Breaking SSL

Why leave to others what you can do yourself?

By Ivan Ristic

SSL LABS

Who is Ivan Ristic? **1)** ModSecurity (open source web application firewall), **2)** *Apache Security* (O'Reilly, 2005), **3)** SSL Labs, **4)** *ModSecurity Handbook* (Feisty Duck, 2010), **5)** Director of Engineering, WAF and SSL @ Qualys.

SSL LABS

SSL and TLS

1) Very well designed
2) Very widely used
3) Security backbone of the Internet
4) Secure on its own
5) Easily compromised when used with HTTP
6) Few people pay attention to it

Why was SSL in the news recently?

2008 – MD5 collision and rogue CA generation
(Sotirov et al.)

2009 – NUL byte certificate attacks
(Moxie & Kaminsky separately)

2009 – Authentication Gap
(Marsh Ray)

(And a couple of other, smaller, issues. Did someone mention SSL VPNs?)

Moxie Marlinspike

If you need convincing how easy it is to defeat SSL, look for Moxie's ***sslstrip*** *and* ***sslsniff*** *tools.*

SSL LABS

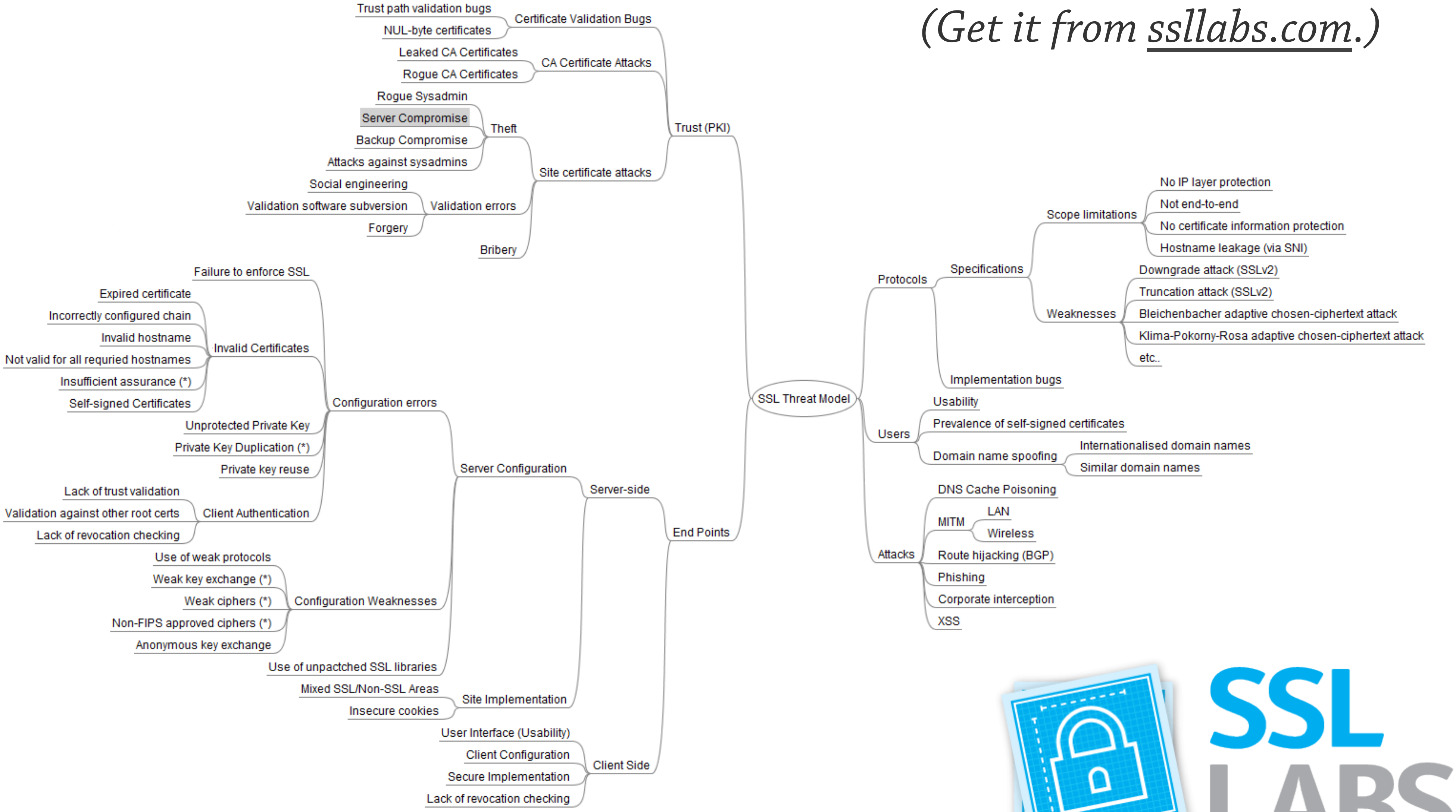
Principal Active Threats

Man-in-the-middle (MITM) attacks:

- Implementation flaws
- Rogue CA certificates
- Rogue certificate authorities
- Usability issues
- App and configuration vulnerabilities

SSL Threat Model

(Get it from ssllabs.com.)

