

A Study of What Really Breaks SSL

HITB Amsterdam 2011

v1.2

Ivan Ristic

Michael Small

20 May 2011



Agenda

1. State of SSL
2. Quick intro to SSL Labs
3. SSL Configuration Surveys
4. Survey of Actual SSL Usage
5. Conclusions

About Ivan Ristic

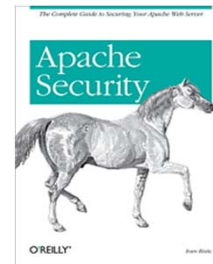
Ivan is a compulsive builder, usually attracted to problems no one else is working on

- **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



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. **An add-on.**
- Designed for HTTP, used for many other protocols.

The original version of the protocol designed at Netscape:

- Version 2 was released 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
- Certificate Authorities and their resellers
- CA/Browser Forum
- SSL Client vendors (esp. major browser vendors)
- SSL library developers
- SSL server vendors
- System administrators
- Developers
- Consumers

Major Challenges Today

1. Fragility of the trust ecosystem
- 2. Incorrect or weak configuration**
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

SSL Attack Model*

SSL can fail in many ways, but there are 3 principal attacks:

- **Passive MITM**
 - **Session hijacking (e.g., using Firesheep)**
- **Active MITM**
 - **SSL bypass (e.g., using sslstrip)**
 - **Attacks against renegotiation**
 - **Rogue certificates**
 - **User attacks (who reads warnings anyway)**
- **Third-party compromise**

(*) For a complete attack model, visit <https://www.ssllabs.com/projects/ssl-threat-model/>

State of the Art Protection

It is possible to have a reasonably secure web site (when it comes to communication security):

- Use an EV certificate (difficult to forge)
- Configure your SSL server properly:
 - Good key size and coverage of desired domain names
 - Good protocols and 128-bit forward-secrecy cipher suites
 - Patches and workarounds applied
- Redirect all port 80 traffic to port 443
- Use HTTP Strict Transport Security
 - Forces all traffic over SSL, even with HTTP links
 - Can include subdomains to address cookie issues

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**

The screenshot shows the Qualys SSL Labs website. At the top, there is a navigation bar with links for Home, Qualys.com, Projects, and Contact. The main header features the Qualys logo and the text 'QUALYS* SSL LABS'. Below this, a large blue banner contains the title 'How Well Do You Know SSL?' and a sub-headline: 'If you want to learn more about the technology that protects the Internet, you've come to the right place.' To the right of the banner, a list of SSL/TLS cipher suites is displayed, including 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, and TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA.

The main content area is divided into three columns:

- Our Stuff:** Lists various tools and documents available for download, such as 'Public SSL Server Database', 'SSL Server Rating Guide', 'HTTP Client Fingerprinting Using SSL Handshake Analysis', 'SSL Threat Model' (marked as NEW), and 'Firefox SSL Add-on Collections'.
- News:** Features two recent articles: 'SSL Labs assessment engine v1.0.59 improvements' (dated June 17, 2010) and 'Qualys acquires SSL Labs' (dated June 15, 2010). The latter article includes a 'Test Your SSL Server Now!' section with a form to enter a domain name for a security assessment.
- About SSL Labs:** Provides background information on the project, stating that SSL is a technology that protects the Internet and that the project aims to transform insecure communication channels into opaque data streams. It also mentions that SSL Labs is a non-commercial research effort and welcomes participation from individuals and organizations interested in SSL.

At the bottom of the page, there is a copyright notice for Qualys, Inc. and a link to the Terms and Conditions.

