

# Internet SSL Survey 2010

## Black Hat USA 2010

Ivan Ristic

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

July 29th, 2010 (v1.6)



# Agenda



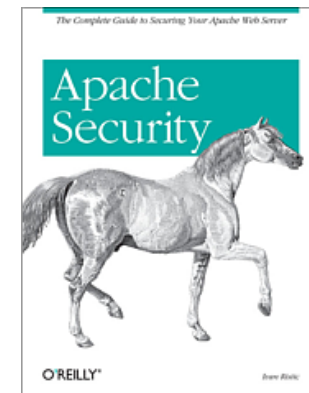
1. Why do we care about SSL?
2. SSL assessment engine overview
3. Finding SSL servers
4. Survey findings
5. Future direction

# About Ivan Ristic



Ivan is a compulsive builder who likes to take on hard problems and drill deep into them.

- Apache Security, O'Reilly (2005)
- ModSecurity, open source web application firewall
- SSL Labs, SSL, TLS, and PKI research
- LibHTTP, HTTP parsing framework
- ModSecurity Handbook, Feisty Duck (2010)



# Part I: Internet SSL Survey 2010

Why Do We Care  
About SSL?



# 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<sup>®</sup> SSL LABS

Home Qualys.com Projects Contact

## 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.

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

### 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.

# 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

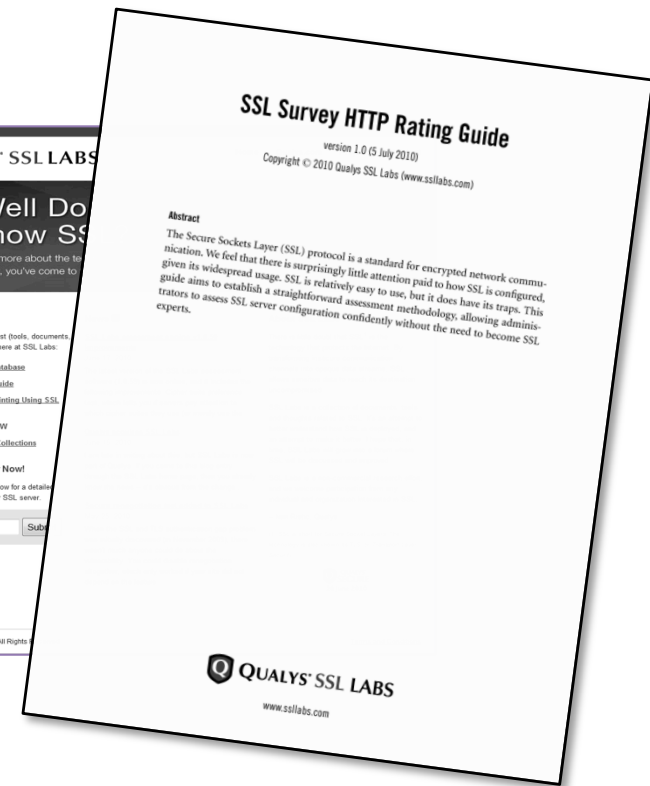
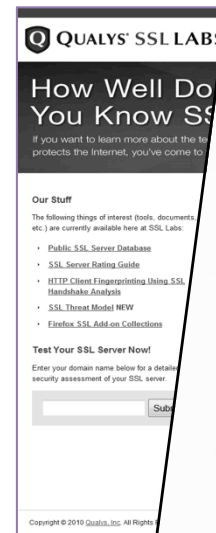


# SSL Rating Guide (Not)



And what is NOT the purpose of the guide?

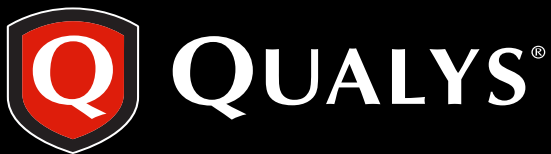
- The scores are not supposed to be a perfect representation of configuration “quality”
- We don’t know what “secure” means to you
- Besides, security has many enemies:
  - *Cost*
  - *Performance*
  - *Interoperability*





Part II: Internet SSL Survey 2010

# SSL Assessment Engine



# 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

The screenshot displays the Qualys SSL Labs website. At the top, there is a navigation bar with the Qualys logo and the text 'QUALYS SSL LABS'. To the right of the logo are links for 'Home', 'Qualys.com', 'Projects', and 'Contact'. Below the navigation bar, a breadcrumb trail reads 'You are here: Home > Projects > Public SSL Server Database / SSL Server Test'. The main heading is 'Public SSL Server Database / SSL Server Test'. A descriptive paragraph explains that the database is an online service for looking up public SSL web server configurations, which are periodically inspected. Below the text is a search form with a 'Domain name:' label, an input field, and a 'Submit' button. The page is divided into three columns: 'Recently Seen', 'Recent Best-Rated', and 'Recent Worst-Rated'. Each column contains a list of domain names with their corresponding SSL ratings. At the bottom of the page, there is a footer with the text 'SSL Report v1.0.59', 'Copyright © 2010 Qualys, Inc. All Rights Reserved.', and a link to 'Terms and Conditions'.

Recently Seen	Recent Best-Rated	Recent Worst-Rated
<a href="#">credit-suisse.hrworkwaysasia...</a> C (61)	<a href="#">www.stronghenge.com</a> A (92)	<a href="#">google.com</a> F (0)
<a href="#">assist.qrbinc.com</a> B (76)	<a href="#">www.startssl.com</a> A (91)	<a href="#">ehrms.embrace.com</a> F (0)
<a href="#">www.hrworkwaysasia.com</a> C (61)	<a href="#">www.defcon-switzerland.org</a> A (91)	<a href="#">members7.praemium.biz</a> F (0)
<a href="#">securewebpoint.com</a> A (85)	<a href="#">www.swissminds.com</a> A (91)	<a href="#">www.meritumbank.pl</a> F (0)
<a href="#">google.com</a> F (0)	<a href="#">www.luqqagepros.com</a> A (91)	<a href="#">www.mojedatovaschranka.cz</a> F (0)
<a href="#">ehrms.embrace.com</a> F (0)	<a href="#">yahoo.com</a> A (88)	<a href="#">www.patelco.com</a> F (0)
<a href="#">www.hotmail.com</a> Err	<a href="#">www.lamarasboutiques.com</a> A (88)	<a href="#">www.mecunet.com</a> F (0)
<a href="#">online.justice.vic.gov.au</a> C (52)	<a href="#">www.patelco.org</a> A (88)	<a href="#">netenterprise.com</a> F (0)
<a href="#">www.comcast.com</a> C (61)	<a href="#">www.elsteronline.de</a> A (88)	<a href="#">communities.vmware.com</a> F (0)
<a href="#">www.stronghenge.com</a> A (92)	<a href="#">www.qualys.com</a> A (88)	<a href="#">dex.edzone.net</a> F (0)

