

# Breaking SSL

**Why leave to others what  
you can do yourself?**

By Ivan Ristic

**Who is Ivan Ristic?**      1) ModSecurity  
(open source web application firewall), 2) *Apache Security* (O'Reilly, 2005), 3) SSL Labs (research and assessment platform), 4) *ModSecurity Handbook* (Feisty Duck, 2010)

# 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.*



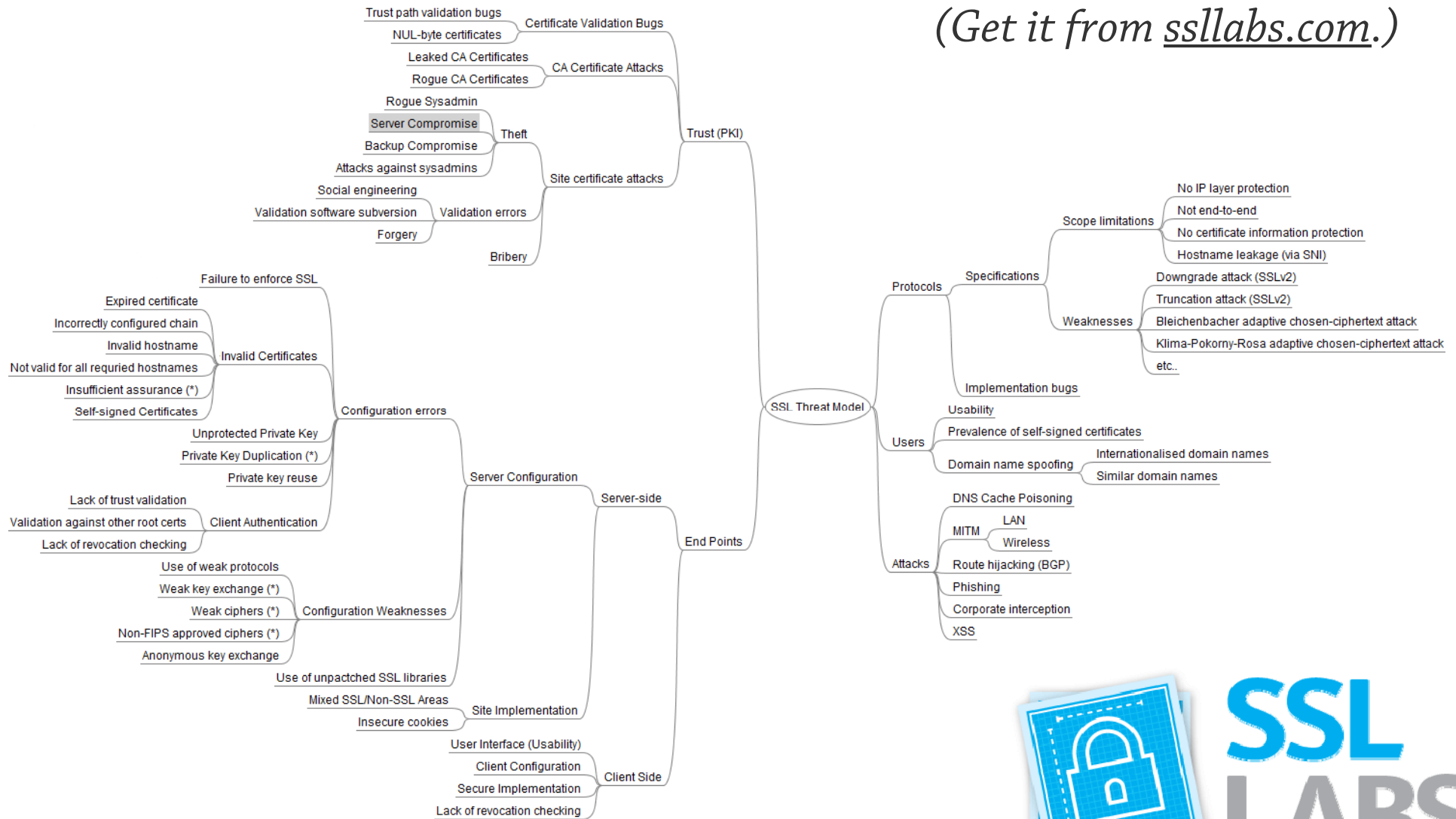
# Principal Active Threats

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

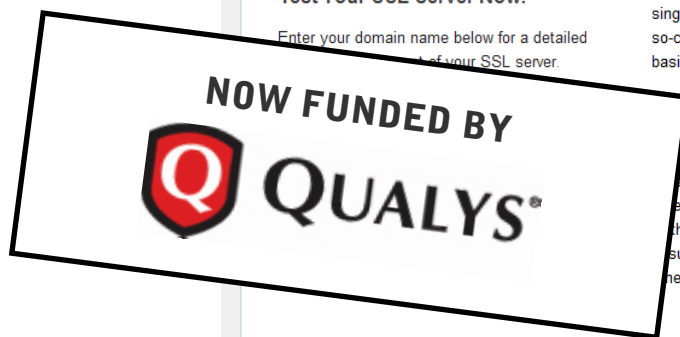
- Rogue CA certificates
- Implementation flaws
- App and configuration vulnerabilities
- Usability issues
- **Rogue certificate authorities!**