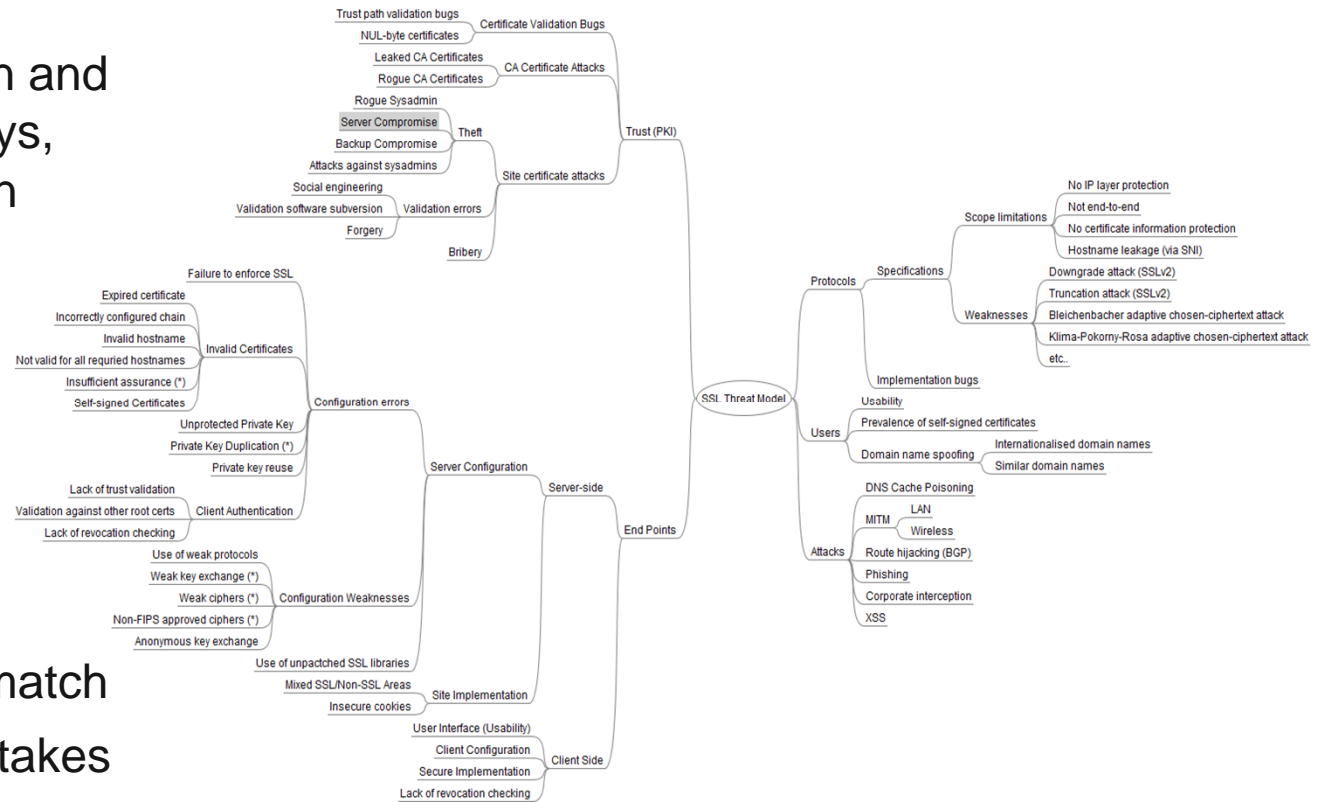
SSL Threat Fail Model

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



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

QUALYS[®] SSL LABS Home Qualys.com Projects Contact

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	Recent Best-Rated	Recent Worst-Rated
credit-suisse.hrworkwaysasia.com C (61)	www.stronghq.com A (92)	google.com F (0)
assist.qrbinc.com B (76)	www.startssl.com A (91)	ehrms.embrace.com F (0)
www.hrworkwaysasia.com C (61)	www.defcon-switzerland.org A (91)	members7.premium.biz F (0)
securewebpoint.com A (85)	www.swissminds.com A (91)	www.meritumbank.pl F (0)
google.com F (0)	www.luqqagepros.com A (91)	www.mojedatovaschranka.cz F (0)
ehrms.embrace.com F (0)	yahoo.com A (88)	www.patelco.com F (0)
www.hotmail.com Err	www.tamarasboutiques.com A (88)	www.mecunet.com F (0)
online.justice.vic.gov.au C (52)	www.patelco.org A (88)	netenterprise.com F (0)
www.comcast.com C (61)	www.elsteronline.de A (88)	communities.vmware.com F (0)
www.stronghq.com A (92)	www.qualys.com A (88)	dex.edzone.net F (0)

SSL Report v1.0.59

Copyright © 2010 Qualys, Inc. All Rights Reserved. [Terms and Conditions](#)