# SSL Assessment Details

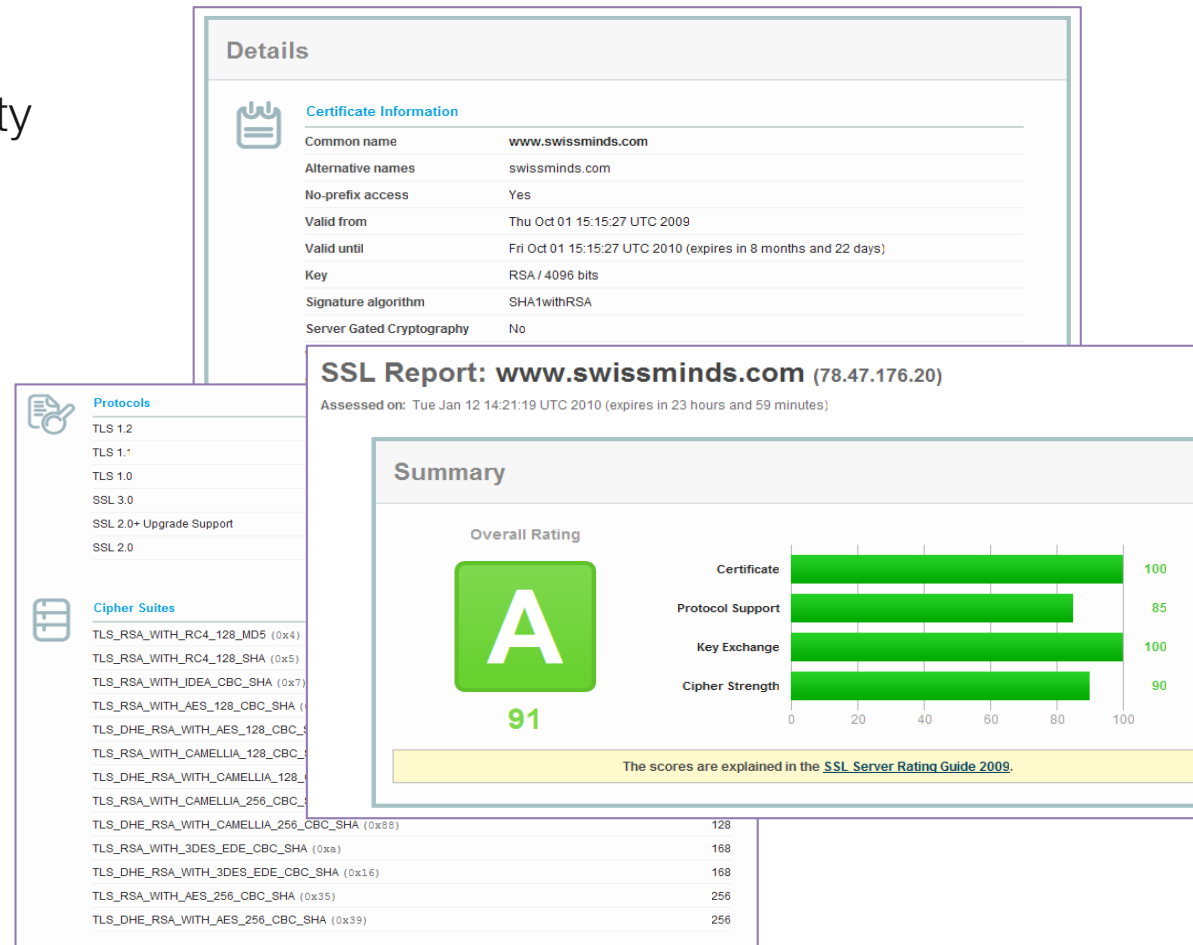


## Highlights:

- 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



# Support for Multiple Servers



## SSL Report: www.paypal.com

Assessed on: Thu Jul 22 11:03:24 UTC 2010 | [Clear cache](#)

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

# Assessment Challenges



Comprehensive assessments are difficult:

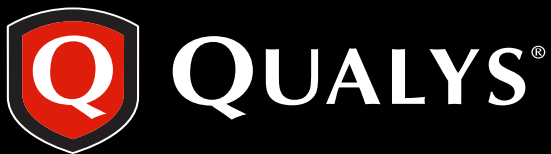
- A naïve approach is to open a connection per cipher suite. *But it doesn't scale.*
- We went to packet level, using partial connections (*with as little crypto as possible*) to extract the information we needed. **Almost no CPU used!**
- Not reliable with multiple servers behind one IP address

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.**

Part III: Internet SSL Survey 2010

# Finding SSL Servers



# 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?

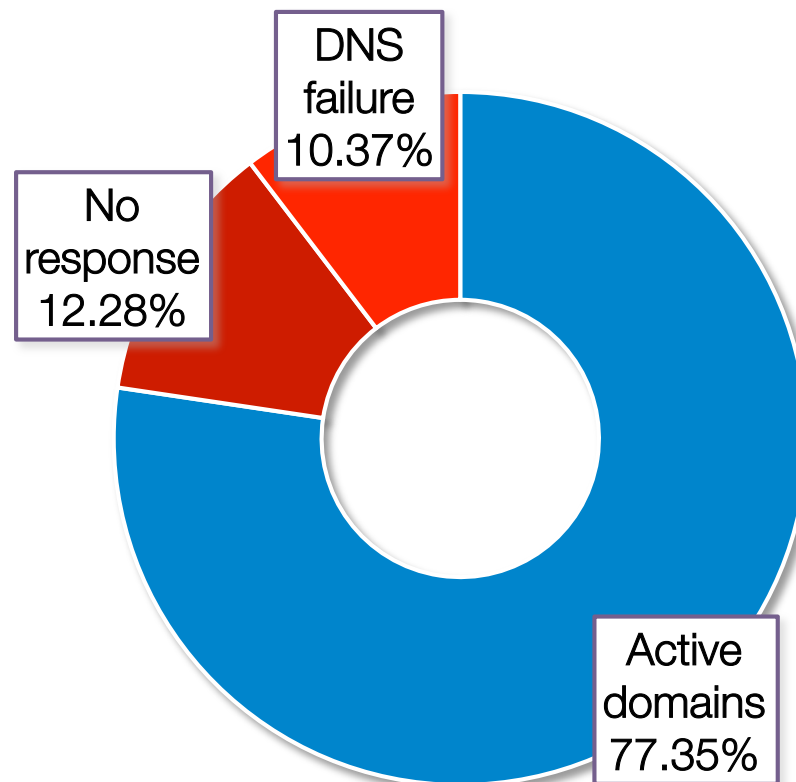
- Single server with 4 GB RAM (not a particularly powerful one)
- DNS resolution + few packets to probe ports 80 and 443 // **Yes, HTTP servers only**
- Naturally, incomplete SSL handshakes
- 2,000 concurrent threads
- Resulted in roughly 1,000 probes per second; fast enough
- **A day and a half for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

# Active Domain Names



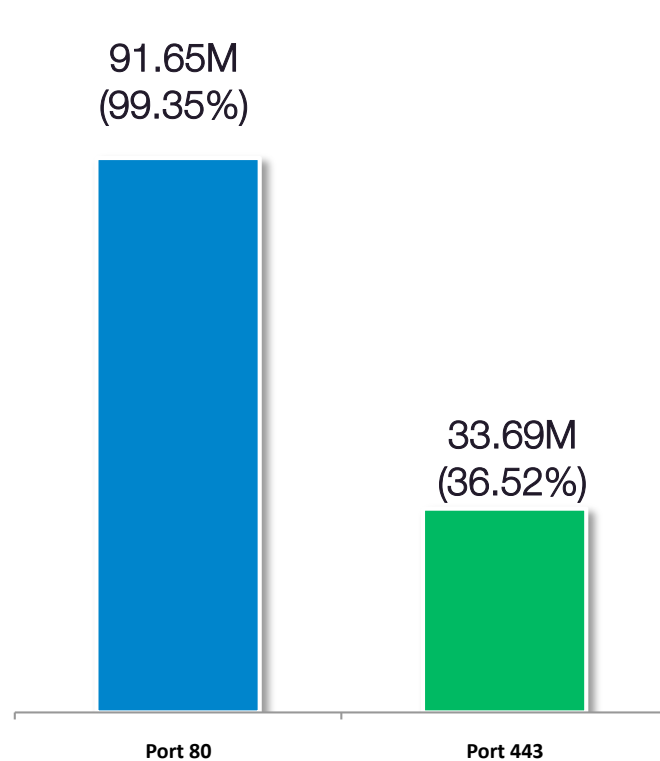
Out of 119m domain names:

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

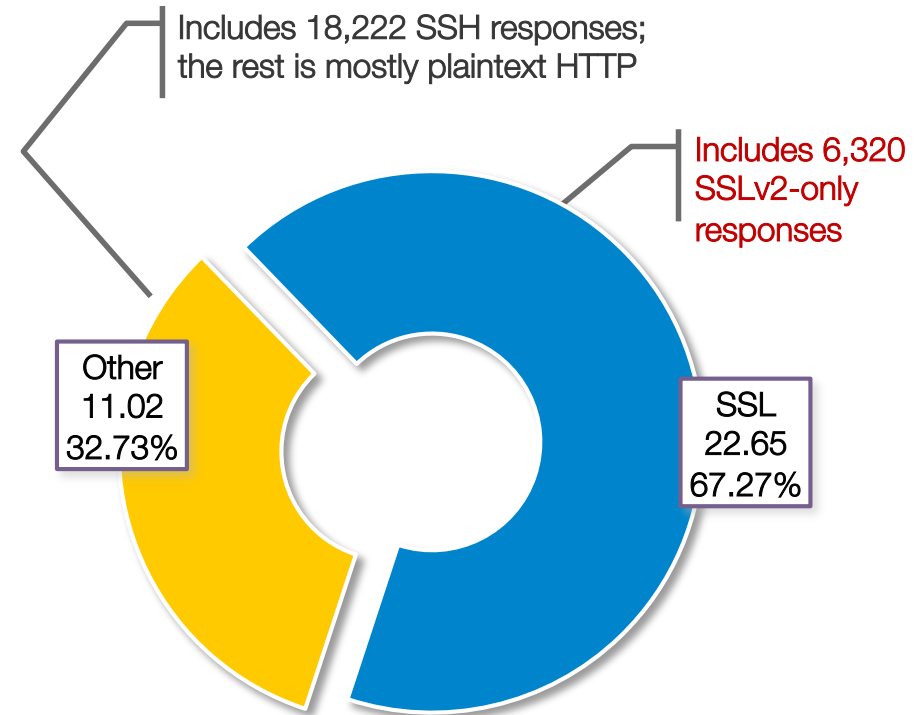


Active means to respond on port 80 or port 443

# Port 80 and 443 Activity Analysis

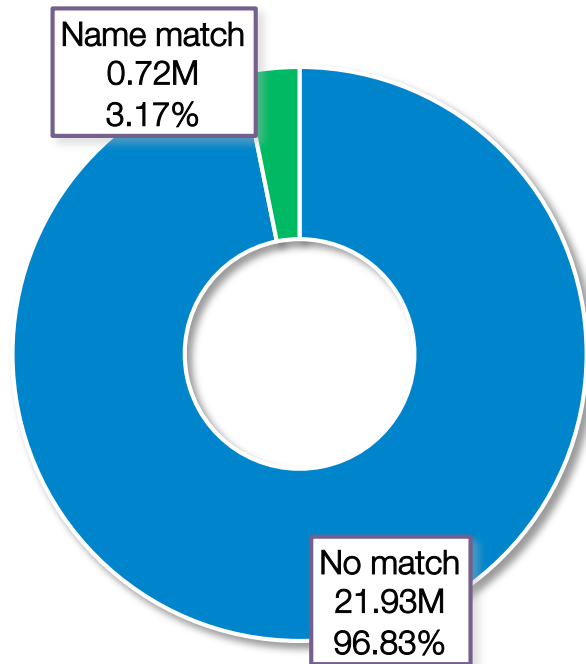


Domain responses on ports 80 and 443

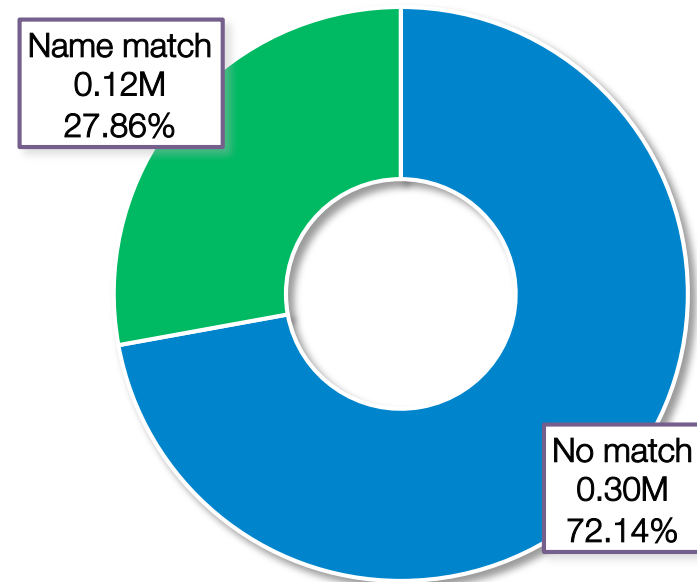


Protocols on port 443 (in millions)

# ~720,000 Potentially Valid SSL Certificates

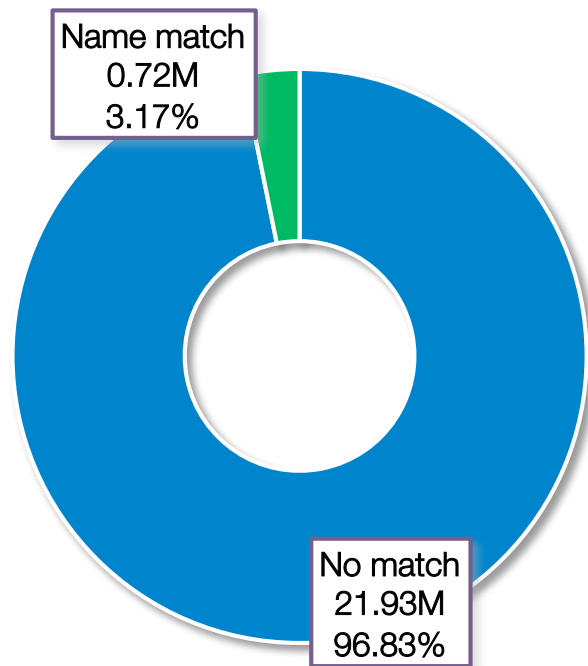


Out of 22.65M domain names with SSL enabled



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 – too many 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

- But we should be able to tell
- DNS SRV records, perhaps?
- Or virtual SSL hosting!
- At least, virtual hosting servers should not respond on port 443

