SSL/TLS Hardening

Xuesong Chen

Why Important

- Foundation of Internet Security
- De-facto standard of web traffic communication security
- Used to secure millions of websites: banking, e-commerce, etc. and private communication: email, messaging, IP-phone call etc.
- Without SSL/TLS, Internet security is non-existent
- Can be used secure any TCP, UDP based protocols like FTP, SMTP etc.

History

- Originally developed by Netscape
- SSL 2.0 – 1995: totally broken
- SSL 3.0 – 1996: complete redesign, not secure any more
- TLS 1.0 – 1999: still secure if configured properly
- TLS 1.1 – 2006: minor upgrade
- TLS 1.2 – 2008: SHA2, AES, AEAD
- TLS 1.3 – draft as of 04/2015; removes support for many insecure/obsolete features and ciphers

Attacks In Recent Years

- Renegotiation – 2009: plaintext injection vulnerability
- BEAST – 2011: Cipher Block Chaining vulnerability
- CRIME/BREACH – 2012/2013: compression(TLS, HTTP) vulnerability
- RC4 – 2013: bias vulnerability
- POODLE – 2014: padding vulnerability in CBC
- FREAK -2014: weak export key vulnerability

Totally Broken?

- Some network security products claim they can decrypt SSL/TLS packets and inspect content inside(MITM)
- SSL/TLS is designed to prevent MITM
- Assumptions:
  1)SSL/TLS implemented/configured properly on server and client

  2)CA, server and client not compromised

Different Aspects Of Hardening

- Implementation coding vulnerabilities
- Protocol design and cipher flaws
- Defence in depth: countermeasures for different kinds of attacks

Choose Support Versions

- Disable SSL 2.0/3.0
- Web app for browsers: TLS 1.0 needs to be supported; TLS 1.1/1.2 preferred
- No browser support needed: TLS 1.2

Choose Ciphers

- Asymmetric crypto: RSA, DSS – at least 2048 bits
- symmetric crypto: AES – at least 128 bits
- Forward Secrecy: Diffie-Hellman – at least 2048 bits
- Message Authentication Code: HMAC-SHA1, HMAC-SHA2(256, 384, 512)
- Elliptic-Curve: at least 224 bits – security equivalent to asymmetric 2048 bits
- Encryption Mode: AEAD(GCM, CCM) preferred, CBC
- Recommendations:
  TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 for TLS1.2;
  TLS_DHE_RSA_WITH_AES_128_CBC_SHA for TLS1.0

Countermeasures For Attacks

- Certificate pinning(MITM when CA compromised)
- Turn off TLS compression(CRIME/BREACH)
- Forbid client initiated renegotiation(DOS)
- HTTP Strict Transport Security(HTTPS striping)
- Fragment packets(BEAST): do not set SSL_OP_DONT_INSERT_EMPTY_FRAGMENTS
- Enable secure renegotiation: do not set SSL_OP_ALLOW_UNSAFE_LEGACY_RENEGOTIATION
- Use predefined DH parameters
- Randomise TLS payload such as CSRF token(BREACH)

Counter Measures For Attacks

- Summarizing Known Attacks on Transport Layer Security (TLS) and Datagram TLS (DTLS) – 02/2015: http://tools.ietf.org/html/rfc7457
- Always update SSL/TLS libraries to latest patch versions from vendors

Implementations differ!

- Read document/manual carefully
- Try to understand every configuration options
- Change default only when you know exactly what you are doing