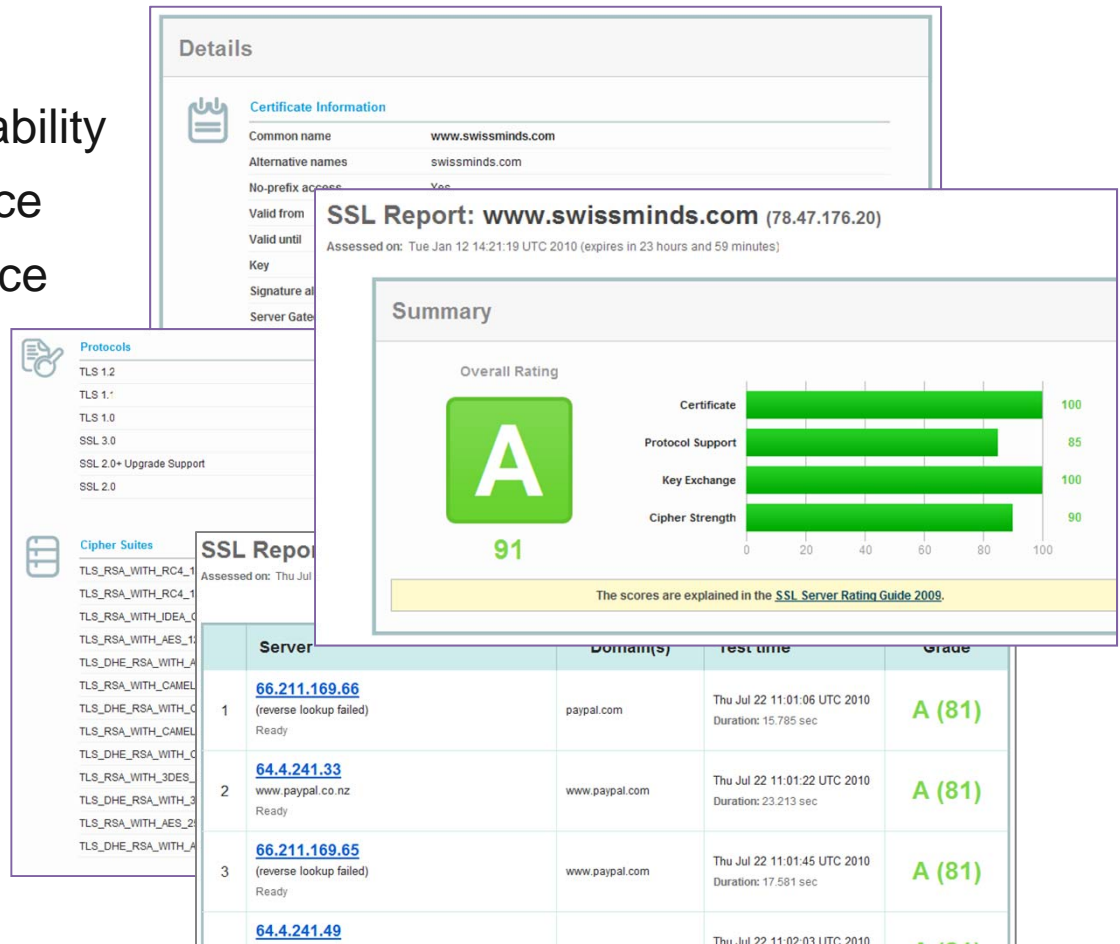
SSL Assessment Details

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



Part IV:

SSL Configuration Surveys



Global SSL Surveys

In our first global survey, in 2010:

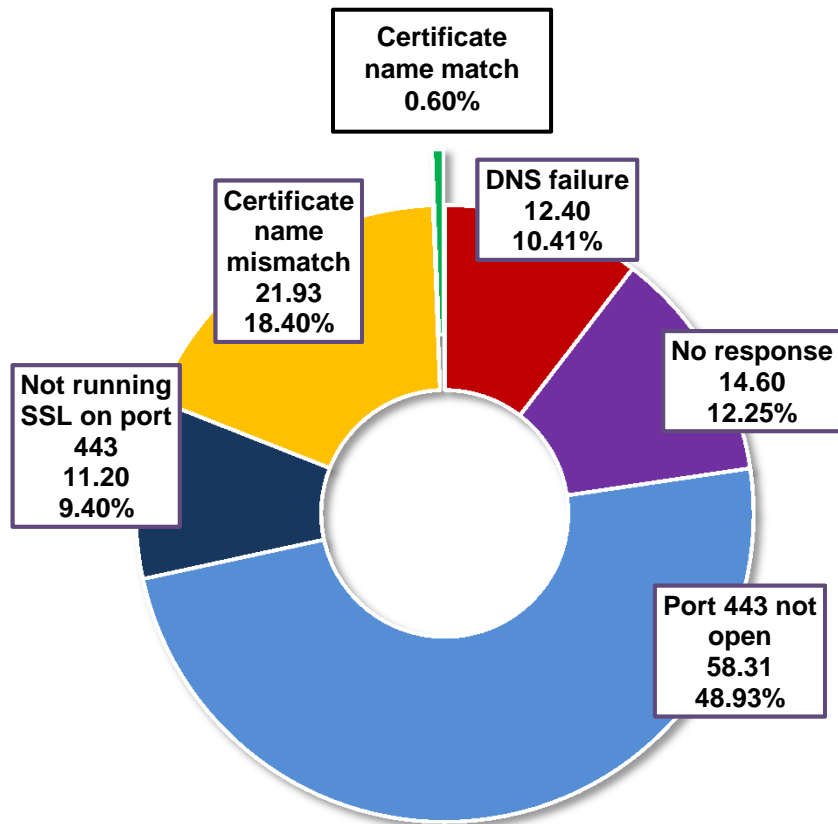
- We looked at 119 million domain name registrations
- Also examined the Alexa's top 1m domain names
- Arrived to about 900,000 server to assess
- About **600,000 were valid** and were used in the survey

In our second global survey, in 2011:

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



High Level View



Only 0.4% domains with properly configured SSL

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**

Deep Survey of Popular Sites

In order to understand impedance mismatch issues, we undertook a deep survey of most popular SSL web sites:

