A Study of What Really Breaks SSL

HITB Amsterdam 2011

v1.0

Ivan Ristic

Michael Small

20 May 2011

QUALYS®

HITBSECCONF2011 AMSTERDAM

Agenda

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

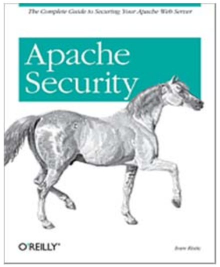
About Ivan Ristic

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



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

QUALYS®

Brief History

Protocol goal:

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

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
- 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
- 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

Part II:

SSL Labs

QUALYS®

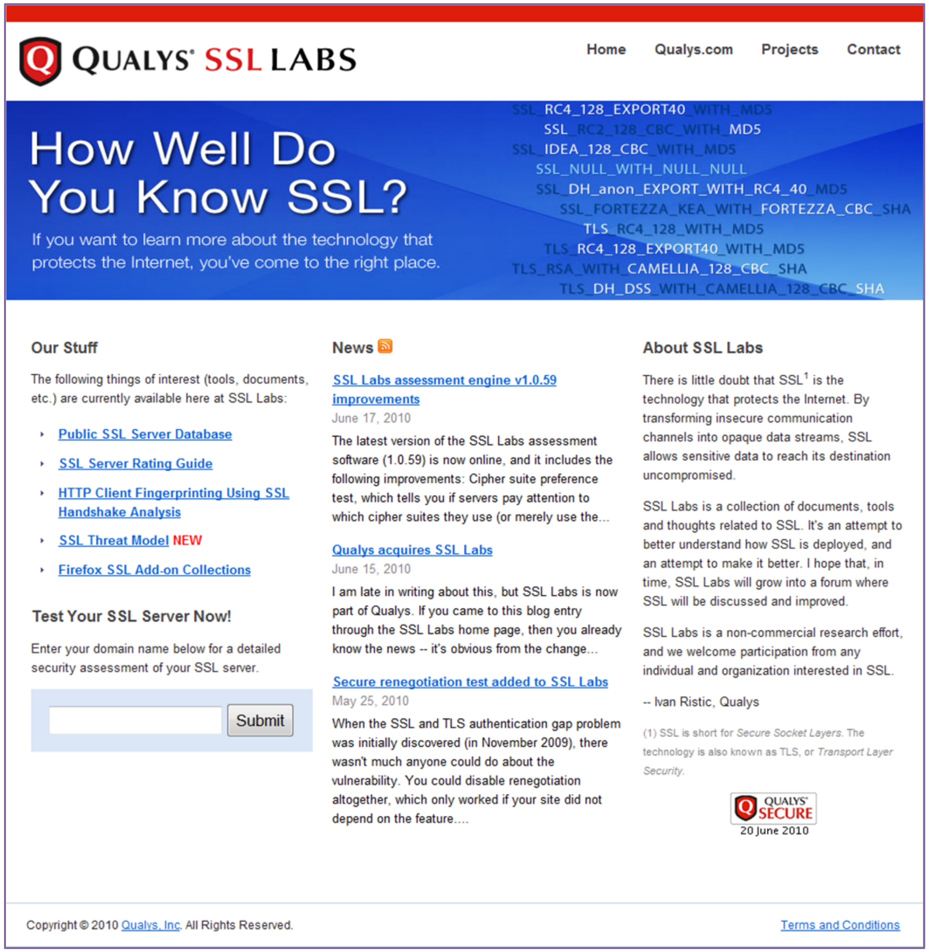
SSL Labs

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

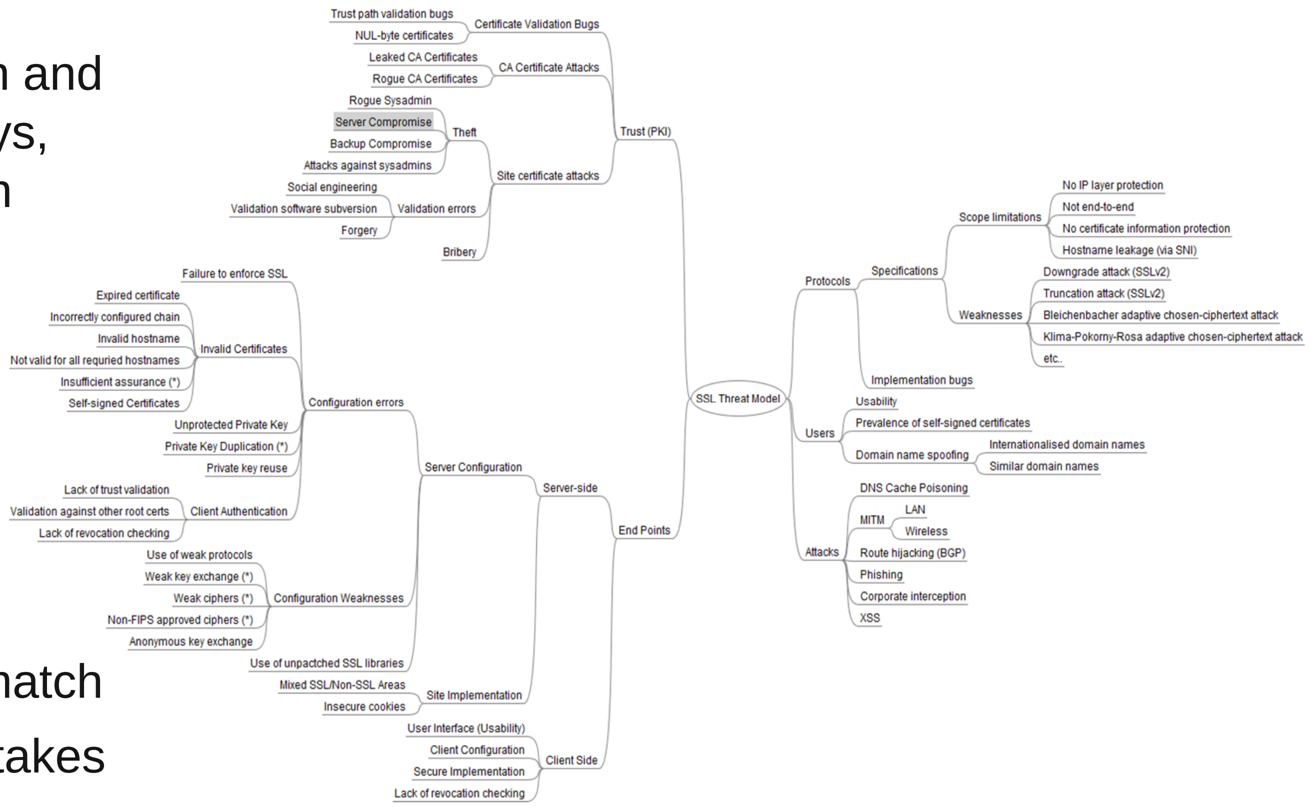
SSL ~~Threat~~ Fail Model

How can SSL fail?

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

Principal issues:

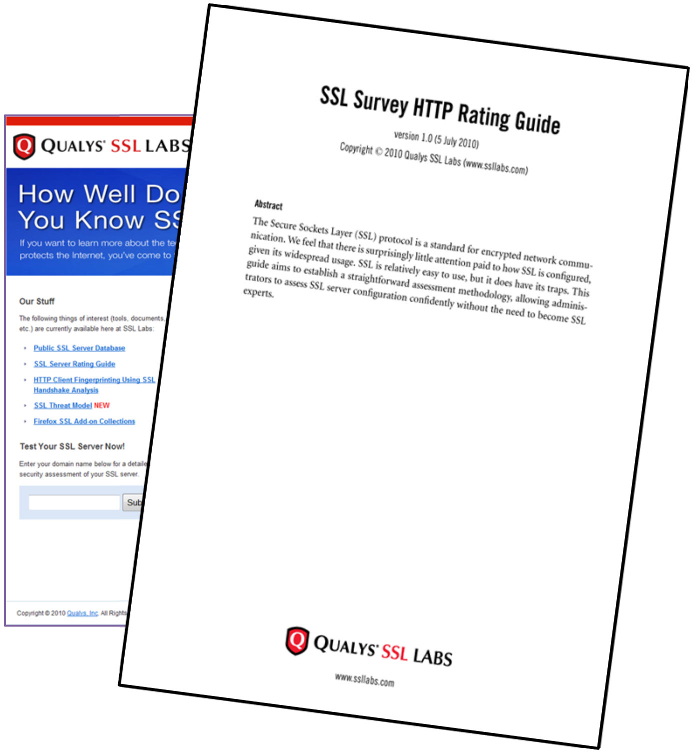
- Implementation flaws
- MITM
- Usability issues
- Impedance mismatch
- Deployment mistakes
- PKI trust challenges



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.