# The End Result...

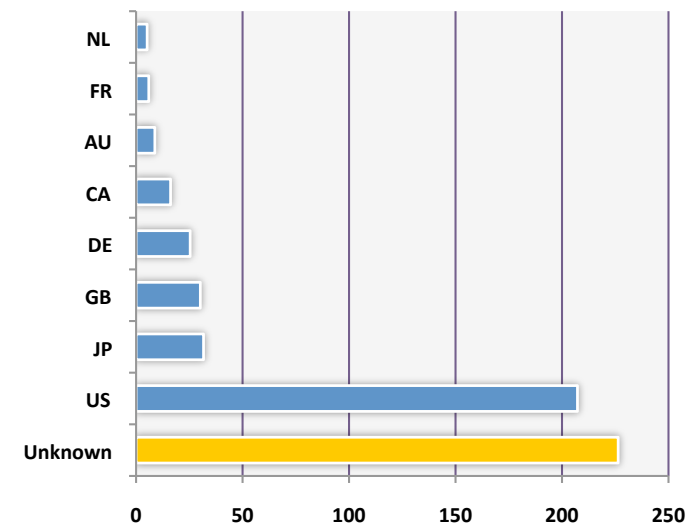


Let's now try to get as many entries as possible

- 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



Part IV: Internet SSL Survey 2010

# SSL Survey Results

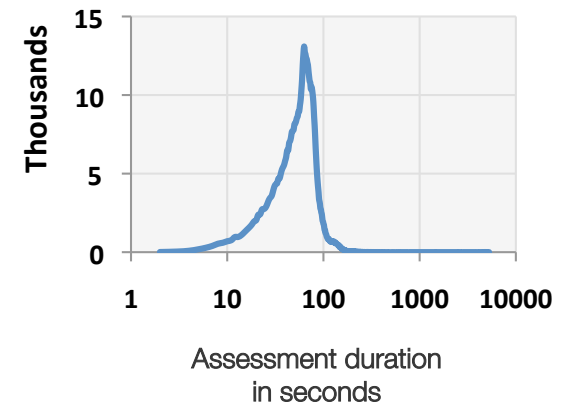


# What Did It Take to Assess All Those Servers?



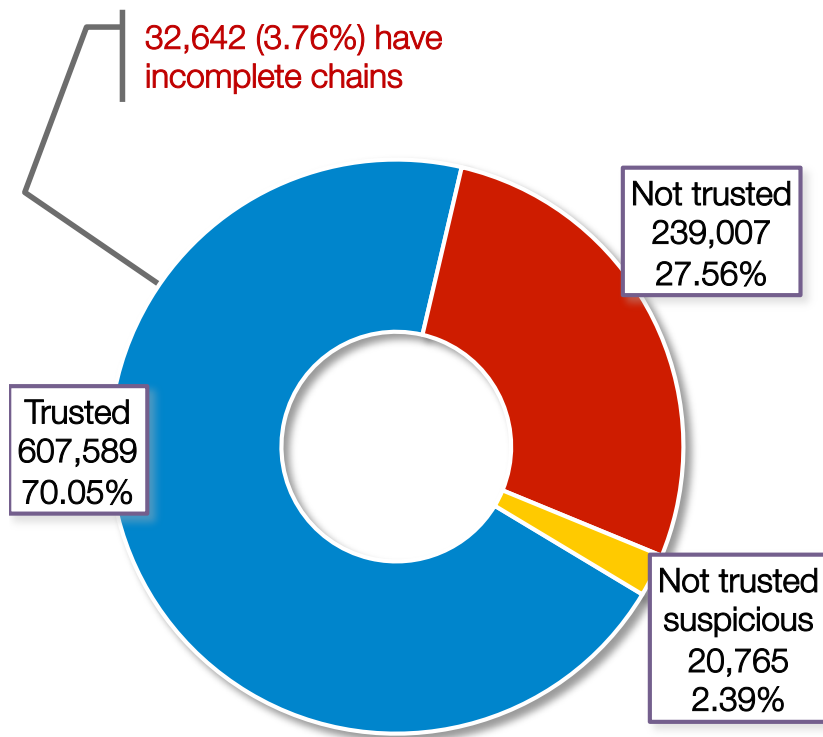
Relatively straightforward, but *very* time consuming:

- Used three servers:
  - One server to host the database
  - Two assessment servers with 200 threads each
  - All three modest virtual servers with 1 GB RAM each
- Assessment speed of about 5 servers / sec
- Median duration ~ 65 seconds
- Performed two full scans @ 2-3 days each
- Multiple partial scans to independently verify results
- About 1 TB of data
- Greatest expense was time: 1-2 man-months, even though we started with a pretty complete single-server assessment engine
  - Troubleshooting even small issues takes a ton of time
  - Result validation too

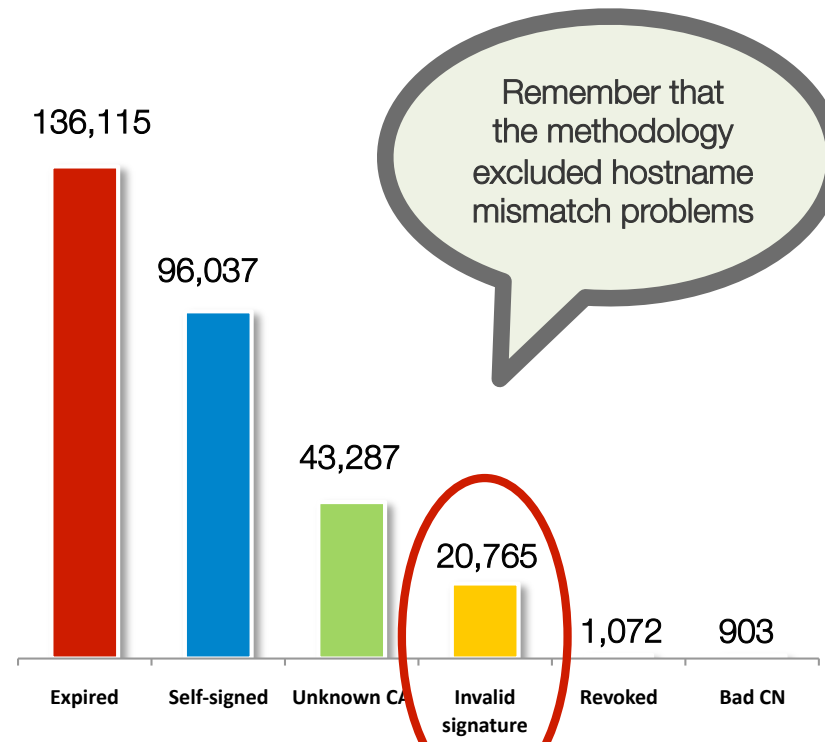




# How Many Certs Failed Validation and Why?



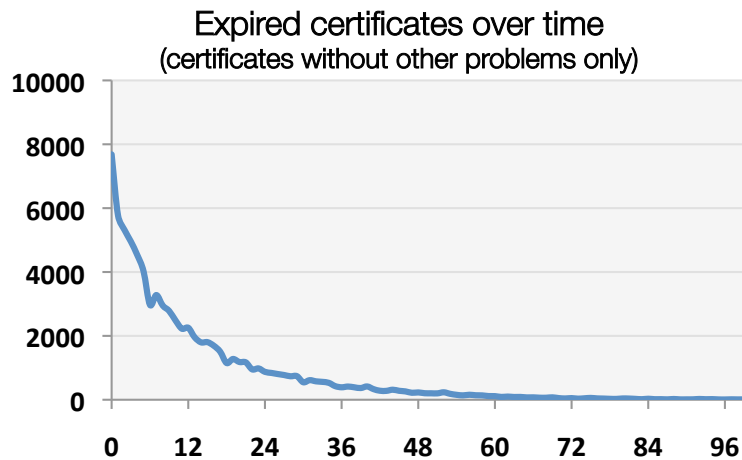
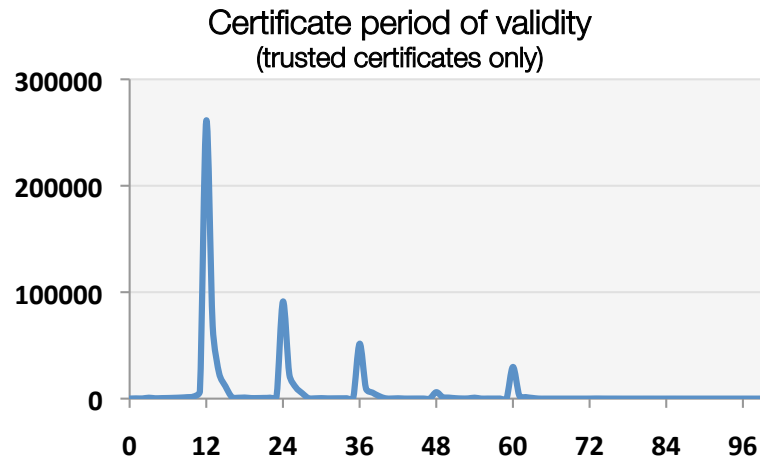
Trusted versus untrusted certificates



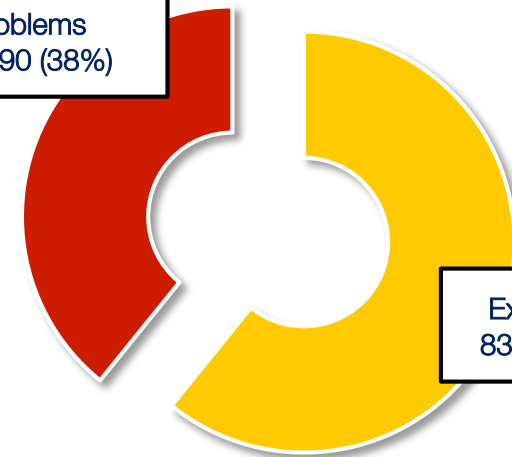
Validation failures

Interoperability issues with JSSE?