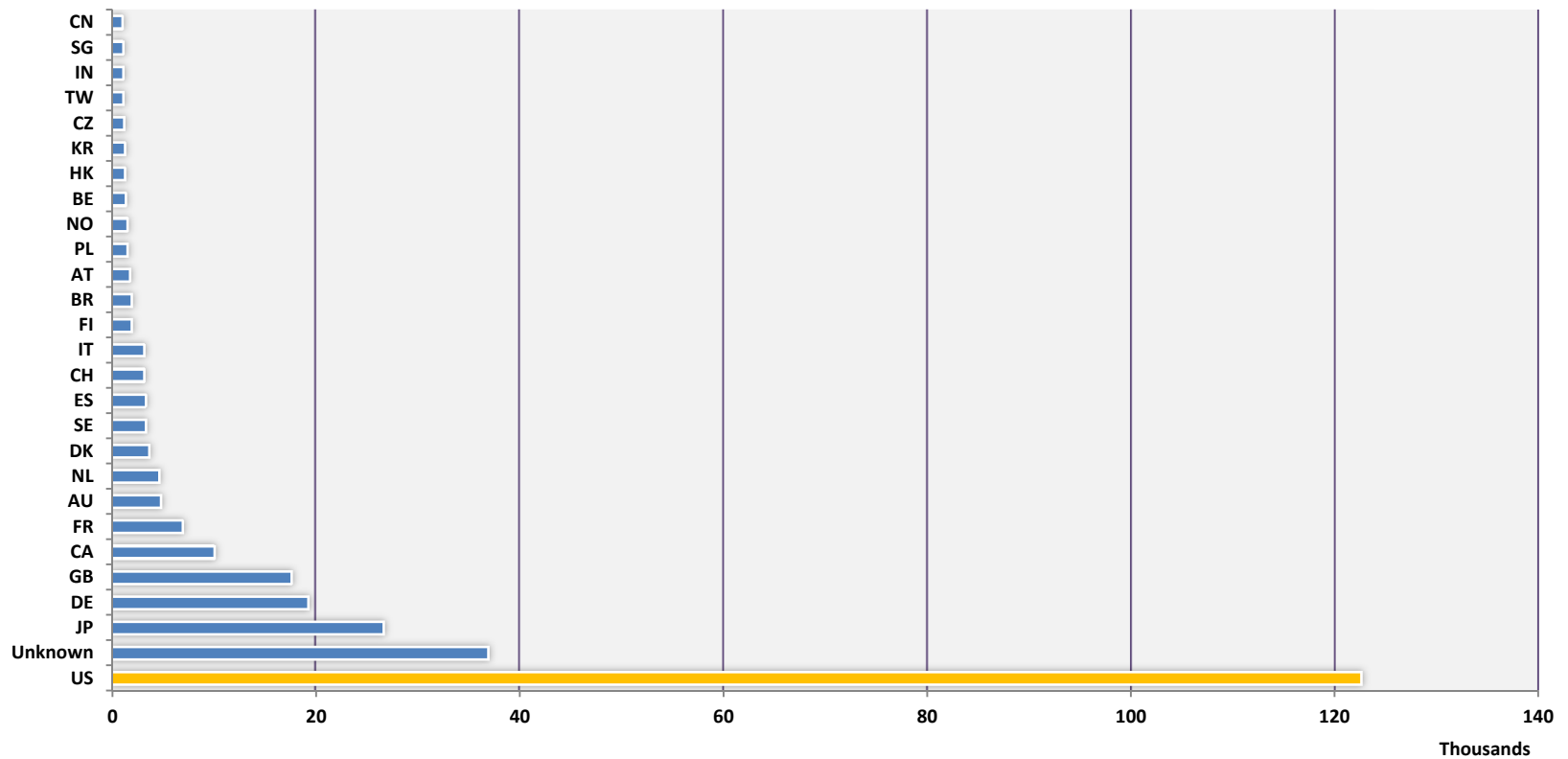
- Start with the top 1M popular sites from Alexa
- And with 1.4m valid SSL sites globally from SSL Observatory
- Cross-reference to arrive to **327,476** SSL sites
- Accept **248,161** sites into the survey

Then:

- Build a custom crawler to visit each site from the list, and examine things such as:
 - Mixed content
 - Insecure cookies
 - Use of third-party resources (delegation of trust)
 - Response header usage

Countries Overview

Countries with over 1,000 certificates:

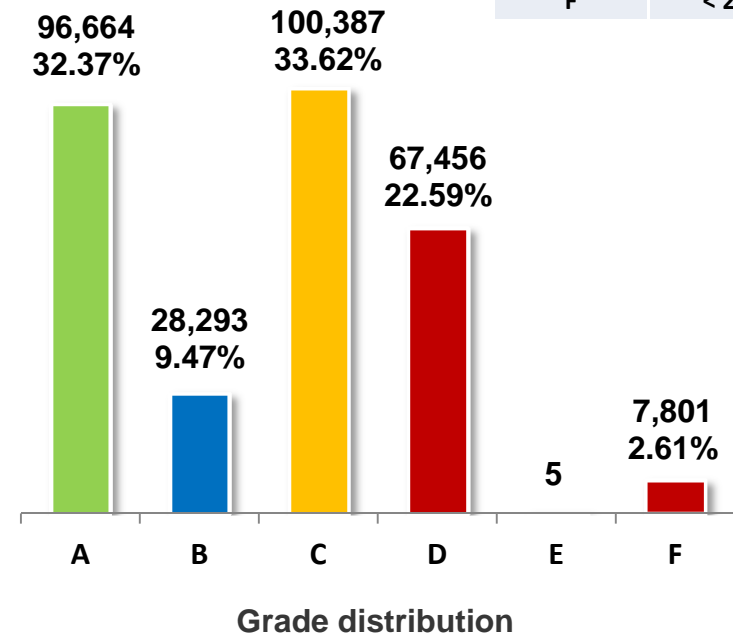
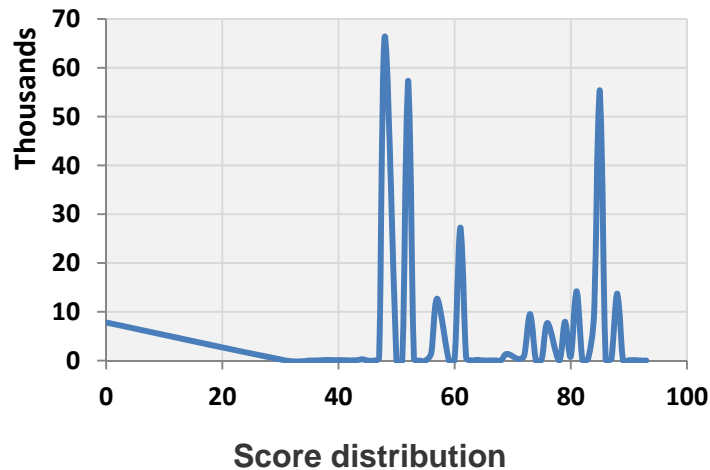


SSL Labs Grade Distribution

Most servers not configured well

- Only 32.37% got an A
- 67.63% got a B or worse
- Most probably just use the default settings of their web server

