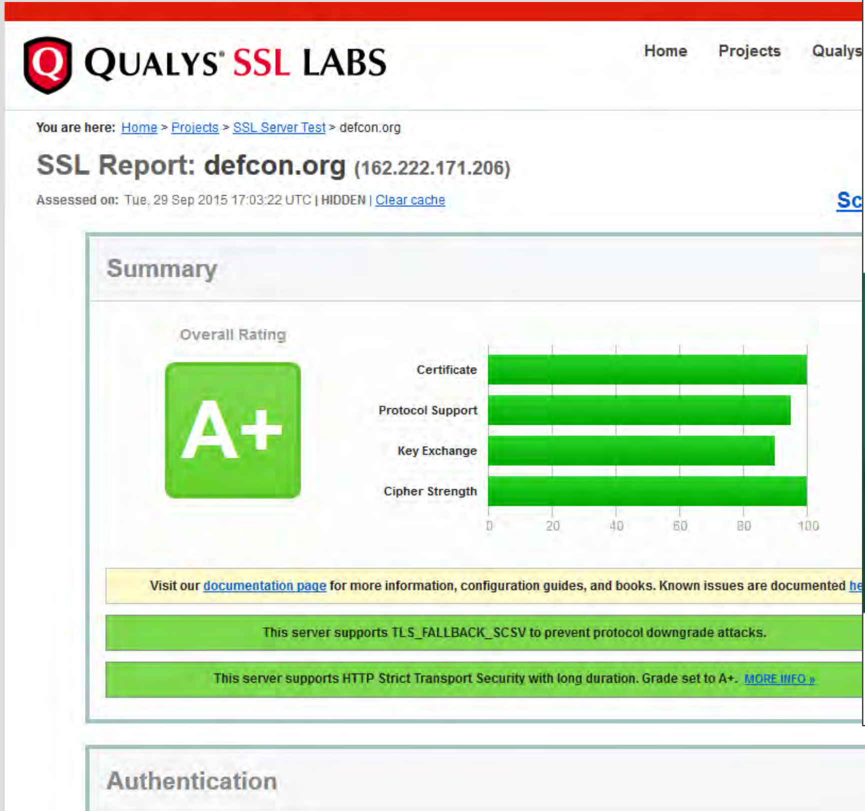
Some Thoughts On SSL/TLS and PKI

Ivan Ristić

Hardenize

My recent work (for context)



QUALYS® SSL LABS

Home Projects Qualys

You are here: Home > Projects > SSL Server Test > defcon.org

SSL Report: defcon.org (162.222.171.206)

Assessed on: Tue, 29 Sep 2015 17:03:22 UTC | HIDDEN | Clear cache

Sc

Summary

Overall Rating

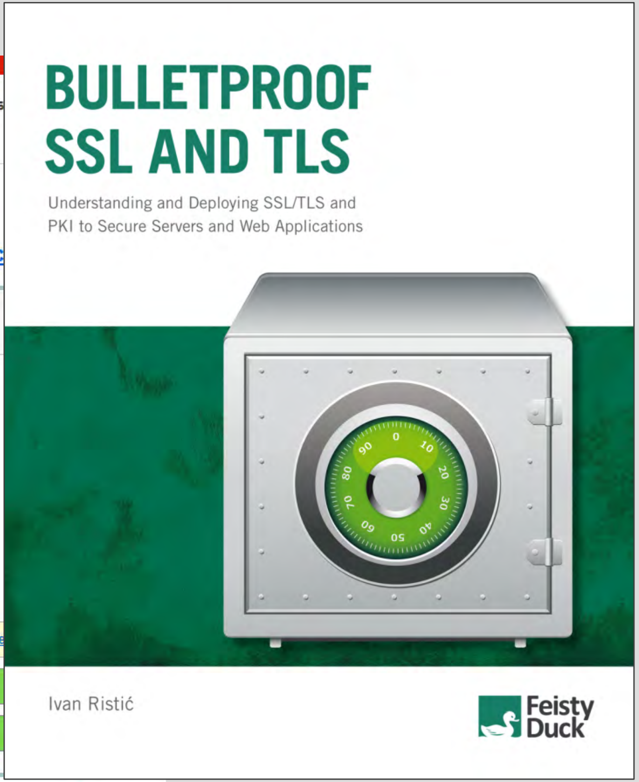
A+

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

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 »

Authentication



BULLETPROOF SSL AND TLS

Understanding and Deploying SSL/TLS and PKI to Secure Servers and Web Applications

Ivan Ristić

Feisty Duck

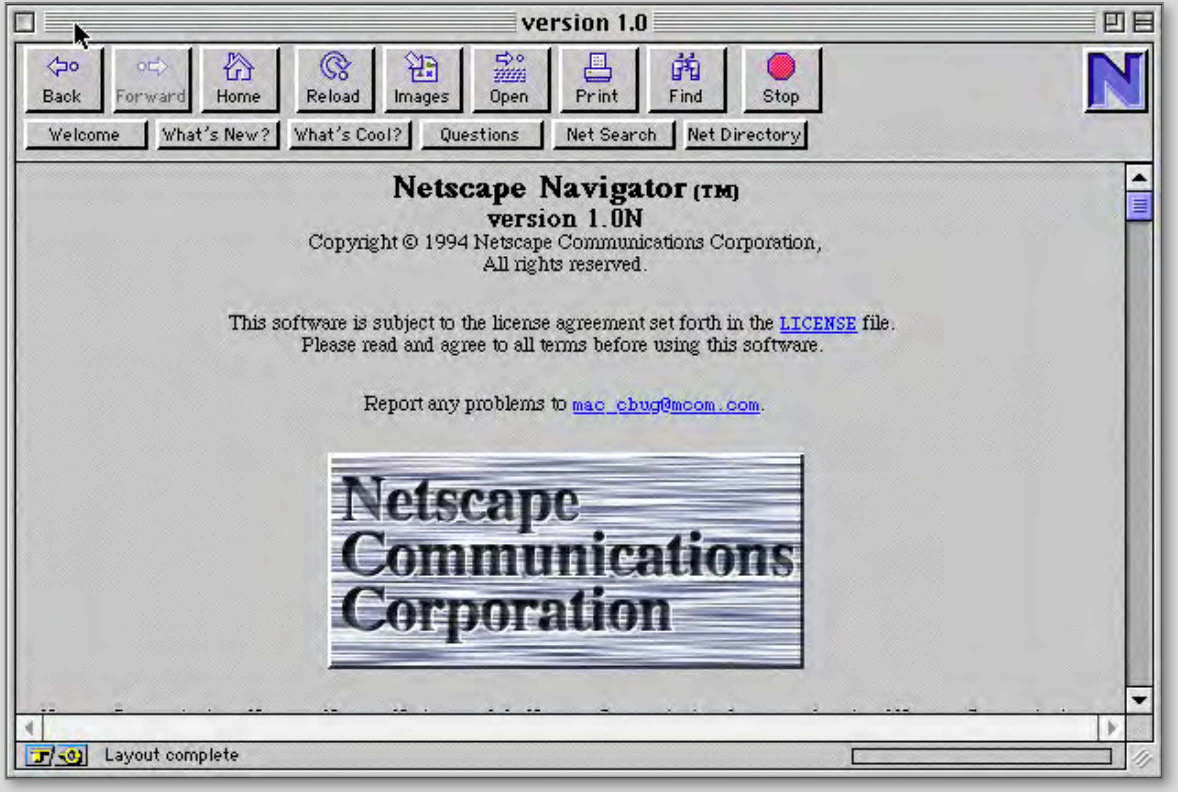
Who uses SSL/TLS and PKI?

Everyone does.

- 2+ billion smart phones
- 170m web sites
- 10s of millions of developers and IT professionals

SSL/TLS and PKI ecosystem

- IETF TLS Working Group
- Library developers
- Operating systems
- Vendors
  - Server vendors
  - Browser vendors
- Certification authorities, partners and resellers



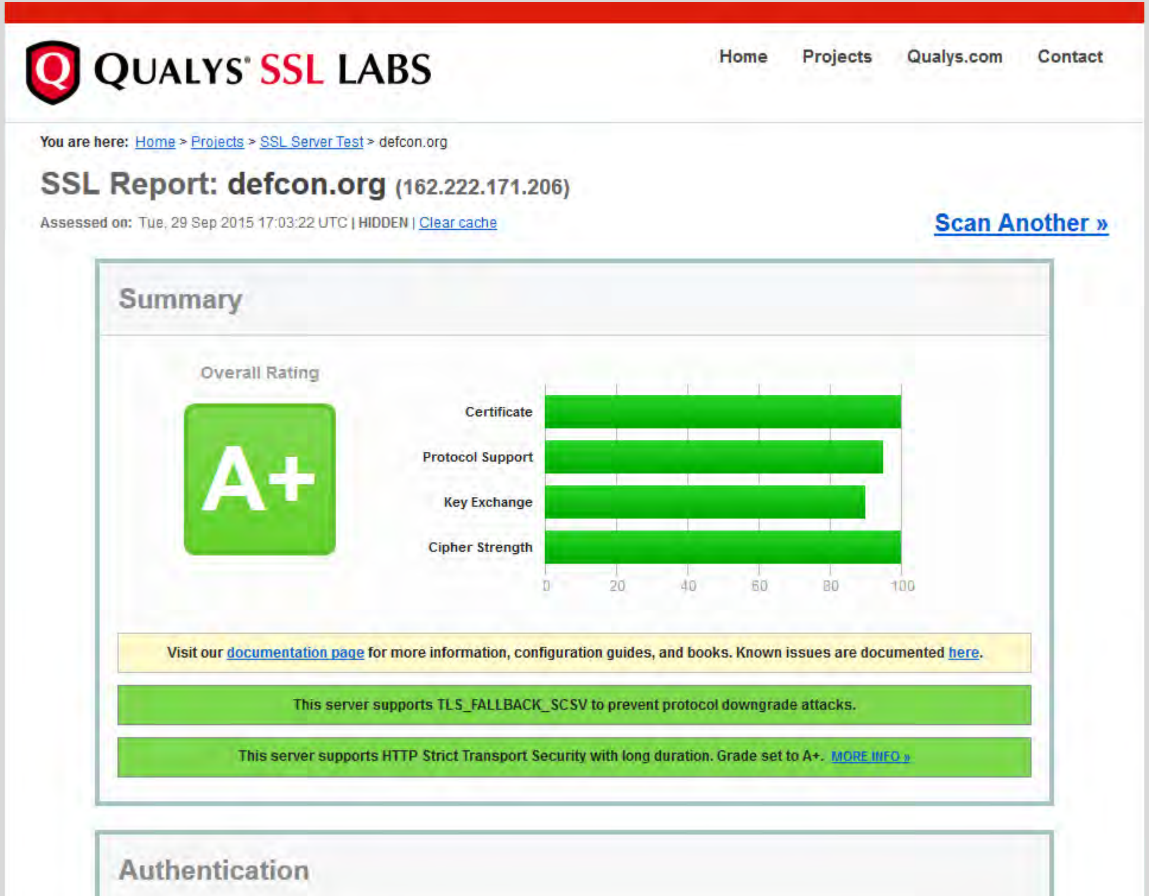
Netscape Navigator (TM)
version 1.0N
Copyright © 1994 Netscape Communications Corporation,
All rights reserved.

This software is subject to the license agreement set forth in the LICENSE file.
Please read and agree to all terms before using this software.

Report any problems to mac_cbug@mcom.com.

Deploying TLS securely is getting more complicated, not less.

SSL Labs



QUALYS® SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > defcon.org

SSL Report: defcon.org (162.222.171.206)

Assessed on: Tue, 29 Sep 2015 17:03:22 UTC | HIDDEN | Clear cache

Scan Another »

Summary

Overall Rating

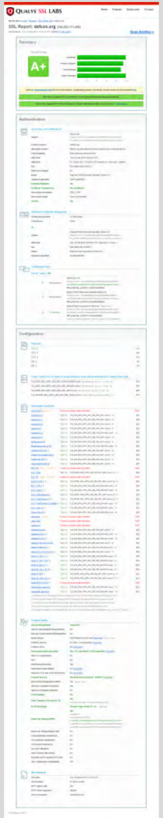
A+

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 »

Authentication

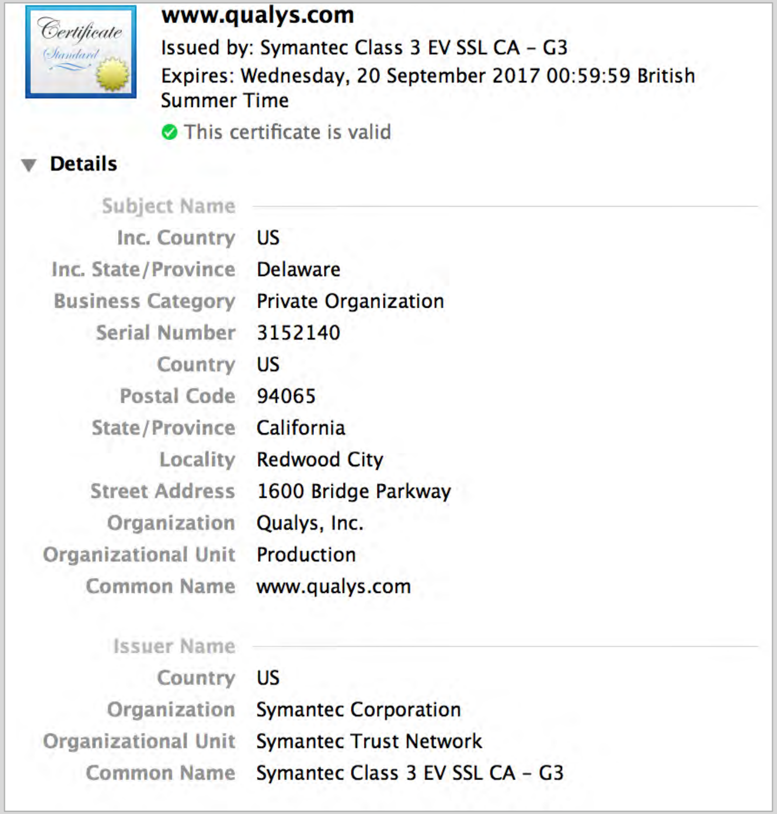


2016

2009

Back in the day, all you needed was a **valid certificate**.

