TLS-Attacker

Evaluating the TLS ecosystem

Juraj Somorovsky

Winter Semester 2020/21

Paderborn University

Transport Layer Security (TLS)

- The most important cryptographic standard

TLS is complex

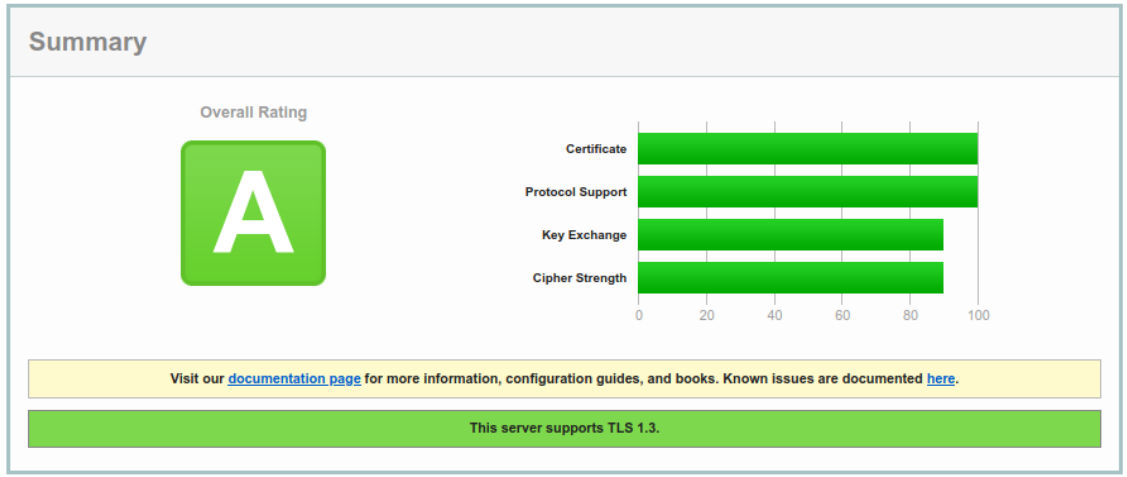
- Many versions, many algorithms, many attacks …

TLS is complex

- Many versions, many algorithms, many attacks …

Configuring a TLS server not that easy

SSL labs

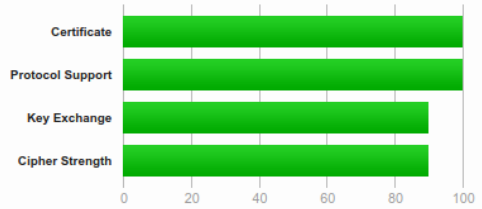

Summary
Overall Rating
A
Certificate
Protocol Support
Key Exchange
Cipher Strength
0
20
40
60
80
100
Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.
This server supports TLS 1.3.

SSL labs

Summary

Overall Rating

A



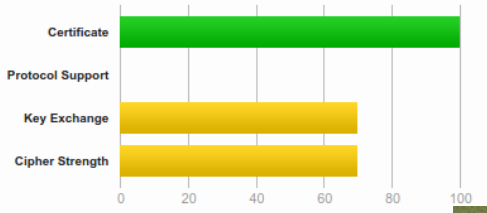
Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports TLS 1.3.

Summary

Overall Rating

F



Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports SSL 2, which is obsolete and insecure, and can be used against TLS (DROWN attack). Grade set to F. MORE I

This server is vulnerable to the POODLE attack. If possible, disable SSL 3 to mitigate. Grade capped to C. MORE INFO »

This server supports weak Diffie-Hellman (DH) key exchange parameters. Grade capped to B. MORE INFO »

The server supports only older protocols, but not the current best TLS 1.2 or TLS 1.3. Grade capped to C. MORE INFO »

This server accepts RC4 cipher, but only with older protocols. Grade capped to B. MORE INFO »

This server does not support Authenticated encryption (AEAD) cipher suites. Grade capped to B. MORE INFO »

This server supports TLS 1.0. Grade capped to B. MORE INFO »

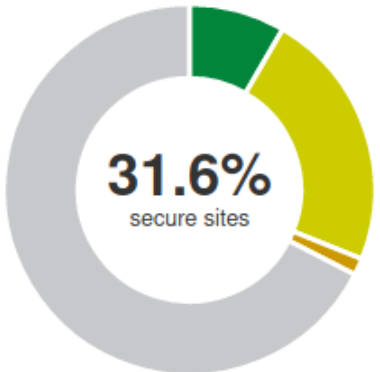
SSL Pulse

SSL Pulse is a continuous and global dashboard for monitoring the quality of SSL / TLS support over time across 150,000 SSL- and TLS-enabled websites, based on Alexa's list of the most popular sites in the world.