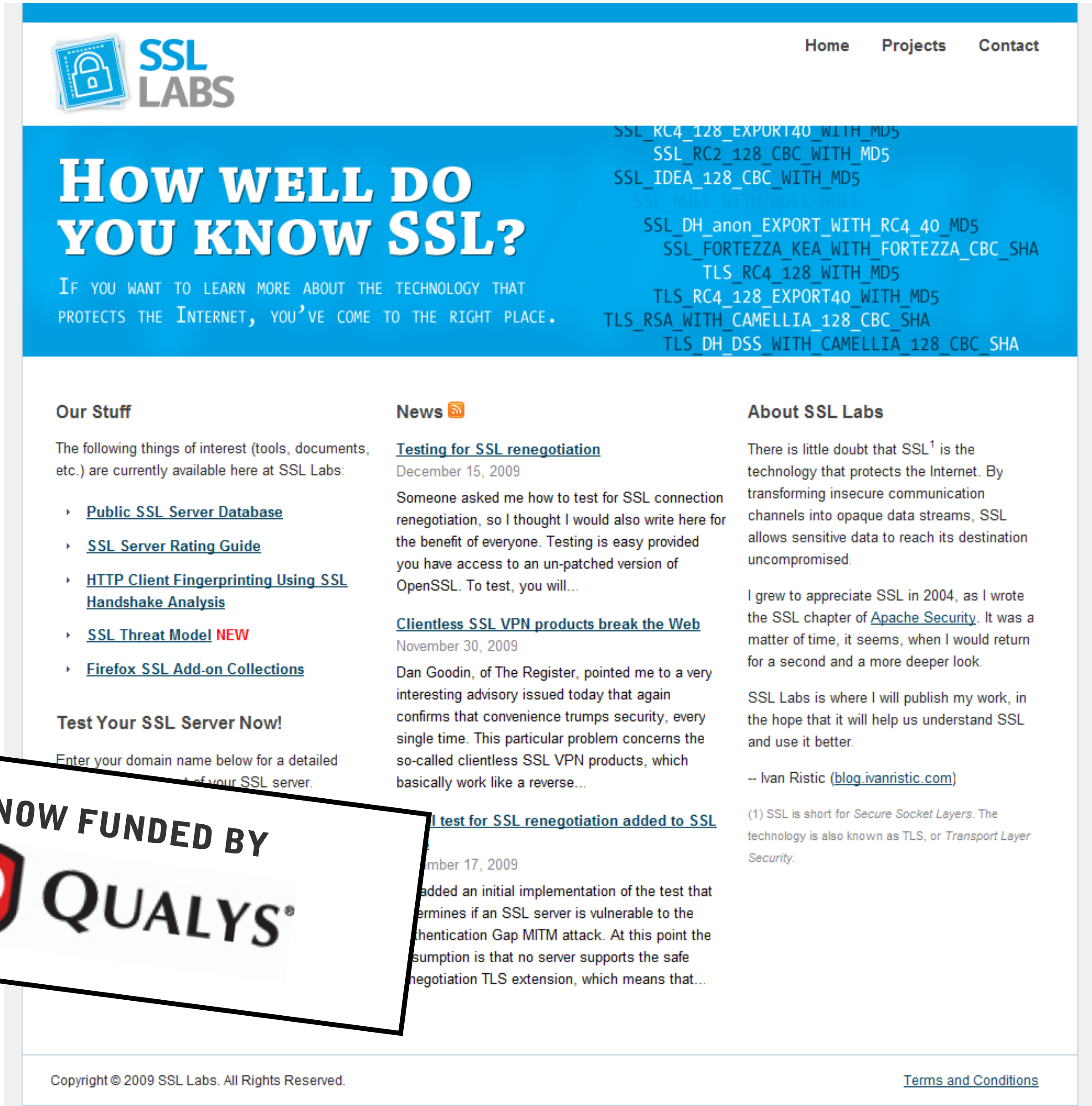


- SSL Threat Model
  - Trust (PKI)
    - Certificate Validation Bugs
      - Trust path validation bugs
      - NUL-byte certificates
    - CA Certificate Attacks
      - Leaked CA Certificates
      - Rogue CA Certificates
    - Site certificate attacks
      - Theft
        - Rogue Sysadmin
        - Server Compromise
        - Backup Compromise
        - Attacks against sysadmins
      - Social engineering
      - Validation errors
        - Validation software subversion
        - Forgery
      - Bribery
  - End Points
    - Server-side
      - Server Configuration
        - Configuration errors
          - Failure to enforce SSL
          - Invalid Certificates
            - Expired certificate
            - Incorrectly configured chain
            - Invalid hostname
            - Not valid for all requried hostnames
            - Insufficient assurance (*)
            - Self-signed Certificates
          - Unprotected Private Key
          - Private Key Duplication (*)
          - Private key reuse
          - Client Authentication
            - Lack of trust validation
            - Validation against other root certs
            - Lack of revocation checking
        - Configuration Weaknesses
          - Use of weak protocols
          - Weak key exchange (*)
          - Weak ciphers (*)
          - Non-FIPS approved ciphers (*)
          - Anonymous key exchange
        - Use of unpactched SSL libraries
      - Site Implementation
        - Mixed SSL/Non-SSL Areas
        - Insecure cookies
    - Client Side
      - User Interface (Usability)
      - Client Configuration
      - Secure Implementation
      - Lack of revocation checking
  - Protocols
    - Specifications
      - Scope limitations
        - No IP layer protection
        - Not end-to-end
        - No certificate information protection
        - Hostname leakage (via SNI)
      - Weaknesses
        - Downgrade attack (SSLv2)