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

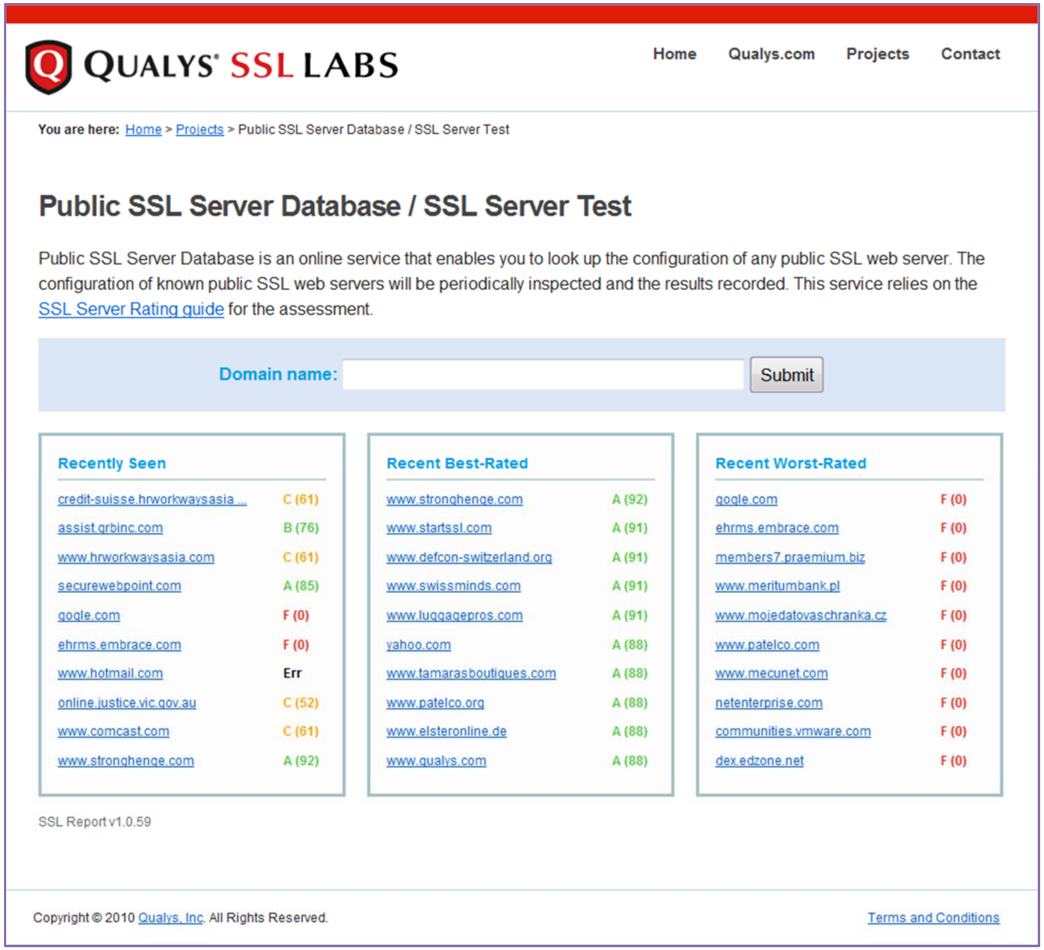
Online SSL Assessment Overview

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.

Recently Seen	
credit-suisse.hrworkwaysasia ...	C (61)
assist.qrbinc.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

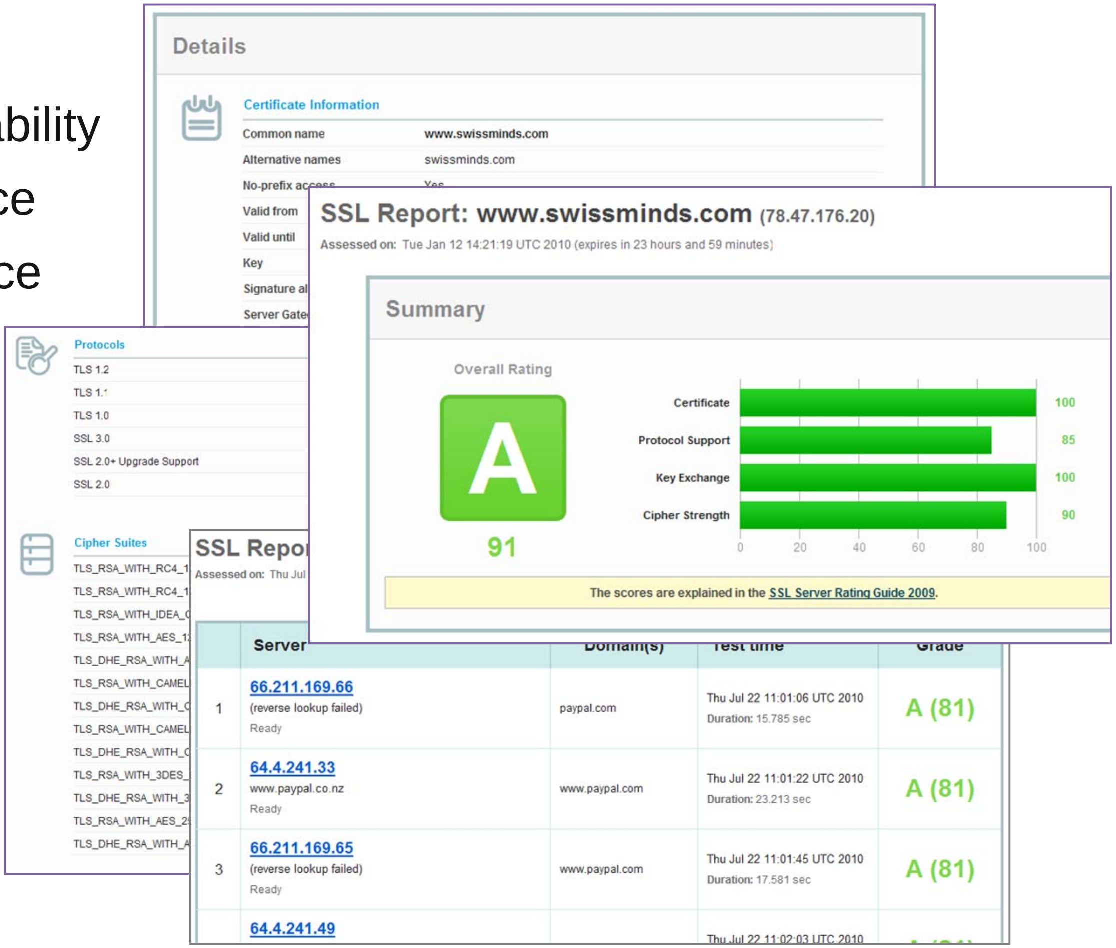
SSL Assessment Details

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 Repo

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	

Part IV:

SSL Configuration Surveys

Global SSL Surveys

In our first global survey, in 2010:

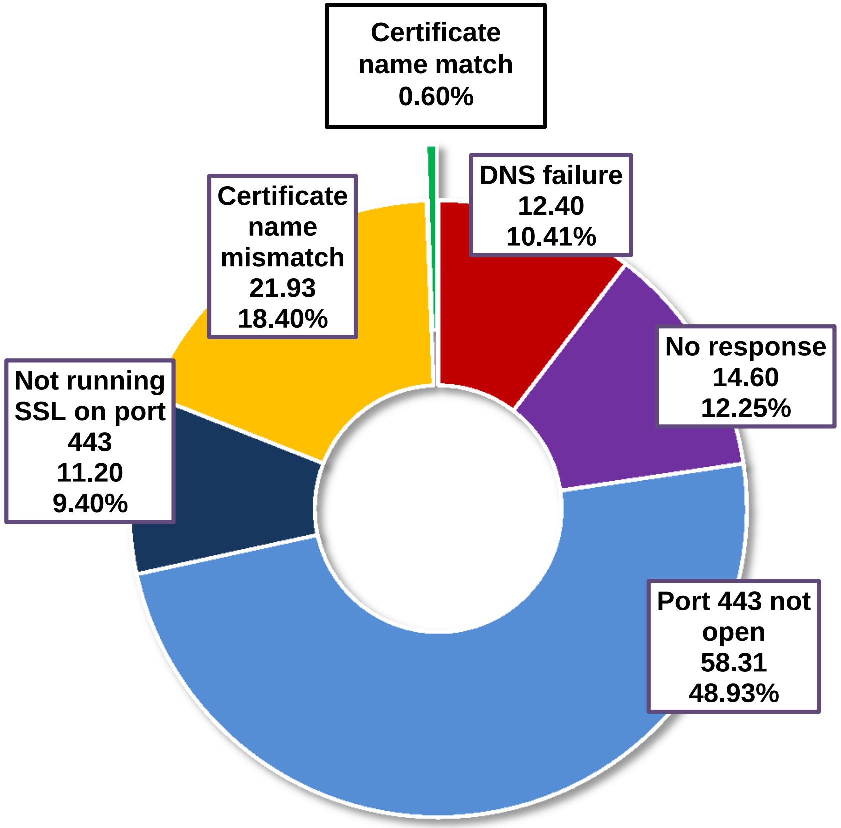
- We looked at 119 million domain name registrations
- Also examined the Alexa’s top 1m domain names
- Arrived to about 900,000 server to assess
- About **600,000 were valid** and were used in the survey

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**

ELECTRONIC FRONTIER FOUNDATION

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:

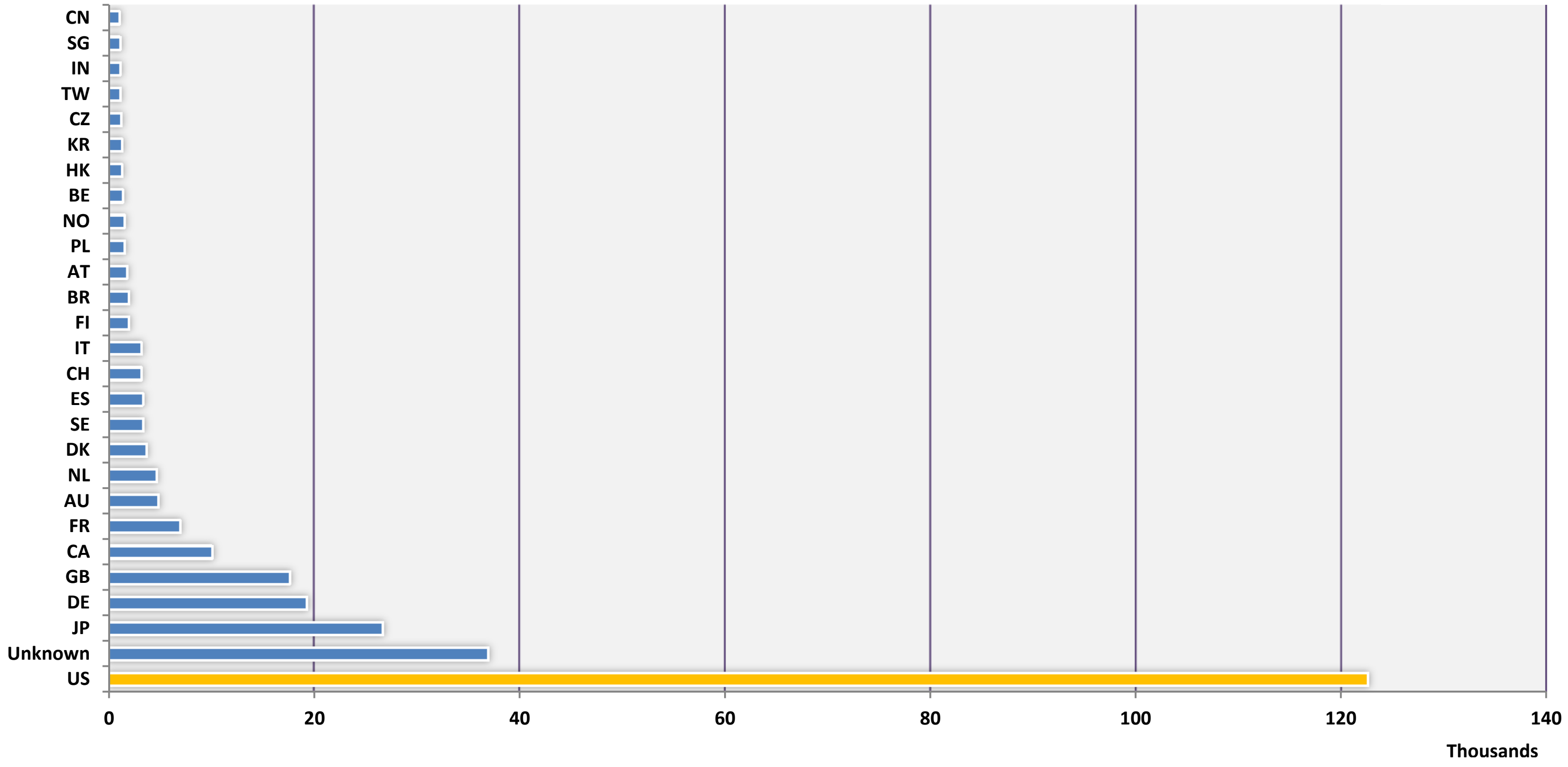
- Start with the top 1M popular sites from Alexa
- And with 1.4m valid SSL sites globally from SSL Observatory
- Cross-reference to arrive to **327,476** SSL sites
- Accept **248,161** sites into the survey