Today, the certificate comes with a **550-page manual**.



www.qualys.com

Issued by: Symantec Class 3 EV SSL CA – G3

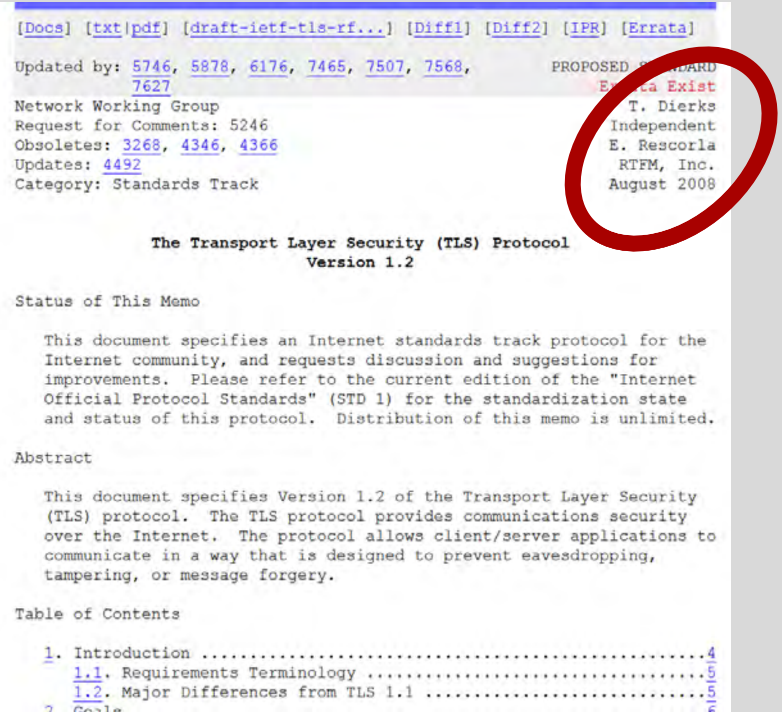
Expires: Wednesday, 20 September 2017 00:59:59 British Summer Time

✓ This certificate is valid

▼ **Details**

Subject Name	
Inc. Country	US
Inc. State/Province	Delaware
Business Category	Private Organization
Serial Number	3152140
Country	US
Postal Code	94065
State/Province	California
Locality	Redwood City
Street Address	1600 Bridge Parkway
Organization	Qualys, Inc.
Organizational Unit	Production
Common Name	www.qualys.com
Issuer Name	
Country	US
Organization	Symantec Corporation
Organizational Unit	Symantec Trust Network
Common Name	Symantec Class 3 EV SSL CA – G3

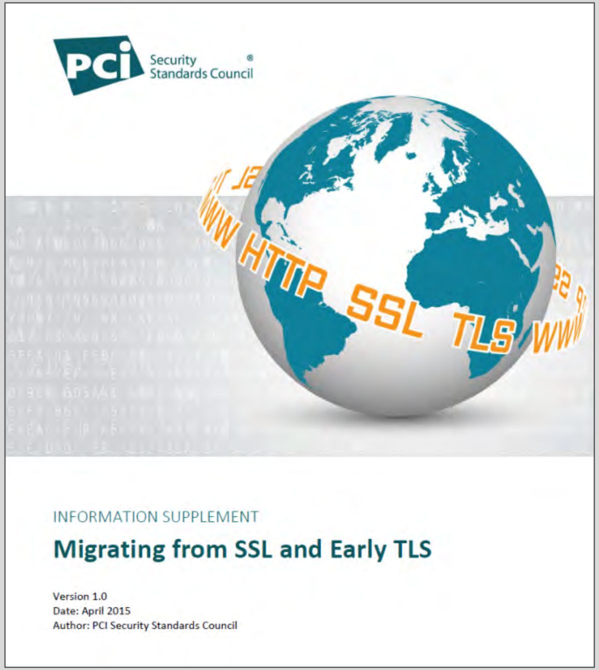
TLS 1.2



```
[Docs] [txt|pdf] [draft-ietf-tls-rf...] [Diff1] [Diff2] [IPR] [Errata]

Updated by: 5746, 5878, 6176, 7465, 7507, 7568,          PROPOSED STANDARD
            7627                                              Errata Exist
Network Working Group                                           T. Dierks
Request for Comments: 5246                                    Independent
Obsoletes: 3268, 4346, 4366                                   E. Rescorla
Updates: 4492                                                  RTFM, Inc.
Category: Standards Track                                     August 2008


              The Transport Layer Security (TLS) Protocol
                              Version 1.2

Status of This Memo

   This document specifies an Internet standards track protocol for the
   Internet community, and requests discussion and suggestions for
   improvements.  Please refer to the current edition of the "Internet
   Official Protocol Standards" (STD 1) for the standardization state
   and status of this protocol.  Distribution of this memo is unlimited.

Abstract

   This document specifies Version 1.2 of the Transport Layer Security
   (TLS) protocol.  The TLS protocol provides communications security
   over the Internet.  The protocol allows client/server applications to
   communicate in a way that is designed to prevent eavesdropping,
   tampering, or message forgery.

Table of Contents

   1. Introduction ....................................................4
      1.1. Requirements Terminology ...................................5
      1.2. Major Differences from TLS 1.1 .............................5
```

1. Released in 2008
2. Browsers started supporting in 2013/2014, after 5 years
3. Only 76% of servers support today
   (SSL Pulse, May 2016)

PCI Security Standards Council



PCI Security Standards Council®

INFORMATION SUPPLEMENT

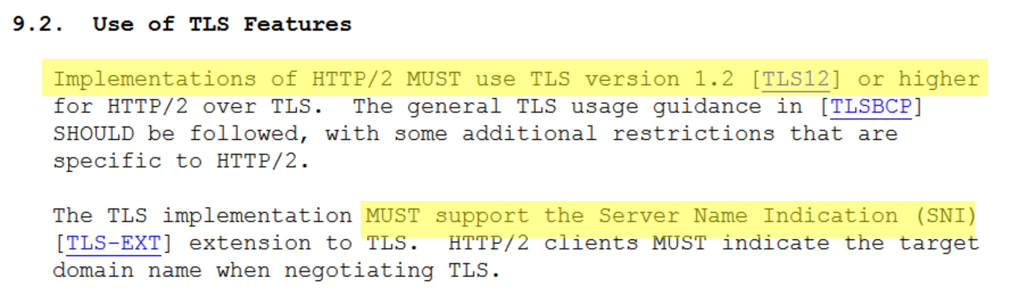
Migrating from SSL and Early TLS

Version 1.0
Date: April 2015
Author: PCI Security Standards Council

“SSL 3 and TLS 1.0 are not secure…”

“Upgrade now, or by June 30 2018 at the latest.”

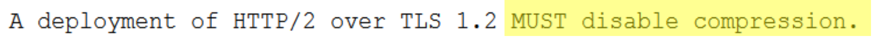
HTTP/2 (RFC 7540)



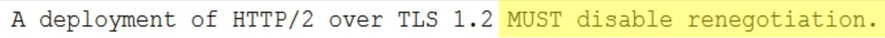
9.2. Use of TLS Features

Implementations of HTTP/2 MUST use TLS version 1.2 [TLS12] or higher for HTTP/2 over TLS. The general TLS usage guidance in [TLSBCP] SHOULD be followed, with some additional restrictions that are specific to HTTP/2.

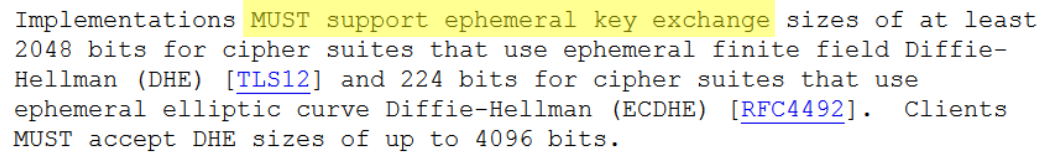
The TLS implementation MUST support the Server Name Indication (SNI) [TLS-EXT] extension to TLS. HTTP/2 clients MUST indicate the target domain name when negotiating TLS.



A deployment of HTTP/2 over TLS 1.2 MUST disable compression.

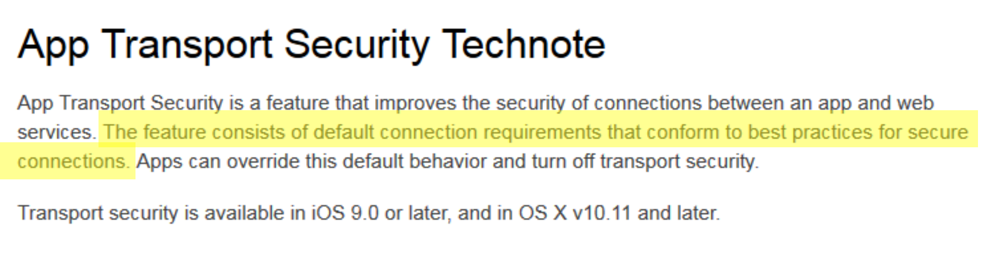


A deployment of HTTP/2 over TLS 1.2 MUST disable renegotiation.



Implementations MUST support ephemeral key exchange sizes of at least 2048 bits for cipher suites that use ephemeral finite field Diffie-Hellman (DHE) [TLS12] and 224 bits for cipher suites that use ephemeral elliptic curve Diffie-Hellman (ECDHE) [RFC4492]. Clients MUST accept DHE sizes of up to 4096 bits.

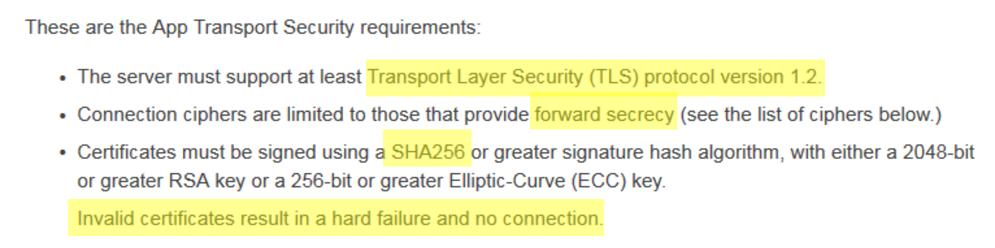
Apple



App Transport Security Technote

App Transport Security is a feature that improves the security of connections between an app and web services. The feature consists of default connection requirements that conform to best practices for secure connections. Apps can override this default behavior and turn off transport security.

Transport security is available in iOS 9.0 or later, and in OS X v10.11 and later.

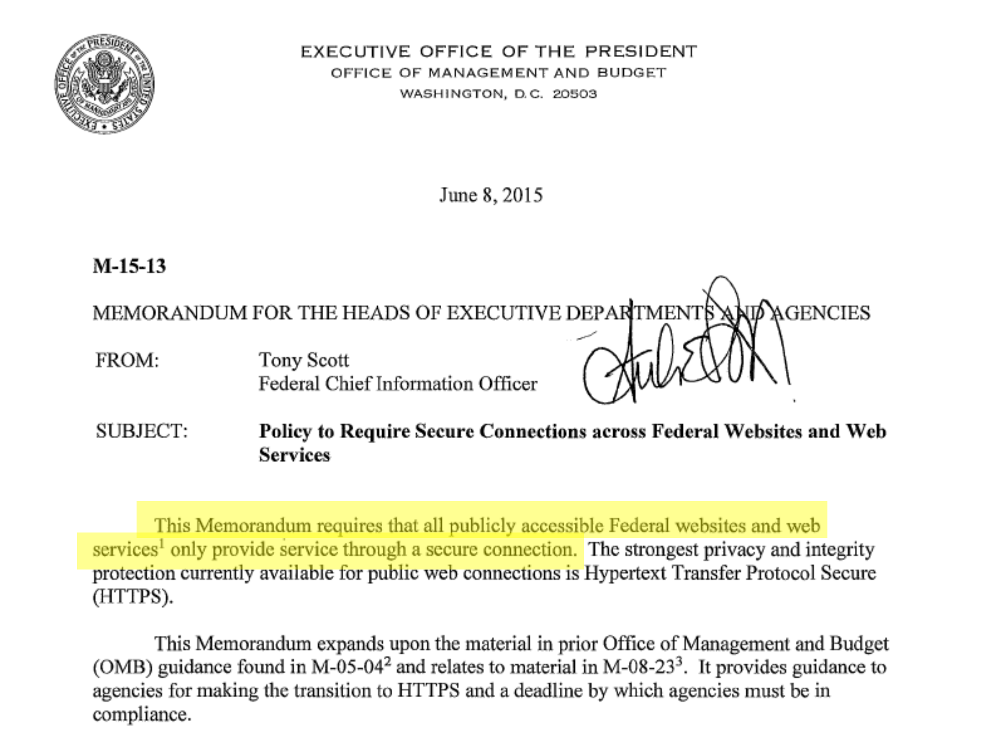


These are the App Transport Security requirements:

- The server must support at least Transport Layer Security (TLS) protocol version 1.2.
- Connection ciphers are limited to those that provide forward secrecy (see the list of ciphers below.)
- Certificates must be signed using a SHA256 or greater signature hash algorithm, with either a 2048-bit or greater RSA key or a 256-bit or greater Elliptic-Curve (ECC) key.

  Invalid certificates result in a hard failure and no connection.

US Government



EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

June 8, 2015

M-15-13

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

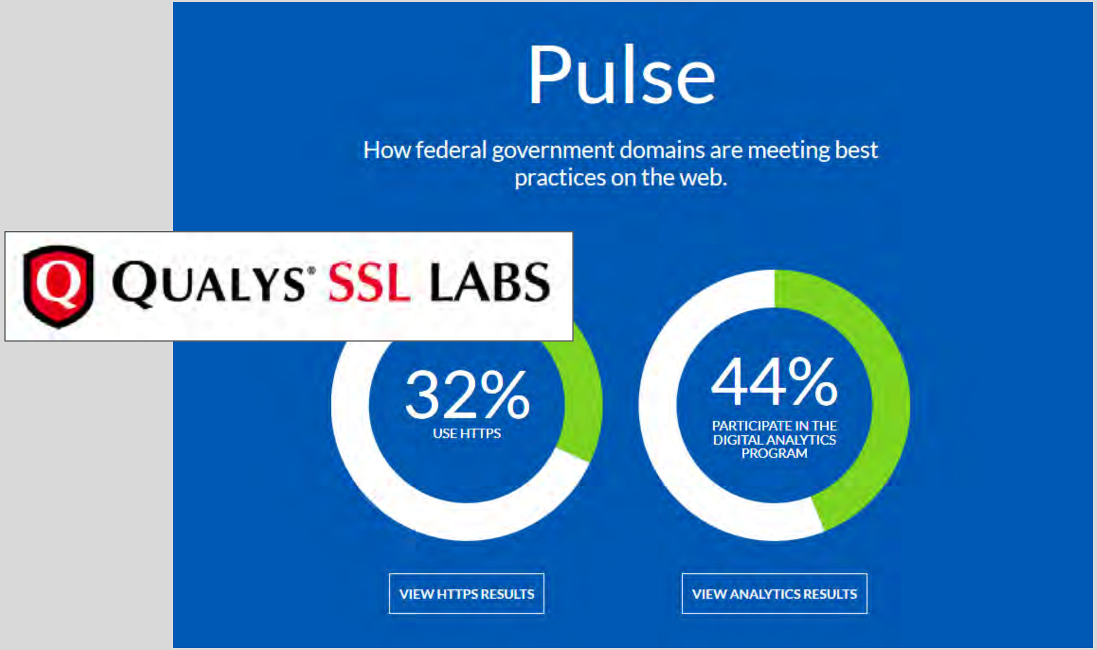
FROM: Tony Scott
Federal Chief Information Officer

SUBJECT: **Policy to Require Secure Connections across Federal Websites and Web Services**

This Memorandum requires that all publicly accessible Federal websites and web services[1] only provide service through a secure connection. The strongest privacy and integrity protection currently available for public web connections is Hypertext Transfer Protocol Secure (HTTPS).

