QUALYS®

Internet SSL Survey 2010

Black Hat USA 2010

Ivan Ristic
Director of Engineering,
Web Application Firewall and SSL
iristic@qualys.com / @ivanristic

July 19th, 2010 (v1.0)

ON DEMAND SECURITY

Agenda

1. **Why do we care about SSL?**
2. **Our SSL assessment engine**
3. **How does one find SSL-enabled servers to study?**
4. **Findings of our large-scale study of SSL servers on the Internet**
5. **Conclusions and future direction**

QUALYS®

Internet SSL Survey 2010

Part I

Why do we care about SSL?

ON DEMAND SECURITY

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**

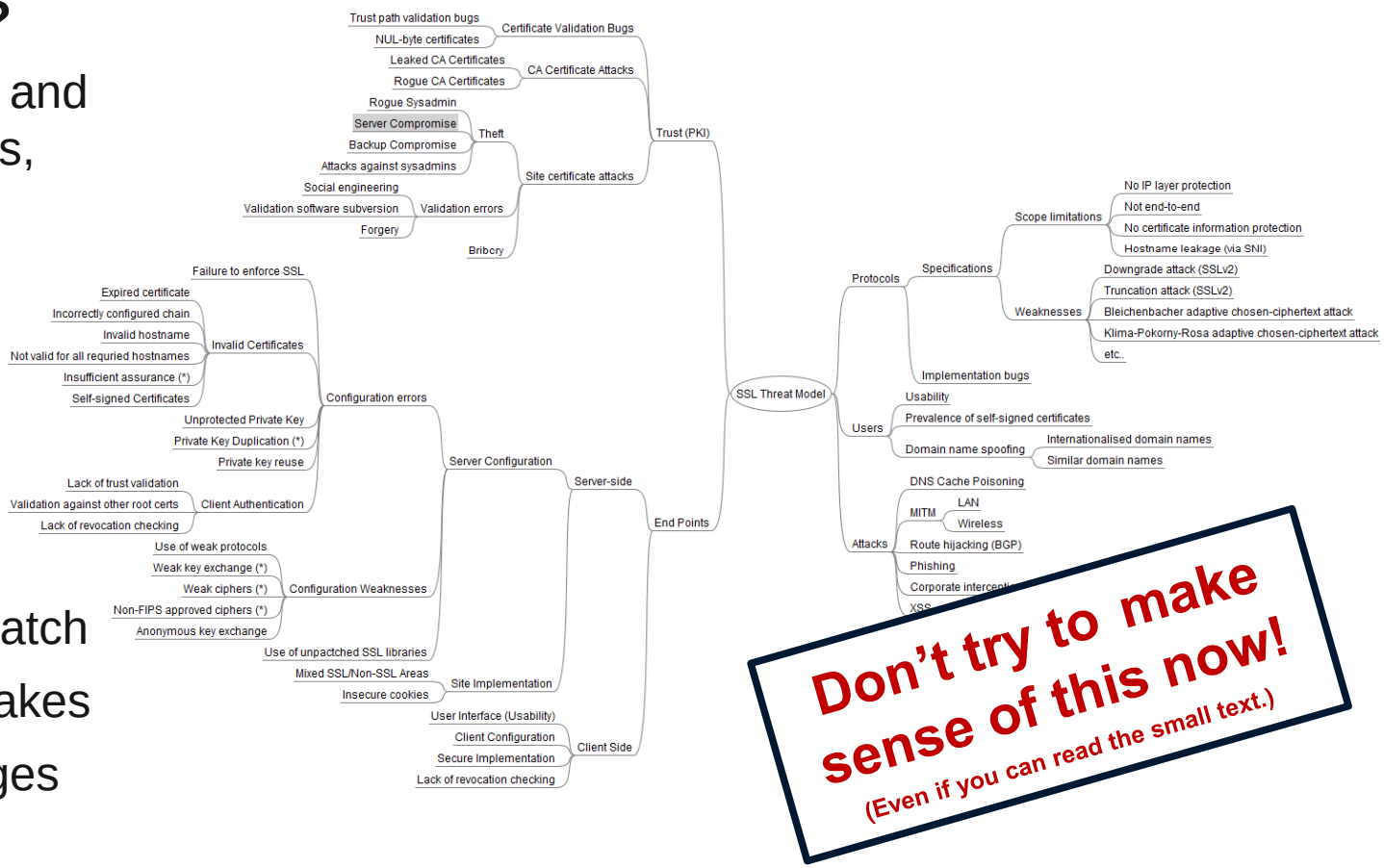
SSL ~~Threat~~ Fail Model

How can SSL fail?

- In about a million and one different ways, actually.

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

SSL Rating Guide (Not)

And what is NOT the purpose of the guide?

- The scores are not supposed to be a perfect representation of configuration “quality”
- We don’t know what “secure” means to you
- Besides, security has many enemies:
  - *Cost*
  - *Performance*
  - *Interoperability*

