SSL Vulnerabilities and best practices to secure your SSL/TLS Implementation

Felipe Tribaldos, CISSP

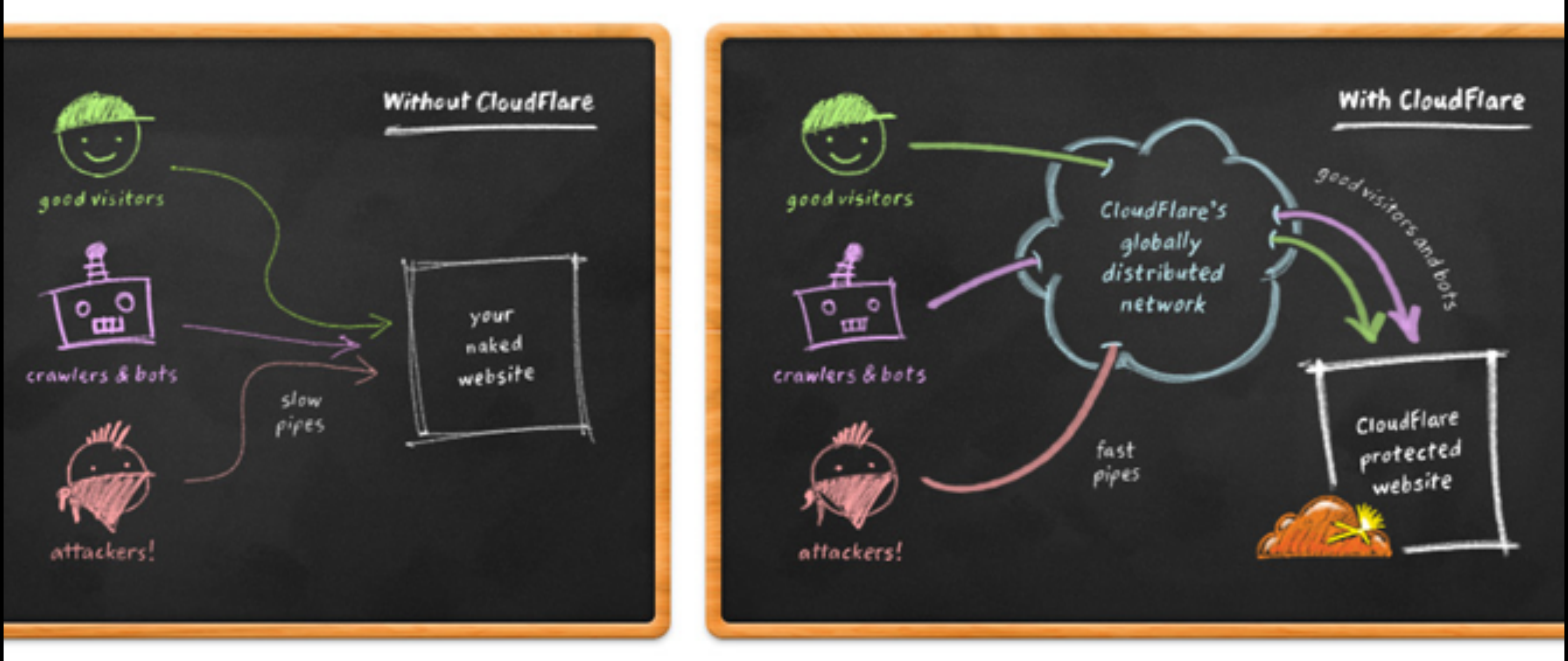
felipe@cloudflare.com

18/22 mayo - lima, perú

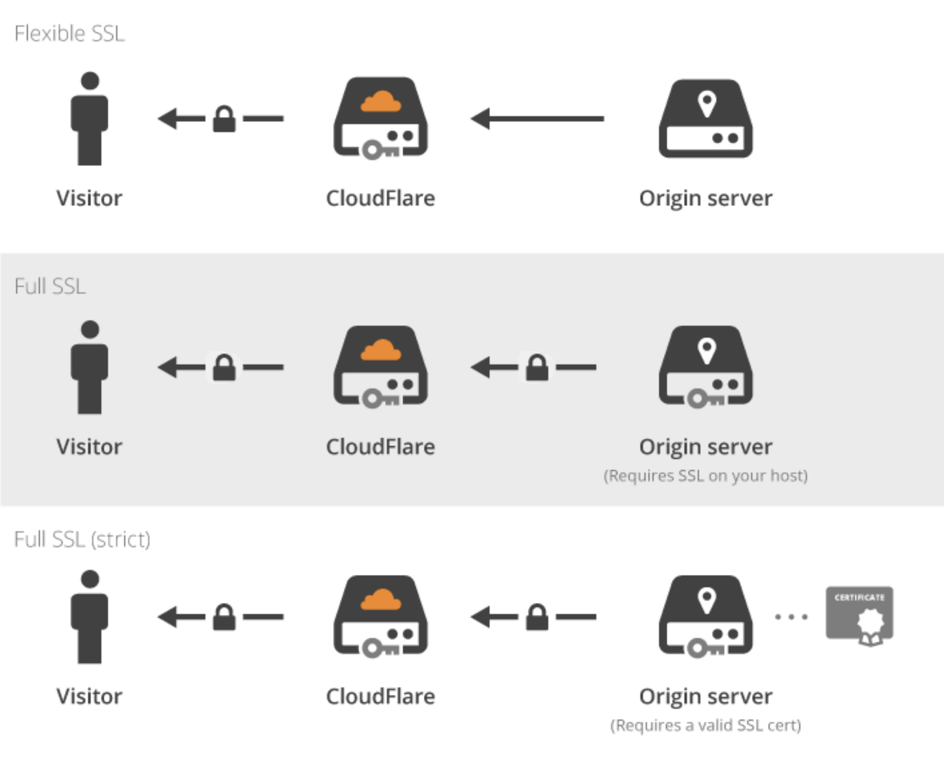
DISCLAIMER:

When we say SSL we mean TLS except when referring to SSL 2.0/3.0

Who are we ?


Without CloudFlare
good visitors
crawlers & bots
attackers!
slow pipes
your naked website
With CloudFlare
good visitors
crawlers & bots
attackers!
CloudFlare's globally distributed network
good visitors and bots
fast pipes
CloudFlare protected website

