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,  
4) ModSecurity Handbook (Feisty Duck, 2010),  
5) Director of Engineering, WAF and SSL @ Qualys.
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?)
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:

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

(Get it from sslabs.com.)
SSL Labs
Dedicated to SSL/TLS research.
Lots of interesting projects.

NOW FUNDED BY QUALYS®
SSL Server Assessment

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

The most comprehensive assessment available.
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
What does *microsoft.com* look like?

<table>
<thead>
<tr>
<th>Server</th>
<th>Domain(s)</th>
<th>Test time</th>
<th>Grade</th>
</tr>
</thead>
</table>
| 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
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 an experienced user
- The green glow helps ensure your users that they are in the right place
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](image)
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
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