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:

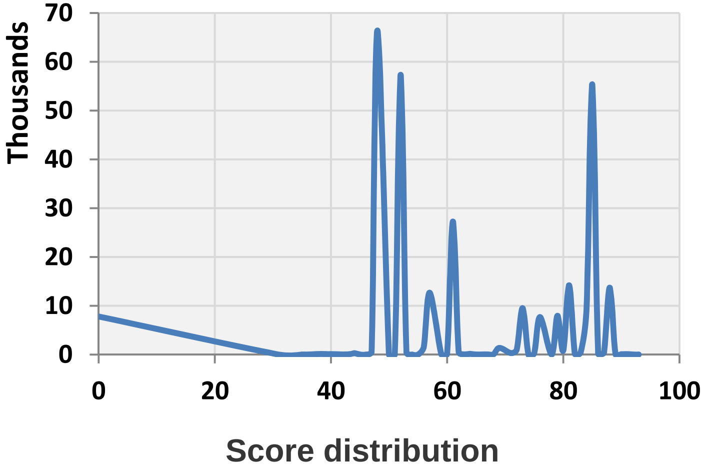


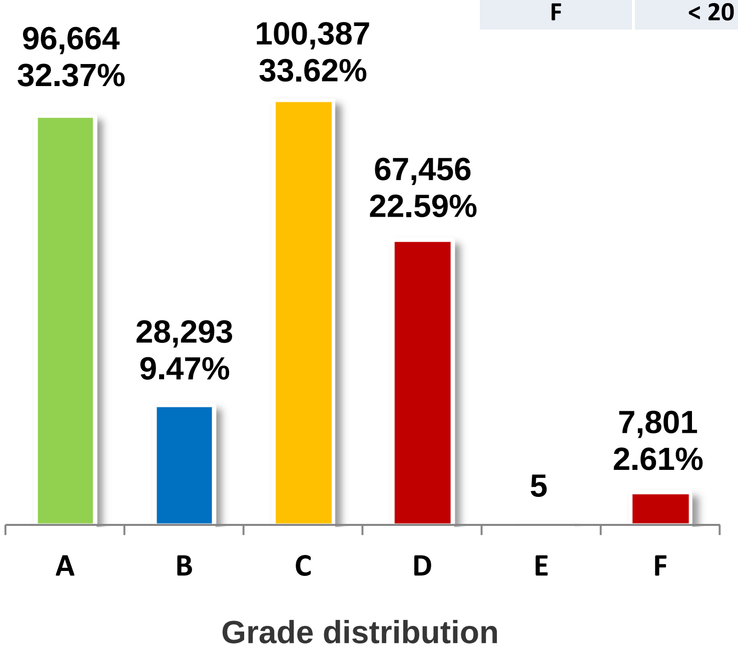
SSL Labs Grade Distribution

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



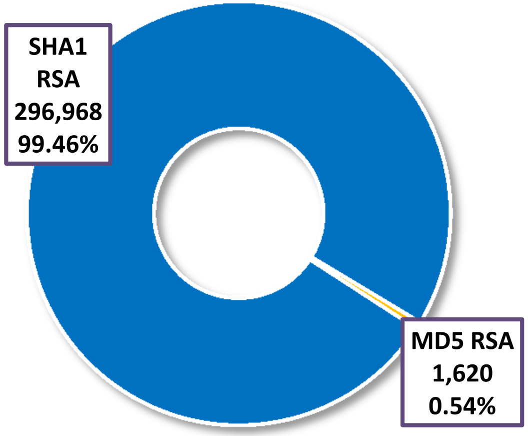


HITBSECCONF2011 AMSTERDAM

Certificates

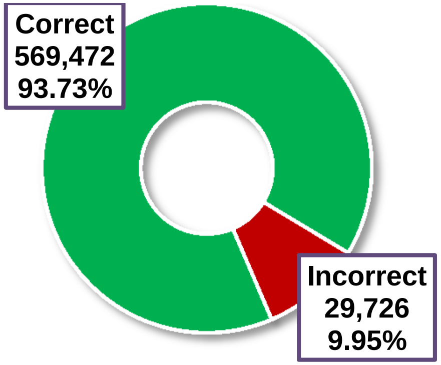
Virtually all trusted certificates use **RSA** keys; **only 9 DSA** keys

- 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

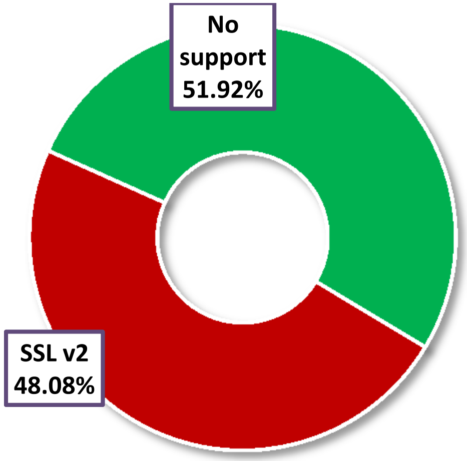
Key length	Certificates seen
512	559
1024	170,423
2048	125,333
4096	2,108
8192	3



