Some Thoughts On SSL/TLS and PKI

Ivan Ristić
My recent work (for context)
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
Deploying TLS securely is getting more complicated, not less.
Back in the day, all you needed was a valid certificate.

Today, the certificate comes with a 550-page manual.
TLS 1.2

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)
“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.
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.
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 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 and relates to material in M-08-23. It provides guidance to agencies for making the transition to HTTPS and a deadline by which agencies must be in compliance.
Pulse
How federal government domains are meeting best practices on the web.

QUALYS’ SSL LABS

32% USE HTTPS

44% PARTICIPATE IN THE DIGITAL ANALYTICS PROGRAM

https://pulse.cio.gov
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

Total sites surveyed
140,865
- 0.2%

Inadequate security
80,159
- 1.4%

Secure sites
- A+
- A
- A-
60,706
+ 1.4%
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
**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.
- 30% (May 2016)
- 30% (2014)

Inbound

- 58% Messages from other providers to Gmail.
- 30% (May 2016)
- 30% (2014)

Outbound

- 83% Messages from other providers.

Inbound

- 78% Messages from other providers to Gmail.

2014

May 2016
Certificate Warnings

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)

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:

example.com

Check status and eligibility

Information

This form is used to submit domains for inclusion in Opera’s HTTP Strict Transport Security (HSTS) preload list. This is a list of sites that are hard-coded 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:
   - ‘max_age’ must be at least eighteen weeks (10884400 seconds).
   - The inclusion of "max_age" directive must be specified.
   - The "preload" directive must be specified.
Level 5

Robust Security

Public Key Pinning?
Public Key Pinning (HPKP)

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
ashton kutcher
@aplusk Los Angeles, California

I make stuff, actually I make up stuff, stories mostly, collaborations of thoughts, dreams, and actions. That's me.
http://www.facebook.com/Ashton

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, we're in @ TED 2011! :O
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://4aq.com/5U6XG
1 day ago
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?
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

- Total sites surveyed: 140,865
- Inadequate security: 80,159
- Secure sites: 60,706

43.1% secure sites
- 0.2%
- 1.4%
- +1.4%
SSL Pulse: Grades

SSL Labs Grade

- No TLS 1.2: B
- Keys < 2048 bits: B
- SSLv2: F*
- POODLE: C
- SSLv3: B
- RC4: B
- SSLv3-only: F
- DH < 2048 bits: B
- No TLS 1.2: C
- CRIME: C
- RC4 w/TLS1.1+: C
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]
SSL/TLS and PKI Timeline

www.feistyduck.com/ssl-tls-and-pki-timeline/
Thank you!

ivanr@feistyduck.com
@ivanristic