	2.87%
CAMELLIA_128_CBC	33,287	2.87%
SEED_CBC	13,406	1.15%
NULL	7,513	0.64%
AES_256_GCM	3	-
AES_128_GCM	1	-
FORTEZZA_CBC	1	-

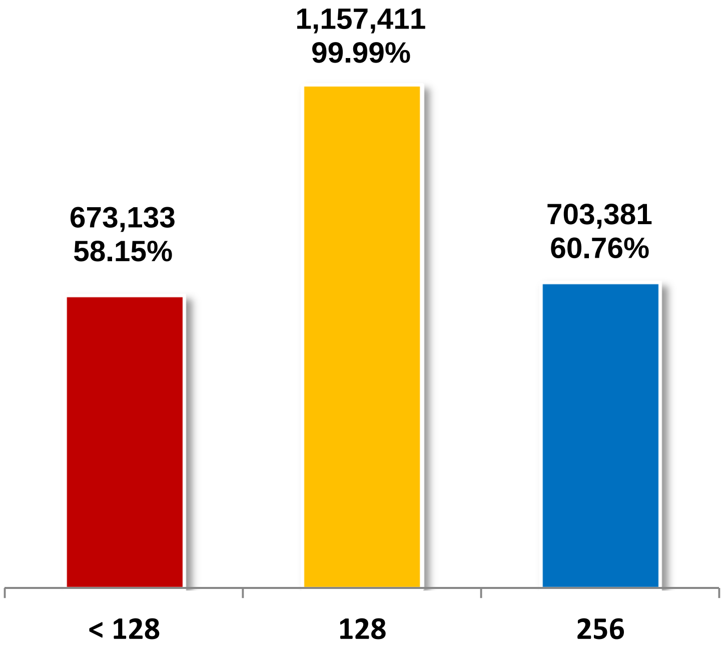
Cipher Strength

All servers support **strong** and most support **very strong** ciphers

- But there is also wide support for weak ciphers



Best cipher strength support



Cipher strength support

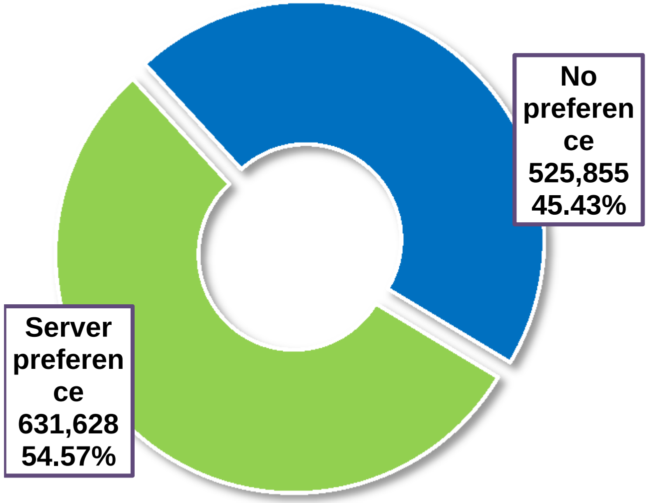
Cipher Suite Support

Most supported cipher suites

Cipher suites	Servers	%
TLS_RSA_WITH_3DES_EDE_CBC_SHA	1,138,049	98.32%
TLS_RSA_WITH_RC4_128_SHA	1,118,532	96.63%
TLS_RSA_WITH_RC4_128_MD5	1,100,319	95.06%
TLS_RSA_WITH_AES_128_CBC_SHA	712,060	61.51%
TLS_RSA_WITH_AES_256_CBC_SHA	702,009	60.64%
TLS_RSA_WITH_DES_CBC_SHA	662,702	57.25%

Most preferred cipher suites

Cipher suite
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA
TLS_RSA_EXPORT1024_WITH_RC4_56_SHA
TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA