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)

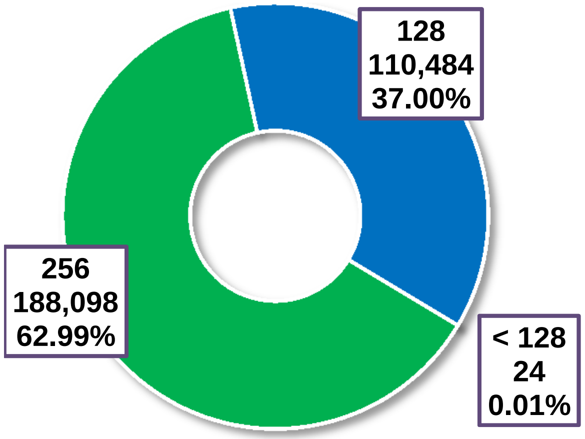


Protocol	Support	Best protocol
SSL v2.0	143,591	110
SSL v3.0	298,078	5,205
TLS v1.0	293,286	292,366
TLS v1.1	916	854
TLS v1.2	69	69

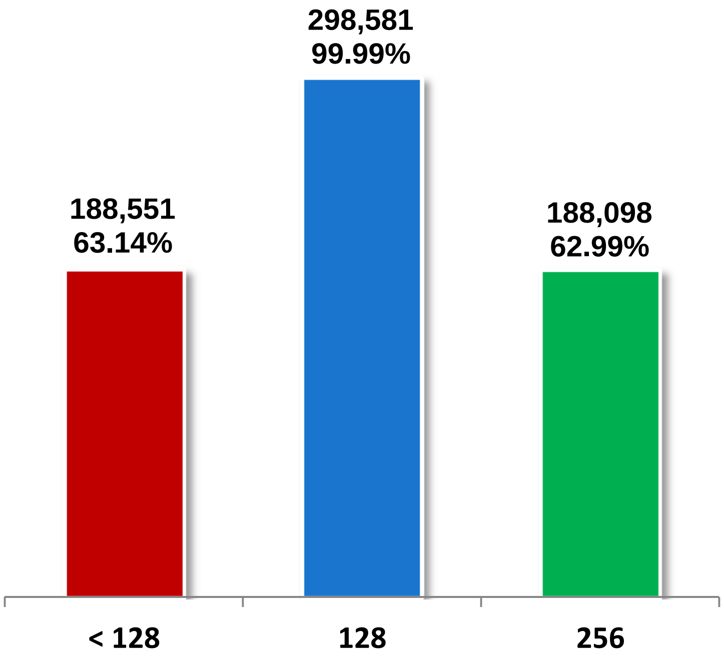
Cipher Strength

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

- But there is also wide support for weak ciphers

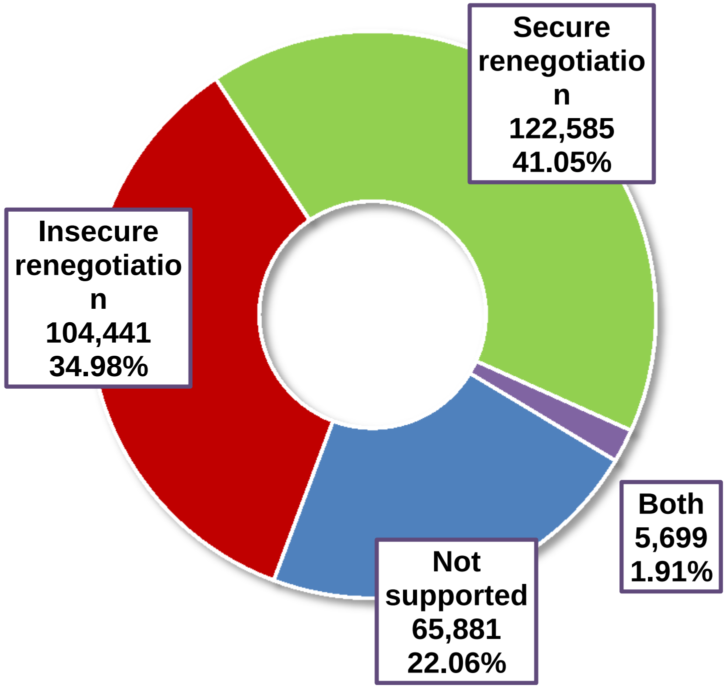


Best cipher strength support



Cipher strength support

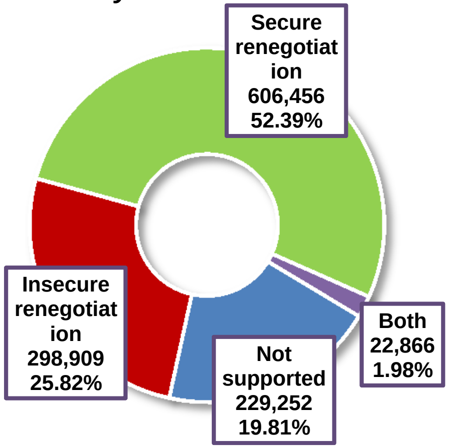