QUALYS®

Internet SSL Survey 2010

Part II

SSL Assessment Engine

ON DEMAND SECURITY

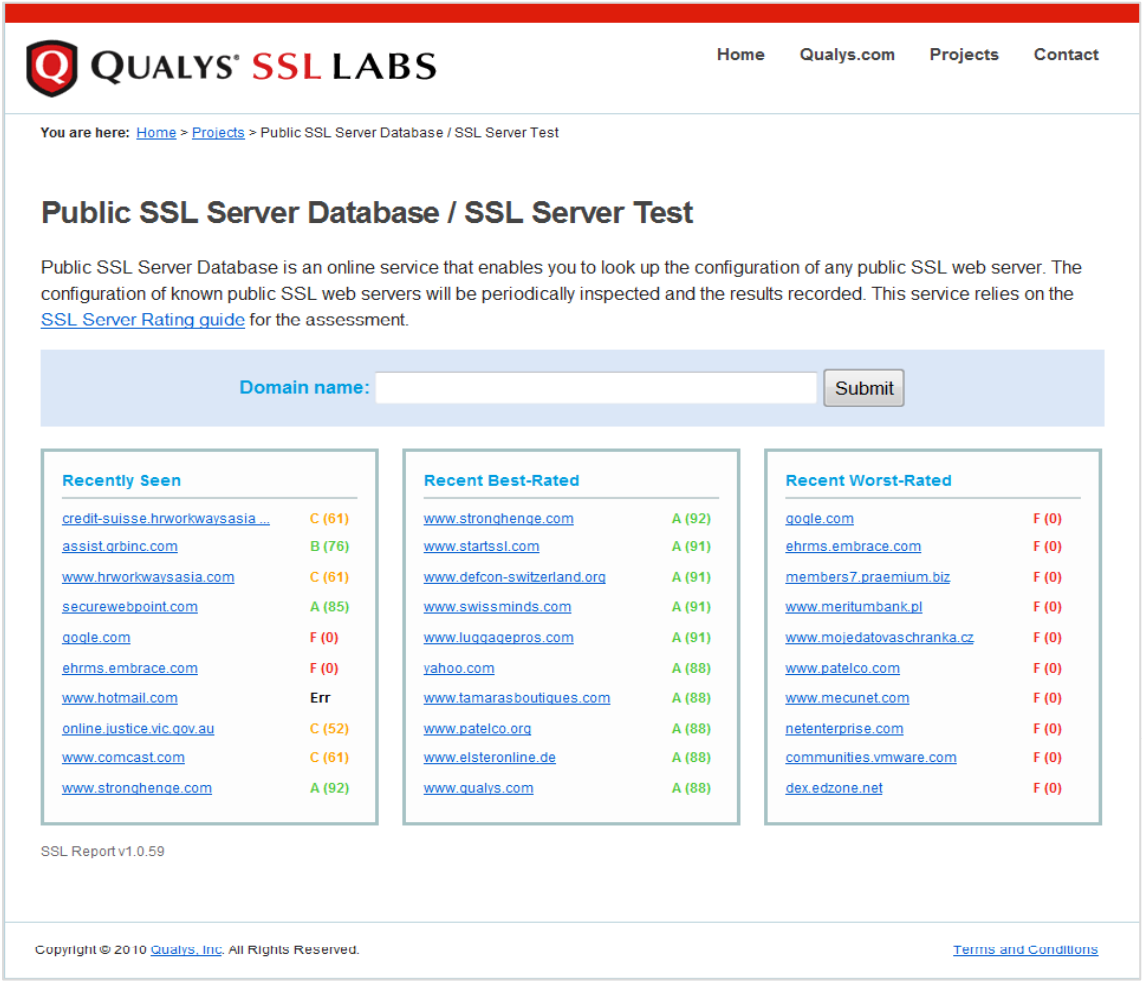
Online SSL assessment overview

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



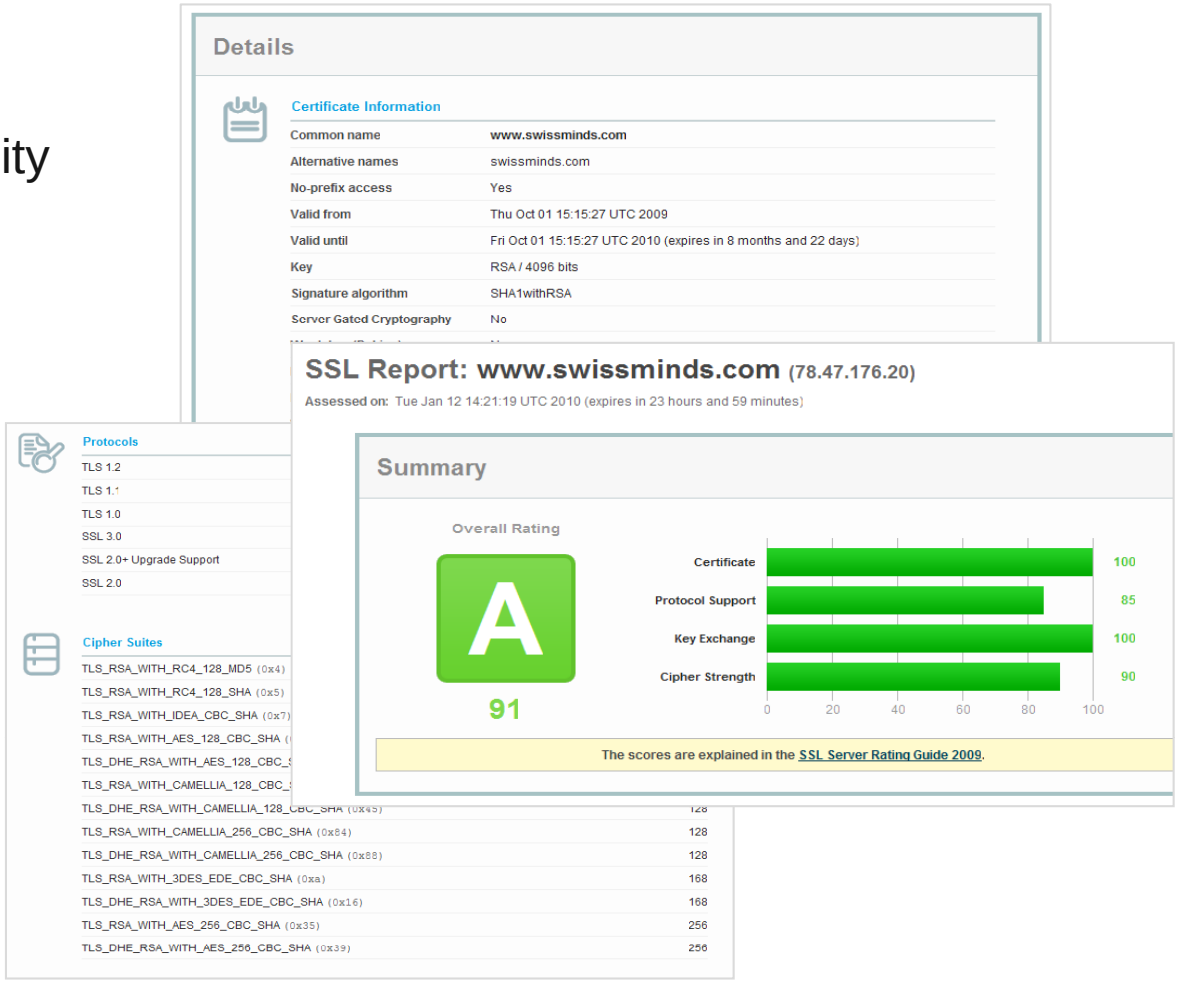
SSL assessment details

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



Assessment Challenges

Comprehensive assessments are difficult:

- A naïve approach is to open a connection per cipher suite. *But it doesn't scale.*
- We went to packet level, using partial connections (*with as little crypto as possible*) to extract the information we needed. **Almost no CPU used!**
- **Not reliable with multiple servers behind one IP address**

Other issues:

- **Complicated topic** – so many RFCs and other documents to read before you can begin to grasp the problem. *It took us ages to just assemble the list of known cipher suites.*
- **Poor programming documentation**; SSL toolkits generally designed to connect (or not), but not for diagnostics.
- **Feature coverage** – toolkits cover only a part of what the protocols can do.
- **Bugs, edge cases, and interoperability issues**.

QUALYS®

Internet SSL Survey 2010

Part III

Finding Servers to Scan

ON DEMAND SECURITY

Finding servers to assess

We have the assessment engine sizzling, but how do we find servers to assess?

- Scan all IPv4 space
- Crawl the Internet
- Start with domain registrations
- Use a browser toolbar
- Wait for SSL Labs to become popular, recording all site names in the meantime

Are we looking for domain names, servers, or certificates?

- TLS SNI allows multiple certificates per IP address
- One domain name may have many servers / IP addresses
- There may be many servers behind one IP address
- The same certificate (esp. a wildcard one) can be used with many servers

Our approach: domain enumeration

How many domain names and certificates are there?

- 193M domain name registrations in total (VeriSign)
- 207M sites (Netcraft)
- 1.2M valid SSL certificates (Netcraft)

Main data set: domain name registrations

- All .com, .net, .org, .biz, .us, and .info domain names
- 119M domain names (57% of the total)

Bonus data sets:

- Alexa's top 1m popular sites
- Collect the names in the certificates we find

First pass: lightweight scan

The purpose of the first-pass lightweight scan is to locate the servers we need to examine in depth:

- Those are servers with certificates whose names match the domain names on which they reside.
- Someone made an effort to match the names, therefore the intent is there!

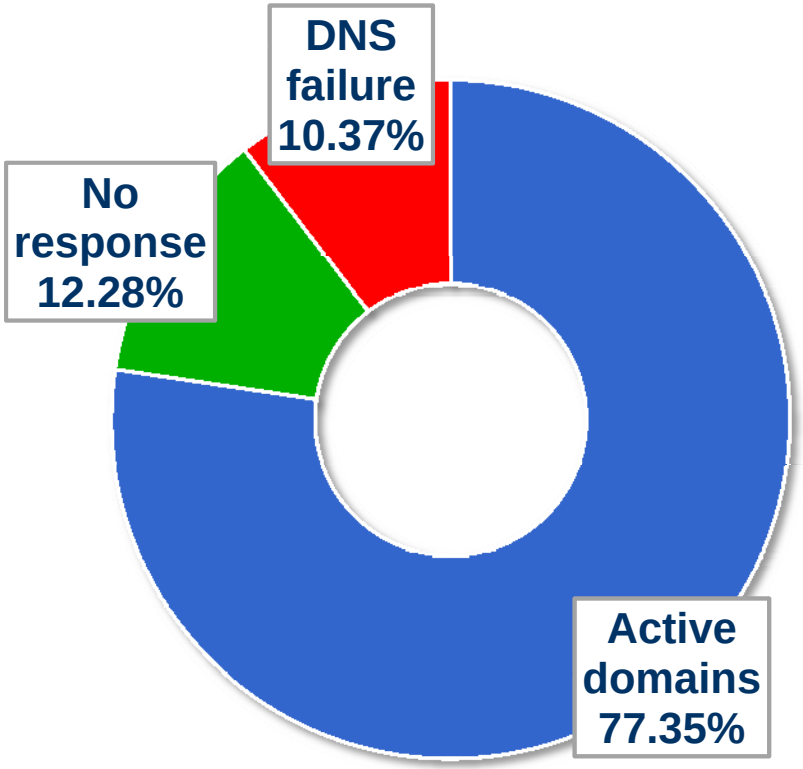
How did we do that?