# Certificate Validity and Expiry Distribution



Expired and other problems  
52,190 (38%)



Expired only  
83,925 (62%)

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

# Unknown Issuers



We saw 43,287 unknown issuers

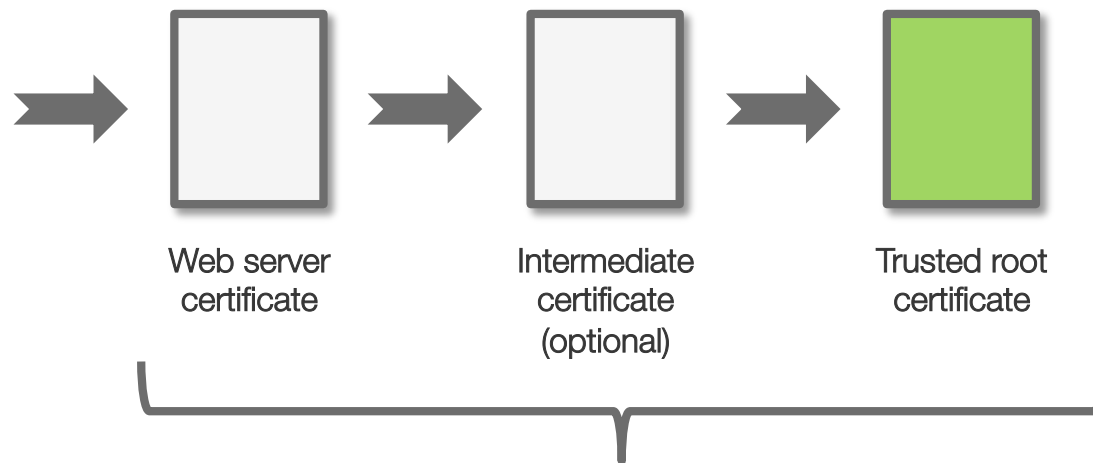
- Great majority of issuers seen only once
- 22 seen in more than 100 certificates
- Manually verified those 22
- Found 4 that one could argue are legitimate, but are not trusted by Mozilla (yet) (<http://www.mozilla.org/projects/security/certs/pending/>)

	Issuer	Seen certificates
	Firstserver Encryption Services	9486
	CAcert	6117
Trusted in other major browsers {	ipsCA	462
	KISA Root CA	162

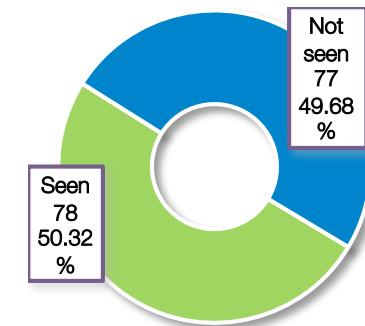
# Trusted Issuers and Chain Length

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



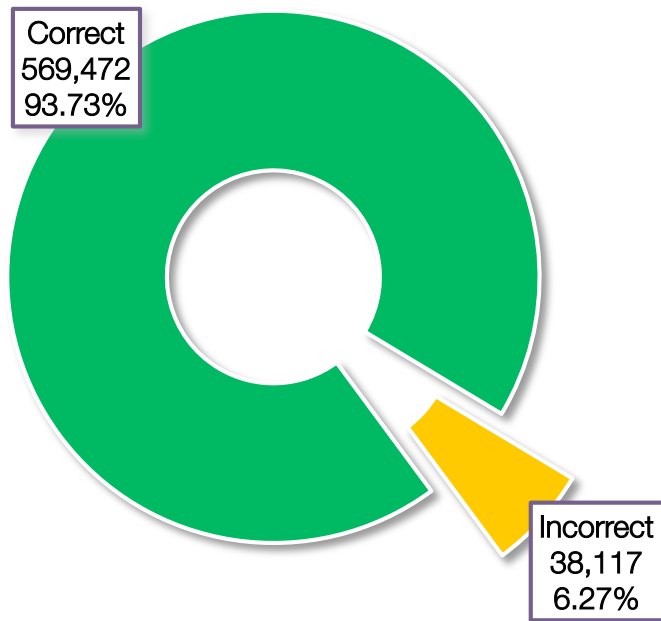
This path is **2 levels deep in 44%** of cases, and **3 levels deep in 55%** of cases.



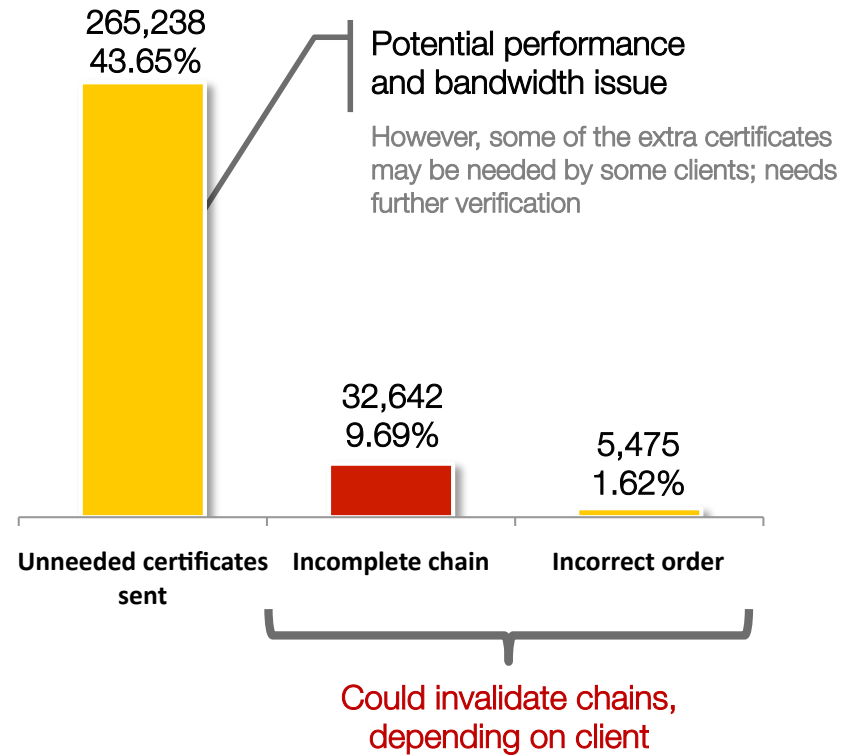
155 trusted CA certificates (from Firefox 3.6.0)

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

# Certificate Chain Correctness



Correct versus incorrect certificate chains



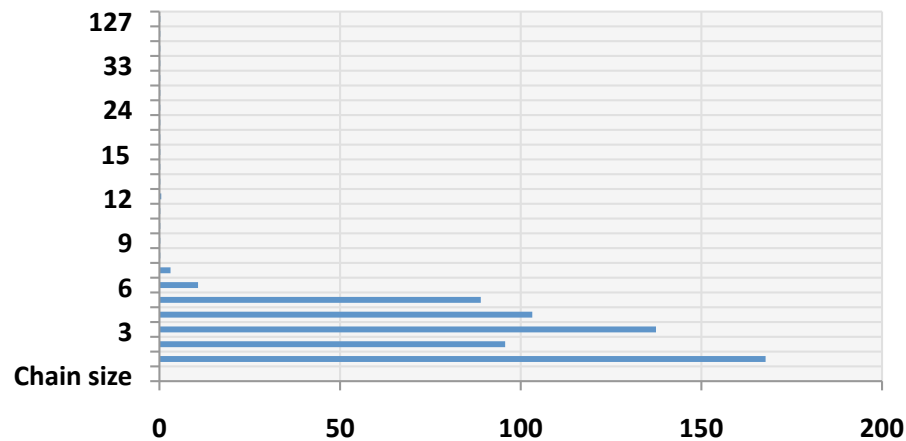
Issues with certificate chains

# 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

Certificate chain sizes in KB



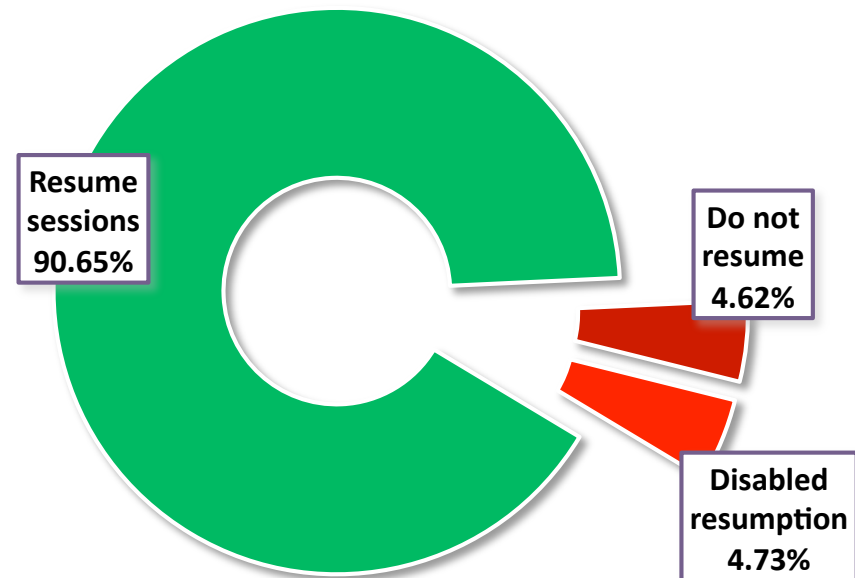
Certs sent	Actual	Should be
1	227,520	270,779
2	181,996	334,248
3	113,672	2,368
4	78,931	186
5	3,320	8
6	1,491	0
7	48	0
8	28	0
9	49	0
10	489	0
11	4	0
12	10	0
13	24	0
15	1	0
16	1	0
17	2	0
61	1	0
70	1	0
116	1	0

