HTTPS: Achievements, Challenges, and Epiphany

Michael Catanzaro <mcatanzaro@igalia.com>

December 7, 2015

Web Engines Hackfest

HTTPS Basics

Man-in-the-Middle (MITM) Attacks

- ARP spoofing
- WPAD hijacking
- DNS hijacking
- DNS cache poisoning
- BGP route hijacking

(List stolen from *Bulletproof SSL and TLS* by Ivan Ristić.)

Secure Sockets Layer (SSL) vs. Transport Layer Security (TLS)

- SSL 2.0 (lol insecure)
- SSL 3.0 (very insecure)
- TLS 1.0 (somewhat secure)
- TLS 1.1 (somewhat secure)
- TLS 1.2 (possibly very secure)

Key Exchange

- RSA: Rivest-Shamir-Adleman
  - Bad, no forward secrecy
  - Slow
- DHE: Ephemeral Diffie-Hellman
  - Bad, allows server to use weak primes to secure key exchange
  - Very slow
- ECDHE: Ephemeral elliptic curve Diffie-Hellman
  - Usually uses RSA or ECDSA
  - Probably not backdoored by NSA
  - Fast!

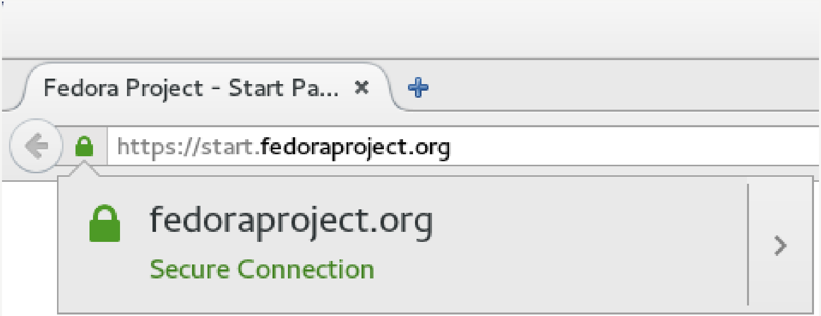
Ciphers

- Stream ciphers: RC4 (insecure)
- Block ciphers: 3DES (OK), AES (good), Camellia (good)
- Block cipher modes: ECB (insecure), CBC (OK), GCM (good)
- Best option is probably AES-128, GCM mode

Message Authentication Codes (MACs)

- SHA-1 (good)
- SHA-256 (wasteful)
- SHA-384

Domain Validation Certificates



Fedora Project - Start Pa...

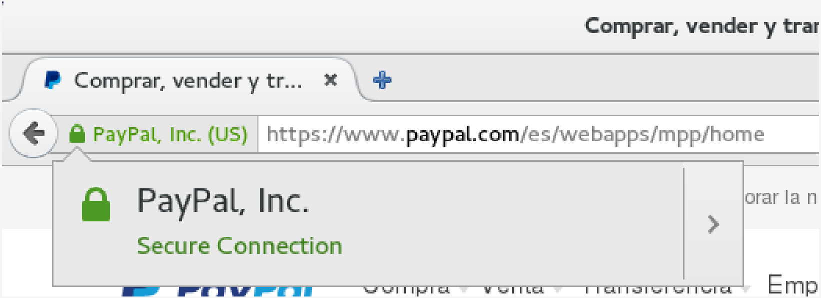
https://start.fedoraproject.org

fedoraproject.org

Secure Connection

Figure 1: Domain validation, organization validation

Extended Validation Certificates



Comprar, vender y trar

Comprar, vender y tr...

PayPal, Inc. (US)

https://www.paypal.com/es/webapps/mpp/home

PayPal, Inc.

Secure Connection

orar la n

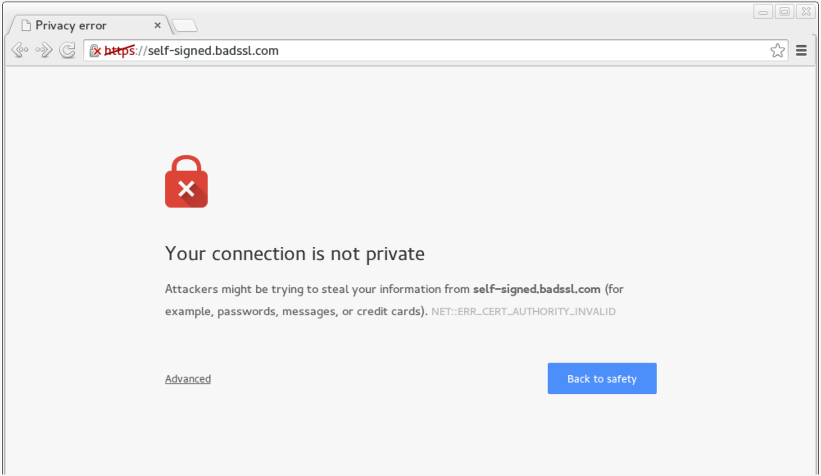
Emp

Figure 2: Extended validation

Certificate Verification

- Server sends a chain of certificates, each signed by the next.
- Final certificate must be signed by a root installed on the system. (Or not.)
- Should be at least two certificates in the chain.