- Single server with 4 GB RAM (not a particularly powerful one)
- DNS resolution + few packets to probe ports 80 and 443 ***//*** **Yes, HTTP servers only**
- Naturally, incomplete SSL handshakes
- 2,000 concurrent threads
- Resulted in roughly 1,000 probes per second; fast enough
- **A day and a half for the entire scan**

Active domain names

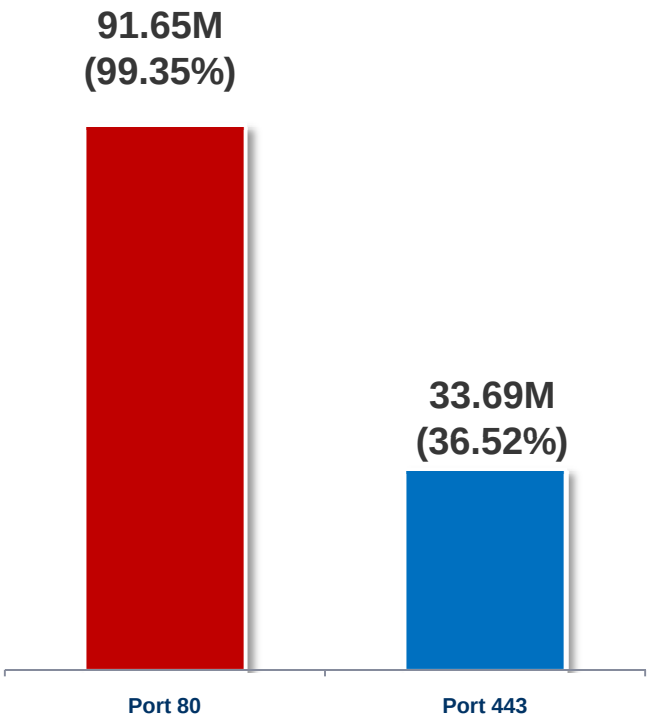
Out of 119m domain names:

- 12.4M (10.37%) failed to resolve
- 14.6M (12.28%) failed to respond
- 92M (77.35%) seemed active

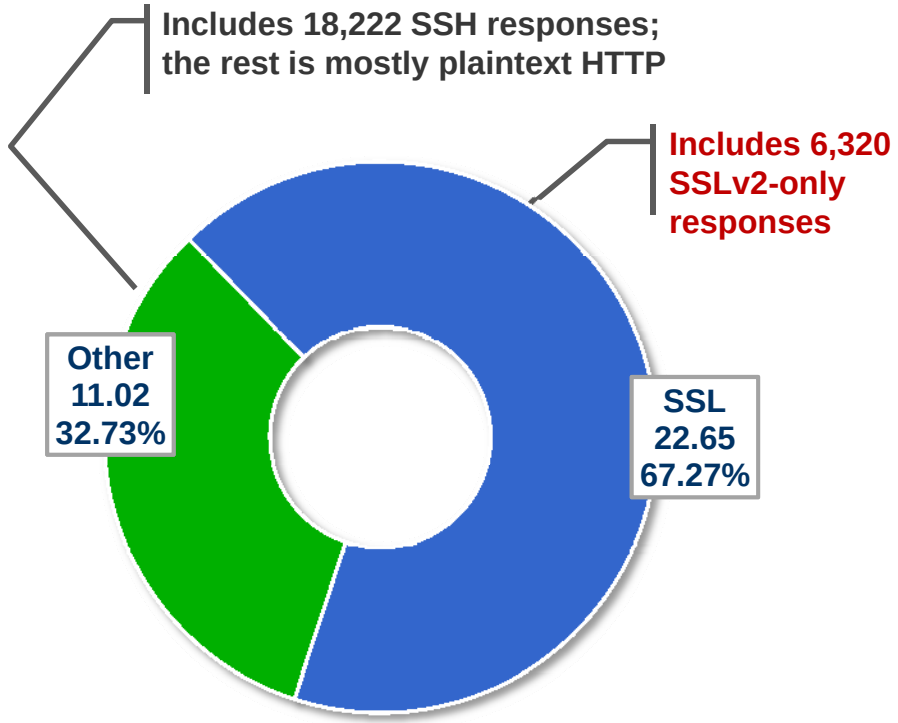


Active means to respond on port 80 or port 443

Port 80 and 443 activity analysis

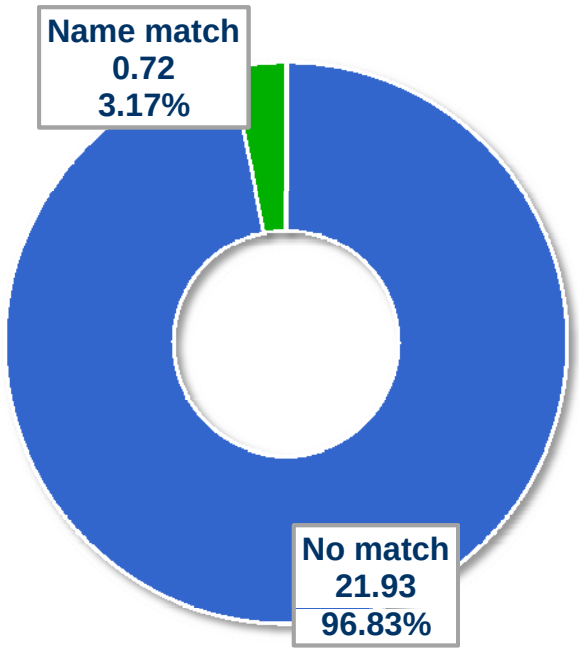


Domain responses on ports 80 and 443

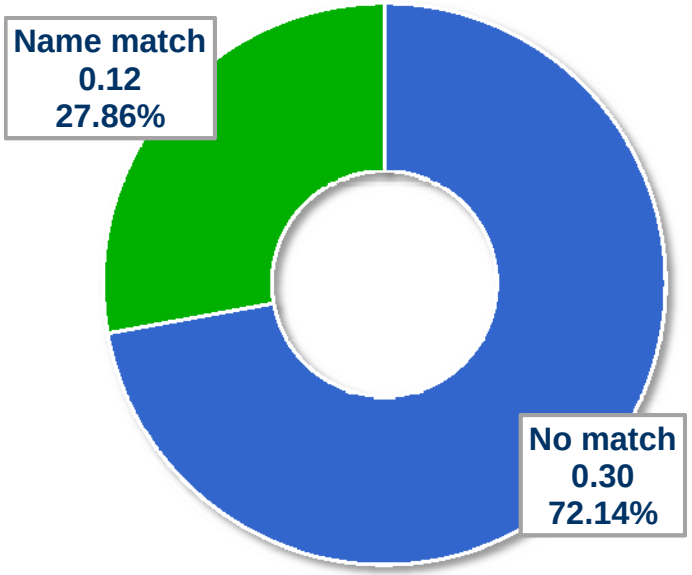


Protocols on port 443 (in millions)

~720,000 potentially valid SSL certificates

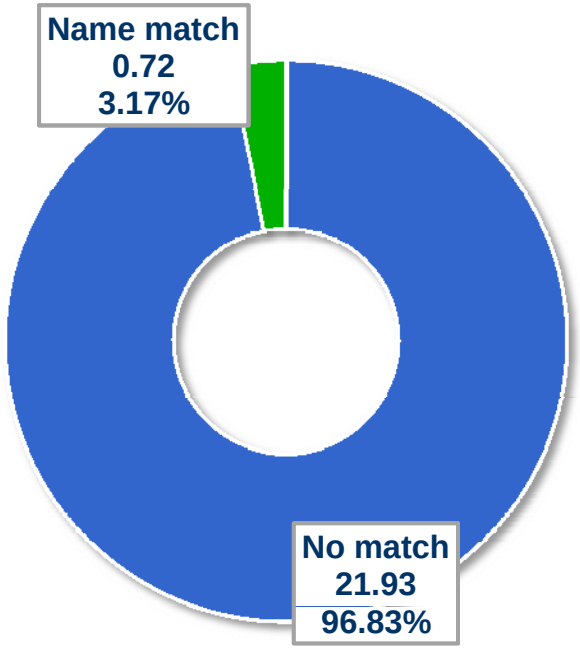


Out of 22.65M domain names with SSL enabled



Alexa's Top 1M domain names

22m invalid certificates! Really!?



Out of 22.65M domain names with SSL enabled

Why so many invalid responses?