Monthly Scan: July 08, 2020

Previous Next

SSL Security Summary

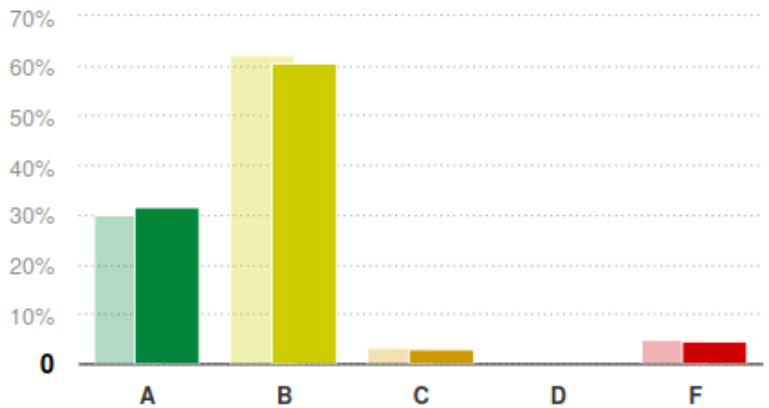


Total sites surveyed
138,709
- 0.3 %

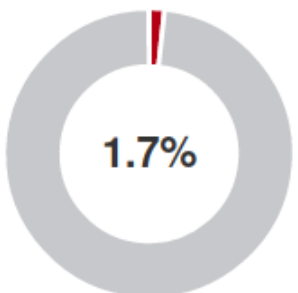
Inadequate security
94,894
- 1.7 %

Secure sites
■ A+ ■ A ■ A-
43,815
+ 1.7 %

SSL Labs Grade Distribution

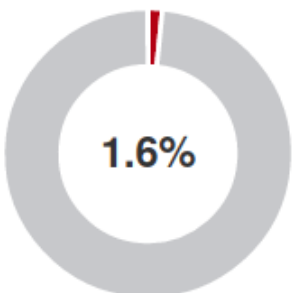


Certificate Chain



Sites with incomplete certificate chain
2,378
- 0.1 %

Cipher Strength



Sites that support weak or insecure cipher suites
2,220
- 0.1 %

SSL Pulse

SSL Pulse is a continuous and global dashboard for monitoring the quality of SSL / TLS support over time across 150,000 SSL- and TLS-enabled websites, based on Alexa's list of the most popular sites in the world.

Monthly Scan: July 08, 2020

Previous Next

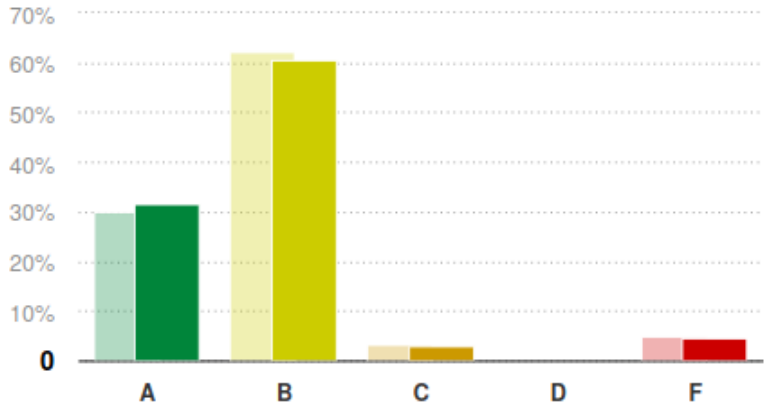
SSL Security Summary

Total sites surveyed
138,709
- 0.3 %

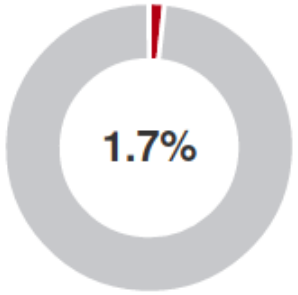
Inadequate security
94,894
- 1.7 %

Secure sites
■ A+ ■ A ■ A-
43,815
+ 1.7 %

SSL Labs Grade Distribution



Certificate Chain



Cipher Strength

ites that support weak
r insecure cipher suites
2,220
- 0.1 %

Provides a nice basic overview

Question: How to improve analyses of the TLS ecosystem?

TLS-Attacker – basis for our project group

- Tool for analyses of TLS implementations
- Scanning, testing, writing attacks
- Offers many nice features
- https://github.com/RUB-NDS/TLS-Attacker

Goal: Analysis of the TLS ecosystem

- Many directions …

- Perform the scans
- Write a website
- Write new security/attack evaluations
- Analyze TLS implementation fingerprinting
- Provide configuration improvement feedback
- Provide server configuration statistics
- Predictions regarding the security statistics

Goal: Analysis of the TLS ecosystem

- Many directions …

- Perform the scans
- Write a website
- Write new security/attack evaluations
- Analyze TLS implementation fingerprinting
- Provide configuration improvement feedback
- Provide server configuration statistics
- Predictions regarding the security statistics

Do some cool stuff

Goal: Analysis of the TLS ecosystem

- Many directions …

- Team:
  - Security experts (RWC engineering students)
  - Website building experts
  - Statistics and machine learning