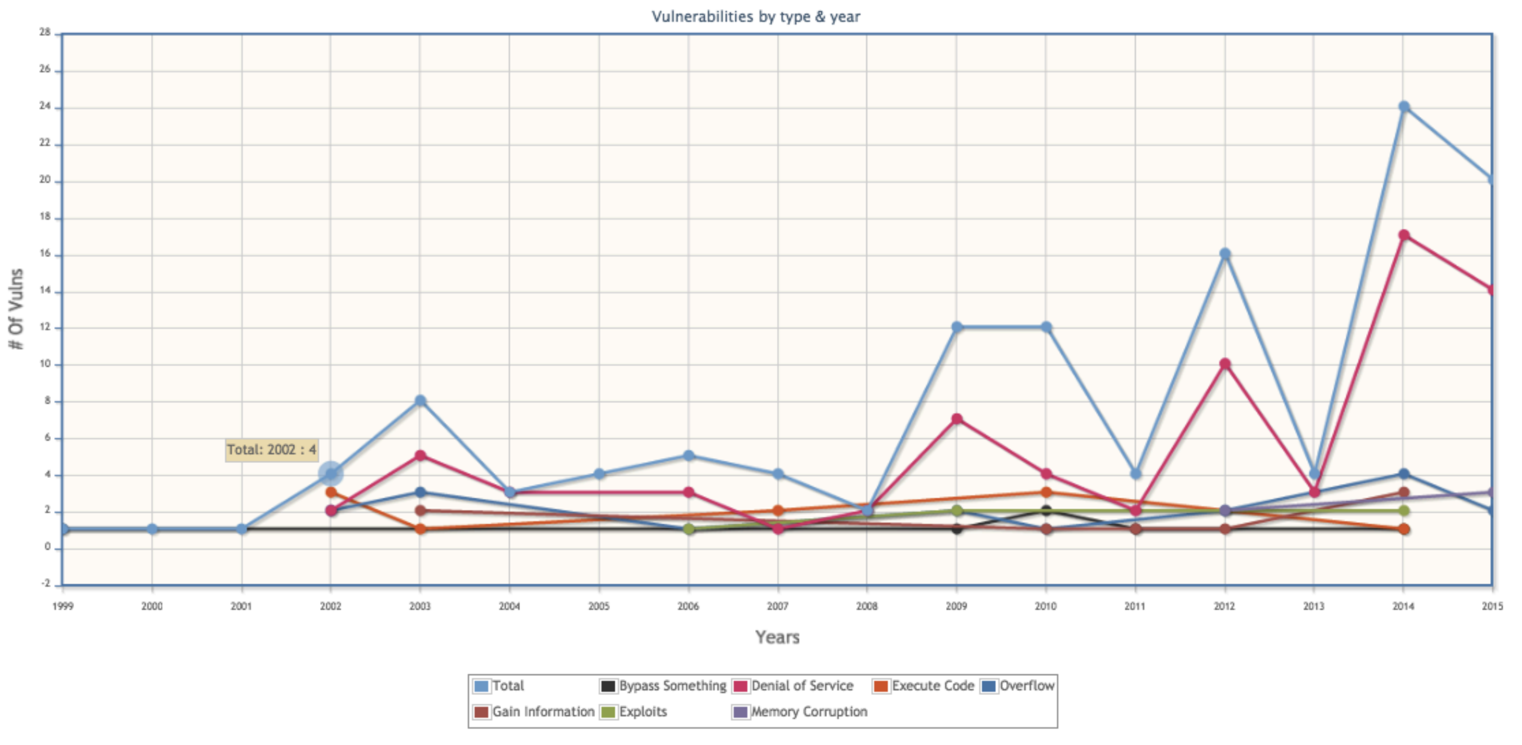
CloudFlare SSL



Many Recent SSL Vulnerabilities

- BEAST – Sept. 2011 (CVE-2011-3389)
- Heartbleed – April 2014 (CVE-2014-0160)
- POODLE Vulnerability (SSL3.0) Oct. 2014 - (CVE-2014-0160)’
- BERserk (Mozilla)
- TLS POODLE – Feb. 2015 - (CVE-2014-8730)
- FREAK SSL/TLS Vulnerability – March 2015 (CVE-2015-0204)
- LOGJAM – May 21
- …

OpenSSL vulnerabilities by year



Source: http://www.cvedetails.com/product/383/Openssl-Openssl.html?vendor_id=217

BEAST – Sept. 2011 (CVE-2011-3389)