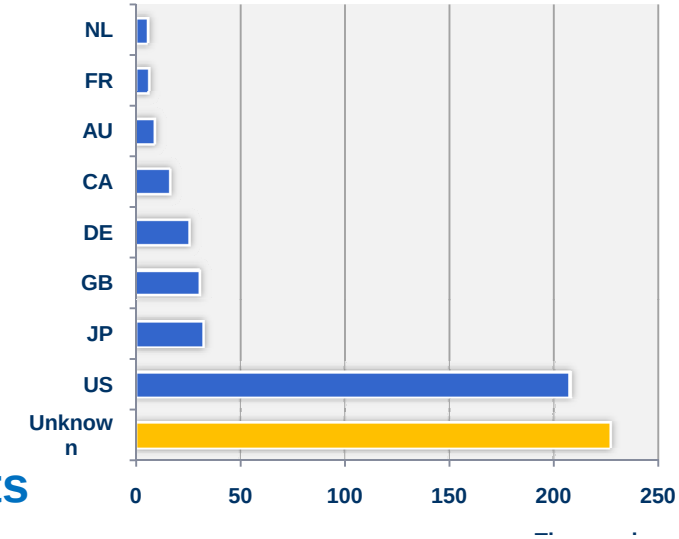
- Virtual web hosting hugely popular
  - 119m domain names represented by about 5.3m IP addresses
  - 22.65m domain names with SSL represented by about 2m IP addresses
- Virtual SSL web hosting practically impossible – the majority of browsers do not support the TLS SNI extension.

We don't know if a site uses SSL, and end up seeing something else because most don't

The end result…

Let's now try to get as many entries as possible

- Add all we have together:
  - 720,000 certificates from the domain name registration data set
  - 120,000 certificates from the Top 1m data set
  - About new 100,000 domains found in certificate names
- Remove duplicates:
  - Unique IP address
  - Unique domain name
  - Unique certificate
- **We ended up with 867,361 entries**
- **Probably 25-50% of all commercial certs**



QUALYS®

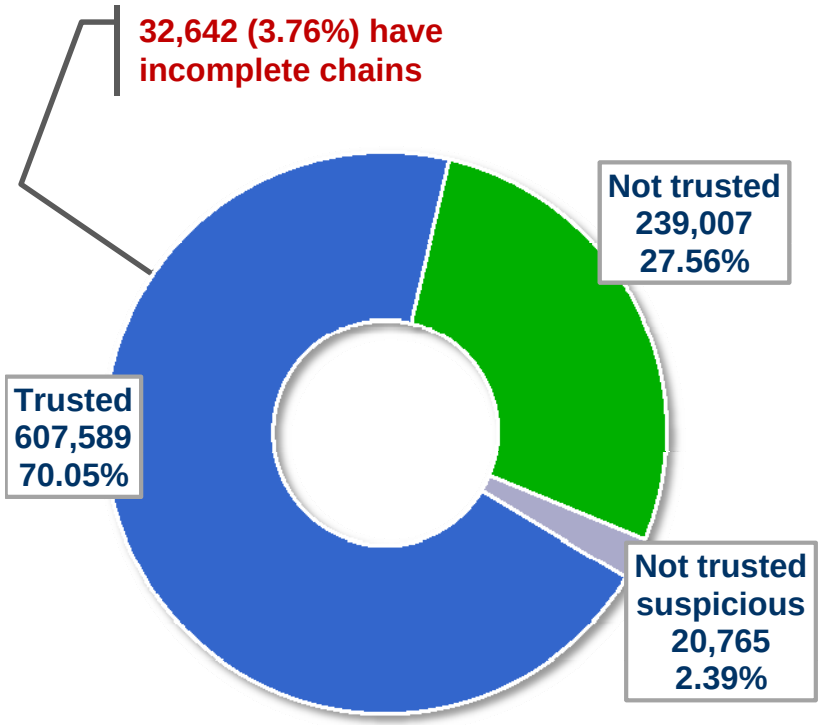
Internet SSL Survey 2010

Part IV

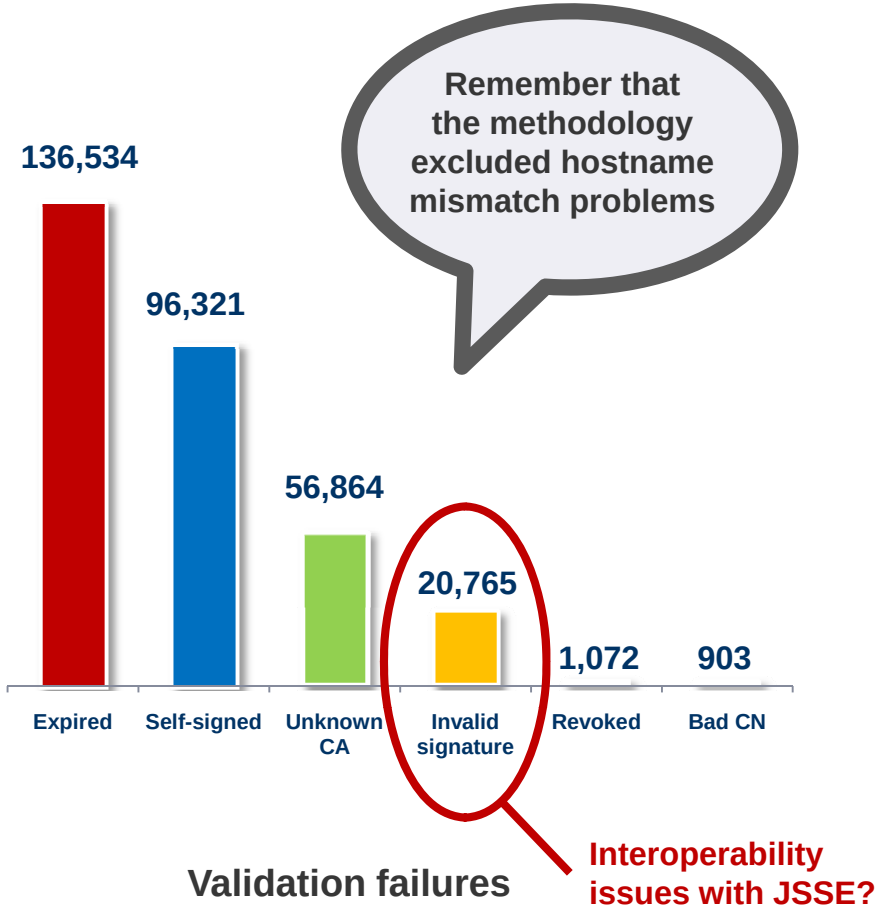
Survey Results

ON DEMAND SECURITY

How many certs failed validation and why?