        - Truncation attack (SSLv2)
        - Bleichenbacher adaptive chosen-ciphertext attack
        - Klima-Pokorny-Rosa adaptive chosen-ciphertext attack
        - etc..
    - Implementation bugs
  - Users
    - Usability
    - Prevalence of self-signed certificates
    - Domain name spoofing
      - Internationalised domain names
      - Similar domain names
  - Attacks
    - DNS Cache Poisoning
    - MITM
      - LAN
      - Wireless
    - Route hijacking (BGP)
    - Phishing
    - Corporate interception
    - XSS

SSL Labs

Dedicated to SSL/TLS research.

Lots of interesting projects.



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
t of your SSL server.

News

Testing for SSL renegotiation
December 15, 2009

Someone asked me how to test for SSL connection renegotiation, so I thought I would also write here for the benefit of everyone. Testing is easy provided you have access to an un-patched version of OpenSSL. To test, you will...

Clientless SSL VPN products break the Web
November 30, 2009

Dan Goodin, of The Register, pointed me to a very interesting advisory issued today that again confirms that convenience trumps security, every single time. This particular problem concerns the so-called clientless SSL VPN products, which basically work like a reverse...

l test for SSL renegotiation added to SSL
mber 17, 2009

added an initial implementation of the test that
ermines if an SSL server is vulnerable to the
hentication Gap MITM attack. At this point the
sumption is that no server supports the safe
negotiation TLS extension, which means that...

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.

I grew to appreciate SSL in 2004, as I wrote the SSL chapter of Apache Security. It was a matter of time, it seems, when I would return for a second and a more deeper look.

SSL Labs is where I will publish my work, in the hope that it will help us understand SSL and use it better.

-- Ivan Ristic (blog.ivanristic.com)