Invalid Certificates



Your connection is not private

Attackers might be trying to steal your information from **self-signed.badssl.com** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

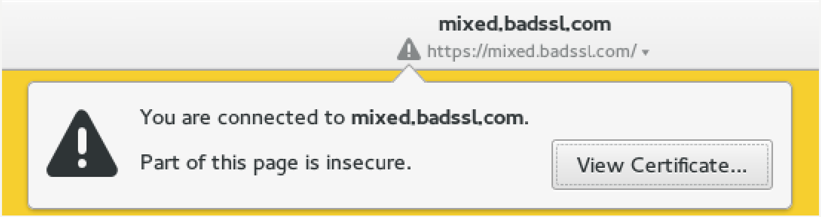
Figure 3: Chrome

Achievements

Removal of Insecure Protocols

- All major browsers, and WebKitGTK+, dropped support for SSL 3.0
- All major browsers pledged to drop support for RC4 in near future; WebKitGTK+ was first!

Mixed Content



mixed.badssl.com

https://mixed.badssl.com/

You are connected to **mixed.badssl.com**.

Part of this page is insecure.

Figure 4: Epiphany

- Solution: upgrade-insecure-requests
  - Content security policy (CSP) header
  - Supported by Firefox and Chrome
  - Not supported in WebKitGTK+

Distrusting Weak Certificates

- 1024-bit RSA keys
  - 1024-bit roots removed from ca-certificates (Firefox)
  - Degrade security indicator in Chrome and Firefox(?)
  - Not detected by WebKitGTK+
- SHA-1 signatures
  - Degrade security indicator in Chrome and Safari
  - Not detected by WebKitGTK+

New Security Features

- HTTP Strict Transport Security (HSTS)
  - Basic requirement for secure web browsing
  - Supported by all major browsers
  - Not supported in WebKitGTK+/libsoup
- HTTP Public Key Pinning (HPKP)
  - Supported by Firefox, Chrome, and Opera
  - Not supported in WebKitGTK+/libsoup
- Certificate Transparency
  - Supported by Chrome
  - Not supported in WebKitGTK+

Challenges

Certificate Revocation

- Certificate revocation lists (CRLs)
  - Bad: too large, slow
- Online Certificate Status Protocol (OCSP)
  - Supported in Internet Explorer, Safari, Firefox, Opera
  - Literally worse than useless
- CRLSet (Chrome)
  - Revocation list for “important” revocations only
- OneCRL (Firefox)
  - Revocation list for intermediate certificates only
- WebKitGTK+/libsoup has no support for certificate revocation

Poor Diffie-Hellman Parameters

- Weak primes (less than 2048 bits)
  - 1024-bit keys permitted by all modern browsers
- Composite (not prime) parameters
  - Permitted by all modern browsers
- Prime reuse
  - Breaking most common prime allows decrypting connections to 18% of top million HTTPS domains
  - Breaking second most common prime allows decrypting connections to 66% of VPN servers, 26% of SSH servers
  - US government has probably done this

Insecure Protocol Version Fallback

- Most browsers attempt TLS 1.2, 1.1, then 1.0
- WebKitGTK+/libsoup attempts only TLS 1.2 then 1.0
- Responsible for severity of POODLE vulnerability
- Firefox allows only for whitelisted (known-broken) sites
- No browsers warn after performing fallback
- Achievement: Fallback SCSV (signaling ciphersuite) allows server to detect a downgrade attack

Other Problems

- Server lacks secure renegotiation extension
- Browser allows key usage violations

Conclusion: Epiphany is the Least-Secure Browser

Summary: Epiphany Has. . .

1. No appropriate UI for EV certificates
2. No support for HSTS
3. No support for HPKP
4. No support for certificate transparency
5. No support for certificate revocation
6. No warning about weak certificates
7. No warning about weak Diffie-Hellman
8. No warnings for other issues

Online TLS Tests

- Client test: https://badssl.com/
- Client test: https://www.ssllabs.com/ssltest/viewMyClient.html
- Server test: https://www.ssllabs.com/ssltest/