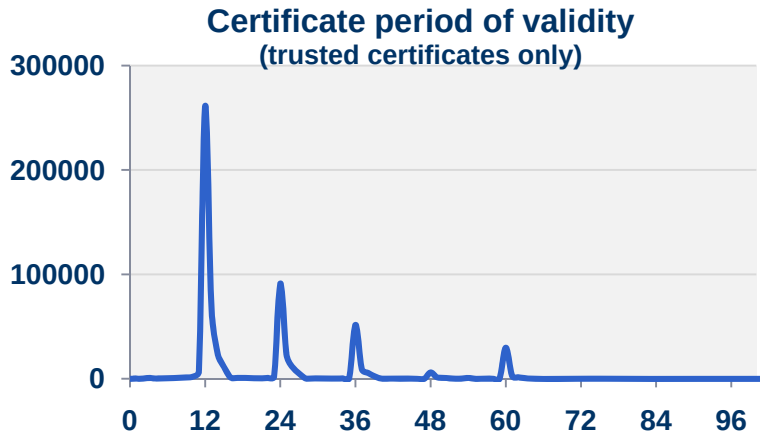


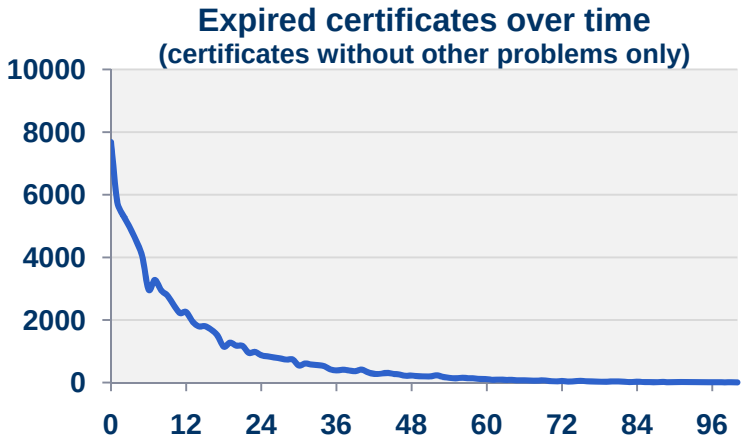
Trusted versus untrusted certificates

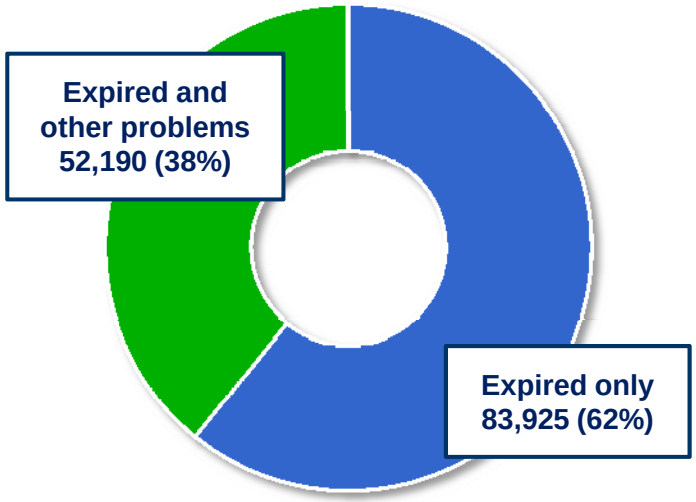


Validation failures

Certificate validity and expiry distribution







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

Unknown issuers

We saw 56,864 unknown issuers

- Great majority of issuers seen only once
- 22 seen in more than 100 certificates
- Manually verified those 22
- Found 4 that one could argue are legitimate, but are not trusted by Mozilla (yet) (http://www.mozilla.org/projects/security/certs/pending/)

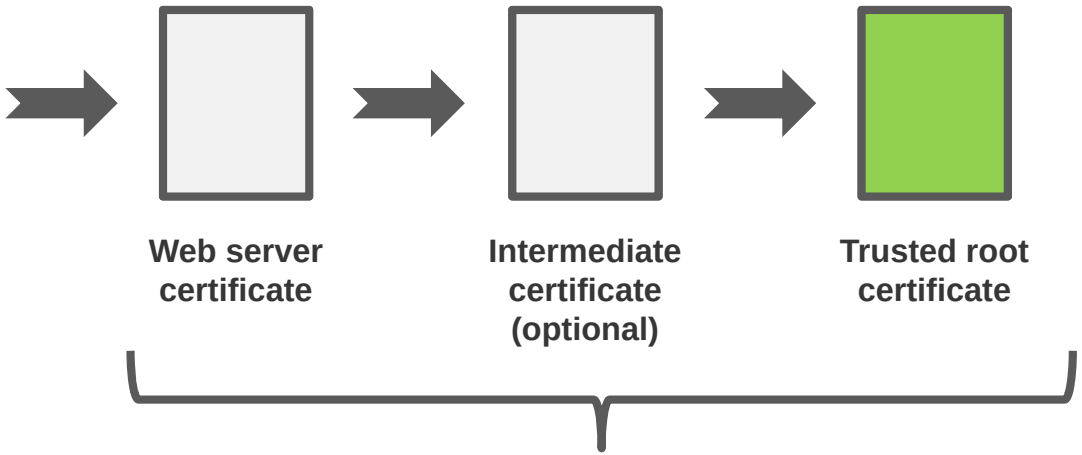
Issuer	Seen certificates
Firstserver Encryption Services	9486
CAcert	6117
ipsCA	462
KISA Root CA	162

Trusted in other major browsers

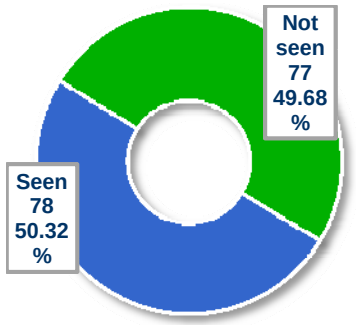
Trusted issuers and chain length

We saw 429 ultimately-trusted certificate issuers

- They led to **78 trust anchors**
- That's **only 50% of our trust base**, which has 155 trust anchors



This path is **2** levels deep in **44%** of cases, and **3** levels deep in **55%** of cases.

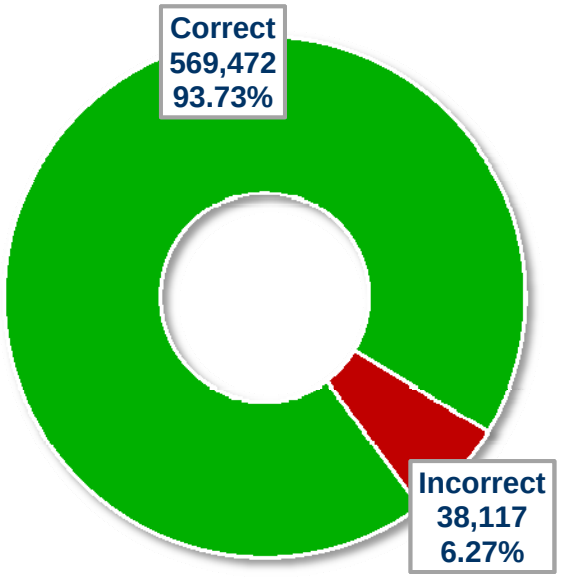


155 trusted CA certificates (from Firefox 3.6.0)

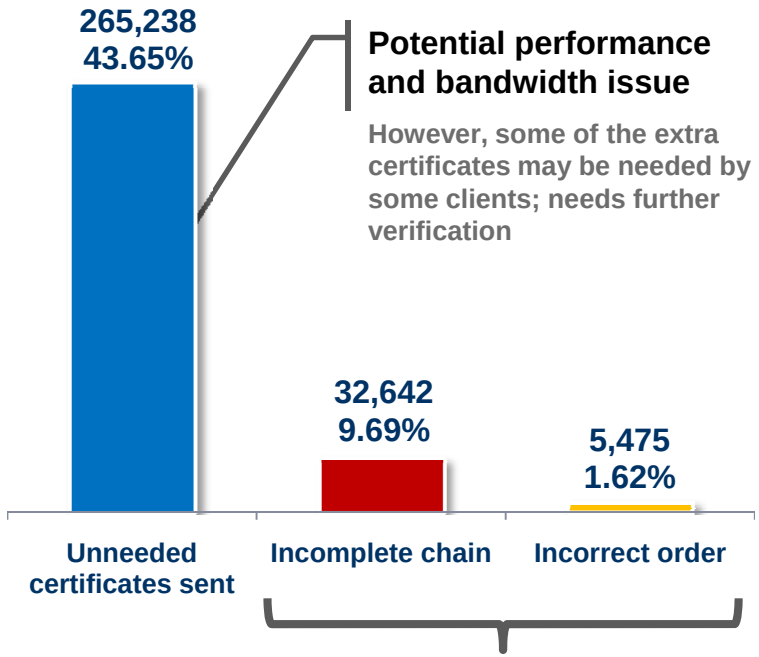
Chain length	Certificates seen
2	270,779
3	334,248
4	2368
5	186
6	8

Recommended length

Certificate chain correctness



Correct versus incorrect certificate chains

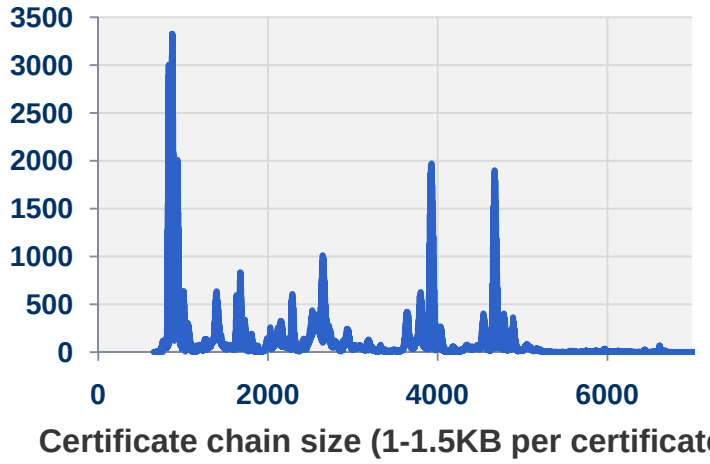


Issues with certificate chains

Certificate chain size and length

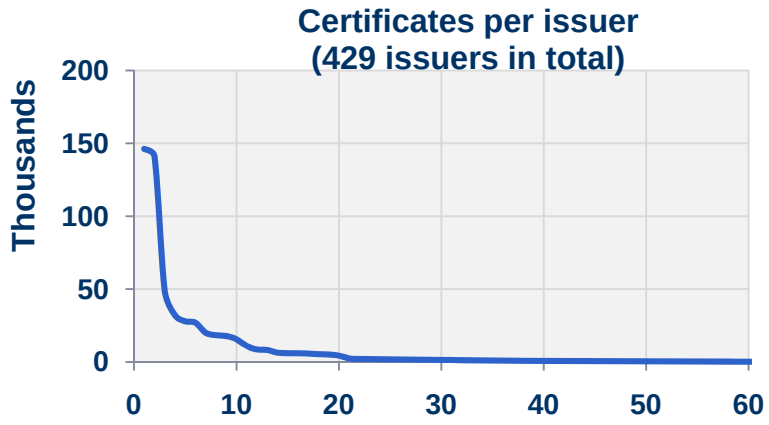
In 43.65% of all cases, there's more certificates sent than needed