- Severity: HIGH
- RCE: No
- MITM Attack: YES
- Mitigation: Update TLS 1.0 & TLS 1.1, Prioritize RC4 Ciphers

- RC4 since been deprecated. Browser support to Mitigate fully.
- Others: CRIME, BREACH

HEARTBLEED – Sept. 2014 (CVE-2014-0160)

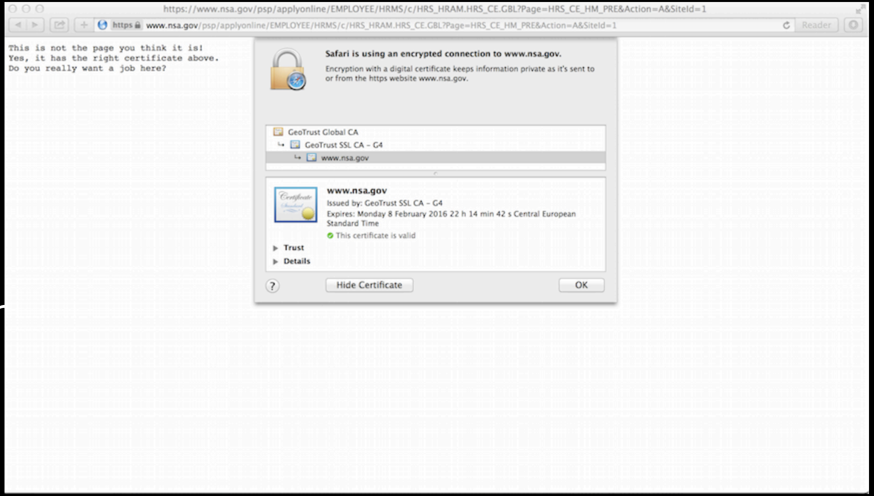
- What: A missing bounds check in the handling of the TLS heartbeat extension can be used to reveal up to 64kB of memory to a connected client or server (a.k.a. Heartbleed)
- Severity: HIGH
- RCE: No
- MITM Attack: YES
- Mitigation: Patch OpenSSL Versions