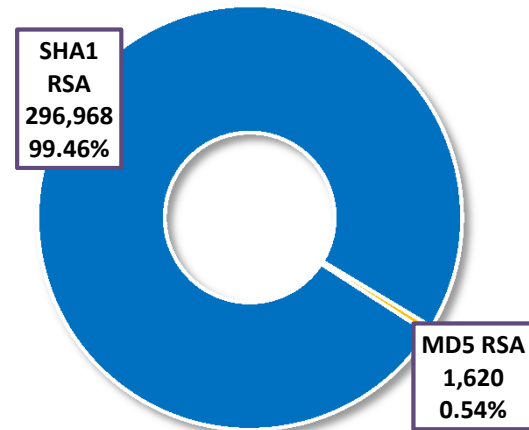
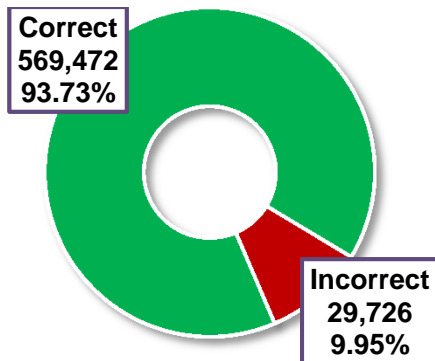
Key length	Score
A	≥ 80
B	≥ 65
C	≥ 50
D	≥ 35
E	≥ 20
F	< 20



Certificates

Virtually all trusted certificates use **RSA** keys; **only 9 DSA** keys

- SHA1 with RSA is the most popular choice for the signature algorithm
- We are starting to see SHA256, but only on 18 certificate
- Virtually all keys 1024 or 2048 bits long
- Still 43 weak RNG keys from Debian
- About 10% incorrect certificate chains



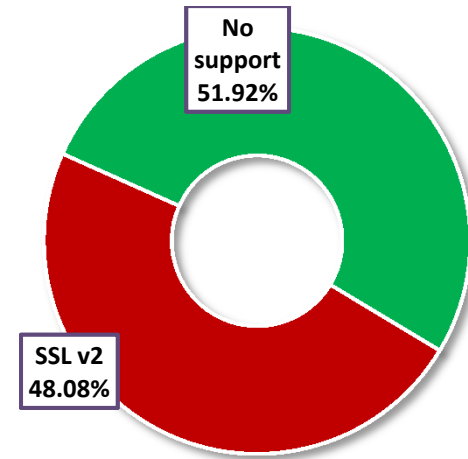
Signature algorithm

Key length	Certificates seen
512	559
1024	170,423
2048	125,333
4096	2,108
8192	3

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)

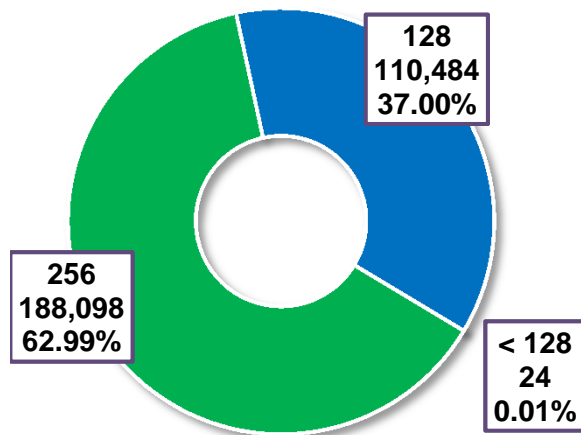


Protocol	Support	Best protocol
SSL v2.0	143,591	110
SSL v3.0	298,078	5,205
TLS v1.0	293,286	292,366
TLS v1.1	916	854
TLS v1.2	69	69