# SSL Threat Model

(Get it from [ssllabs.com](https://ssllabs.com).)



**SSL Labs**  
*Dedicated to  
SSL/TLS research.  
Lots of interesting  
projects.*



Home 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\_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 report 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...

**Test for SSL renegotiation added to SSL Server Rating Guide**  
November 17, 2009

I have recently added an initial implementation of the test that determines if an SSL server is vulnerable to the Authentication Gap MITM attack. At this point the assumption is that no server supports the safe renegotiation TLS extension, which means that...

**About SSL Labs**

There is little doubt that SSL<sup>1</sup> 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](http://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](#)



# SSL Server Assessment

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

The screenshot shows the SSL Labs website interface. At the top, there is a navigation menu with 'Home', 'Projects', and 'Contact'. The main heading is 'Public SSL Server Database / SSL Server Test'. Below this, there is a description of the service and a search form with a 'Domain name:' input field and a 'Submit' button. Three columns of results are displayed: 'Recently Seen', 'Recent Best-Rated', and 'Recent Worst-Rated'. Each column lists domain names with their corresponding SSL ratings.

**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	
<a href="#">customer.eu.clickandbuy.com</a>	A (85)	<a href="#">webmail.shellium.org</a>	A (91)	<a href="#">www.etfbl.net</a>	F (0)
<a href="#">www.etfbl.net</a>	F (0)	<a href="#">www.mortnet.pl</a>	A (91)	<a href="#">www.blic.net</a>	F (0)
<a href="#">www.lanaco.net</a>	Err	<a href="#">backup.barracuda.com</a>	A (91)	<a href="#">millennium.pt</a>	F (0)
<a href="#">www.teol.net</a>	Err	<a href="#">mrejata.us</a>	A (91)	<a href="#">portal.telenor.no</a>	F (0)
<a href="#">webmail.teol.net</a>	Err	<a href="#">lol.bg</a>	A (91)	<a href="#">purchasing-ga-ga-vm01.evip.a...</a>	F (0)
<a href="#">www.blic.net</a>	F (0)	<a href="#">www.luqqagepros.com</a>	A (91)	<a href="#">isp-stage.netscape.com</a>	F (0)
<a href="#">webmail.shellium.org</a>	A (91)	<a href="#">web.mysecurityvue.com</a>	A (91)	<a href="#">isp-stage-vm01.evip.aol.com</a>	F (0)
<a href="#">www.microsoft.com</a>	Err	<a href="#">www.swissminds.com</a>	A (91)	<a href="#">comp.makonetworks.com</a>	F (0)
<a href="#">ekort.swedbank.se</a>	B (69)	<a href="#">www.thierfreund.de</a>	A (91)	<a href="#">portal.omam.co.uk</a>	F (0)
<a href="#">portail2.sniram.ameli.fr</a>	B (73)	<a href="#">wallaqq.com</a>	A (91)	<a href="#">www.esclondon.eu</a>	F (0)

SSL Report v1.0.48

Copyright © 2009 SSL Labs. All Rights Reserved. [Terms and Conditions](#)

# SSL Server Assessment

*The most comprehensive assessment available.*

## Details



### Certificate Information

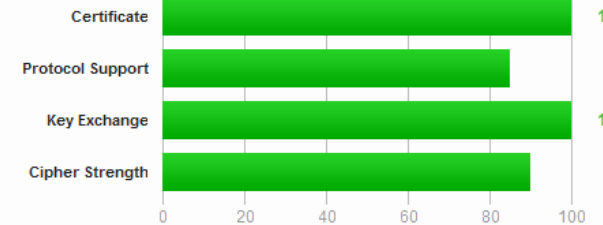
Common name	www.swissminds.com
Alternative names	swissminds.com
No-prefix access	Yes
Valid from	Thu Oct 01 15:15:27 UTC 2009
Valid until	Fri Oct 01 15:15:27 UTC 2010 (expires in 8 months and 22 days)

## 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)

## Summary

### Overall Rating



The scores are explained in the [SSL Server Rating Guide 2009](#).