This Memorandum expands upon the material in prior Office of Management and Budget (OMB) guidance found in M-05-04[2] and relates to material in M-08-23[3]. It provides guidance to agencies for making the transition to HTTPS and a deadline by which agencies must be in compliance.

US Government



QUALYS® SSL LABS

Pulse

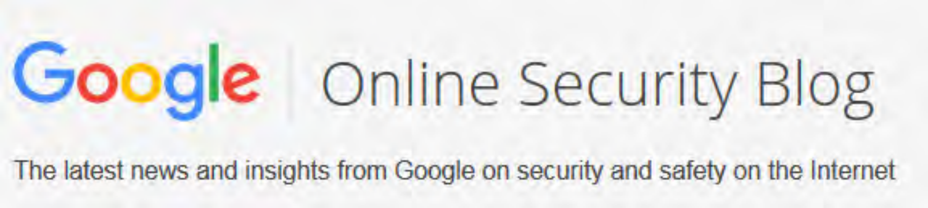
How federal government domains are meeting best practices on the web.

32%
USE HTTPS

44%
PARTICIPATE IN THE DIGITAL ANALYTICS PROGRAM

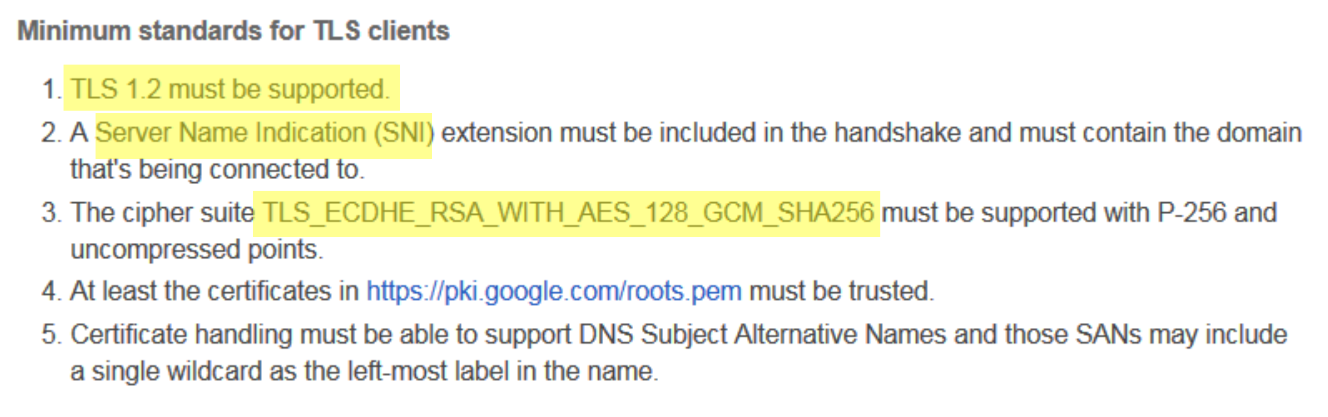
https://pulse.cio.gov

Google



Google Online Security Blog

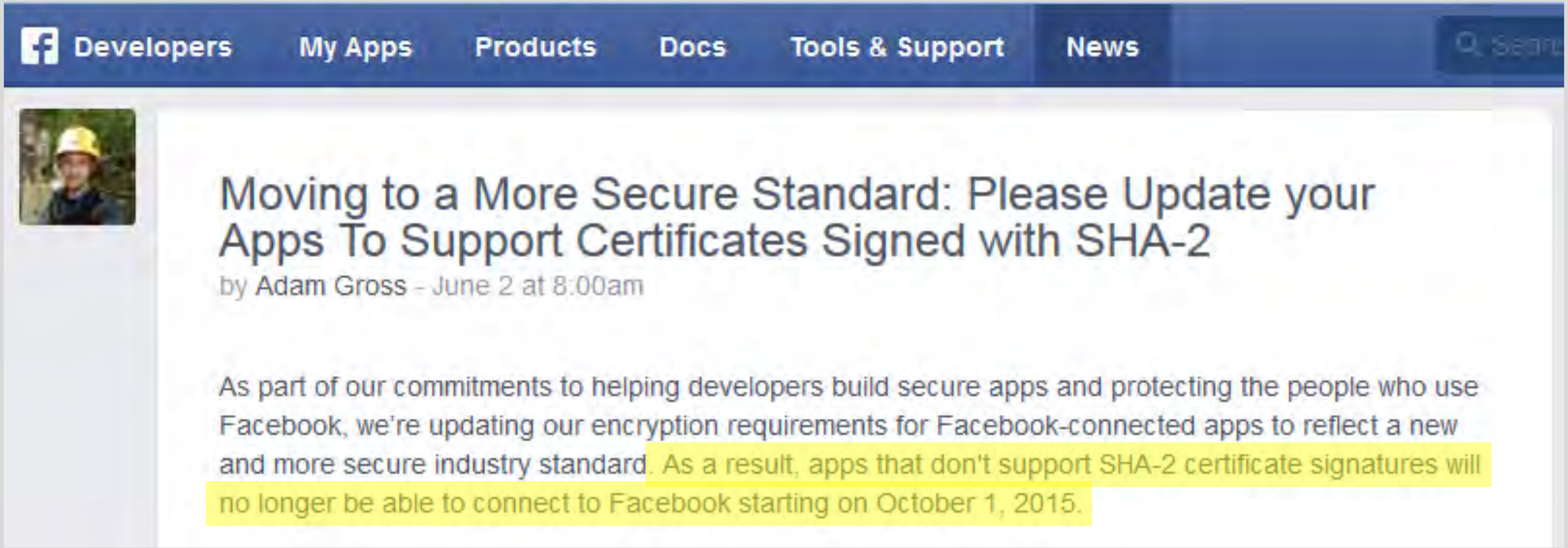
The latest news and insights from Google on security and safety on the Internet



Minimum standards for TLS clients

1. TLS 1.2 must be supported.
2. A Server Name Indication (SNI) extension must be included in the handshake and must contain the domain that's being connected to.
3. The cipher suite TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 must be supported with P-256 and uncompressed points.
4. At least the certificates in https://pki.google.com/roots.pem must be trusted.
5. Certificate handling must be able to support DNS Subject Alternative Names and those SANs may include a single wildcard as the left-most label in the name.

Facebook

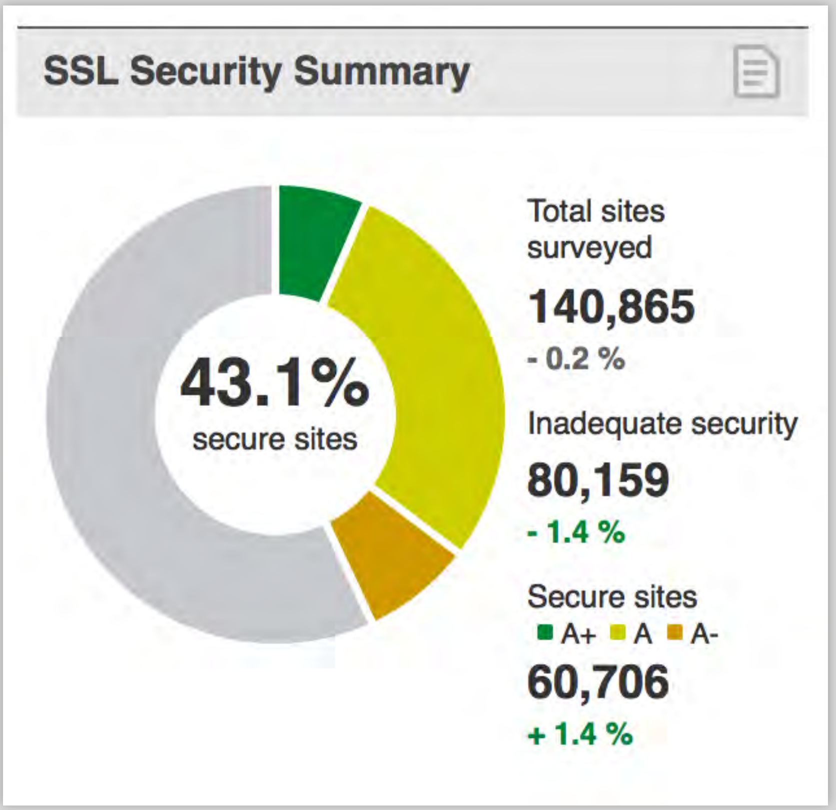


Moving to a More Secure Standard: Please Update your Apps To Support Certificates Signed with SHA-2

by Adam Gross - June 2 at 8:00am

As part of our commitments to helping developers build secure apps and protecting the people who use Facebook, we're updating our encryption requirements for Facebook-connected apps to reflect a new and more secure industry standard. As a result, apps that don't support SHA-2 certificate signatures will no longer be able to connect to Facebook starting on October 1, 2015.

SSL Pulse



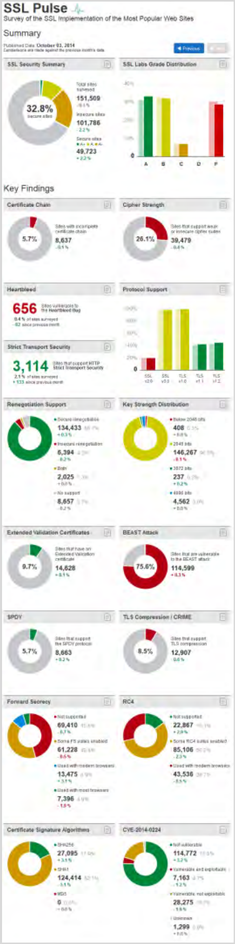
SSL Security Summary

43.1%
secure sites

Total sites surveyed
140,865
- 0.2 %

Inadequate security
80,159
- 1.4 %

Secure sites
🟩 A+ 🟨 A 🟧 A-
60,706
+ 1.4 %



SSL Pulse
Survey of the SSL Implementation of the Most Popular Web Sites

Summary

Published Date: October 03, 2014
Comparisons are made against the previous month's data

◀ Previous

SSL Security Summary

32.8%
secure sites

Total sites surveyed
151,509
-0.1 %

Insecure sites
101,786
- 2.2 %

Secure sites
● A+ ● A ● A-
49,723
+ 2.2 %

SSL Labs Grade Distribution

Key Findings

Certificate Chain

5.7%
Sites with incomplete certificate chain
8,637
-0.1 %

Cipher Strength

26.1%
Sites that support weak or insecure cipher suites
39,479
-0.4 %

Heartbleed

656 Sites vulnerable to the Heartbleed Bug
0.4 % of sites surveyed
-82 since previous month

Strict Transport Security

3,114 Sites that support HTTP Strict Transport Security
2.1 % of sites surveyed
+ 133 since previous month