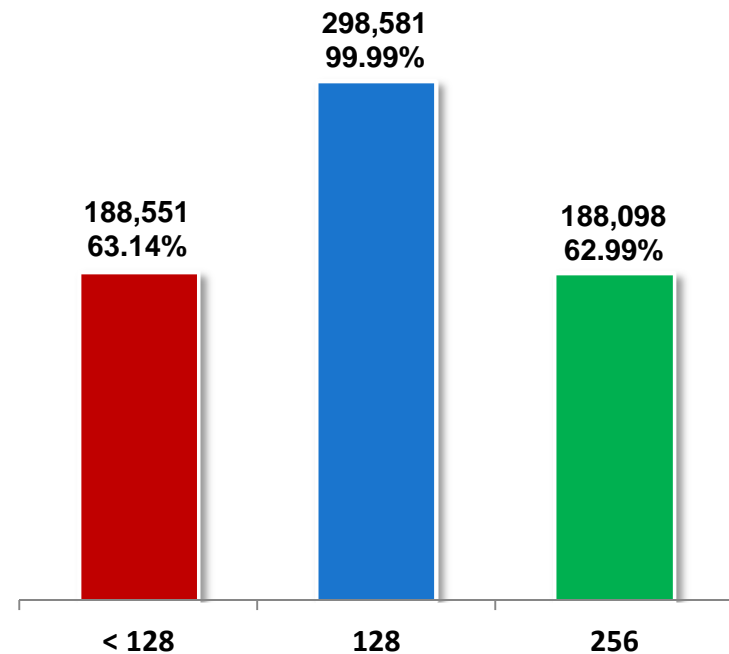
Cipher Strength

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

- But there is also wide support for weak ciphers

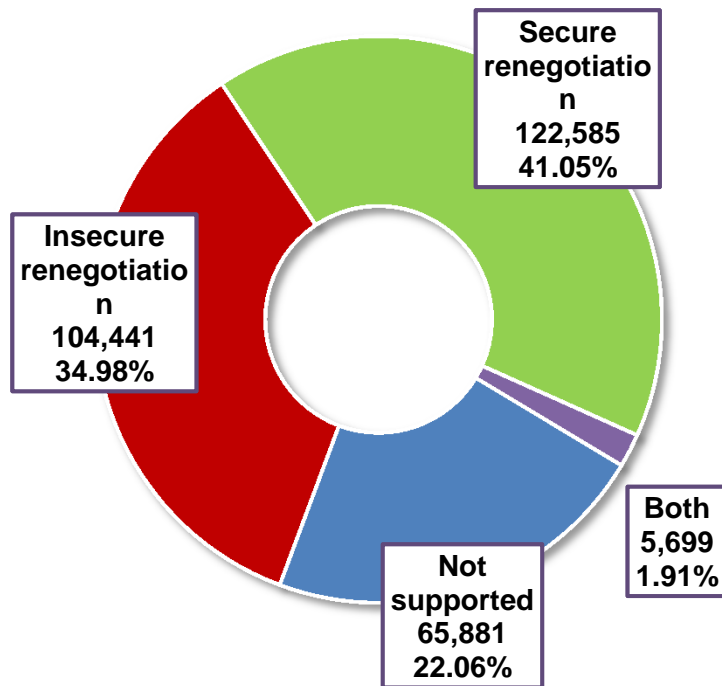


Best cipher strength support



Cipher strength support

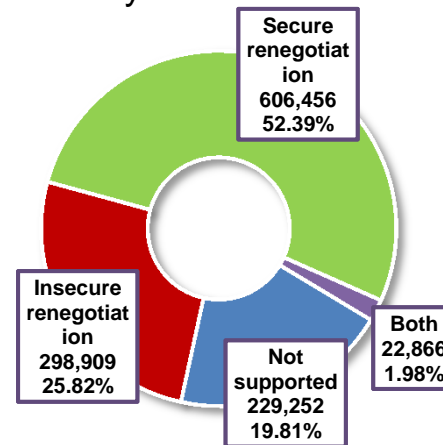
Secure and Insecure Renegotiation



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
- Globally:



Part V:

Survey of Actual SSL Usage



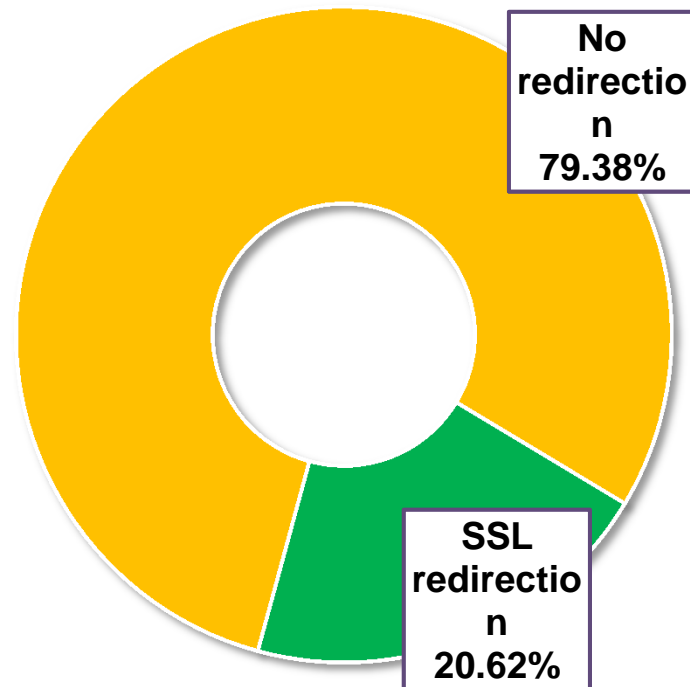
Basics

First we wanted to know how many sites make exclusive use of SSL:

- Out of 248,161 sites tested (remember, all support SSL)
- **20.61% (51,160) redirect to SSL**

The rest, **79.29% sites**, may or may not (most likely not) redirect to SSL for authentication. :

- Sites without redirection are easily exploitable via *sslstrip* or *Firesheep*



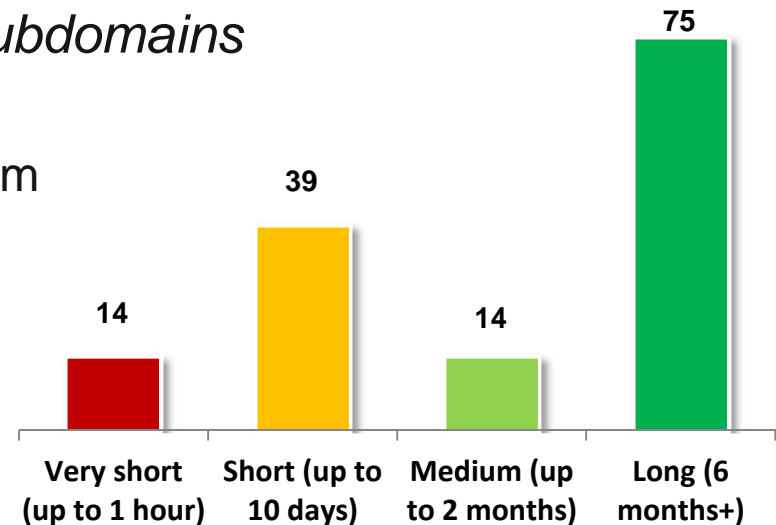
Strict Transport Security

Next we looked at HTTP Strict Transport Security:

- Out of 248,161 sites tested
- **Only 80 use HSTS**
 - 162 globally (out of 1.2m SSL servers)

We saw 142 different HSTS responses, and looked at the *max-age* and *includeSubdomains* settings:

- Varied approaches to max-age, from short term to long term
- **13 out of 142 use HSTS to include subdomains**
 - These are safe from cookie forcing attacks



State of the Art Protection

Proper deployment of HSTS requires a redirection, so we cross-references the list of sites that support HSTS with the list of sites that have redirection in place:

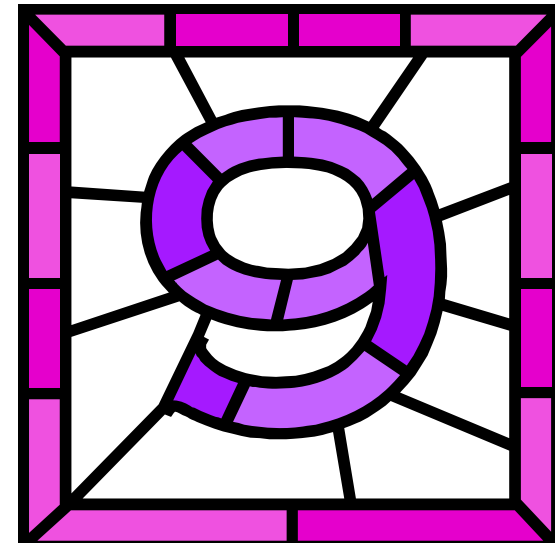
- Out of 51,160 sites with redirection
- **Only 55 use HSTS**

The final piece here is the EV certificate:

- Out of 55 sites with HSTS and redirection
- **Only 9 have an EV certificate**

Thus:

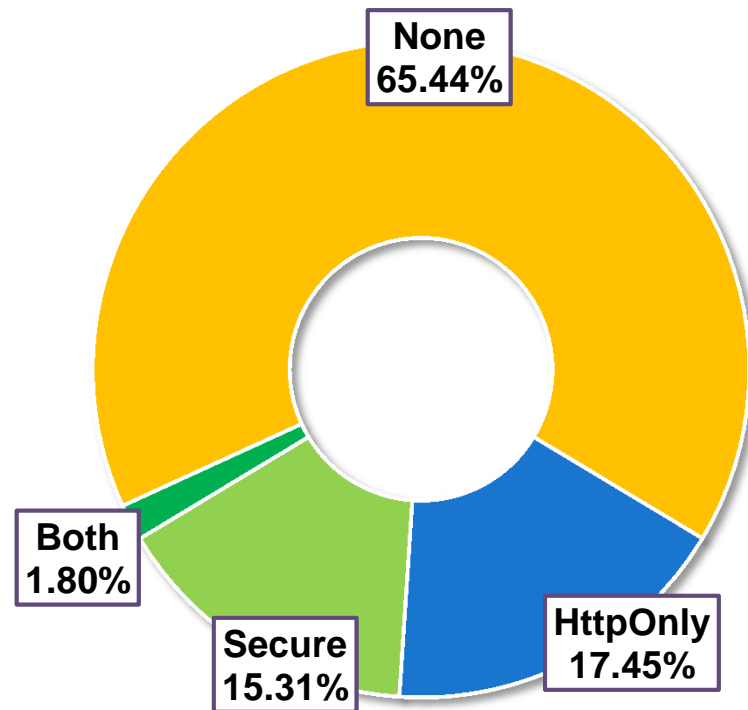
- Out of 248,161 sites tested
- **Only 9 have state of the art protection**
- **Actually, it's 0 if you consider *includeSubdomains* important**



Cookies

In most web applications, cookies are used for authentication for the duration of the session:

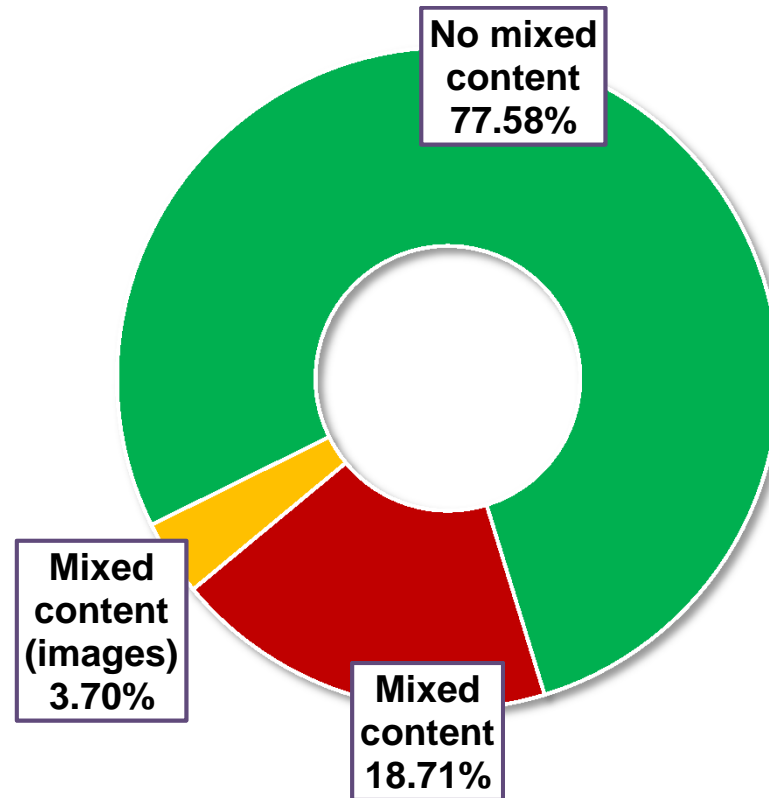
- Out of 248,161 sites tested
- We saw **36.80% (91,335)** sites with session cookies
- **16,530 HttpOnly**
- **14,506 Secure**
- **1,706 HttpOnly and Secure**



