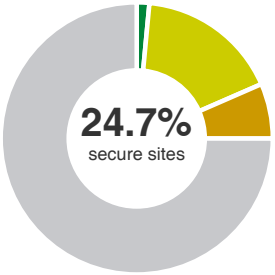
SSL Pulse

Survey of the SSL Implementation of the Most Popular Web Sites

Summary

Published Date: **May 07, 2015**
Comparisons are made against the previous month's data.

SSL Security Summary

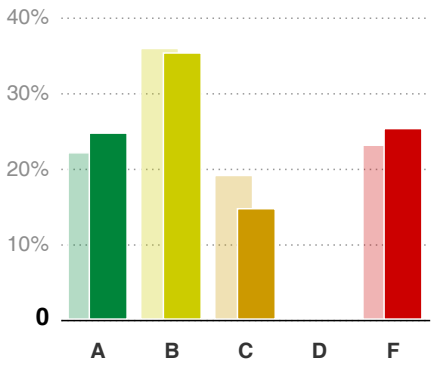


Total sites surveyed
146,462
- 0.4 %

Inadequate security
110,246
- 2.6 %

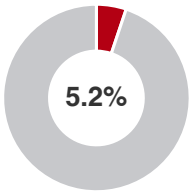
Secure sites
■ A+ ■ A ■ A-
36,216
+ 2.6 %

SSL Labs Grade Distribution



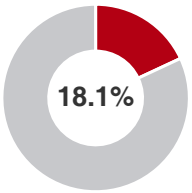
Key Findings

Certificate Chain



Sites with incomplete certificate chain
7,558
+ 0.0 %

Cipher Strength

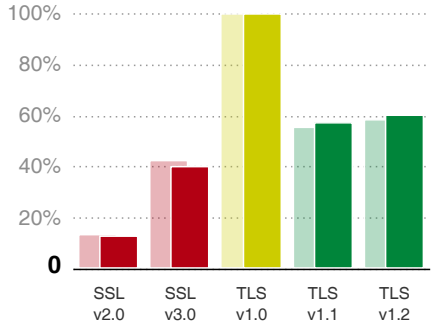


Sites that support weak or insecure cipher suites
26,458
- 1.1 %

Heartbleed

416 Sites vulnerable to the **Heartbleed Bug**
0.3 % of sites surveyed
- 16 since previous month

Protocol Support



Strict Transport Security

4,908 Sites that support **HTTP Strict Transport Security**
3.4 % of sites surveyed
+ 310 since previous month

Renegotiation Support

Key Strength Distribution

SSL Server Test

Enter domain name for testing:

e.g. mycompany.com Submit

About This Project

Title: **SSL Pulse**
Created by: **SSL Labs**
Date Published: **April 25, 2012**

Details:
SSL Pulse is a continuous and global dashboard for monitoring the quality of SSL support across the top one million web sites. SSL Pulse is powered by the assessment technology of SSL Labs, which is focused on auditing the SSL ecosystem, raising awareness, and providing tools and documentation to web site owners so they can improve their SSL implementations.

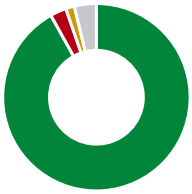
Read the blog post.

Trustworthy Internet Movement Picks SSL Implementation and Governance as First Initiative
April 26, 2012

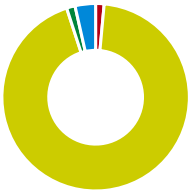
Methodology

The goal of the SSL Labs surveys is to measure the *effective security* of SSL. After some experimentation with an assessment of substantially all public SSL sites (about 1.5 million of them), we settled on a smaller list of about 200,000 SSL-enabled web sites, based on Alexa's list of most popular sites in the world. Working with a smaller list is more manageable and allows us to conduct the surveys more often. It also allows us to conduct more thorough analysis to look for application-layer issues that may subvert SSL security. In addition, focusing on popular sites – we believe – gives us more relevant results and also excludes abandoned sites.