Secure and Insecure Renegotiation



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

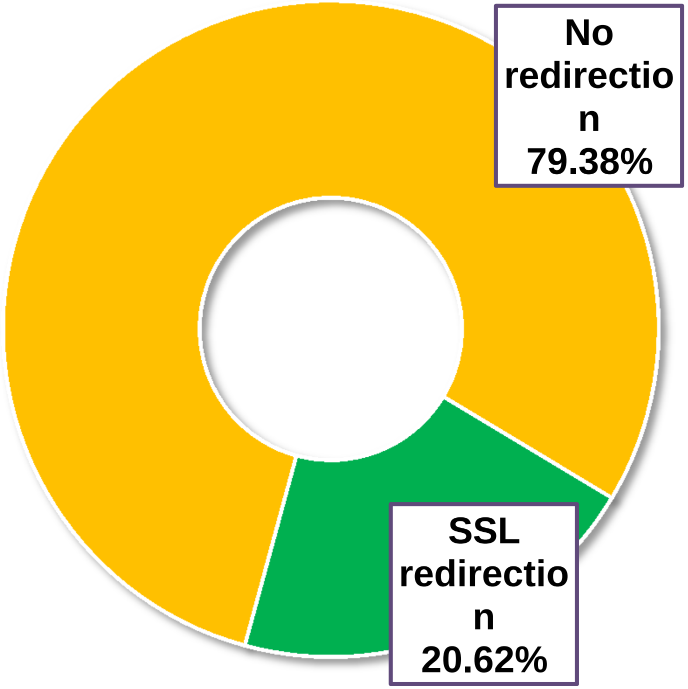
Basics

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*



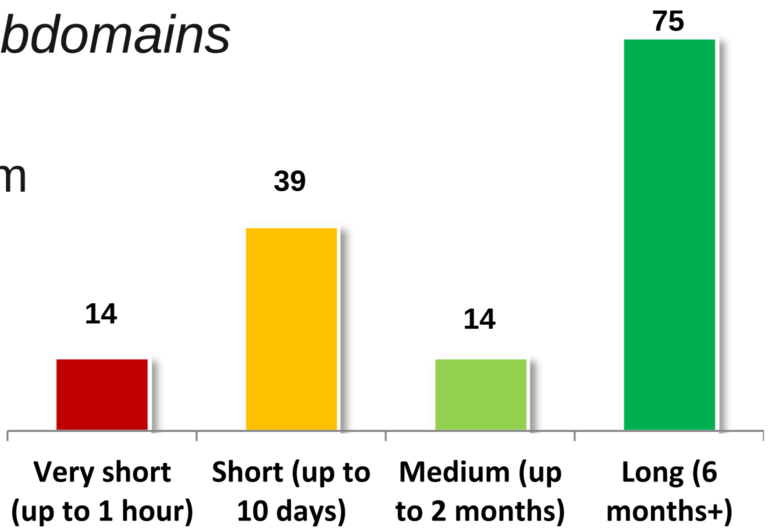
Strict Transport Security

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



HITBSECCONF2011 AMSTERDAM

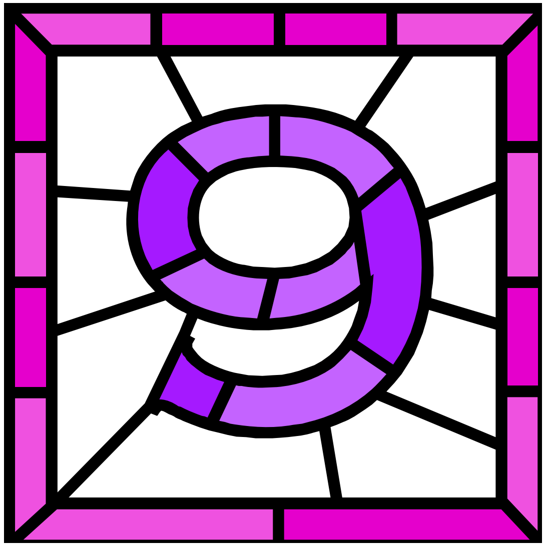
State of the art protection

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**



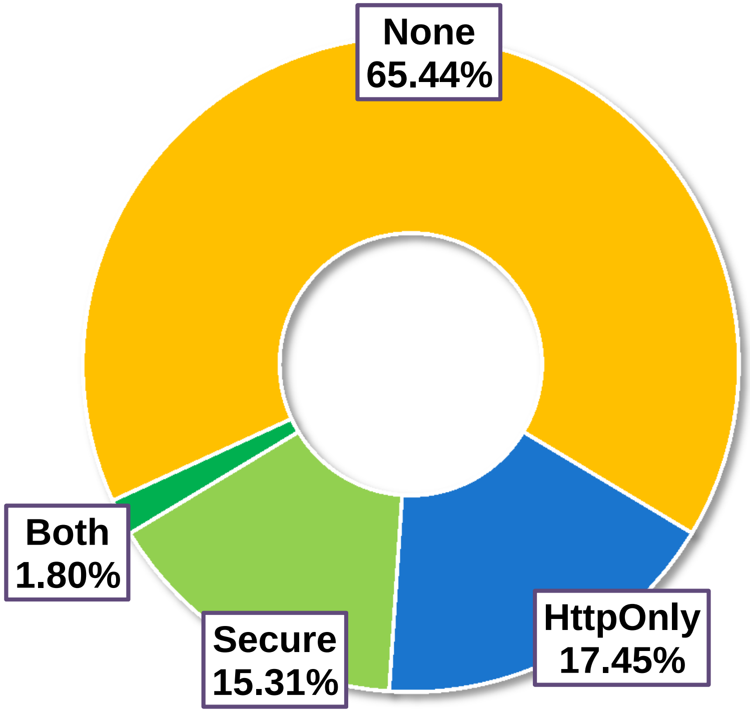
Thus:

- 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**

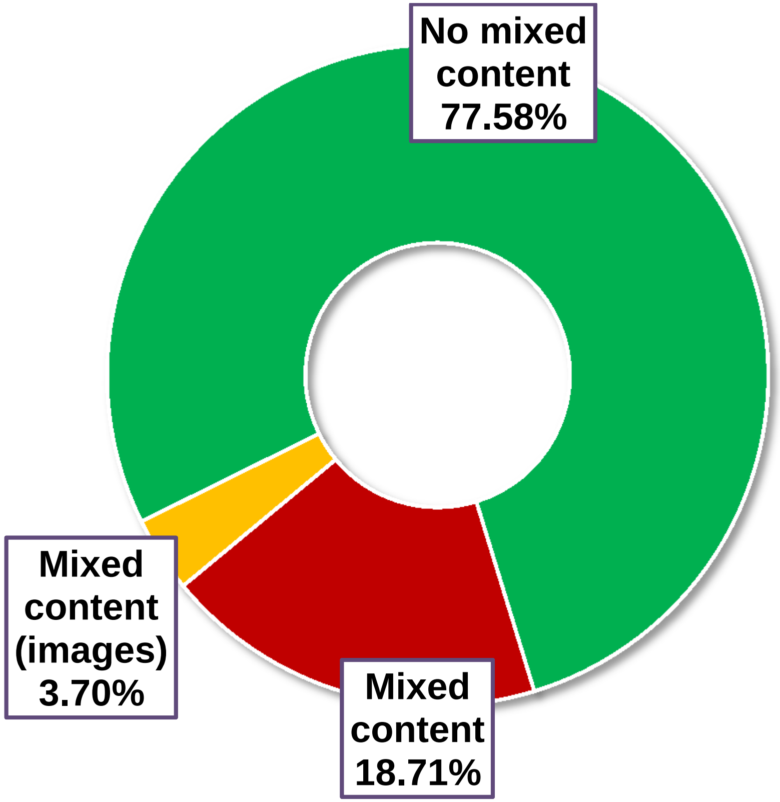


HITBSECCONF2011 AMSTERDAM

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

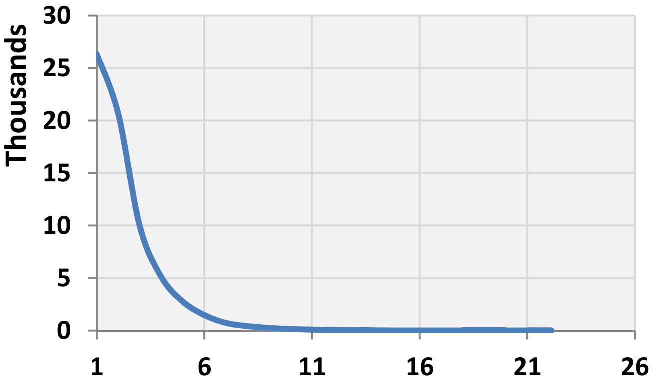


Distribution of Trust

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…

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

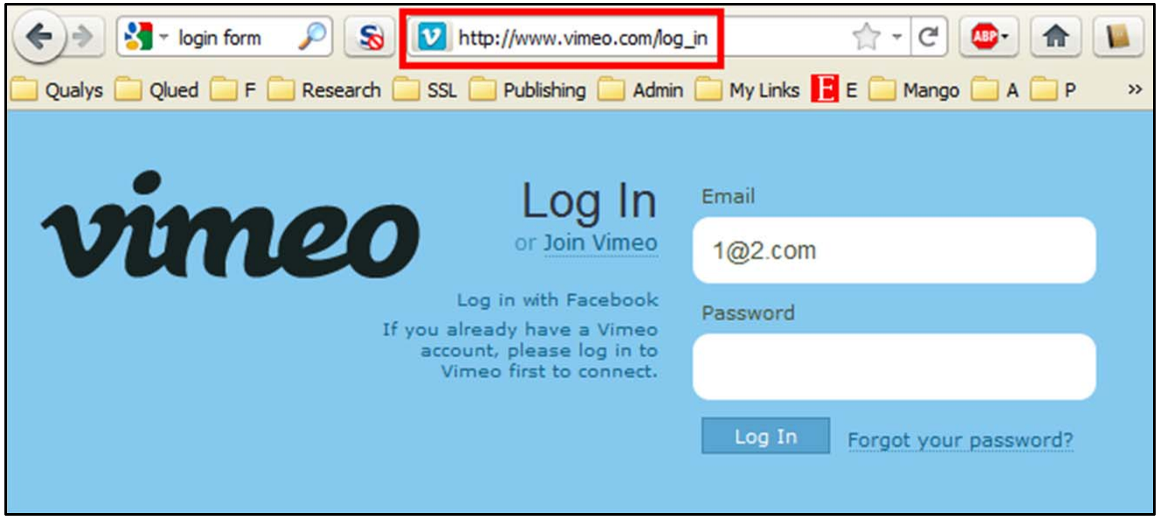


HITBSECCONF2011 AMSTERDAM

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
- Less than half of forms is 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

QUALYS®

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