POODLE – Sept. 2014 (CVE-2014-0160)

- What: A missing bounds check in the handling of the TLS heartbeat extension can be used to reveal up to 64kB of memory to a connected client or server (a.k.a. Heartbleed)
- Severity: HIGH
- RCE: No
- MITM Attack: YES
- Mitigation: Deprecate SSL 3.0, Patch OpenSSL Versions
- TLS POODLE: Feb. 2015

FREAK SSL/TLS Vulnerability – (CVE-2015-0204)

- What: FREAK (Factoring Attack on RSA-EXPORT Keys CVE-2015-0204) is a weakness in some implementations of SSL/TLS that may allow an attacker to decrypt secure communications between vulnerable clients and servers.
- Severity: LOW (sort of)
- RCE: No
- MITM Attack: YES
- Mitigation: Update OpenSSL, Remove EC Er
- NSA Site was compromised



https://www.nsa.gov/psp/applyonline/EMPLOYEE/HRMS/c/HRS_HRAM.HRS_CE.GBL?Page=HRS_CE_HM_PRE&Action=A&SiteId=1

https www.nsa.gov/psp/applyonline/EMPLOYEE/HRMS/c/HRS_HRAM.HRS_CE.GBL?Page=HRS_CE_HM_PRE&Action=A&SiteId=1

```
This is not the page you think it is!
Yes, it has the right certificate above.
Do you really want a job here?
```

Safari is using an encrypted connection to www.nsa.gov.

Encryption with a digital certificate keeps information private as it's sent to or from the https website www.nsa.gov.

GeoTrust Global CA
↳ GeoTrust SSL CA – G4
↳ www.nsa.gov

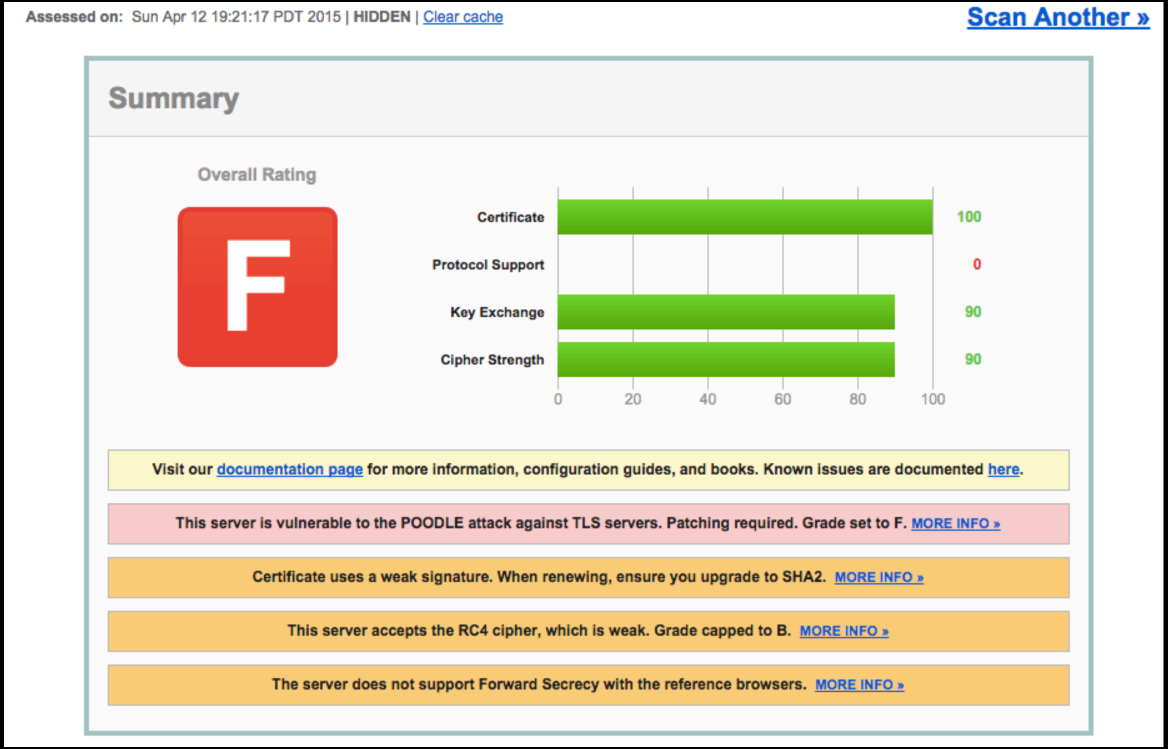
www.nsa.gov
Issued by: GeoTrust SSL CA – G4
Expires: Monday 8 February 2016 22 h 14 min 42 s Central European Standard Time
✓ This certificate is valid