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

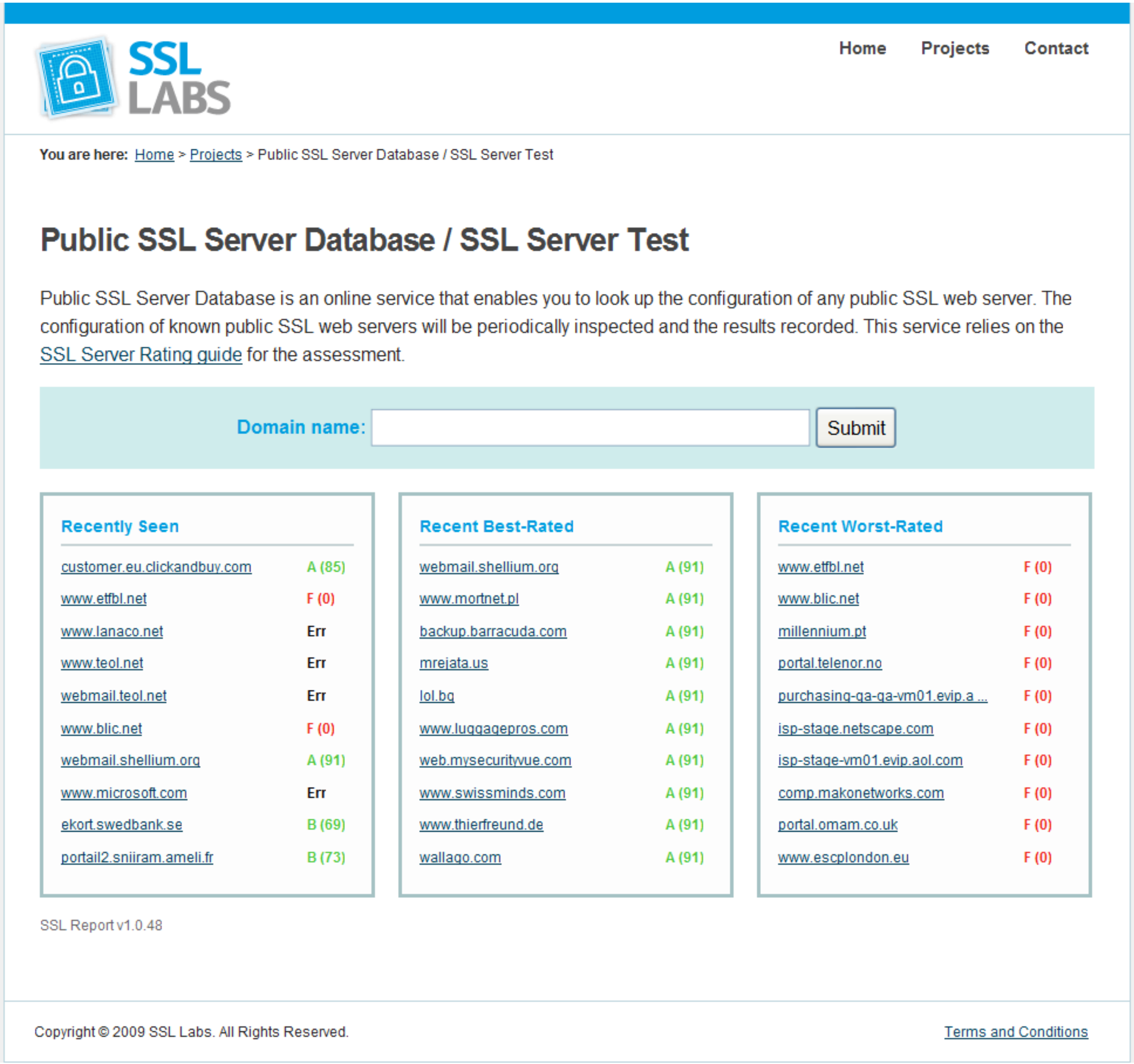
Copyright © 2009 SSL Labs. All Rights Reserved.

Terms and Conditions

NOW FUNDED BY QUALYS®

SSL Server Assessment

The most popular part of the site is the free SSL Sever Assessment tool.



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	
customer.eu.clickandbuy.com	A (85)
www.etfbl.net	F (0)
www.lanaco.net	Err
www.teol.net	Err
webmail.teol.net	Err
www.blic.net	F (0)
webmail.shellium.org	A (91)
www.microsoft.com	Err
ekort.swedbank.se	B (69)
portail2.sniiram.ameli.fr	B (73)

Recent Best-Rated	
webmail.shellium.org	A (91)
www.mortnet.pl	A (91)
backup.barracuda.com	A (91)
mrejata.us	A (91)
lol.bg	A (91)
www.luggagepros.com	A (91)
web.mysecurityvue.com	A (91)
www.swissminds.com	A (91)
www.thierfreund.de	A (91)
wallago.com	A (91)