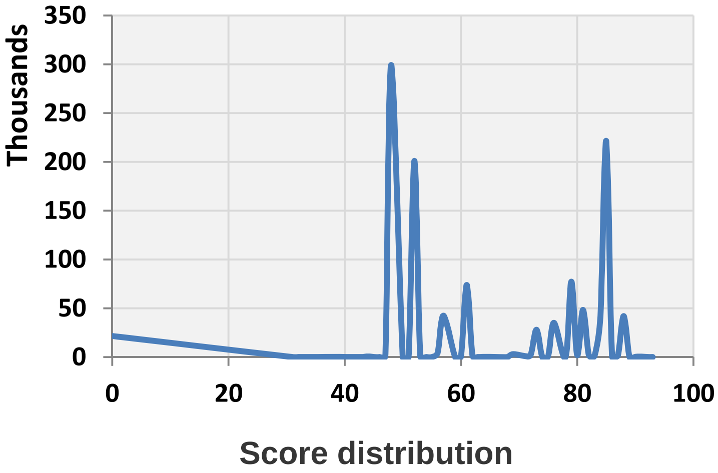
Cipher suite server preference

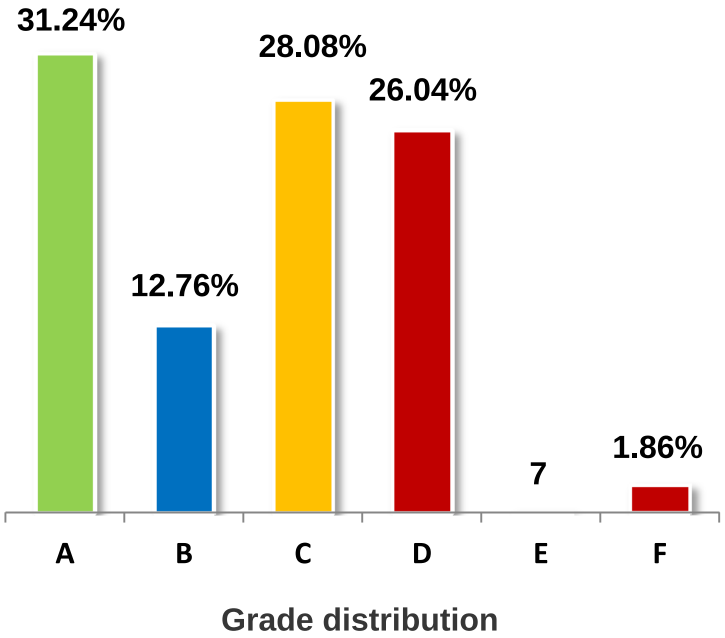
SSL Labs Grade Distribution

Most servers not configured well

- Only 31.24% got an A
- 68.76% got a B or worse
- Most probably just use the default settings of their web server

Key length	Score
A	>= 80
B	>= 65
C	>= 50
D	>= 35
E	>= 20
F	< 20





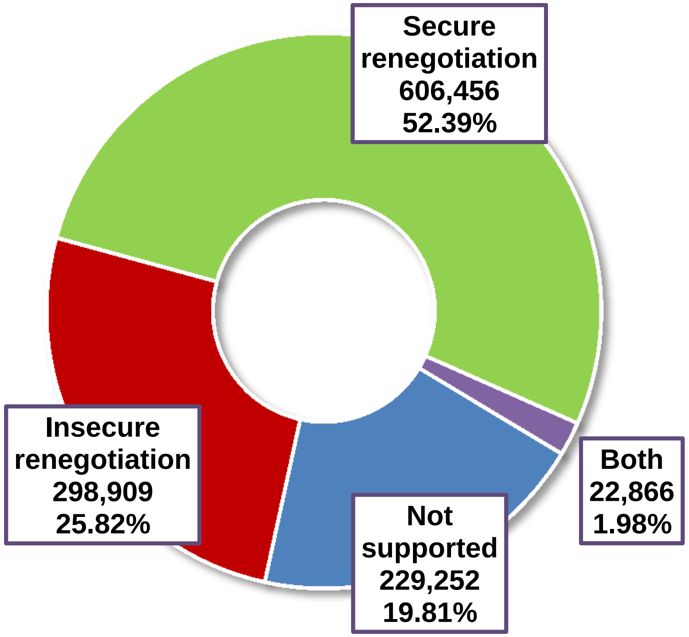
Strict Transport Security (STS)