Concerted industry efforts

- HTTPS Everywhere
  - Google, Yahoo, others
- EFF – Lets Encrypt –
- CF Universal SSL
- Move sites to full HTTPS

What are the Risks in the real world.

Many Financial Sites are Vulnerable



Assessed on: Sun Apr 12 19:21:17 PDT 2015 | HIDDEN | Clear cache

Scan Another »

Summary

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

This server is vulnerable to the POODLE attack against TLS servers. Patching required. Grade set to F. MORE INFO »

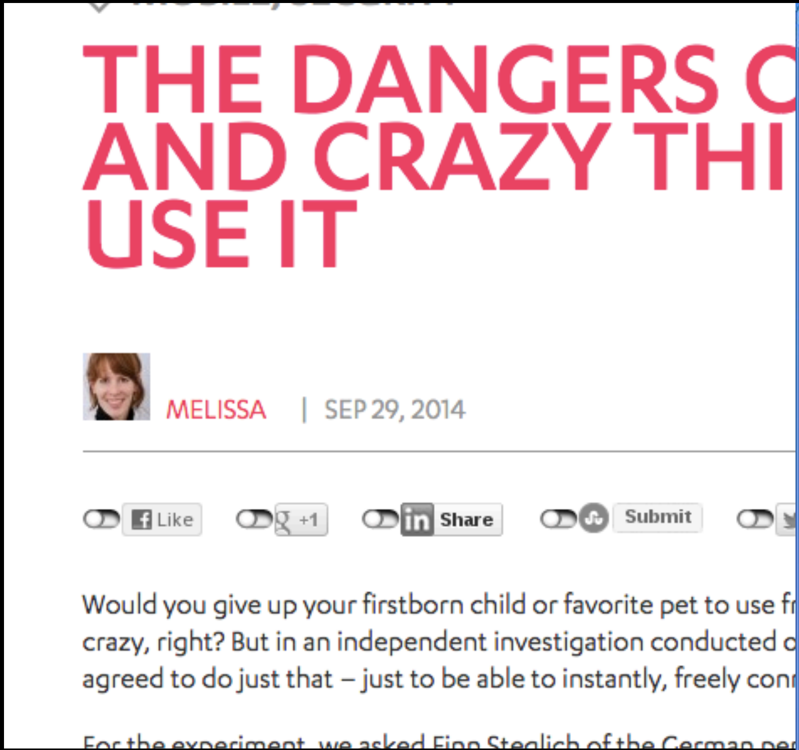
Certificate uses a weak signature. When renewing, ensure you upgrade to SHA2. MORE INFO »

This server accepts the RC4 cipher, which is weak. Grade capped to B. MORE INFO »

The server does not support Forward Secrecy with the reference browsers. MORE INFO »