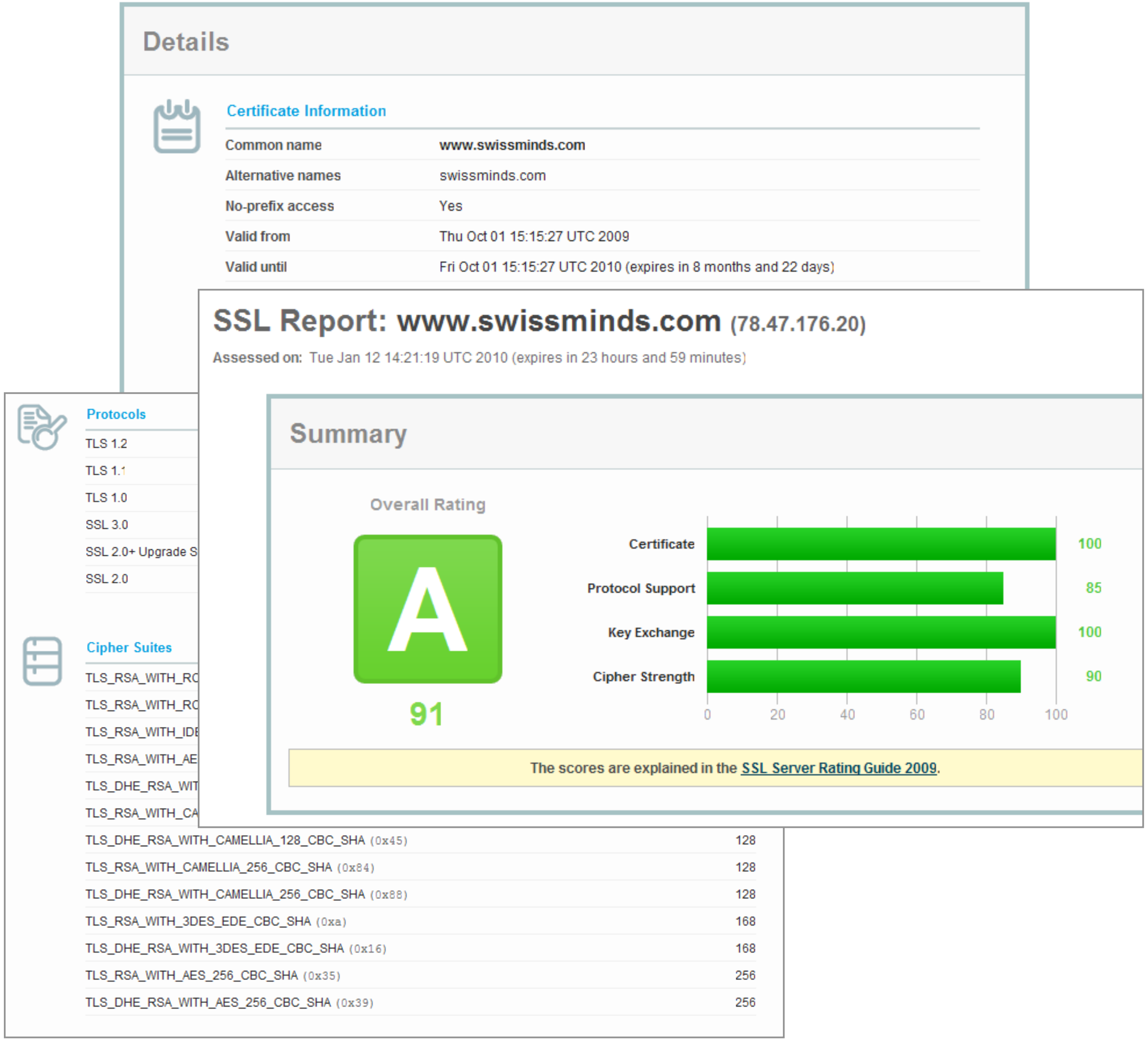
Recent Worst-Rated	
www.etfbl.net	F (0)
www.blic.net	F (0)
millennium.pt	F (0)
portal.telenor.no	F (0)
purchasing-qa-qa-vm01.evip.a ...	F (0)
isp-stage.netscape.com	F (0)
isp-stage-vm01.evip.aol.com	F (0)
comp.makonetworks.com	F (0)
portal.omam.co.uk	F (0)
www.escplondon.eu	F (0)

SSL Report v1.0.48

Terms and Conditions

SSL Server Assessment

The most comprehensive assessment available.



Details

Certificate Information

Common name	**www.swissminds.com**
Alternative names	swissminds.com
No-prefix access	Yes
Valid from	Thu Oct 01 15:15:27 UTC 2009
Valid until	Fri Oct 01 15:15:27 UTC 2010 (expires in 8 months and 22 days)

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)

Protocols

TLS 1.2
TLS 1.1
TLS 1.0
SSL 3.0
SSL 2.0+ Upgrade S
SSL 2.0

Cipher Suites

TLS_RSA_WITH_RC	
TLS_RSA_WITH_RC	
TLS_RSA_WITH_IDE	
TLS_RSA_WITH_AE	
TLS_DHE_RSA_WIT	
TLS_RSA_WITH_CA	
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA (0x45)	128
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (0x84)	128
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA (0x88)	128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	168
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (0x16)	168
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x39)	256