Protocol Support

Renegotiation Support

● Secure renegotiation
134,433
+ 0.3 %

● Insecure renegotiation
6,394
- 0.2 %

● Both
2,025
+ 0.0 %

● No support
8,657
- 0.2 %

Key Strength Distribution

● Below 2048 bits
408
+ 0.0 %

● 2048 bits
146,267
- 0.1 %

● 3072 bits
237
+ 0.2 %

● 4096 bits
4,562
+ 0.0 %

Extended Validation Certificates

9.7%
Sites that have an Extended Validation certificate
14,628
+ 0.1 %

BEAST Attack

75.6%
Sites that are vulnerable to the BEAST attack
114,599
+ 0.3 %

SPDY

5.7%
Sites that support the SPDY protocol
8,663
+ 0.2 %

TLS Compression / CRIME

8.5%
Sites that support TLS compression
12,907
- 0.6 %

Forward Secrecy

● Not supported
69,410
- 0.7 %

● Some FS suites enabled
61,228
- 0.5 %

● Used with modern browsers
13,475
+ 3.1 %

● Used with most browsers
7,396
- 1.9 %

RC4

● Not supported
22,867
+ 2.9 %

● Some RC4 suites enabled
85,106
- 2.3 %

● Used with modern browsers
43,536
- 8.5 %

Certificate Signature Algorithms

● SHA256
27,095
+ 3.1 %

● SHA1
124,414
- 3.1 %

● MD5
0
+ 0.0 %

CVE-2014-0224

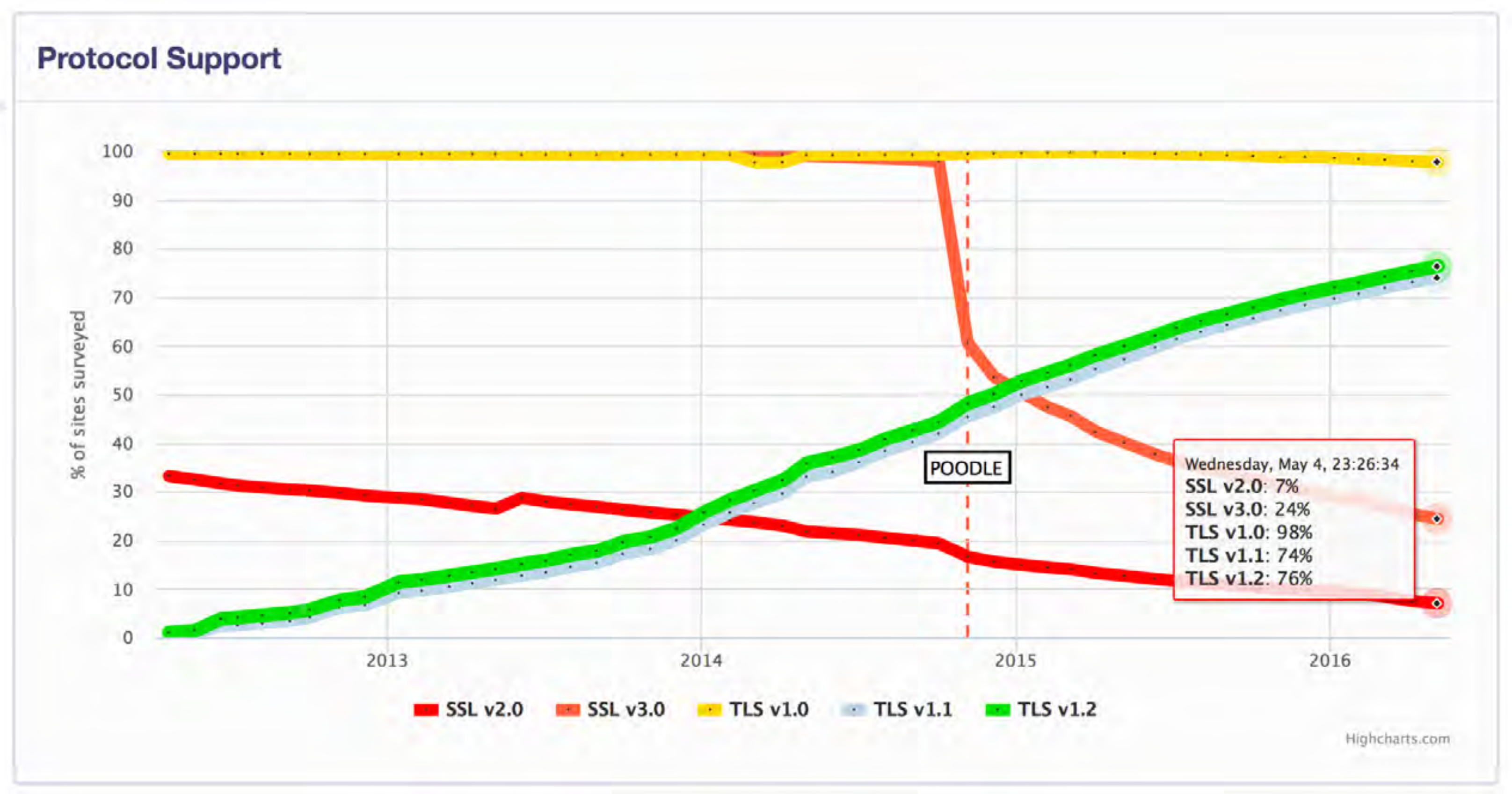
● Not vulnerable
114,772
+ 3.2 %

● Vulnerable and exploitable
7,163
- 1.2 %

● Vulnerable, not exploitable
28,275
- 1.9 %

● Unknown
1,299
+ 0.0 %

SSL Pulse: Protocols



In the meantime, TLS 1.3 is getting a **complete overhaul**

Work began in 2013

Current Status

Enable TLS 1.2

Use AEAD cipher suites

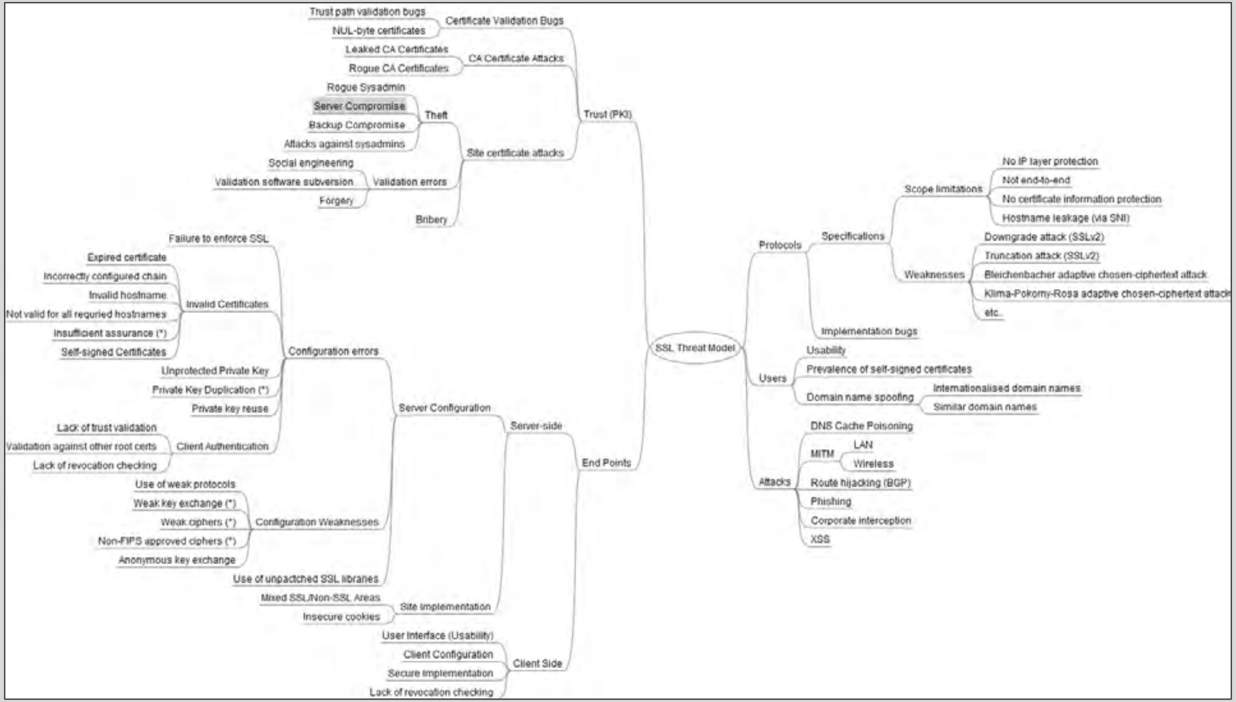
Disable SSL 3 and
(if you can) TLS 1.0

Stop using RC4

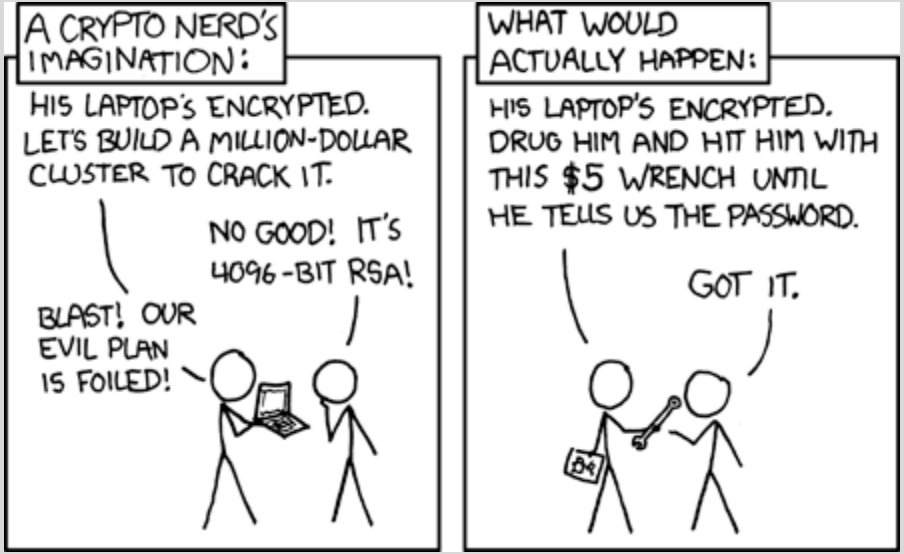
Stop using SHA1 certs

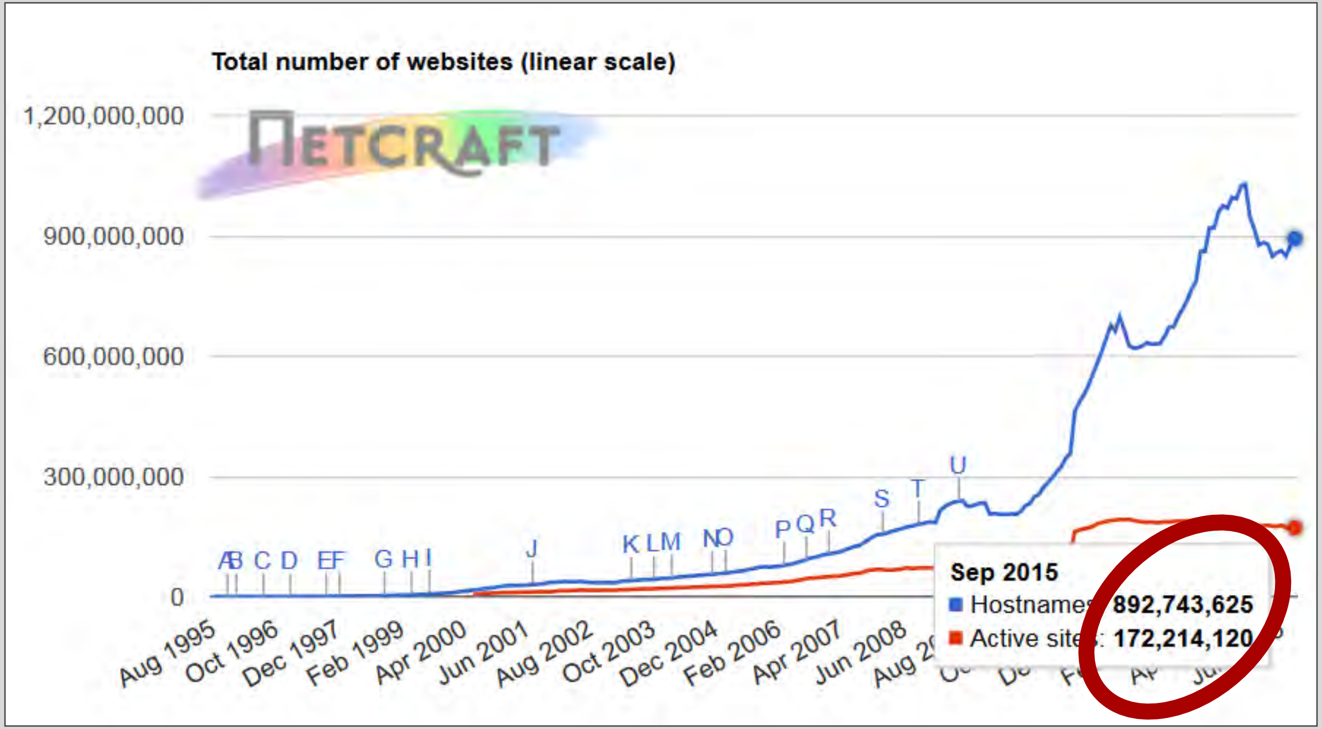
What is your **threat model**?

My 2009 Model



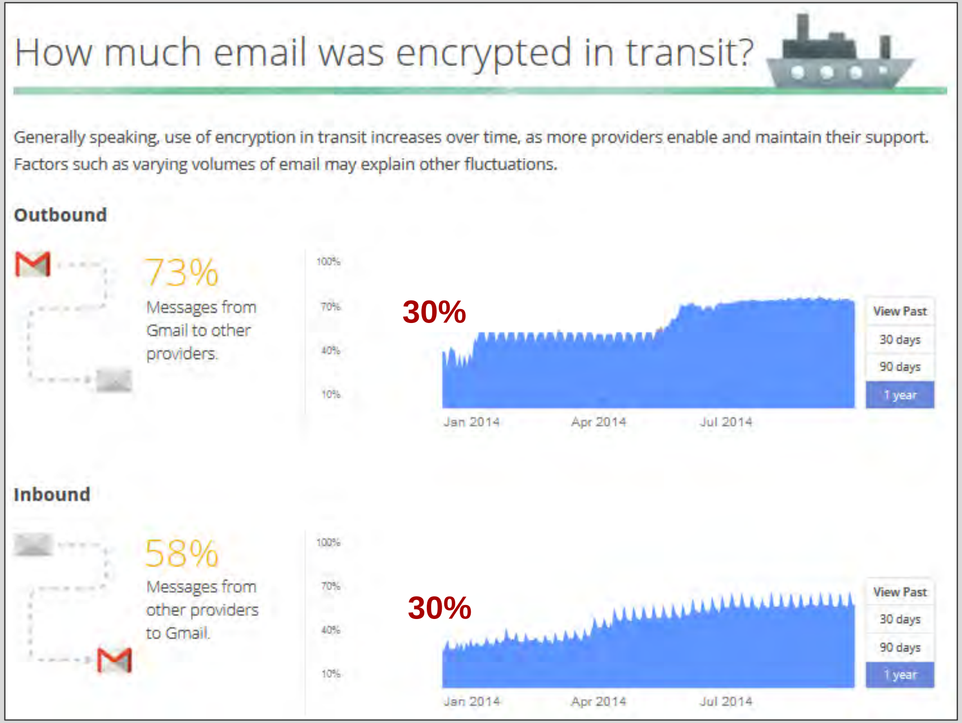
- SSL Threat Model
  - Trust (PKI)
    - Certificate Validation Bugs
      - Trust path validation bugs
      - NUL-byte certificates
    - CA Certificate Attacks
      - Leaked CA Certificates
      - Rogue CA Certificates
    - Site certificate attacks
      - Theft
        - Rogue Sysadmin
        - Server Compromise
        - Backup Compromise
        - Attacks against sysadmins
      - Validation errors
        - Social engineering
        - Validation software subversion
        - Forgery
      - Bribery
  - End Points
    - Server-side
      - Server Configuration
        - Configuration errors
          - Failure to enforce SSL
          - Invalid Certificates
            - Expired certificate
            - Incorrectly configured chain
            - Invalid hostname
            - Not valid for all requried hostnames
            - Insufficient assurance (*)
            - Self-signed Certificates
          - Unprotected Private Key
          - Private Key Duplication (*)
          - Private key reuse
          - Client Authentication
            - Lack of trust validation
            - Validation against other root certs
            - Lack of revocation checking
        - Configuration Weaknesses
          - Use of weak protocols
          - Weak key exchange (*)
          - Weak ciphers (*)
          - Non-FIPS approved ciphers (*)
          - Anonymous key exchange
        - Use of unpactched SSL libraries
      - Site implementation
        - Mixed SSL/Non-SSL Areas
        - Insecure cookies
    - Client Side
      - User Interface (Usability)
      - Client Configuration
      - Secure implementation
      - Lack of revocation checking
  - Protocols
    - Specifications
      - Scope limitations
        - No IP layer protection
        - Not end-to-end
        - No certificate information protection
        - Hostname leakage (via SNI)
      - Weaknesses
        - Downgrade attack (SSLv2)
        - Truncation attack (SSLv2)
        - Bleichenbacher adaptive chosen-ciphertext attack
        - Klima-Pokorny-Rosa adaptive chosen-ciphertext attack
        - etc.
    - Implementation bugs
  - Users
    - Usability
    - Prevalence of self-signed certificates
    - Domain name spoofing
      - Internationalised domain names
      - Similar domain names
  - Attacks
    - DNS Cache Poisoning
    - MITM
      - LAN
      - Wireless
    - Route hijacking (BGP)
    - Phishing
    - Corporate interception
    - XSS


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.



About 170m active sites. Probably less than 5% encrypted.

Lack of Encryption



How much email was encrypted in transit?

Generally speaking, use of encryption in transit increases over time, as more providers enable and maintain their support. Factors such as varying volumes of email may explain other fluctuations.

Outbound

73%

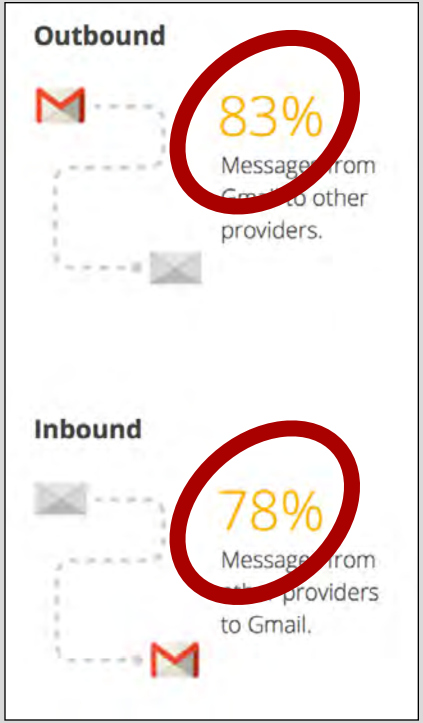
Messages from Gmail to other providers.