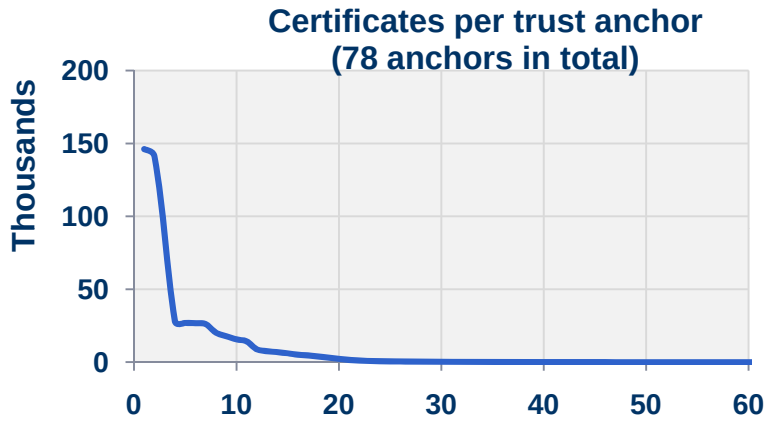
- When latency between client and server is high, the unneeded certificates waste the precious initial bandwidth
- Important when you need to want the performance to be as good as possible



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

Trust anchors





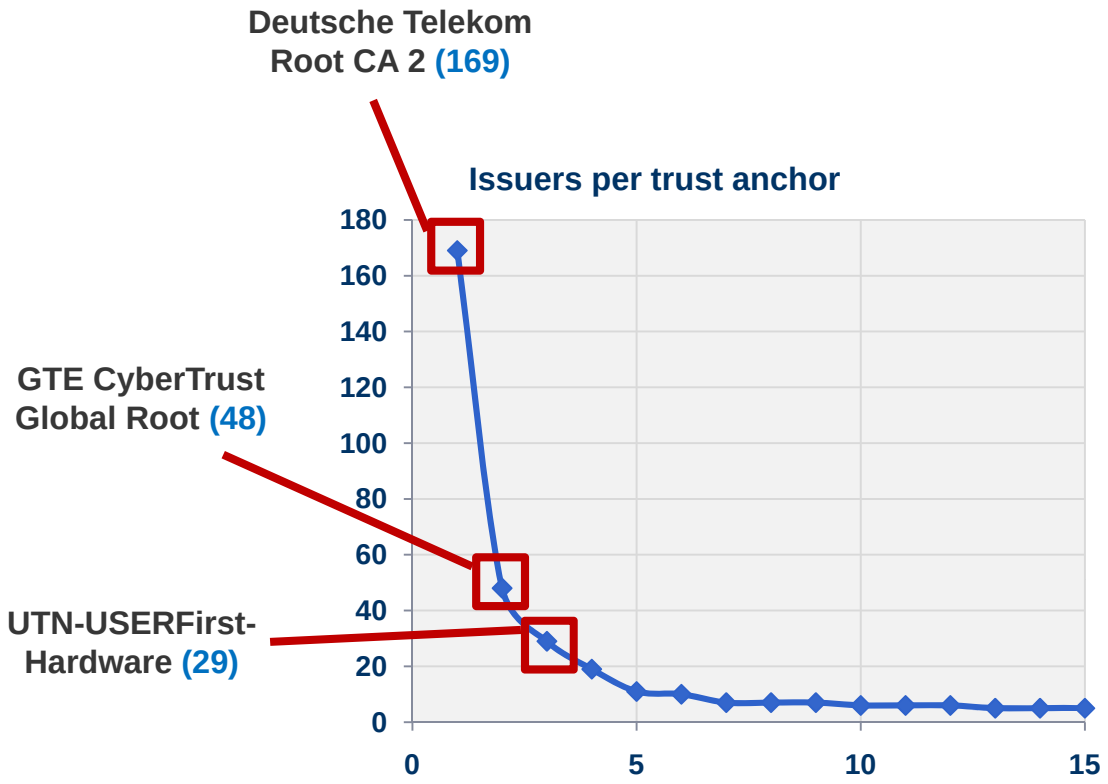
Trust Anchor	Certificates
Go Daddy Class 2 Certification Authority	146,173
Equifax Secure Certificate Authority	141,210
UTN-USERFirst-Hardware	86,868
Thawte Premium Server CA	27,976
Thawte Server CA	26,972
Class 3 Public Primary Certification Authority	26,765
VeriSign Trust Network	26,163
GlobalSign Root CA	20,290
Starfield Class 2 Certification Authority	17,824
Equifax Secure Global eBusiness CA-1	15,662
COMODO Certification Authority	14,296
SecureTrust CA	8,793
VeriSign Class 3 Public Primary Certification Authority - G5	7,619
DigiCert High Assurance EV Root CA	6,769
StartCom Certification Authority	6,197
Entrust.net Secure Server Certification Authority	5,068
GTE CyberTrust Global Root	4,659

17 trust anchors on this page account for 589,304 (97%) certificates

Trust anchors and trust delegation

On average, there will be 5.5 issuers for every trust anchor.

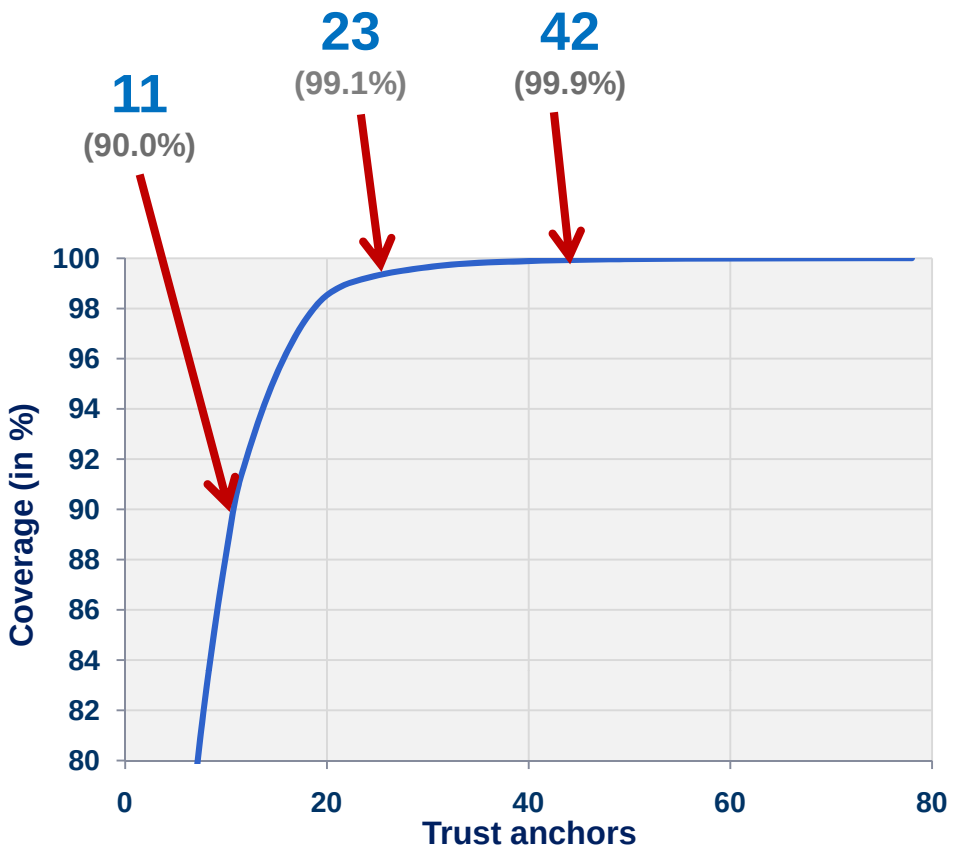
- Top 6 anchors have more than 10 issuers each
- They account for a total of 286 issuers, or 67% of all
- Deutsche Telekom alone accounts for 39% of all issuers we saw



How many trust anchors do we need?