Summary

Overall Rating

A

91

Certificate	100
Protocol Support	85
Key Exchange	100
Cipher Strength	90

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

SSL Labs projects

- SSL Server Security Rating Guide
- SSL Server Security Online Assessment
- SSL Threat Model
- Passive SSL Client Fingerprinting tools

Planned:

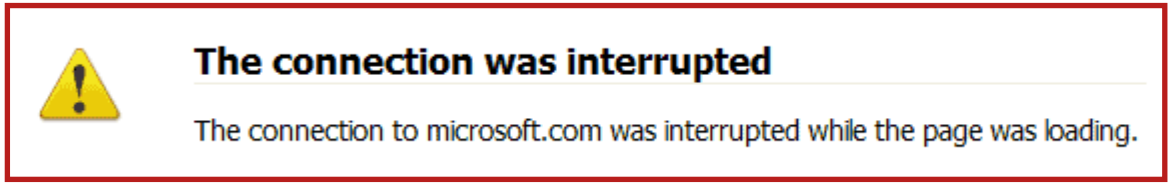
- SSL Client Capabilities Database
- SSL Usage Tracking
- SSL Internet Survey (in progress!)

Feature Presentation

SSL Deployment Mistakes

1 Inconsistent DNS configuration

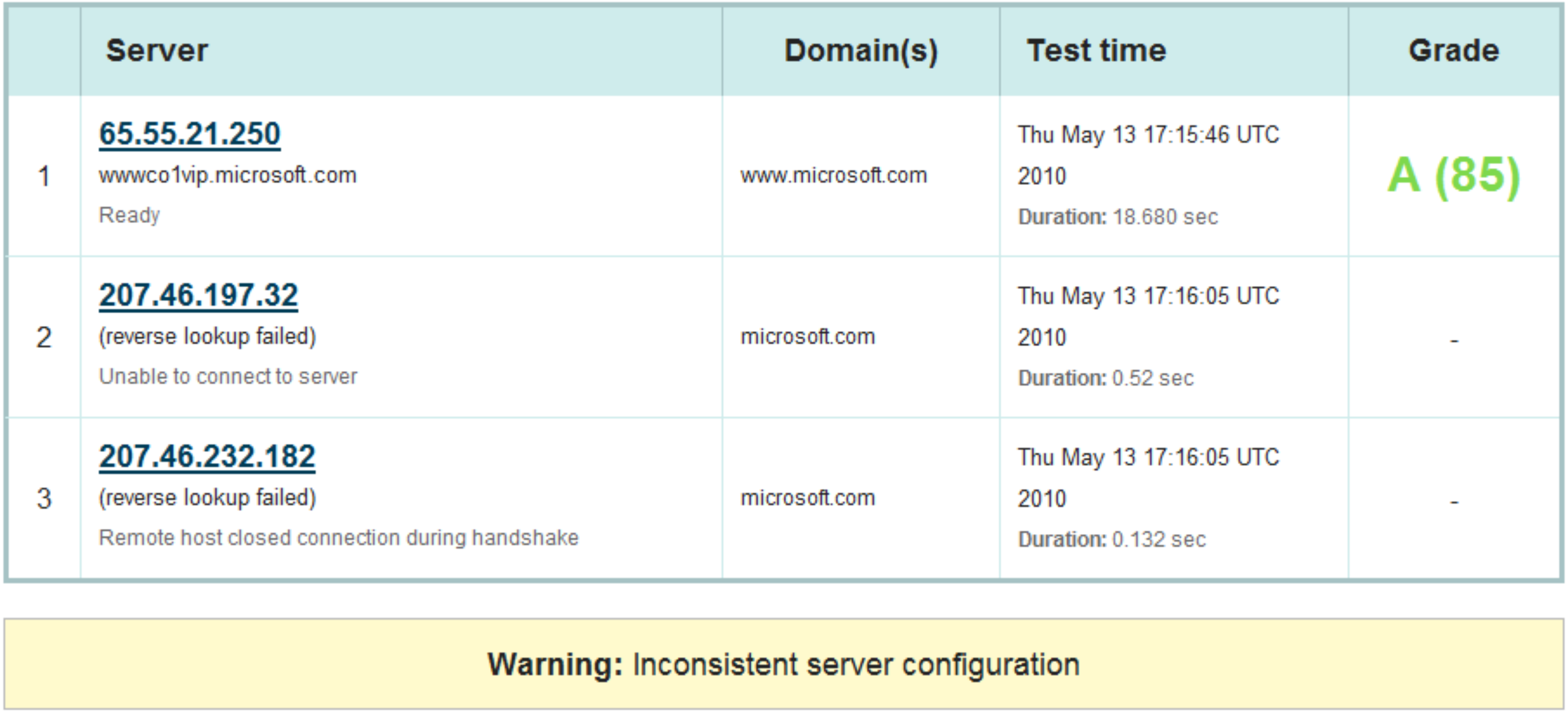
- Your *www.example.com* address points to one web server, while *example.com* points to another
- It surprising how many high-profile sites suffer from this problem



The connection was interrupted

The connection to microsoft.com was interrupted while the page was loading.