Inbound

58%

Messages from other providers to Gmail.

2014



Outbound

83%

Messages from Gmail to other providers.

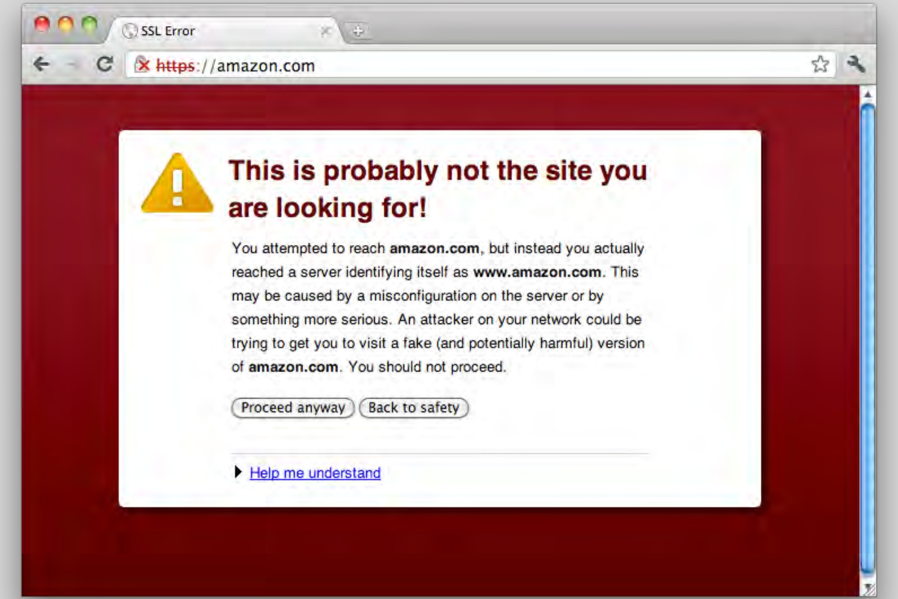
Inbound

78%

Messages from other providers to Gmail.

May 2016

Certificate Warnings



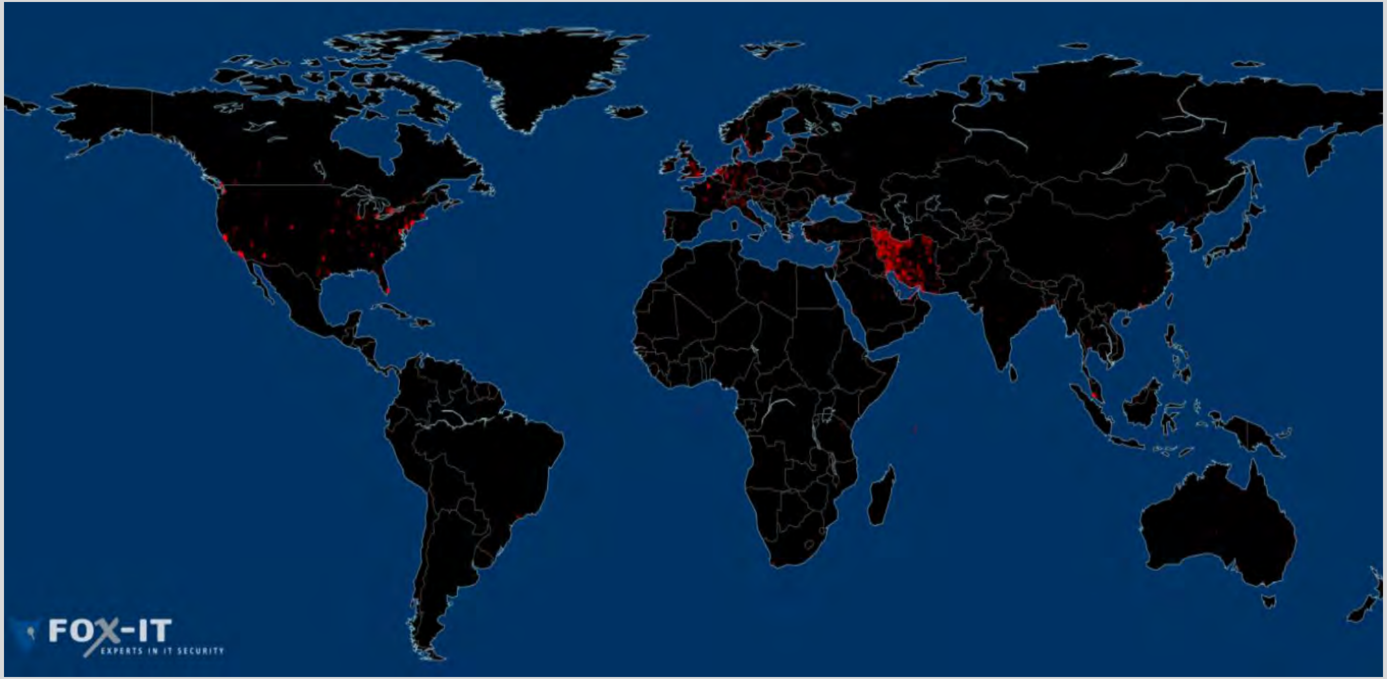
This is probably not the site you are looking for!

You attempted to reach **amazon.com**, but instead you actually reached a server identifying itself as **www.amazon.com**. This may be caused by a misconfiguration on the server or by something more serious. An attacker on your network could be trying to get you to visit a fake (and potentially harmful) version of **amazon.com**. You should not proceed.

Click-through rate: 30-70%

Depends on browser/message style

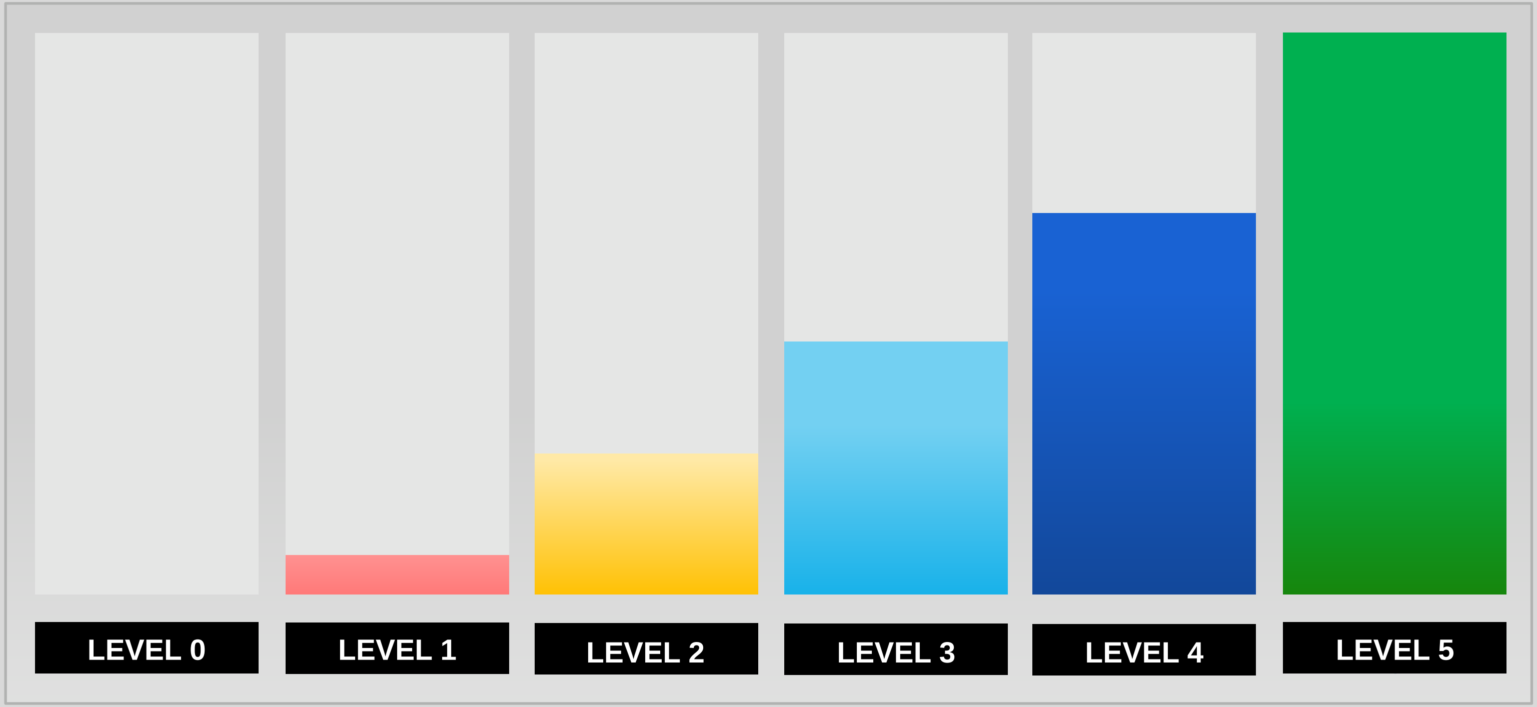
Fraudulent Certificates



The Fall of DigiNotar, 2011

Approx. 300,000 users affected.

TLS Maturity Model



Zero

Chaos

Level 1

Visibility

Level 2
Encryption

Protocols

Cipher Suites

Key

Certificate

Level 3
Application security

All traffic encrypted

Secure cookies

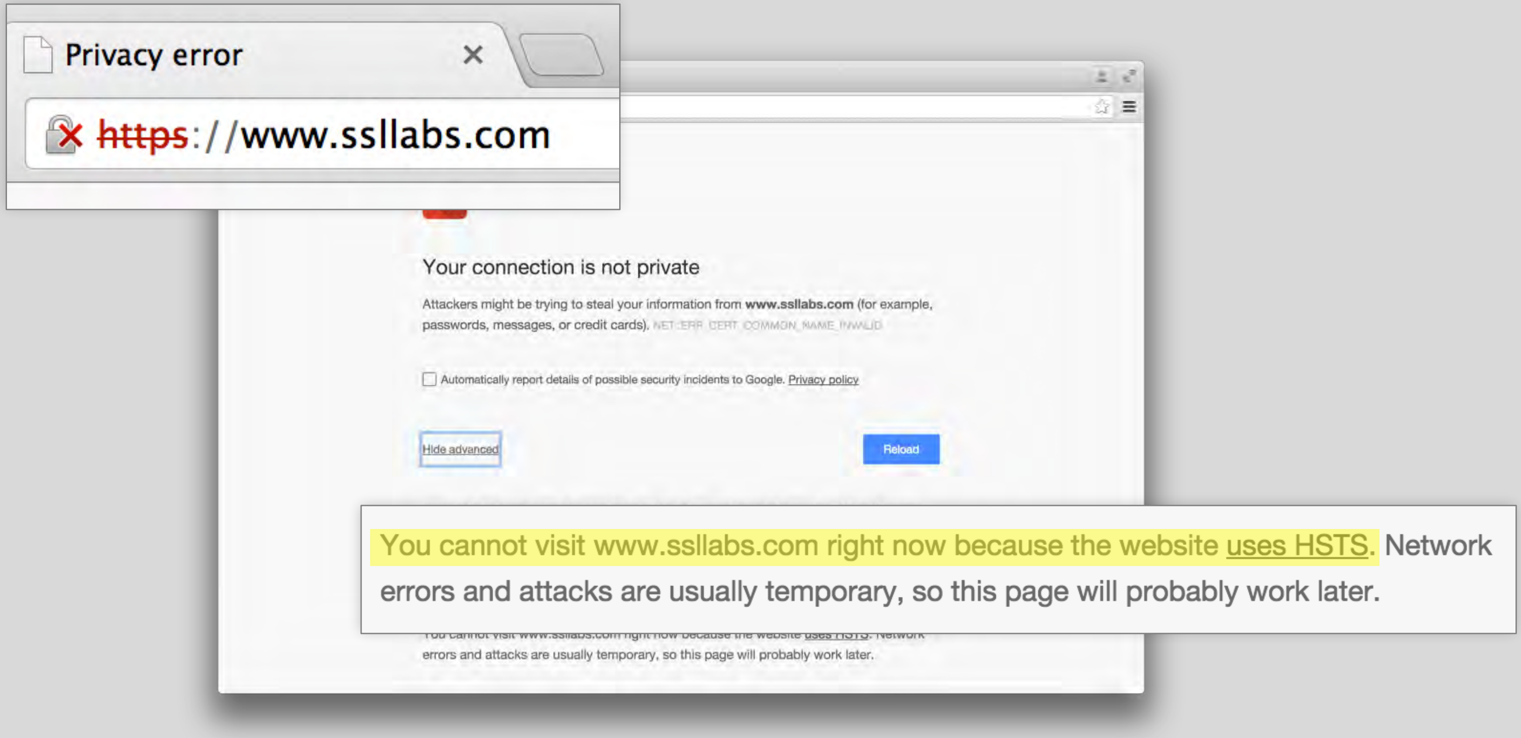
No mixed content

Level 4

Commitment

HTTP Strict Transport Security

Strict Transport Security (HSTS)



Privacy error

~~https~~://www.ssllabs.com

Your connection is not private

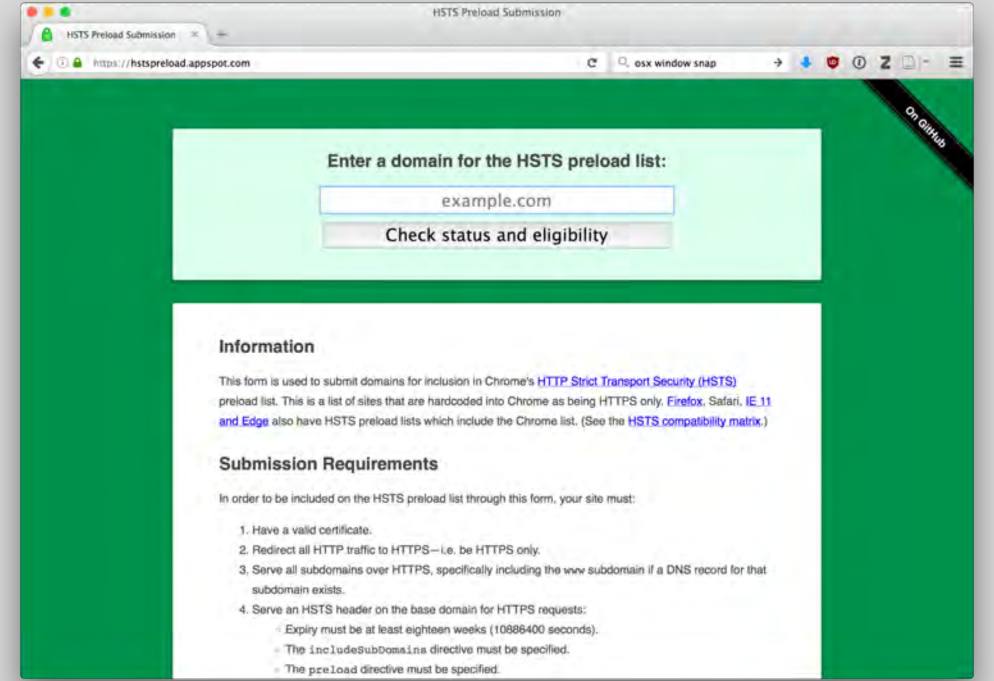
Attackers might be trying to steal your information from **www.ssllabs.com** (for example, passwords, messages, or credit cards). NET::ERR_CERT_COMMON_NAME_INVALID

□ Automatically report details of possible security incidents to Google. Privacy policy

You cannot visit www.ssllabs.com right now because the website uses HSTS. Network errors and attacks are usually temporary, so this page will probably work later.