Mixed Content

When it comes to mixed content, we wanted an indication of how many sites are suffering from this problem:

- Out of 248,161 sites tested
- **22.41% (55,628)** use mixed content
- **18.71% (46,434)** use mixed content, excluding images

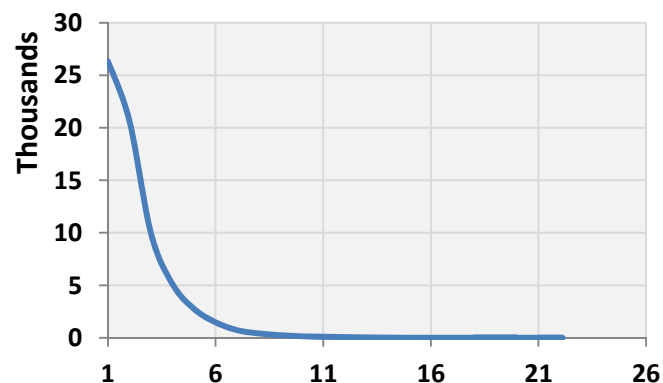


Distribution of Trust

27.4% (68,020) include services of other web sites, and thus rely on other sites' security:

- Most of these have one or two links
- A small number uses many (up to 22)
- The usual suspects:
 - Google Analytics
 - Google Ads
 - Quantcast
 - Twitter
 - Google jQuery hosting
 - Facebook
 - And a long tail...

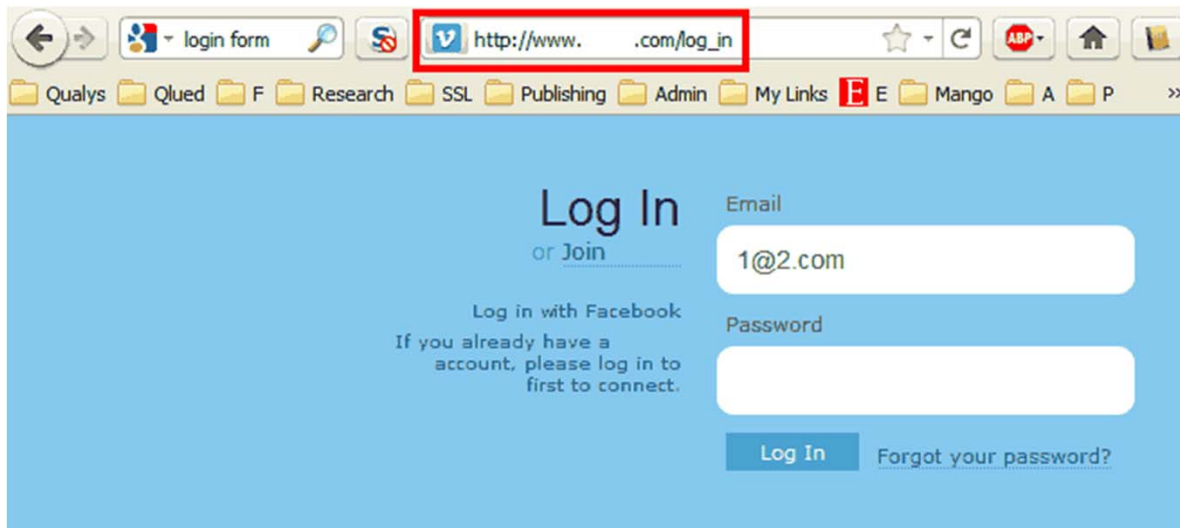
3 rd party links	Sites
1	26,322
2	20,648
3	9,938
4	5,108
5	2,756
6	1,473



Authentication

You would expect that most sites understand the need to protect user credentials:

- **25.91%** (64,321) sites have a login form
- But **68.96%** (44,361) over HTTP
- And **54.39%** (34,990) submit over HTTP too
- About a third of the forms protected using SSL



Bonus: Overview of Various Declarative Protection Measures

Declarative protection measures are very effective because they can often be implemented in configuration, and after the fact:

- Out of **248,161** sites tested

Measure	Sites	Popularity
HttpOnly	16,530	6.66%
Secure	14,506	5.84%
X-Frame-Options	686	0.27%
X-XSS-Protection	200	0.080%
Strict-Transport-Security	80	0.032%
X-Content-Type-Options	67	0.027%
Access-Control-Allow-Origin	47	0.019%
X-Content-Security-Policy	12	0.005%

Part VI:
Conclusions



Conclusions

We conclude:

1. Systemic issues are hotly debated by the community and the press
2. In real life, however, it's deployment and implementation issues that break SSL
3. It's possible to achieve reasonable security, but most sites choose not to do it
4. Among the popular sites, only a handful have decent SSL deployments, when all is taken into account

Q & A

Thank You

Ivan Ristic

iristic@qualys.com

[@ivanristic](https://twitter.com/ivanristic)