What does *microsoft.com* look like?



	Server	Domain(s)	Test time	Grade
1	65.55.21.250 wwwco1vip.microsoft.com Ready	www.microsoft.com	Thu May 13 17:15:46 UTC 2010 **Duration:** 18.680 sec	A (85)
2	207.46.197.32 (reverse lookup failed) Unable to connect to server	microsoft.com	Thu May 13 17:16:05 UTC 2010 **Duration:** 0.52 sec	-
3	207.46.232.182 (reverse lookup failed) Remote host closed connection during handshake	microsoft.com	Thu May 13 17:16:05 UTC 2010 **Duration:** 0.132 sec	-

Warning: Inconsistent server configuration

2 Different sites on 80 and 443

- You type ***https://www.ssllabs.com*** and expect to see the same site as on ***http://www.ssllabs.com***
- This is the fate of every single site that uses virtual hosting
- Would you mind if questionable content appeared on ***https://www.yourcompany.com***?

3 Self-signed certificates

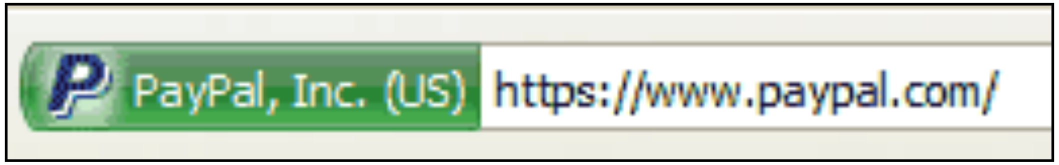
- Self-signed certificates are spoiling SSL security for all of us
- They are insecure
- Prevalent on intranets; teaching users to ignore warnings
- It's cheaper to buy a certificate than support a self-signed one

This Connection is Untrusted

You have asked Firefox to connect securely to **www.pen**
connection is secure.

4 Not using EV certificates

- High-value web sites will often be a target of phishing attacks
- It is easy to mistype and end up at the wrong place, even if you are en experienced user
- The green glow helps ensure your users that they are in the *right* place

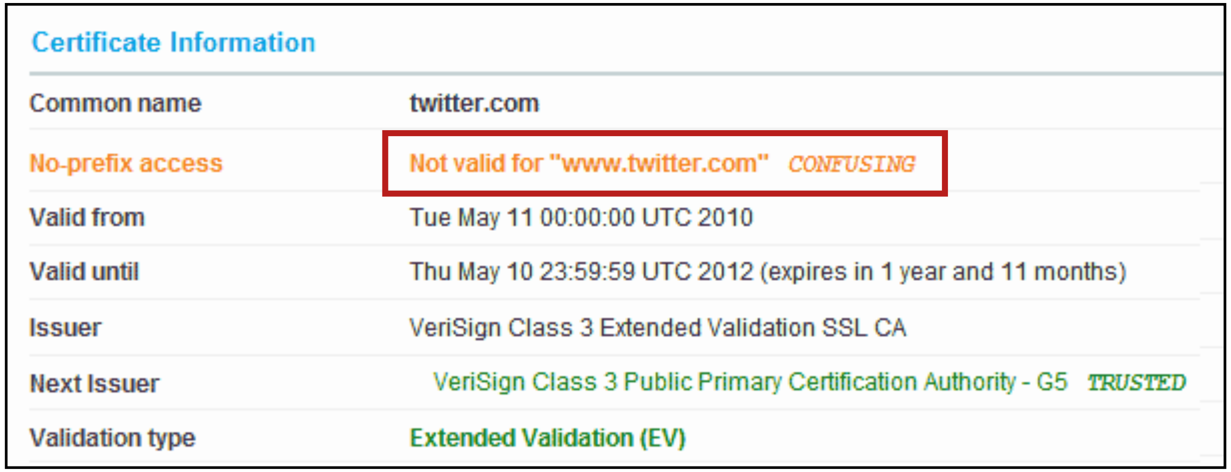

PayPal, Inc. (US) https://www.paypal.com/

5 Badly configured SSL servers

- Many deployments rely on default settings, but they are often wrong and possibly insecure
- Weak protocols and cipher suites
- Performance issues
- Unpatched software
- Easy to fix – use the online assessment tool and tune configuration until satisfactory