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

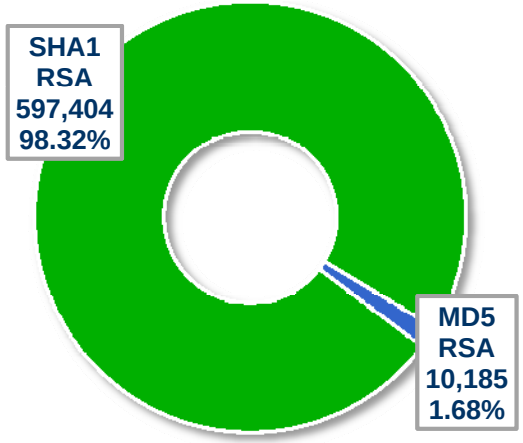
- Of course, this is **very subjective**
- Our data set is biased and contains predominantly U.S. web sites
- Your browsing habits are probably different
- **Still, it's interesting to see that you probably need only between 10 and 20 trust anchors.**
- But your selection may be different from mine!



Certificate keys and signatures

Virtually all trusted certificates use RSA keys; only 3 DSA keys

- 127 DSA keys across all certificates (i.e., including those certs we could not validate)
- SHA1 with RSA is the most popular choice for the signature algorithm
- A very small number of stronger hash functions seen across all certificates:
  - SHA256 with RSA: 190
  - SHA385 with RSA: 1
  - SHA512 with RSA: 75
- Virtually all keys 1024 or 2048 bits long
- Only 99 weak RNG keys from Debian (but 3,938 more among the untrusted)
- Only 8% servers support server-gated crypto



Signature algorithm

Key length	Certificates seen
512	3,005
1024	386,694
2048	211,155
4096	6,315
8192	14
Other	406

Support for multiple domain names

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

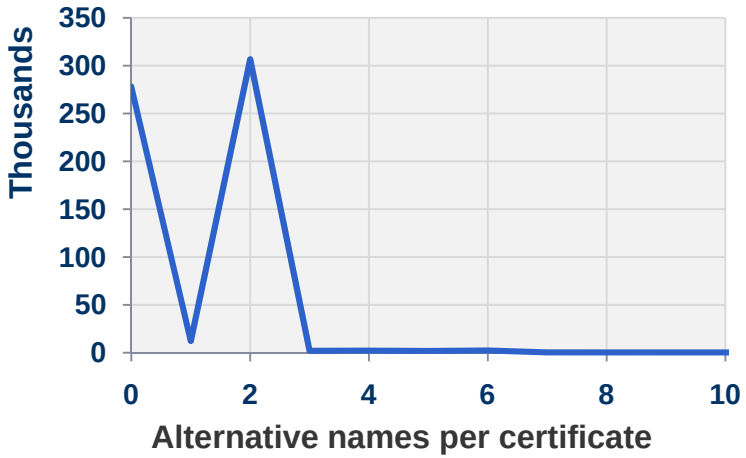
- Some CAs will automatically add 2 alternative domain names (“example.com” and www.example.com)
- Untrusted 3o.hu has 354 (8.2 KB cert)!
- Untrusted www.epi.es has 287 and they are all wildcards (7.5 KB cert)!

About 4.44% certificates use wildcards

- 2.72% as the common name
- 1.72% in the alternative name

About 35.59% certificates support access with and without the “www” part.

- 88% of the domains tested are under a TLD

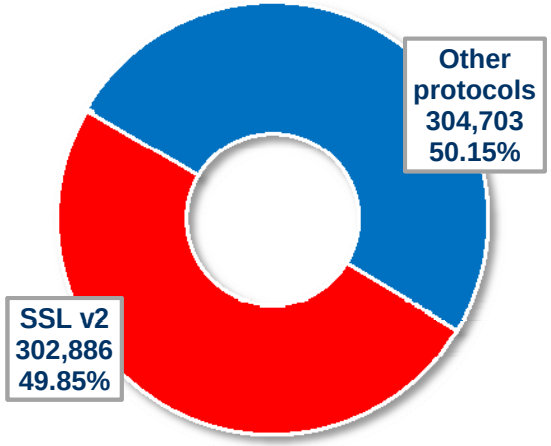


Alternative names	Name
252	www.hu-berlin.de
191	www.tu-berlin.de
153	*.abyx.com
150	www.newcreditera.com
116	edgecastcdn.net
101	jpbsecurehostingservice.com www.indiebound.org
100	quotes.usinsuranceonline.com

Protocol support

Half of all trusted servers support the insecure SSL v2 protocol

- Modern browsers won't talk 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 10,462 servers will accept SSLv2 but only deliver a user-friendly error message over HTTP



Protocol	Support	Best protocol
SSL v2.0	302,886	-
SSL v3.0	607,249	3,249
TLS v1.0	604,242	603,404
TLS v1.1	838	827
TLS v1.2	11	11

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	607,582	99.99%
DHE_RSA	348,557	57.36%
RSA_EXPORT	319,826	52.63%
RSA_EXPORT_1024	193,793	31.89%
DHE_RSA_EXPORT	176,258	29.00%

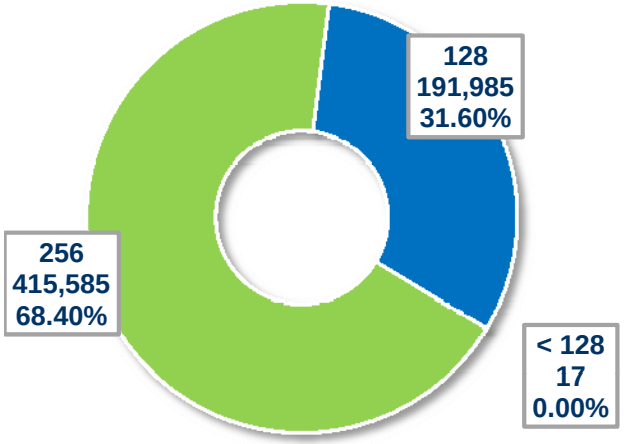
Hash	Servers	Percentage
SHA	606,489	99.81%
MD5	591,433	97.34%
SHA256	4	-
SHA384	156	-

Cipher	Servers	Percentage
3DES_EDE_CBC	603,888	99.39%
RC4_128	596,363	98.15%
AES_128_CBC	418,095	68.81%
AES_256_CBC	415,585	68.39%
DES_CBC	341,145	56.14%
RC4_40	320,689	52.78%
RC2_CBC_40	314,689	51.79%
RC2_128_CBC	283,416	46.64%
DES_CBC_40	192,558	31.69%
RC4_56	192,192	31.63%
IDEA_CBC	52,762	8.68%
RC2_CBC_56	50,897	8.37%
CAMELLIA_256_CBC	29,709	4.88%
CAMELLIA_128_CBC	29,708	4.88%
SEED_CBC	14,796	2.43%
NULL	2,185	0.35%
AES_128_GCM	2	-
AES_256_GCM	1	-
FORTEZZA_CBC	1	-