Having worked with several data sets, each drawing from a different list of sites, we have come to understand that what we are presenting in our surveys is not a measurement, but a reasonable approximation of the state of SSL. More important than the

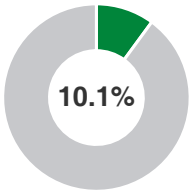


- Secure renegotiation
  135,275 92.4%
  + 0.6 %
- Insecure renegotiation
  4,094 2.8%
  - 0.1 %
- Both
  1,510 1.0%
  - 0.1 %
- No support
  5,583 3.8%
  - 0.3 %



- Below 2048 bits
  141 0.1%
  + 0.0 %
- 2048 bits
  139,925 95.5%
  - 0.2 %
- 3072 bits
  1,081 0.7%
  + 0.0 %
- 4096 bits
  5,286 3.6%
  + 0.1 %

Extended Validation Certificates

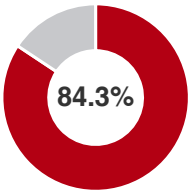


Sites that have an Extended Validation certificate

14,741

+ 0.1 %

BEAST Attack

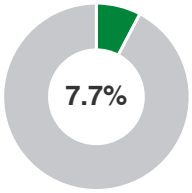


Sites that are vulnerable to the BEAST attack

123,488

+ 1.2 %

SPDY

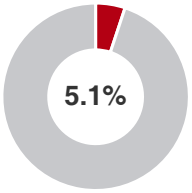


Sites that support the SPDY protocol

11,286

+ 0.2 %

TLS Compression / CRIME



Sites that support TLS compression

7,461

- 0.4 %

Forward Secrecy

- Not supported
  50,985 34.8%
  - 1.9 %
- Some FS suites enabled
  53,320 36.4%
  - 0.1 %
- Used with modern browsers
  18,307 12.5%
  + 0.1 %
- Used with most browsers
  23,850 16.3%
  + 1.8 %

RC4

- Not supported
  49,345 33.7%
  + 2.9 %
- Some RC4 suites enabled
  69,695 47.6%
  - 1.4 %
- Used with modern browsers
  27,422 18.7%
  - 1.5 %

Certificate Signature Algorithms

CVE-2014-0224

results from any one round of tests is how the measurements change over time. The adoption of a single selection methodology and a switch to monthly testing should give us an indicator of where we're heading, which is what we believe matters.

Documentation

SSL Server Rating Guide

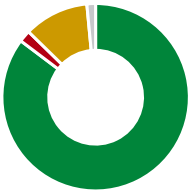
BEAST and How to Fix It

Insecure Renegotiation and How to Fix It

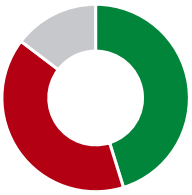
SSL/TLS Deployment Best Practices

- SHA256
  80,812 55.2%
  + 6.3 %
- SHA1
  65,643 44.8%
  - 6.2 %
- MD5
  0 0.0%
  + 0.0 %

- Not vulnerable
  136,242 93.0%
  + 0.2 %
- Vulnerable and exploitable
  6,663 4.5%
  - 0.5 %
- Unknown
  3,493 2.4%
  + 0.2 %



- Not vulnerable
  125,332 85.6%
  + 0.9 %
- Vulnerable and exploitable
  2,996 2.0%
  - 0.2 %
- Vulnerable, not exploitable
  16,460 11.2%
  - 0.8 %



- Supported
  66,196 45.2%
  + 2.1 %
- Not Supported
  58,796 40.1%
  - 2.1 %
- Unknown
  21,470 14.7%
  + 0.0 %

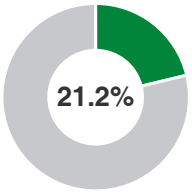
Sites that require RC4

1,218 Sites that support only **RC4 cipher suites**

0.8 % of sites surveyed

- 337 since previous month

OCSP Stapling



Sites that support OCSP stapling

31,089

+ 0.3 %

Key Exchange Strength