Important LATAM Financial Institution

MITM is very easy in Public Networks

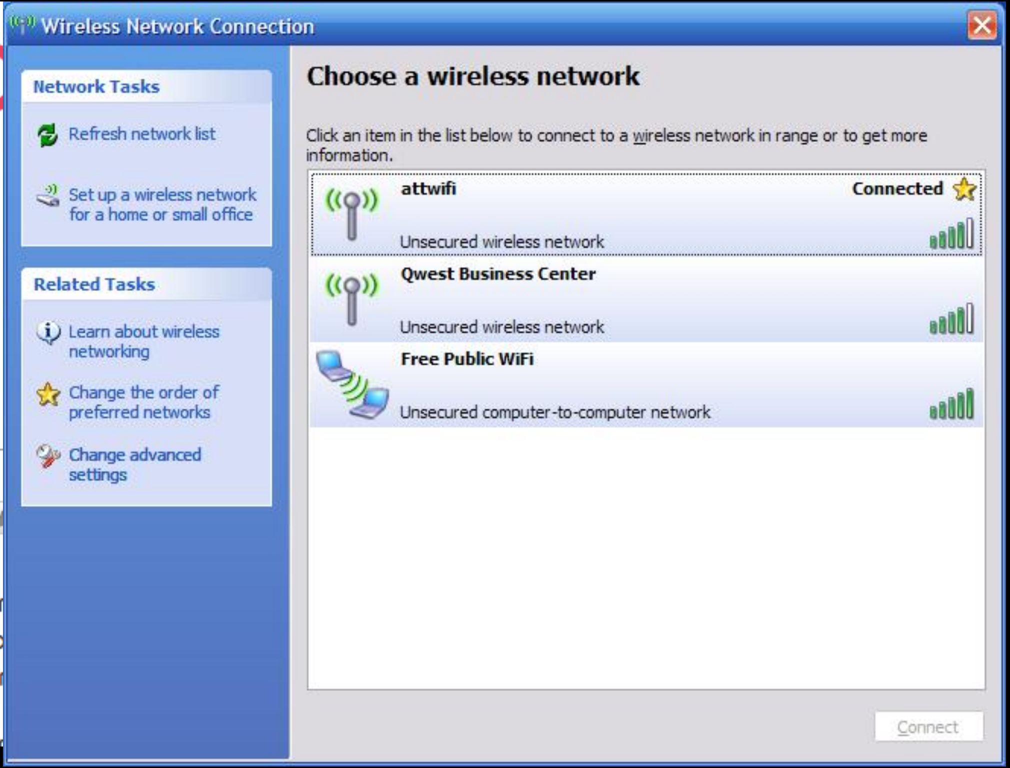


THE DANGERS O
AND CRAZY THI
USE IT

MELISSA | SEP 29, 2014

Would you give up your firstborn child or favorite pet to use fr
crazy, right? But in an independent investigation conducted o
agreed to do just that – just to be able to instantly, freely conn

For the experiment, we asked Finn Steglich of the German per



Wireless Network Connection
Network Tasks
Refresh network list
Set up a wireless network for a home or small office
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

attwifi — Connected — Unsecured wireless network

Qwest Business Center — Unsecured wireless network

Free Public WiFi — Unsecured computer-to-computer network

Lack of Urgency

- Many Enterprise Managers see MITM as a remote possibility.
- Difficulty in Patching Legacy Systems
- Obsolete Network Devices unable to support newer protocols

BANK with POODLE Vulnerable E-Banking Servers (supporting SSL2 and SSL3)

“Es un issue conocido por nosotros, pero negocios mantiene la decisión de soportar todavía IE 6. Felipe, gracias por el heads up. Es un tema que debemos revisar este trimestre nuevamente. “

| Gerente de Seguridad de la Información - Cumplimiento y Seguridad

Recommendations

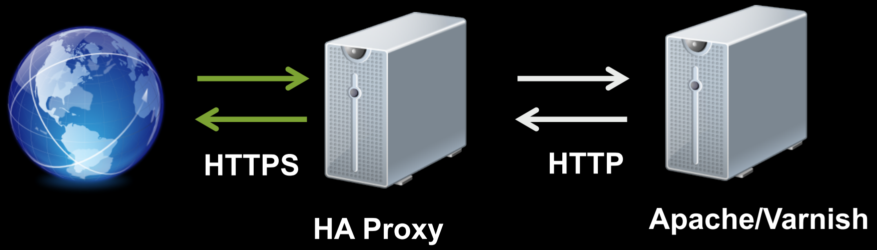
- Patch your SSL/TLS Regularly (configuration builder)
- If not possible on servers implement Proxy Services either Cloud or SSL Offload (Load Balancers, HA Proxy).
- Update to newest Protocol Support: TLS 1.2, TLS 1.1 (TLS 1.3 IETF Draft)
- Remove Deprecated Protocols: SSL 2.0, SSL 3.0, RC4, TLS 1.0
- PCI Council– "no version of SSL meets PCI SSC's definition of "strong cryptography,"
  - PCI 3.1 (June 2016) – Mandate TLS 1.2