You cannot visit www.ssllabs.com right now because the website uses HSTS. Network errors and attacks are usually temporary, so this page will probably work later.

HSTS Preloading



Enter a domain for the HSTS preload list:

Information

This form is used to submit domains for inclusion in Chrome's HTTP Strict Transport Security (HSTS) preload list. This is a list of sites that are hardcoded into Chrome as being HTTPS only. Firefox, Safari, IE 11 and Edge also have HSTS preload lists which include the Chrome list. (See the HSTS compatibility matrix.)

Submission Requirements

In order to be included on the HSTS preload list through this form, your site must:

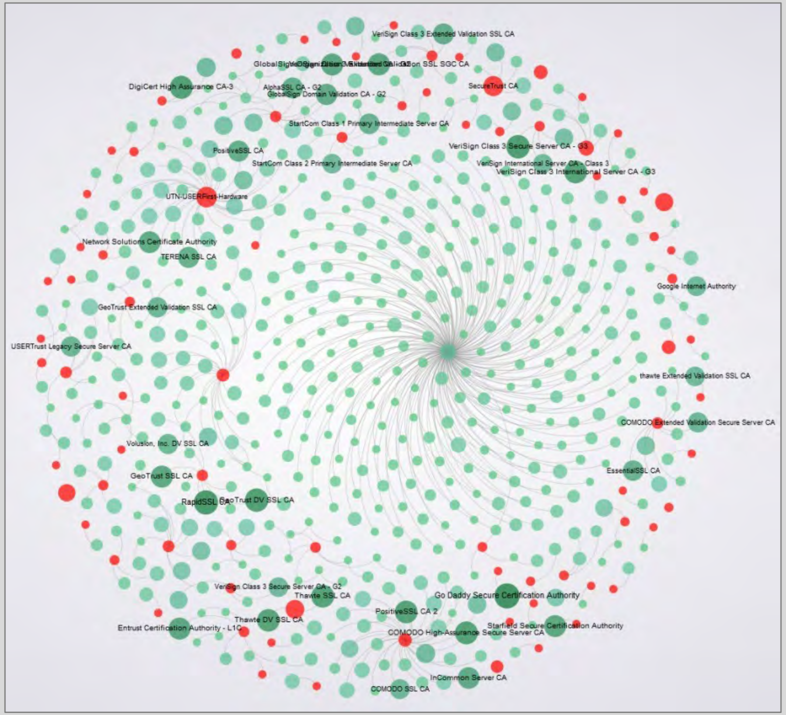
1. Have a valid certificate.
2. Redirect all HTTP traffic to HTTPS—i.e. be HTTPS only.
3. Serve all subdomains over HTTPS, specifically including the www subdomain if a DNS record for that subdomain exists.
4. Serve an HSTS header on the base domain for HTTPS requests:
   - Expiry must be at least eighteen weeks (10886400 seconds).
   - The `includeSubDomains` directive must be specified.
   - The `preload` directive must be specified.

Level 5

Robust Security

Public Key Pinning?

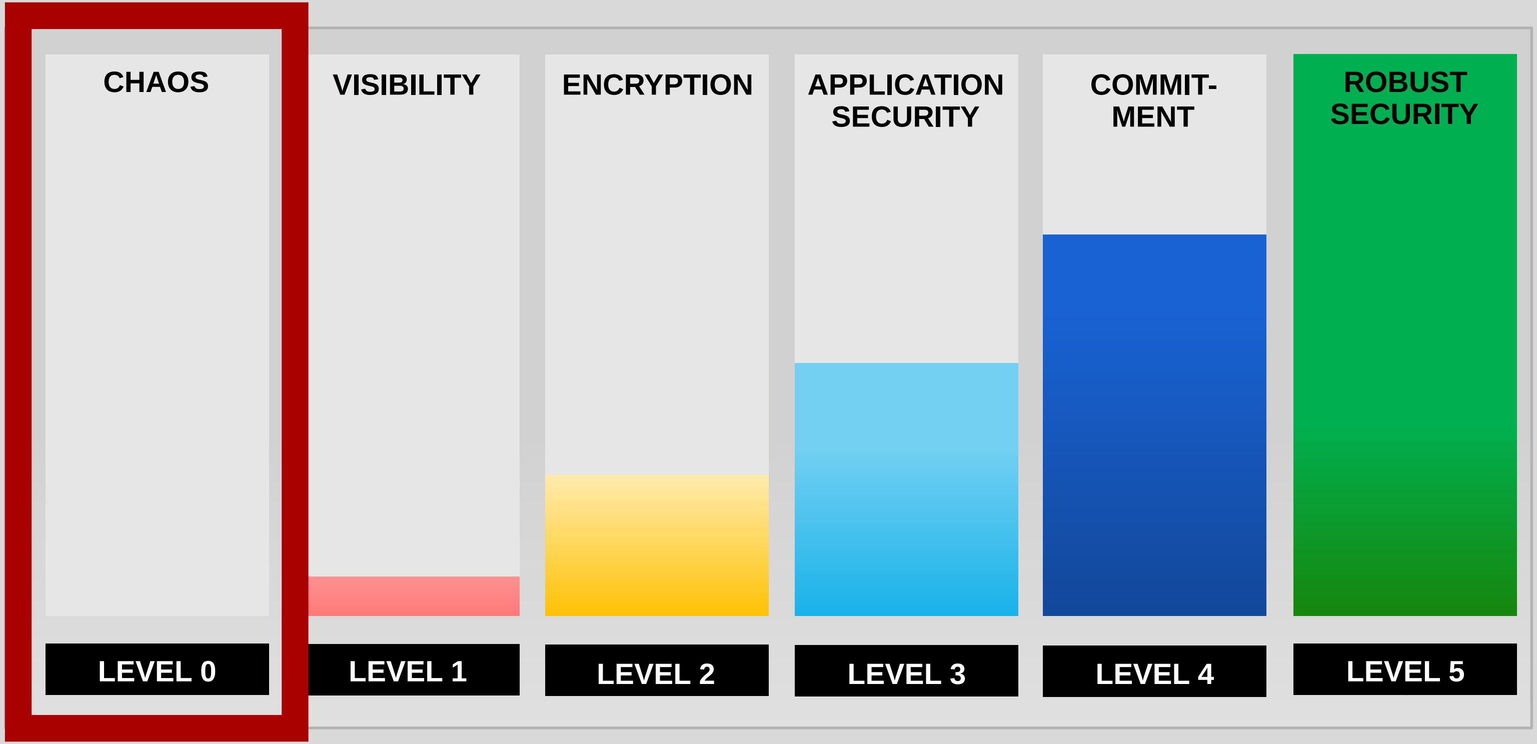
Public Key Pinning (HPKP)


VeriSign Class 3 Extended Validation SSL CA
DigiCert High Assurance CA-3
AlphaSSL CA - G2
GlobalSign Domain Validation CA - G2
SecureTrust CA
StartCom Class 1 Primary Intermediate Server CA
PositiveSSL CA
VeriSign Class 3 Secure Server CA - G3
StartCom Class 2 Primary Intermediate Server CA
VeriSign International Server CA - Class 3
VeriSign Class 3 International Server CA - G3
UTN-USERFirst-Hardware
Network Solutions Certificate Authority
TERENA SSL CA
Google Internet Authority
GeoTrust Extended Validation SSL CA
USERTrust Legacy Secure Server CA
thawte Extended Validation SSL CA
COMODO Extended Validation Secure Server CA
Volusion, Inc. DV SSL CA
GeoTrust SSL CA
EssentialSSL CA
RapidSSL CA
GeoTrust DV SSL CA
VeriSign Class 3 Secure Server CA - G2
Thawte SSL CA
Go Daddy Secure Certification Authority
PositiveSSL CA 2
Thawte DV SSL CA
Starfield Secure Certification Authority
Entrust Certification Authority - L1C
COMODO High-Assurance Secure Server CA
InCommon Server CA
COMODO SSL CA

ICSI Tree of Trust

https://notary.icsi.berkeley.edu/trust-tree/

TLS Maturity Model in Practice



Horizontal vs Vertical Improvement

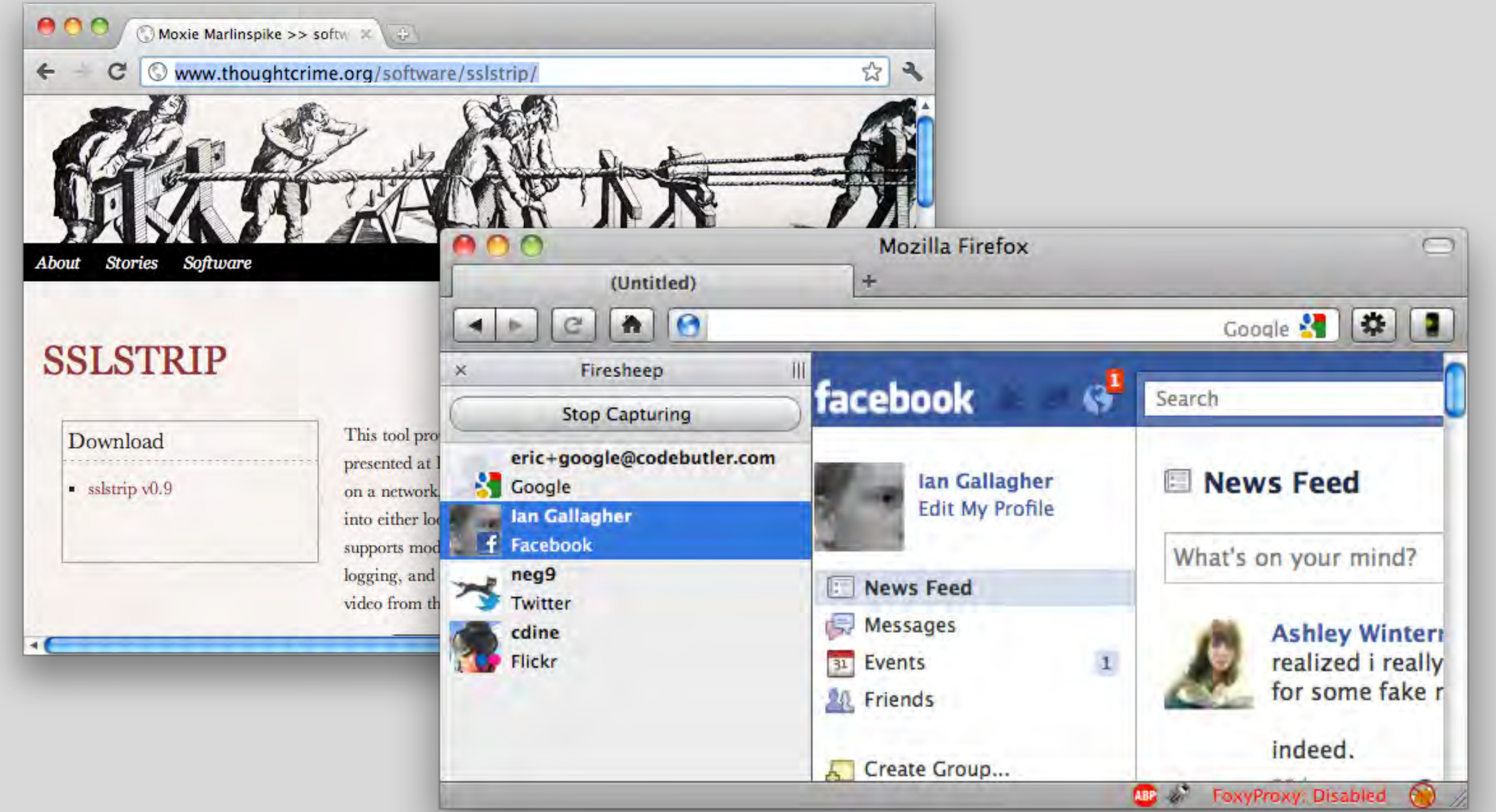
TLS Maturity Model

1. First, achieve **Visibility (1)**
2. Triage
3. Move important sites as fast as possible to **Commitment (4)** or even **Robust Security (5)**
4. Move all sites to **Encryption (2)**
5. Continue bringing the bottom up

Key problems we seemingly solved (or will probably solve)

1 Lack of interest for security until ~2008

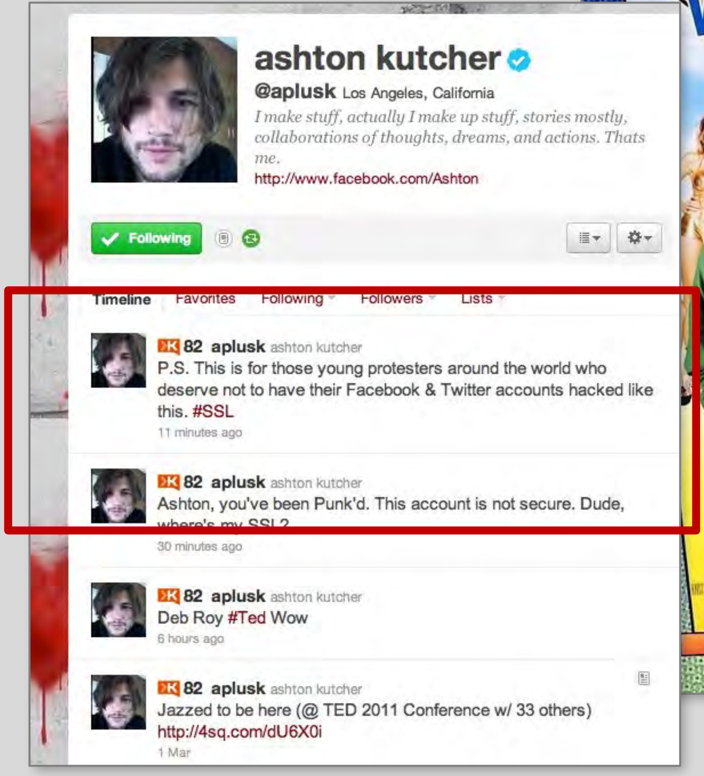
2 Lack of motivation: cost, resources, performance



This tool pro
presented at I
on a network
into either lo
supports mod
logging, and
video from th

realized i really
for some fake r

indeed.



ashton kutcher

@aplusk Los Angeles, California

I make stuff, actually I make up stuff, stories mostly, collaborations of thoughts, dreams, and actions. Thats me.

http://www.facebook.com/Ashton

✓ Following

Timeline Favorites Following Followers Lists

82 aplusk ashton kutcher
P.S. This is for those young protesters around the world who deserve not to have their Facebook & Twitter accounts hacked like this. #SSL
11 minutes ago

82 aplusk ashton kutcher
Ashton, you've been Punk'd. This account is not secure. Dude, where's my SSL?
30 minutes ago

82 aplusk ashton kutcher
Deb Roy #Ted Wow
6 hours ago

82 aplusk ashton kutcher
Jazzed to be here (@ TED 2011 Conference w/ 33 others) http://4sq.com/dU6X0i
1 Mar

ASHTON KUTCHER
SEANN WILLIAM SCOTT
DUDE, Where's my SSL?
AFTER A NIGHT THEY CAN'T REMEMBER, COMES A DAY THEY'LL NEVER FORGET.