6 Using incomplete certificates

- You type ***https://ssllabs.com*** and expect to see the same site as on ***https://www.ssllabs.com***
- Very confusing for users



Certificate Information

Common name	twitter.com
No-prefix access	Not valid for "www.twitter.com" *CONFUSING*
Valid from	Tue May 11 00:00:00 UTC 2010
Valid until	Thu May 10 23:59:59 UTC 2012 (expires in 1 year and 11 months)
Issuer	VeriSign Class 3 Extended Validation SSL CA
Next Issuer	VeriSign Class 3 Public Primary Certification Authority - G5 *TRUSTED*
Validation type	Extended Validation (EV)

7 Mixing SSL and plain-text on a site

- Difficult to implement securely
- Leads to user session compromise
- Trivial for the man in the middle to use *sslstrip* to convert HTTPS links to HTTP
- Even redirections problematic – only secure bookmarks work

8 Using SSL for “important” bits

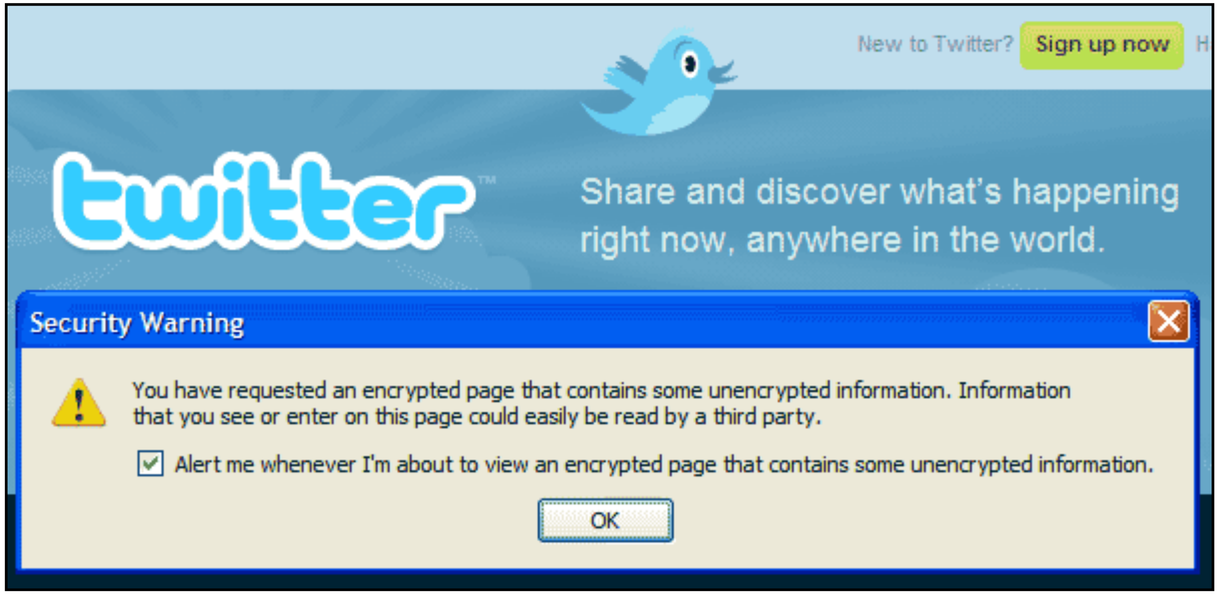
- Some sites will use SSL to protect authentication and nothing else
- They are vulnerable to session hijacking
- Some even allow users to change password without knowing the current one

9 Not using secure cookies

- Secure cookies are transmitted only over SSL
- Even if your site does not use plain-text anywhere (and does not even run on port 80), browsers can be tricked into revealing non-secure cookies by a MITM attacker
- You *must* use secure cookies everywhere

10 Mixed page content

- A single plain-text link is enough to compromise the entire "secure" SSL site


New to Twitter?
Sign up now
twitter
Share and discover what's happening right now, anywhere in the world.
Security Warning
OK

You have requested an encrypted page that contains some unencrypted information. Information that you see or enter on this page could easily be read by a third party.

☑ Alert me whenever I'm about to view an encrypted page that contains some unencrypted information.

Message for today

SSL is a rare application security area where we can make things virtually 100% secure, with relatively small effort. **Why not get it right?**

Thank you!

The slides are available for download
from https://www.ssllabs.com