# Session Resumption



Session resumption is an very important performance optimization

- It avoids the expensive handshake operations on all but first connection
- Most sites support it, but about 9% don't
- A small number of sites claim to support it, but do not resume sessions
- Session resumption may be challenging to deploy when load balancing is used
- We did not test for Session Ticket support on this occasion

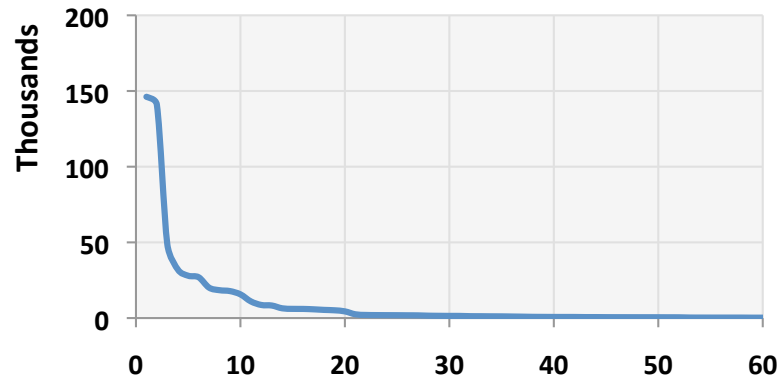


Session resumption support

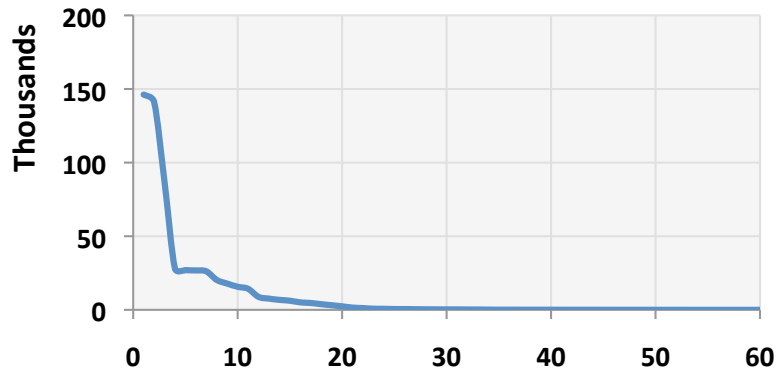
# Trusted Anchors



Certificates per issuer  
(429 issuers in total)



Certificates per trust anchor  
(78 anchors in total)



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 Primary Certification Authority (VeriSign)	26,765
VeriSign Trust Network	26,163
GlobalSign Root CA	20,290
Network Solutions Certificate Authority	19,437
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

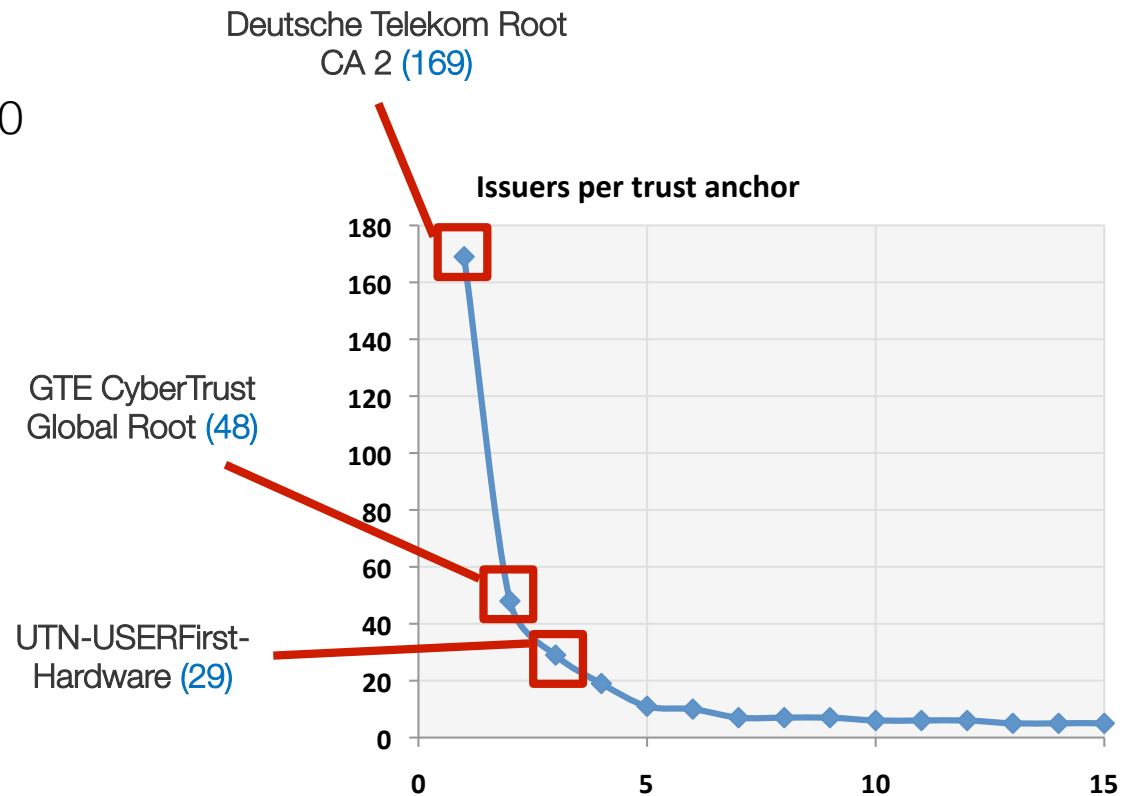
18 trust anchors on this page account for 608,741 (97%) certificates



# Trusted Anchors and Trust Delegation

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

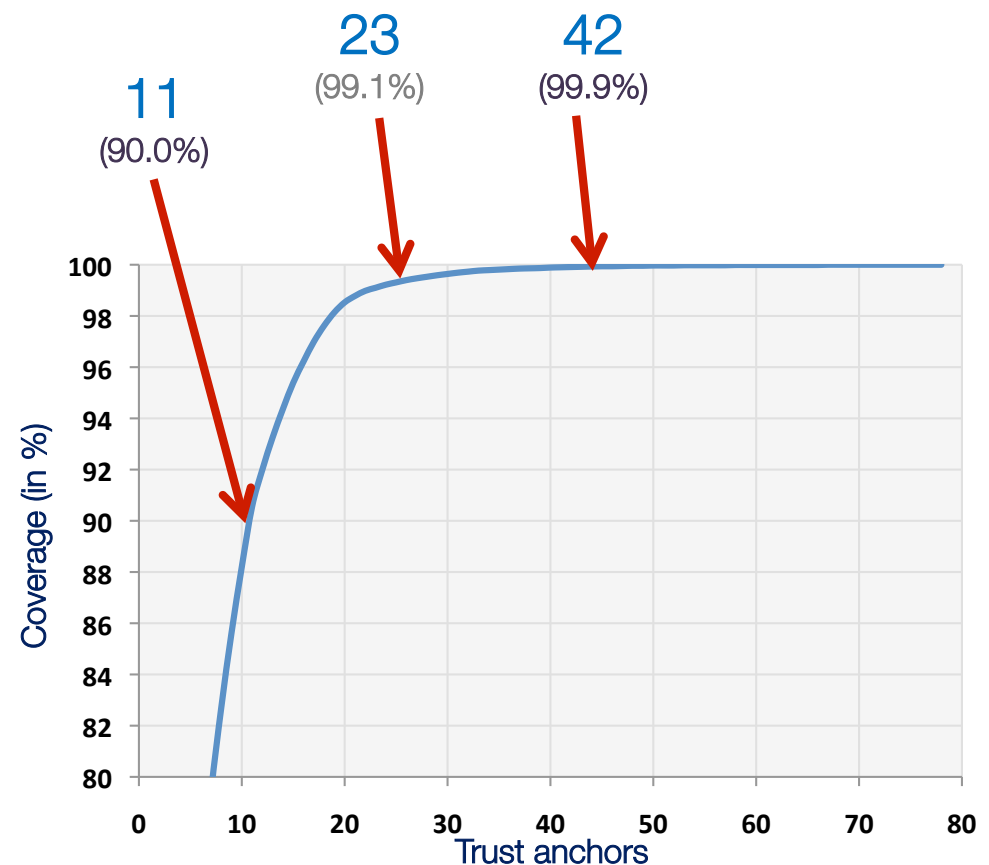
- Top 6 anchors have more than 10 issuers each
- They account for a total of 286 issuers, or 67% of all
- Deutsche Telekom alone accounts for 39% of all issuers we saw