### 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)
- TLS\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA (0x84)
- TLS\_DHE\_RSA\_WITH\_CAMELLIA\_256\_CBC\_SHA (0x88)
- TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (0xa)
- TLS\_DHE\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA (0x16)
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA (0x35)
- TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA (0x39)



# 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	<u>65.55.21.250</u> wwwco1vip.microsoft.com Ready	www.microsoft.com	Thu May 13 17:15:46 UTC 2010 Duration: 18.680 sec	<b>A (85)</b>
2	<u>207.46.197.32</u> (reverse lookup failed) Unable to connect to server	microsoft.com	Thu May 13 17:16:05 UTC 2010 Duration: 0.52 sec	-
3	<u>207.46.232.182</u> (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 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" <b>CONFUSING</b>
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 <b>TRUSTED</b>
Validation type	<b>Extended Validation (EV)</b>



# 4 Self-signed certificates

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



# 5 Own CA certificates

- You configure a web site, don't want to pay small \$ for a proper certificate, but don't mind spending a lot of time creating a custom CA?!
- Encouraging others to use your CA root is terribly insecure
- How well is your CA root protected?
- Any CA root can sign any site!

## 6 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

# 7 Using SSL for “important” bits

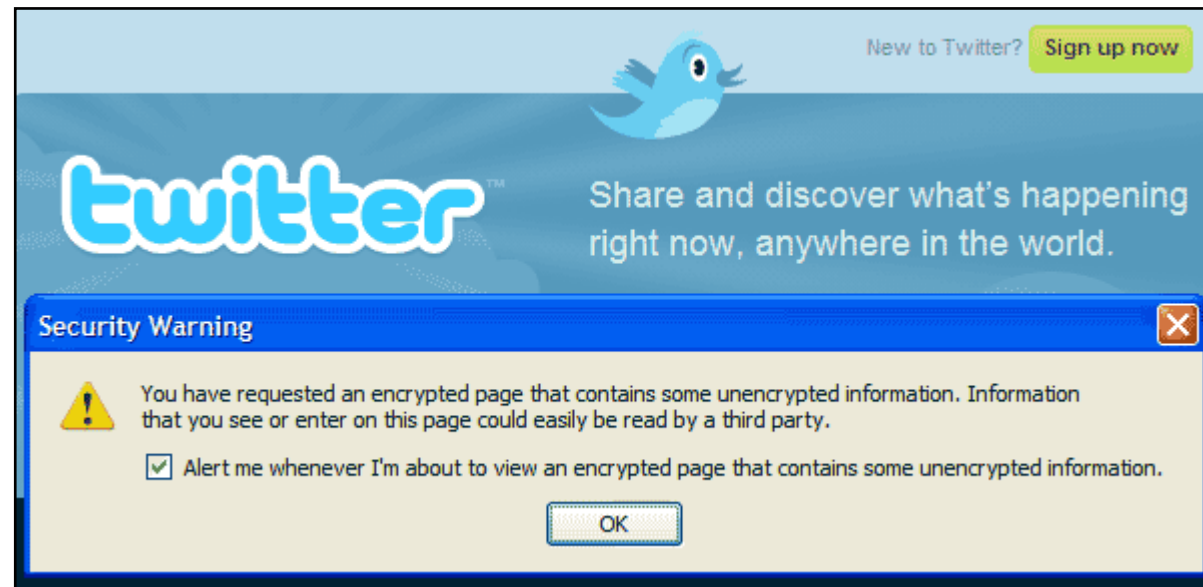
- Some sites will use SSL to protect authentication and nothing else
- They are vulnerable to session hijacking
- Some even allow users to change password without knowing the old ones

## 8 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

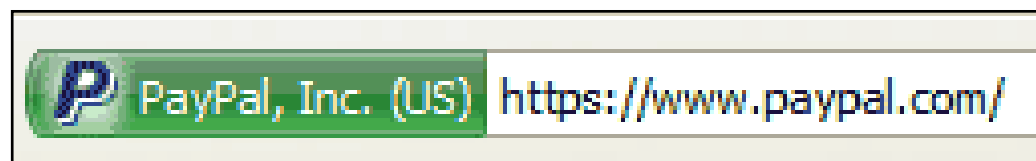
# 9 Mixed page content

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



# 10 Not using an EV certificate

- 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 an experienced user
- The green glow helps ensure your users that they are in the *right* place



# Core Issues

- 1) Browsers accept invalid certificates
- 2) Insufficient security indications
- 3) Decoupled nature of HTTP and SSL
- 4) No broad support for virtual SSL hosting
- 5) Some sites use SSL some don't
- 6) The burden of security is on users



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

# Thank you!

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