Only **162** trusted sites seem to support HTTP Strict Transport Security (HSTS)

- Compared to 12 last year
- STS allows sites to say that they do not want plain-text traffic
- Just send a *Strict-Transport-Security* response header from the SSL portion of the site
- Supported in Chrome, NoScript, and Firefox 4
- HTTP Strict Transport Security (HSTS) http://tools.ietf.org/html/draft-hodges-strict-transport-sec

12 early adopters from 2010
secure.grepular.com
secure.informaction.com
www.acdet.com
www.datamerica.com
www.defcon.org
www.elanex.biz
www.feistyduck.com
www.paypal.com
www.squareup.com
www.ssllabs.com
www.strongspace.com
www.voipscanner.com

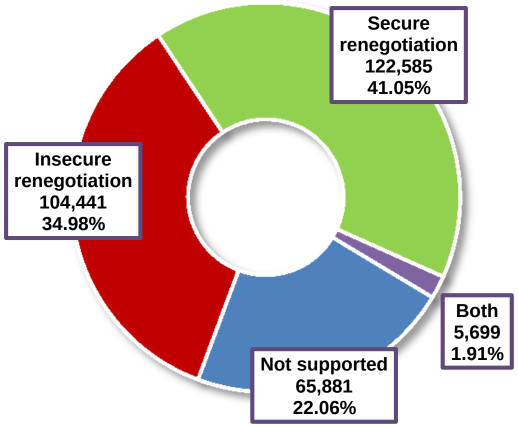
Secure and Insecure Renegotiation



Support for secure and insecure client-initiated renegotiation

Insecure renegotiation is the closest thing to a serious TLS protocol flaw so far:

- Published in November 2009
- RFC 5746: Transport Layer Security (TLS) Renegotiation Indication Extension published in February 2010
- Last major vendor patched in January 2011
- On a sample of 300,000 top 1m sites:



Part V:

What Next?

Conclusions

Good:

- Virtually all deployments have strong key size, support strong protocols and strong ciphers

Bad:

- Bad configuration on almost 70% of all servers
  - Most probably just use default settings
  - SSLv2 still widely supported!
- **Lack of support for TLS v1.1 and v1.2 is a cause for concern**
- It takes a serious vulnerability for things to start improving (and then only slowly) – **25%-35% servers still support insecure renegotiation**
- **Too many organizations involved in the trust ecosystem**

Major Challenges Today

1. Fragility of the trust ecosystem
2. Bad SSL configuration is common
3. Slow adoption of modern standards
4. Lack of support for virtual SSL hosting
5. Mismatch between HTTP and SSL
6. Performance and caching challenges

Future Work

Current status:

- There is no need to perform full surveys more than once a year
- We may perform partial scanning for certain aspects, for example support for insecure renegotiation
- We may also expand into other protocols (e.g., SMTP)

There are certain issues pure SSL scanning is unable to detect, and for those we are building another assessment tool. These issues are:

- Insecure cookies
- Same-page mixed content
- Sites that mix HTTP and HTTPS

First results will be released in late May.

Future of SSL

Situation at present:

- So far, most are choosing barely-acceptable security
- The only way to achieve real security is by encrypting all traffic
- We are going there slowly; now in a transition phase

It’s not going to be easy:

- Shock is pretty much the only mechanism to force change
- We do have a strong core security community
- DNSSEC may help fix some aspects of trust

Google is a significant force in this area:

- Has a browser and enough infrastructure to make a difference on the server side
- Sponsors protocol improvements to increase performance
- SPDY is not only faster, but also always encrypted

Q & A

Thank You

Ivan Ristic
iristic@qualys.com
@ivanristic

VM PC PCI WAS MAL

QUALYS®