# How Many Trust Anchors Do We Need?

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

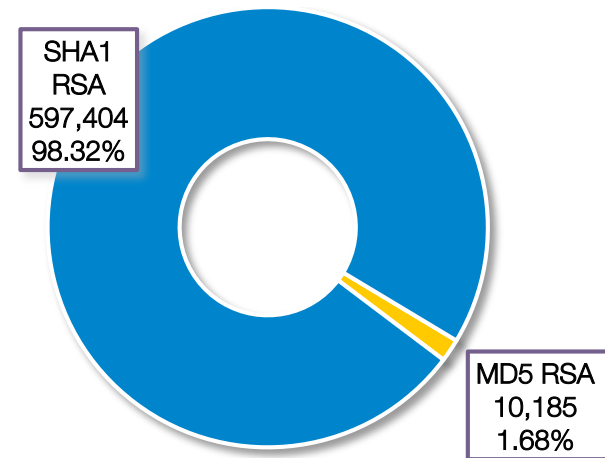
- Of course, this is **very subjective**
- Our data set is biased and contains predominantly U.S. web sites
- Your browsing habits are probably different
- Still, it's interesting to see that you probably need only between 10 and 20 trust anchors.
- But your selection may be different from mine!



# 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
  - SHA384 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

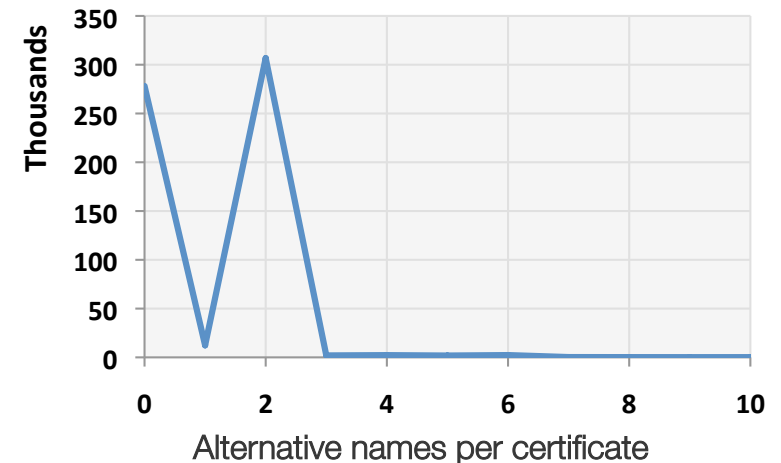
- Some CAs will automatically add 2 alternative domain names (“example.com” and “www.example.com”)
- Untrusted [3o.hu](http://3o.hu) has 354 (8.2 KB cert)!
- Untrusted [www.epi.es](http://www.epi.es) has 287 and they are all wildcards (7.5 KB cert)!

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



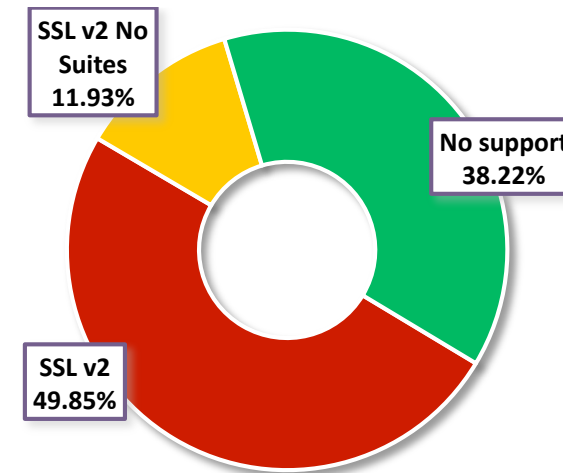
Alternative names	Name
252	www.hu-berlin.de
191	www.tu-berlin.de
153	*.abyx.com
150	www.newcreditera.com
116	edgecastcdn.net
101	jpbsecurehostingservice.com www.indiebound.org
100	quotes.usinsuranceonline.com

# Protocol Support



Half of all trusted servers support the insecure SSL v2 protocol

- Modern browsers won't 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	-

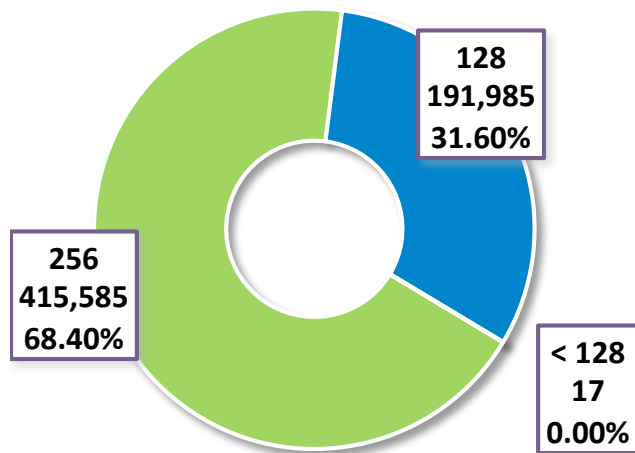
Cipher	Servers	Percentage
3DES_EDE_CBC	603,888	99.39%
RC4_128	596,363	98.15%
AES_128_CBC	418,095	68.81%
AES_256_CBC	415,585	68.39%
DES_CBC	341,145	56.14%
RC4_40	320,689	52.78%
RC2_CBC_40	314,689	51.79%
RC2_128_CBC	283,416	46.64%
DES_CBC_40	192,558	31.69%
RC4_56	192,192	31.63%
IDEA_CBC	52,762	8.68%
RC2_CBC_56	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