Recommendations

- Best Current Practices - RFC7525
  - Remove SSL2.0 and SSL3.0, Should Not TLS 1.0 & 1.1.
  - Must support and prefer TLS 1.2
  - HSTS (Must support, should use)
  - Safe TLS compression (based on protocol) and Session Resumption
  - Cipher Suites (Remove RC4, Export, <128-bits)
- Mozilla Configuration Builder for server Apache, Nginx, HAProxy, AWS
  - https://mozilla.github.io/server-side-tls/ssl-config-generator/

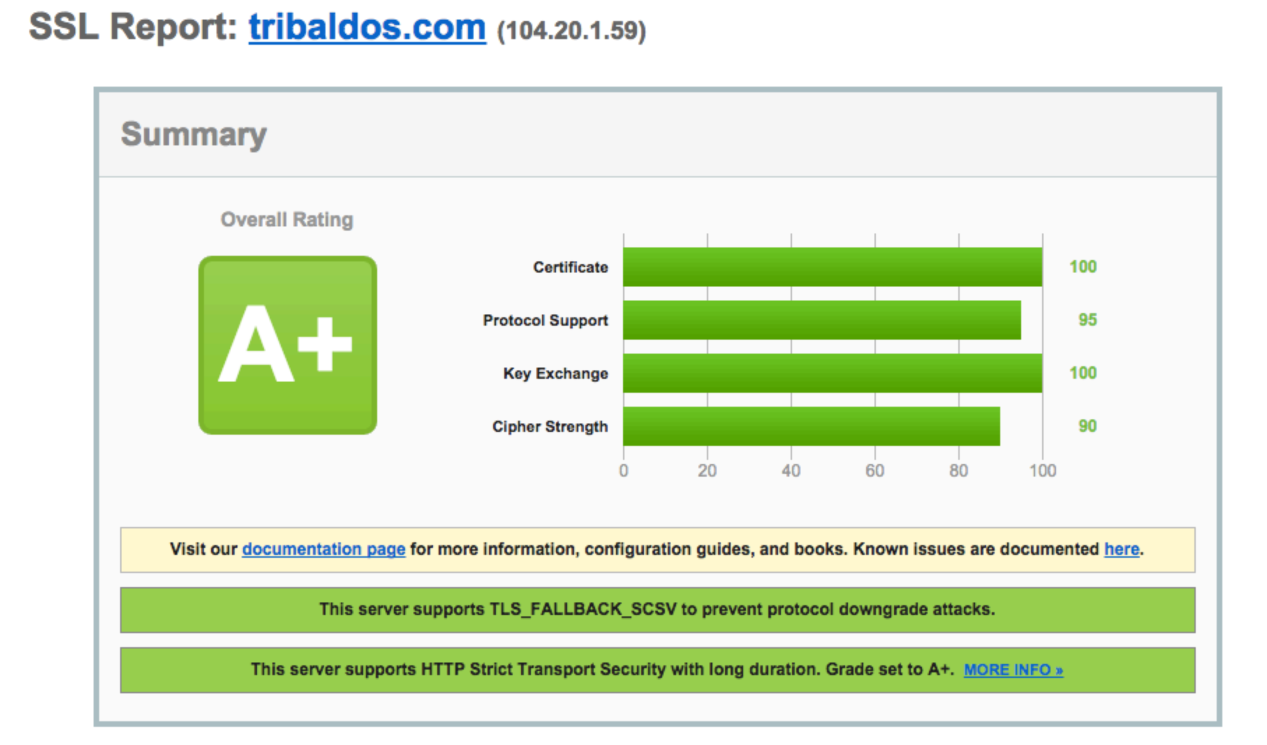
In the Lab

- Build your own Security Proxy
  - Useful for forcing HTTPS and avoiding mixed content messages.
  - How to get A+ Rating on ssllabs.com: Forward Secrecy, Session Tickets, HSTS



- Guide: http://arstechnica.com/information-technology/2015/05/web-served-how-to-make-your-site-all-https-all-the-time-for-everyone/

Happy Place



SSL Report: tribaldos.com (104.20.1.59)

Summary

Overall Rating

A+

Certificate	100
Protocol Support	95
Key Exchange	100
Cipher Strength	90

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

This server supports TLS_FALLBACK_SCSV to prevent protocol downgrade attacks.

This server supports HTTP Strict Transport Security with long duration. Grade set to A+. MORE INFO »

Thank you

Felipe Tribaldos
felipe@cloudflare.com
Twitter: @ftribaldos