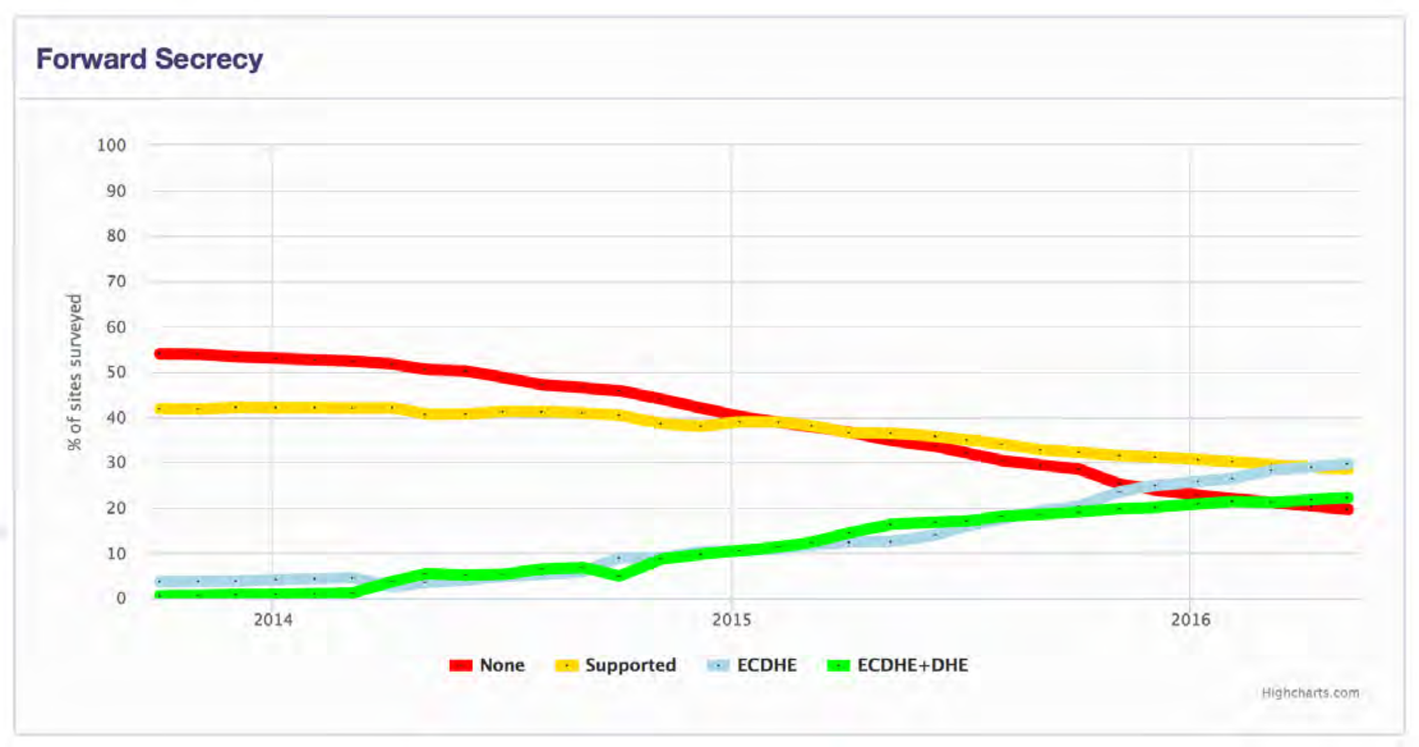
3 Conflicting browser vendor goals: be secure but don’t break anything

4 Virtual secure server hosting not feasible

5 Manual key and certificate management

6 Too many protocol options; sad defaults

SSL Pulse: Forward Secrecy



Positives

- Security became important
- Opt-in mechanisms
- HTTP/2, TLS 1.3, DANE
- Low-cost or free DV certificates
- Automated certificate issuance
- Virtual secure hosting (SNI)

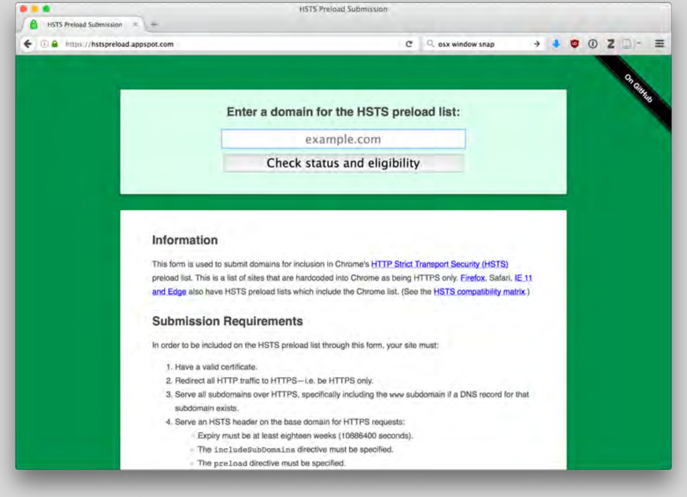
Some remaining rough edges

Public Key Pinning

- HPKP unlikely to be widely adopted
  - Difficult and tricky
  - Very dangerous
  - Requires time, effort, skills

HSTS Preload Scaling

HSTS preload is taking off,
but how to scale it?



Enter a domain for the HSTS preload list:

example.com

Check status and eligibility

Information

This form is used to submit domains for inclusion in Chrome's HTTP Strict Transport Security (HSTS) preload list. This is a list of sites that are hardcoded into Chrome as being HTTPS only. Firefox, Safari, IE 11 and Edge also have HSTS preload lists which include the Chrome list. (See the HSTS compatibility matrix.)

Submission Requirements

In order to be included on the HSTS preload list through this form, your site must:

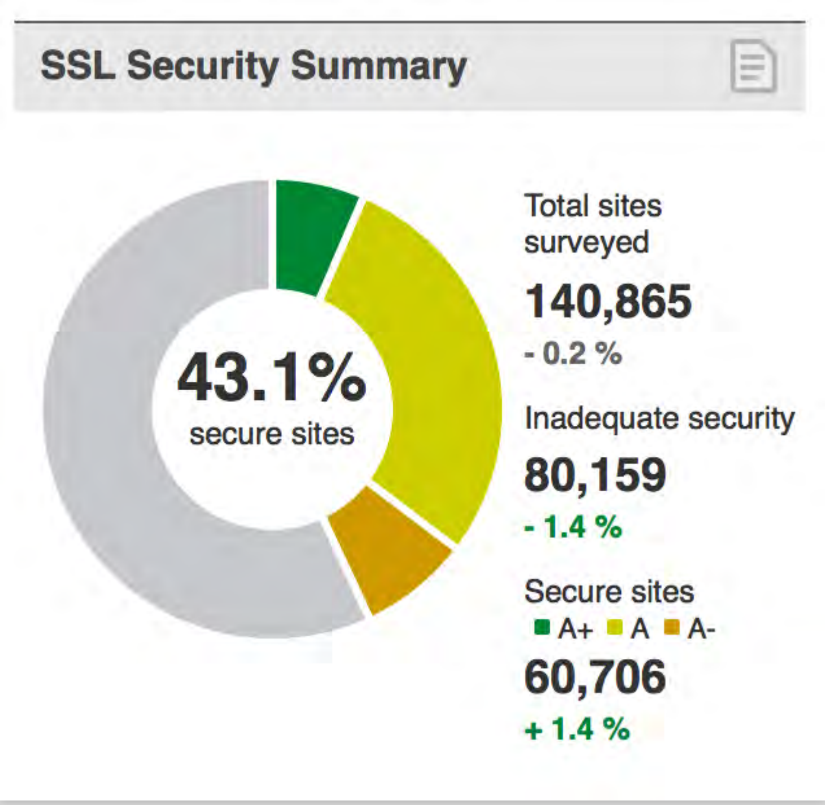
1. Have a valid certificate.
2. Redirect all HTTP traffic to HTTPS—i.e. be HTTPS only.
3. Serve all subdomains over HTTPS, specifically including the www subdomain if a DNS record for that subdomain exists.
4. Serve an HSTS header on the base domain for HTTPS requests:
   - Expiry must be at least eighteen weeks (10886400 seconds).
   - The `includeSubDomains` directive must be specified.
   - The `preload` directive must be specified.

Revocation Doesn’t Work

- Must-staple to the rescue!
- OCSP client implementations not good enough
- Minimising damage of fraudulent certificates?
  - CAA + must-staple?
  - HSTS + must-staple?
- Can must-staple be a lightweight alternative to HPKP?

Ecosystem Monitoring

SSL Pulse



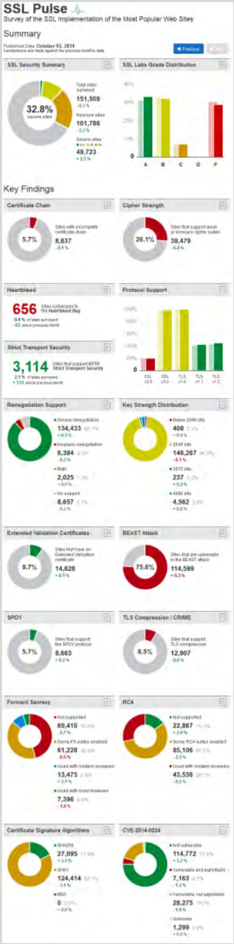
SSL Security Summary

43.1%
secure sites

Total sites surveyed
140,865
- 0.2 %

Inadequate security
80,159
- 1.4 %

Secure sites
🟩 A+ 🟨 A 🟧 A-
60,706
+ 1.4 %



SSL Pulse
Survey of the SSL Implementation of the Most Popular Web Sites

Summary

Published Date: October 03, 2014
Comparisons are made against the previous month's data

SSL Security Summary

32.8%
secure sites

Total sites surveyed
151,509
-0.1 %

Insecure sites
101,786
- 2.2 %

Secure sites
■ A+ ■ A ■ A-
49,723
+ 2.2 %

SSL Labs Grade Distribution

Key Findings

Certificate Chain
5.7%
Sites with incomplete certificate chain
8,637
-0.1 %

Cipher Strength
26.1%
Sites that support weak or insecure cipher suites
39,479
- 0.4 %

Heartbleed
656 Sites vulnerable to the Heartbleed Bug
0.4 % of sites surveyed
-82 since previous month

Strict Transport Security
3,114 Sites that support HTTP Strict Transport Security
2.1 % of sites surveyed
+ 133 since previous month

Protocol Support

Renegotiation Support
● Secure renegotiation
134,433 88.7%
+ 0.3 %
● Insecure renegotiation
6,394 4.2%
- 0.2 %
● Both
2,025 1.3%
+ 0.0 %
● No support
8,657 5.7%
- 0.2 %

Key Strength Distribution
● Below 2048 bits
408 0.3%
+ 0.0 %
● 2048 bits
146,267 96.5%
- 0.1 %
● 3072 bits
237 0.2%
+ 0.2 %
● 4096 bits
4,562 3.0%
+ 0.0 %

Extended Validation Certificates
9.7%
Sites that have an Extended Validation certificate
14,628
+ 0.1 %

BEAST Attack
75.6%
Sites that are vulnerable to the BEAST attack
114,599
+ 0.3 %

SPDY
5.7%
Sites that support the SPDY protocol
8,663
+ 0.2 %

TLS Compression / CRIME
8.5%
Sites that support TLS compression
12,907
- 0.6 %

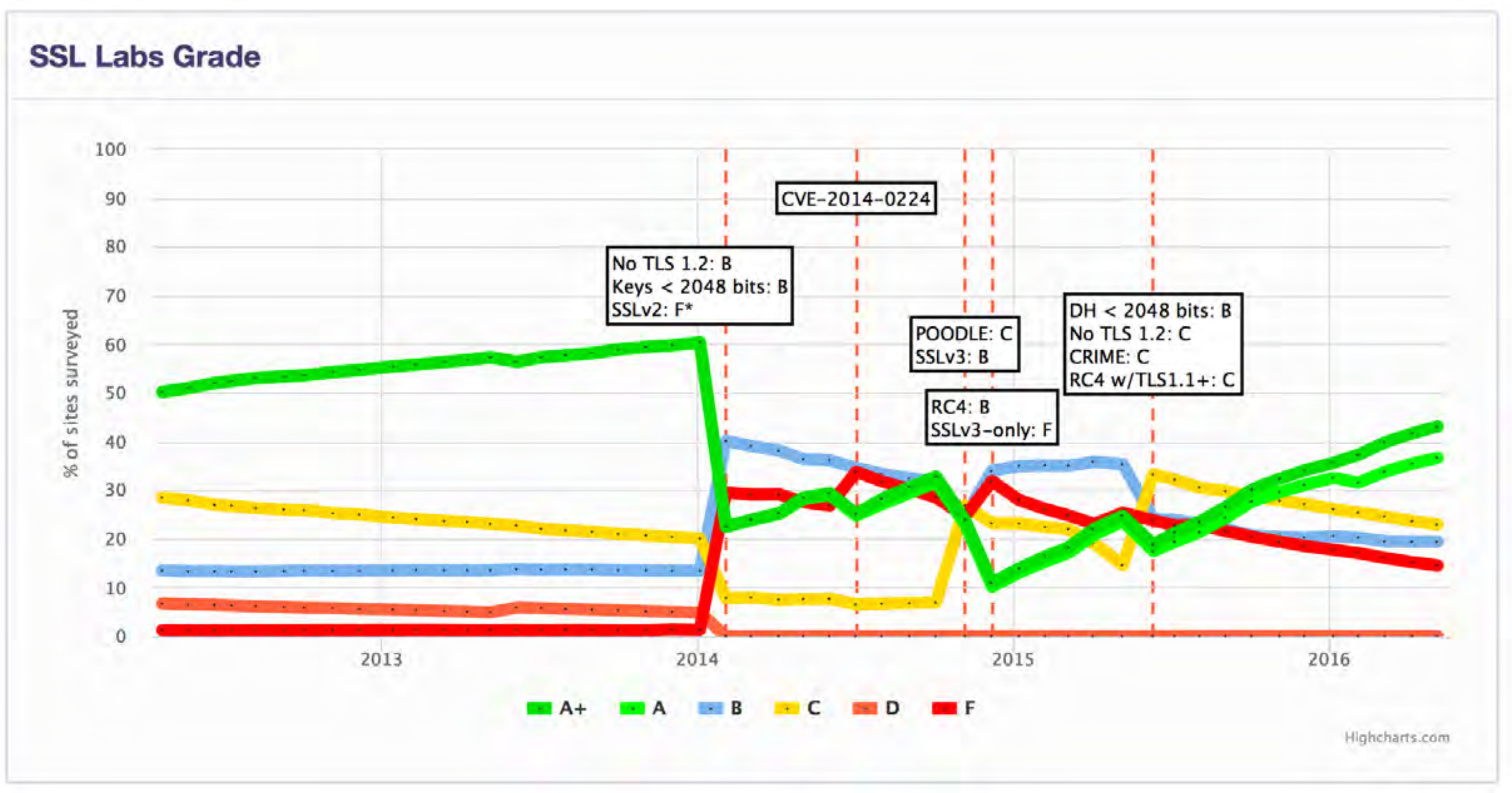
Forward Secrecy
● Not supported
69,410 45.8%
- 0.7 %
● Some FS suites enabled
61,228 40.4%
- 0.5 %
● Used with modern browsers
13,475 8.9%
+ 3.1 %
● Used with most browsers
7,396 4.9%
- 1.9 %