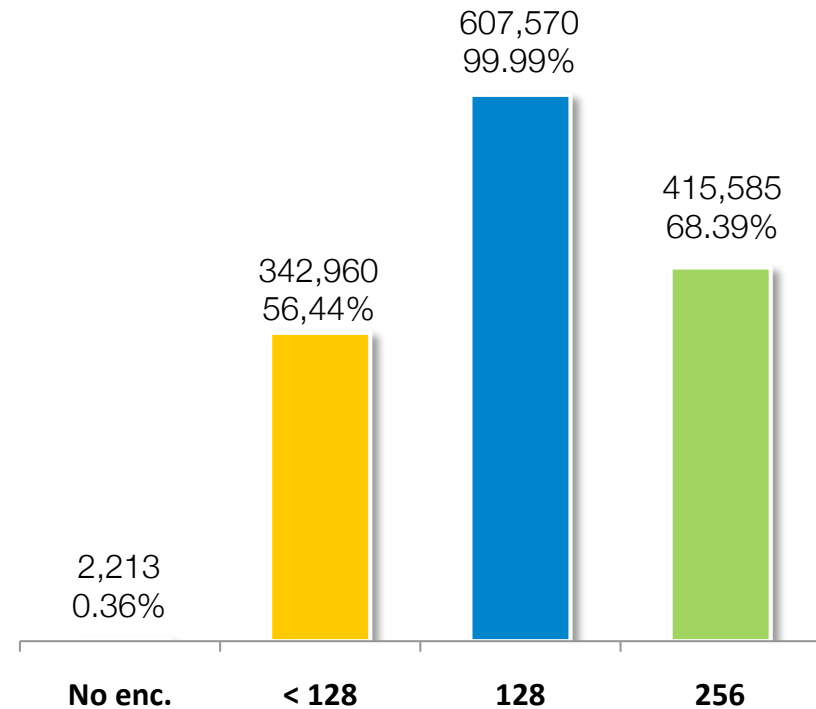


All servers support **strong** and most support **very strong** ciphers

- But there is also wide support for weak ciphers



Best cipher strength support



Cipher strength support

# Cipher Suite Support

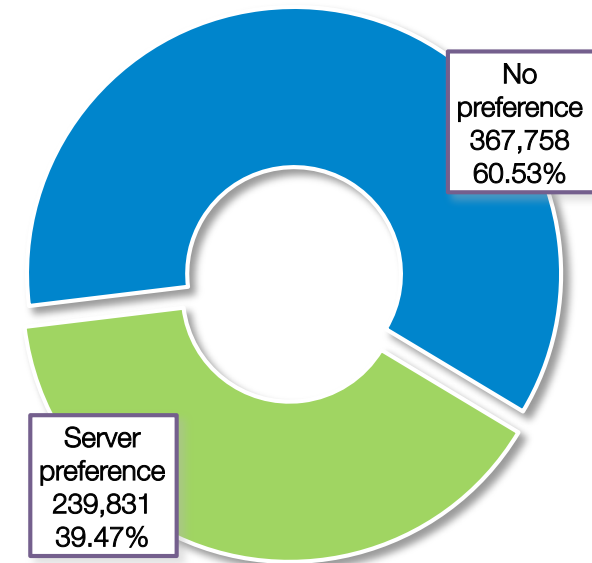


## Most supported cipher suites

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



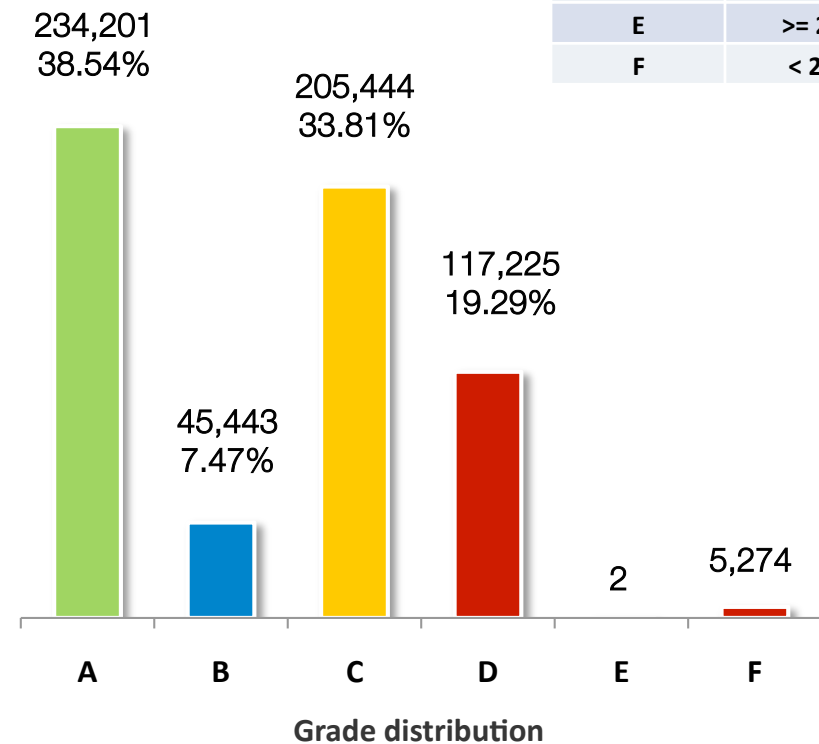
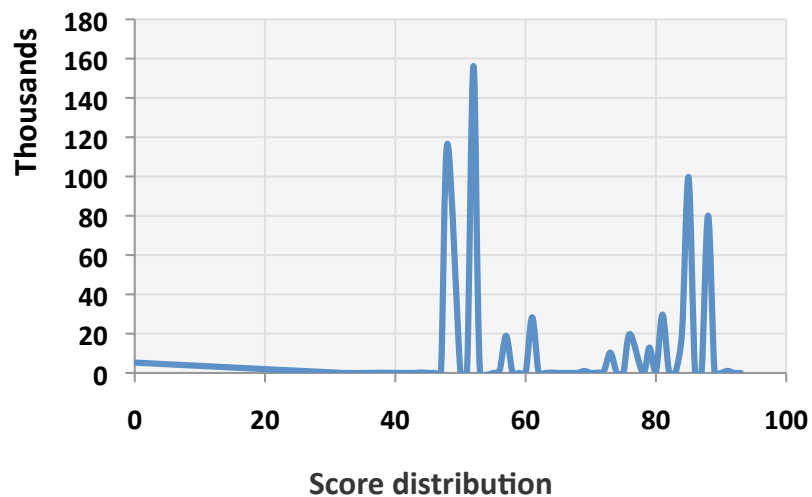
# SSL Labs Grade Distribution



Most servers not configured well

- Only 38.54% got an A
- 61.46% got a B or worse
- Most probably just use the default settings of their web server

Key length	Score
A	$\geq 80$
B	$\geq 65$
C	$\geq 50$
D	$\geq 35$
E	$\geq 20$
F	$< 20$



# Strict Transport Security (STS)



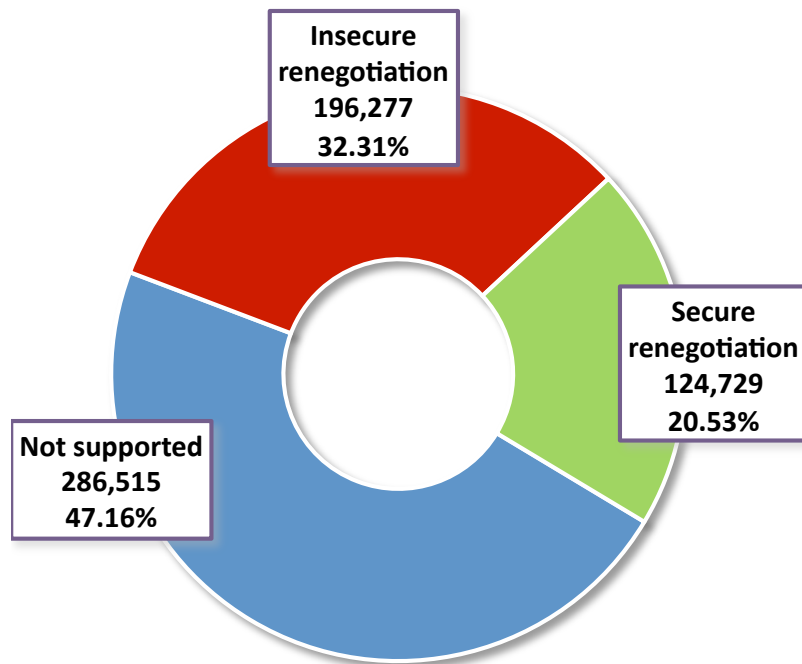
Only **12** trusted sites seem to support Strict Transport Security (STS)

- 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 serious 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

Part V: Internet SSL Survey 2010

# What Next?



# Conclusions



## Good:

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

## Bad:

- No thought given to configuration in most deployments
  - Most probably just use default settings
  - SSLv2 still widely supported after 14 years!
- Lack of support for TLS v1.1 and v1.2 is cause for concern
- It takes a serious vulnerability for things to start changing (and then only slowly)

## Long term:

- Support for virtual SSL hosting (TLS SNI) is needed to take SSL further
- We need to find a way to motivate vendors to use better defaults and library developers to remove obsolete features and add new features

# Possible Future Improvements, Part I



## 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 II



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

Q & A

Thank You

Ivan Ristic  
iristic@qualys.com  
@ivanristic