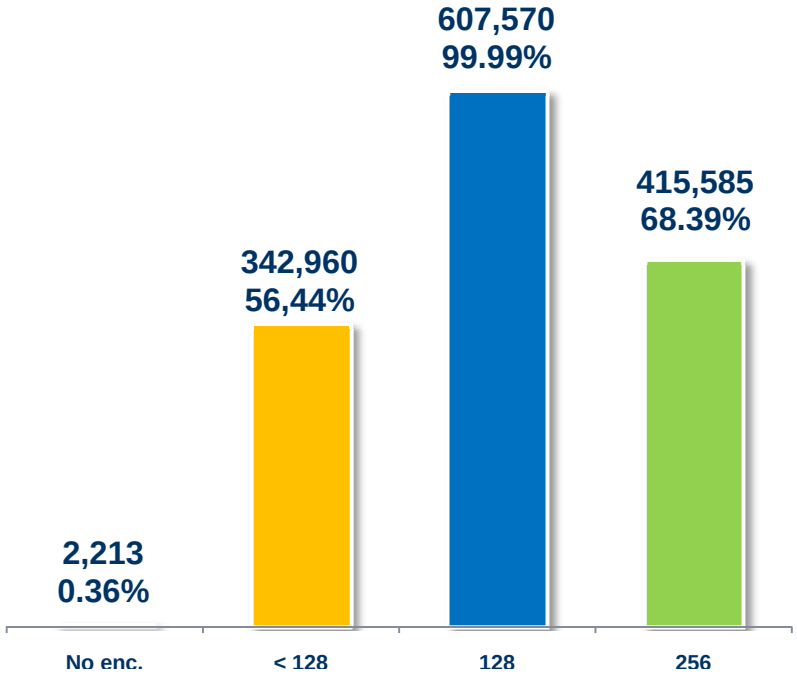
Cipher strength

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

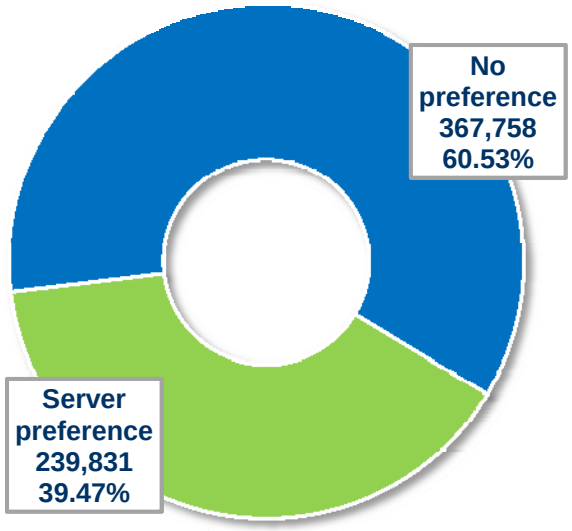
Cipher suite support

Most supported cipher suites

Cipher suites	Servers	Percentage
TLS_RSA_WITH_3DES_EDE_CBC_SHA	603,545	99.33%
TLS_RSA_WITH_RC4_128_SHA	593,884	97.74%
TLS_RSA_WITH_RC4_128_MD5	590,901	97.25%
TLS_RSA_WITH_AES_128_CBC_SHA	417,866	68.77%
TLS_RSA_WITH_AES_256_CBC_SHA	415,348	68.36%
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	347,729	57.23%

Most preferred cipher suites

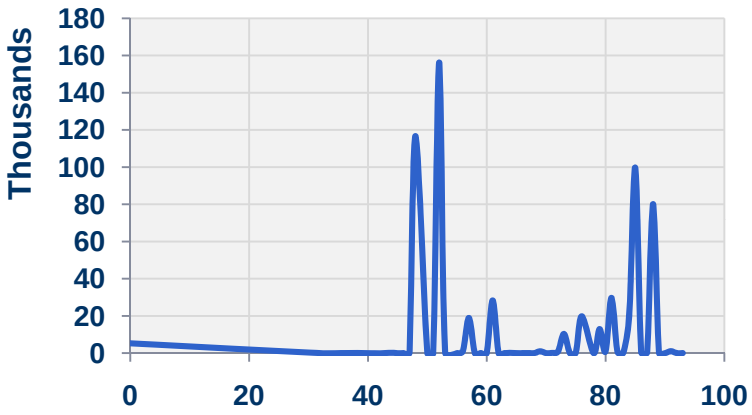
Cipher suite
TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_EXPORT1024_WITH_RC4_56_SHA
TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA

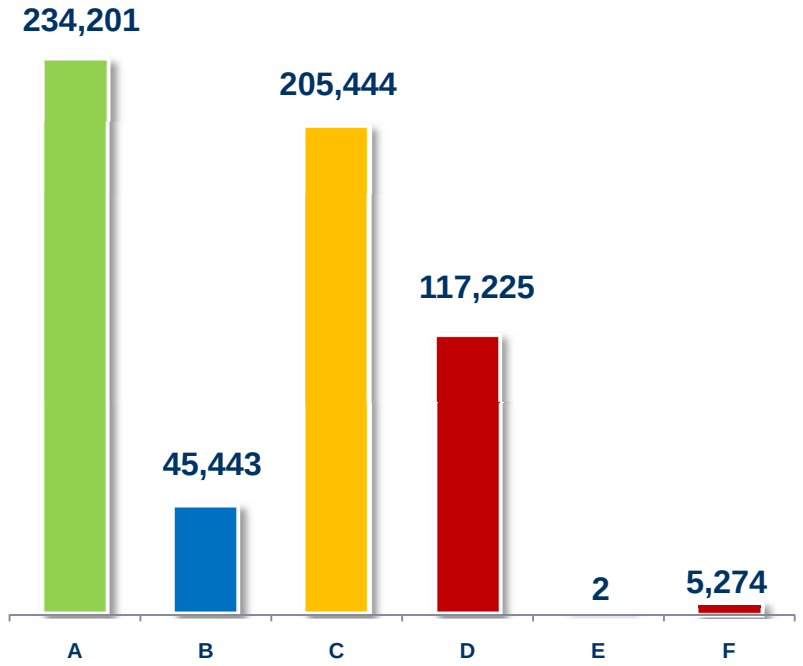


Cipher suite server preference

SSL Labs grade distribution

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





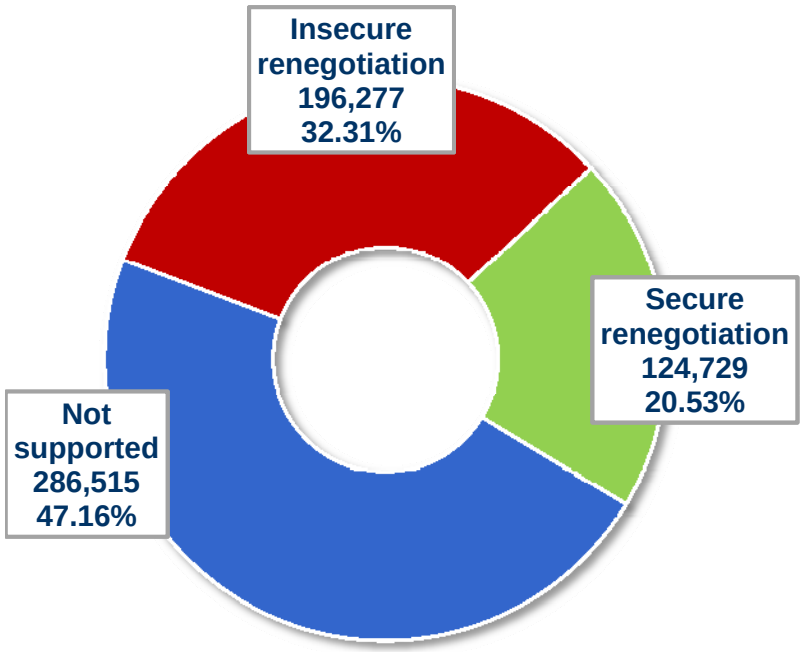
Strict Transport Security (STS)

Only 12 trusted sites seem to support Strict Transport Security (STS)

- Supported by further 3 untrusted sites
- 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 and Firefox with NoScript
- Internet draft http://tools.ietf.org/html/draft-hodges-strict-transport-sec

Sites that support STS
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 TLS protocol flaw so far

- Became public in November 2009
- Initial response was to disable renegotiation
- But not all sites can do that
- RFC 5746: Transport Layer Security (TLS) Renegotiation Indication Extension published in February 2010
- Some vendors have started to support it
- We are seeing servers patched at about 4% per month
- **There are 68 sites that support insecure and secure renegotiation at the same time**

QUALYS®

Internet SSL Survey 2010

Part V

What Next?

ON DEMAND SECURITY

Possible future improvements, part 1

Fix small assessment engine issues:

- JSSE interoperability issue
- Inability to assess SSLv2-only servers and some other edge cases

Improve process:

- Automate assessment
- Automate report generation

Assessment improvements:

- Deeper look into protocols (e.g., SNI, compression, exotic extensions)
- Deeper look into chain failures (e.g., expired intermediate certificates)
- Improve detection of error pages that are used with weak protocols and suites
- SSL server fingerprinting

Possible future improvements, part 2

Should we try to find all servers and certificates?

- It's very time consuming
- Would finding all of them substantially add to our knowledge?

Or, should we scale down and add more depth instead?

- Expand into protocols other than HTTP
- Insecure cookie usage
- Same-page mixed content
- Sites that mix HTTP and HTTPS

That’s all for today

Thank you for being here today

Do you have any questions?