RC4
● Not supported
22,867 15.1%
+ 2.9 %
● Some RC4 suites enabled
85,106 56.2%
- 2.3 %
● Used with modern browsers
43,536 28.7%
- 0.5 %

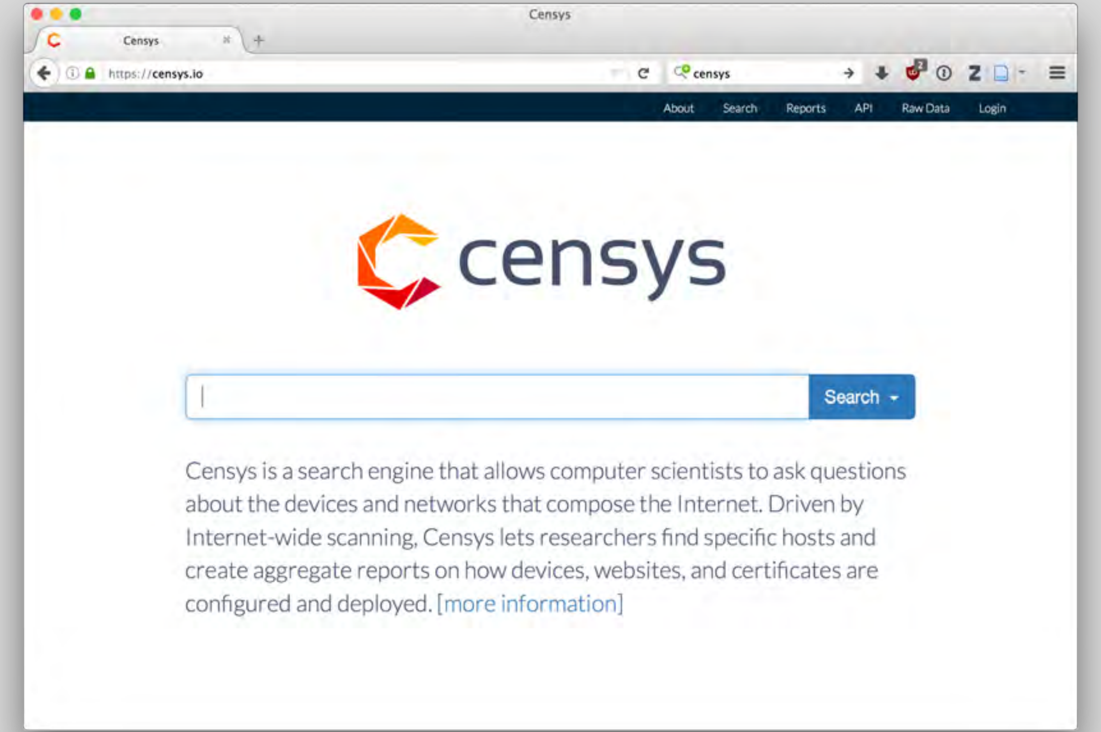
Certificate Signature Algorithms
● SHA256
27,095 17.9%
+ 3.1 %
● SHA1
124,414 82.1%
- 3.1 %
● MD5
0 0.0%
+ 0.0 %

CVE-2014-0224
● Not vulnerable
114,772 75.8%
+ 3.2 %
● Vulnerable and exploitable
7,163 4.7%
- 1.2 %
● Vulnerable, not exploitable
28,275 18.7%
- 1.9 %
● Unknown
1,299 0.9%
+ 0.0 %

SSL Pulse: Grades



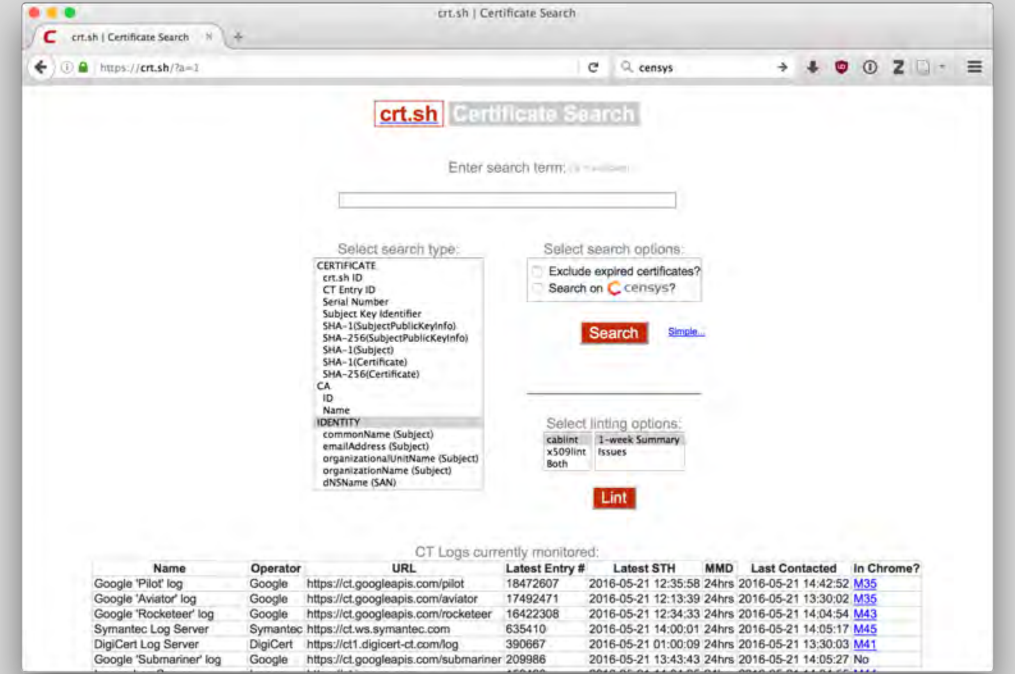
Censys



Censys is a search engine that allows computer scientists to ask questions about the devices and networks that compose the Internet. Driven by Internet-wide scanning, Censys lets researchers find specific hosts and create aggregate reports on how devices, websites, and certificates are configured and deployed. [more information]

censys.io

crt.sh



crt.sh Certificate Search

Enter search term:

Select search type:

CERTIFICATE
crt.sh ID
CT Entry ID
Serial Number
Subject Key Identifier
SHA-1(SubjectPublicKeyInfo)
SHA-256(SubjectPublicKeyInfo)
SHA-1(Subject)
SHA-1(Certificate)
SHA-256(Certificate)
CA
ID
Name
IDENTITY
commonName (Subject)
emailAddress (Subject)
organizationalUnitName (Subject)
organizationName (Subject)
dNSName (SAN)

Select search options:

□ Exclude expired certificates?
□ Search on censys?

Search Simple...

Select linting options:

cablint
x509lint
Both

1-week Summary
Issues

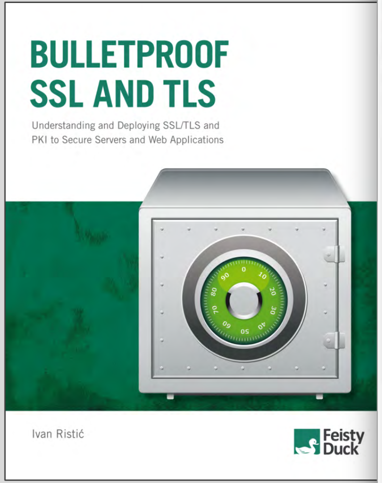
Lint

CT Logs currently monitored:

Name	Operator	URL	Latest Entry #	Latest STH	MMD	Last Contacted	In Chrome?
Google 'Pilot' log	Google	https://ct.googleapis.com/pilot	18472607	2016-05-21 12:35:58	24hrs	2016-05-21 14:42:52	M35
Google 'Aviator' log	Google	https://ct.googleapis.com/aviator	17492471	2016-05-21 12:13:39	24hrs	2016-05-21 13:30:02	M35
Google 'Rocketeer' log	Google	https://ct.googleapis.com/rocketeer	16422308	2016-05-21 12:34:33	24hrs	2016-05-21 14:04:54	M43
Symantec Log Server	Symantec	https://ct.ws.symantec.com	635410	2016-05-21 14:00:01	24hrs	2016-05-21 14:05:17	M45
DigiCert Log Server	DigiCert	https://ct1.digicert-ct.com/log	390667	2016-05-21 01:00:09	24hrs	2016-05-21 13:30:03	M41
Google 'Submariner' log	Google	https://ct.googleapis.com/submariner	209986	2016-05-21 13:43:43	24hrs	2016-05-21 14:05:27	No

crt.sh

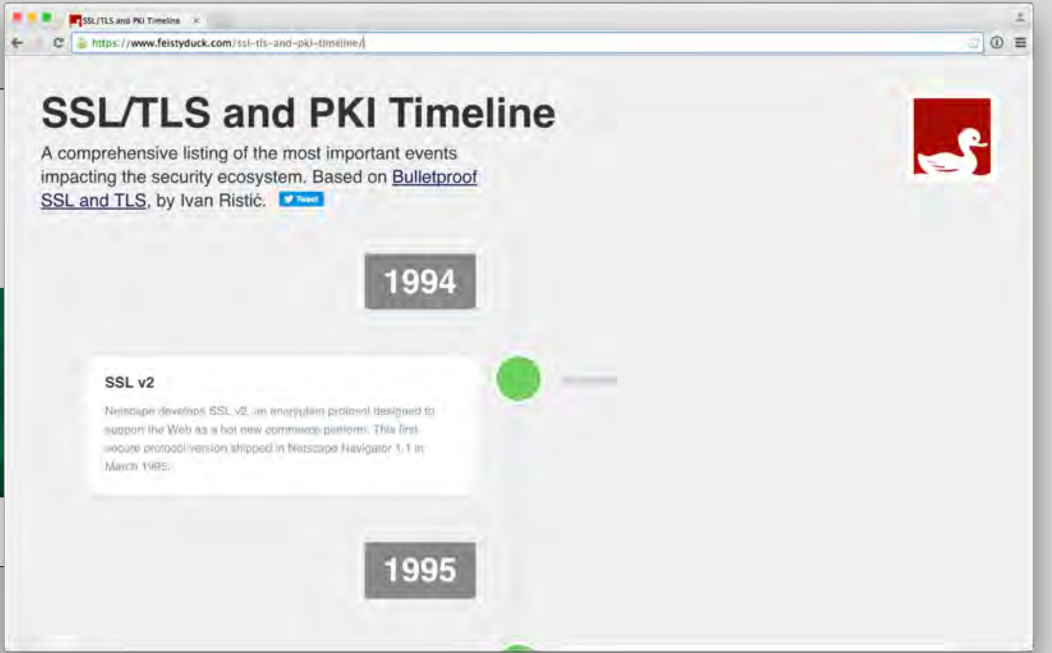
SSL/TLS and PKI Timeline



BULLETPROOF SSL AND TLS

Understanding and Deploying SSL/TLS and PKI to Secure Servers and Web Applications

Ivan Ristić



SSL/TLS and PKI Timeline

A comprehensive listing of the most important events impacting the security ecosystem. Based on Bulletproof SSL and TLS, by Ivan Ristić.

1994

SSL v2

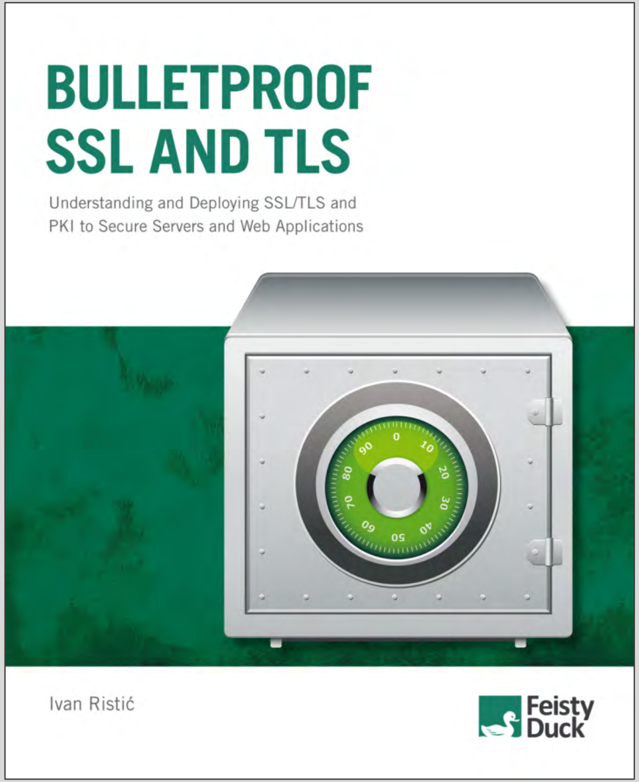
Netscape develops SSL v2, an encryption protocol designed to support the Web as a hot new commerce platform. This first secure protocol version shipped in Netscape Navigator 1.1 in March 1995.

1995

www.feistyduck.com/ssl-tls-and-pki-timeline/

Thank you!

ivanr@feistyduck.com
@ivanristic



BULLETPROOF SSL AND TLS

Understanding and Deploying SSL/TLS and
PKI to Secure Servers and Web Applications

Ivan Ristić

Feisty Duck