SSL/TLS: Still Alive?

Pascal Junod // HEIG-VD
26-03-2015
Agenda

• SSL/TLS Protocol
• Attacks
• What’s next?
SSL/TLS Protocol

https://freakattack.com
SSL/TLS Protocol

- Family of cryptographic protocols offering following functionalities:
  - Entity authentication (uni- or bi-directional, via X.509v3)
  - Communications confidentiality and integrity
  - Cipher suites negotiation
  - Key session management
  - Compression
SSL/TLS Implementations

wolfSSL (formerly cyaSSL)

GnuTLS

NSS

Mozilla

Secure Transport

Developer

MatrixSSL

JSSE

Java

Bouncy Castle

BSAFE

NSS

mozilla

OpenSSL

Cryptography and SSL/TLS Toolkit

libreSSL

Botan

Schannel

mbed TLS

Microsoft

ARM mbed

# History of SSL/TLS

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Developer</th>
<th>Year</th>
<th>Standard/Reference</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL v1.0</td>
<td>Netscape</td>
<td>1993</td>
<td>N/A</td>
<td>Never published</td>
</tr>
<tr>
<td>SSL v2.0</td>
<td>Netscape</td>
<td>1995</td>
<td>N/A</td>
<td>Many security flaws</td>
</tr>
<tr>
<td>SSL v3.0</td>
<td>Netscape</td>
<td>1996</td>
<td>RFC 6101</td>
<td></td>
</tr>
<tr>
<td>TLS 1.0</td>
<td>IETF</td>
<td>1999</td>
<td>RFC 2246. Most frequent</td>
<td></td>
</tr>
<tr>
<td>TLS 1.1</td>
<td>IETF</td>
<td>2006</td>
<td>RFC 4346. Fixes security issues related to CBC</td>
<td></td>
</tr>
<tr>
<td>TLS 1.2</td>
<td>IETF</td>
<td>2008</td>
<td>RFC 5246 and RFC 6176. Supports SHA-256</td>
<td></td>
</tr>
<tr>
<td>TLS 1.3</td>
<td>IETF</td>
<td>N/A</td>
<td>Under development</td>
<td></td>
</tr>
</tbody>
</table>
Attacks against PKIs (1)

- Issuing fake certificates:
  - Verisign / 2001: fake Microsoft code-signing
  - Thawte / 2008: fake certificate for login.live.com issued to security researcher
- CA breached:
  - StartCom / 2008: website breached, validation for any domain
  - Comodo / 2008: validation for any domain
  - Comodo resellers / 2011: breach, issue of 9 fake certificates for popular domain names
  - StartCom / 2011: breach, no fraudulent certificate issued (?)
  - DigiNotar / 2011: complete breach, voluntary bankruptcy
Attacks against PKIs (2)

- Cryptography breached or too weak:
  - RapidSSL / 2008: rogue certificate exploiting MD5 flaws
  - Flame malware / 2011: rogue certificate exploiting MD5 flaws
  - Digicert / 2011: issuing very weak certificates

- Rogue intermediate CAs:
  - Turktrust / 2012: rogue certificated issued
  - ANSSI / 2013: subordinate CA has been found in transparent interception device

- …
Protocol Attacks
Insecure Renegotiation

• aka TLS Authentication Gap

• Discovered by Marsh Ray and Steve Dispensa in 2009

• Leads to a MitM attack

• Mitigation: either disable renegotiation or use Renegotiation Indication extension (2010)
Protocol Attacks

BEAST

• Discovered by Duong and Rizzo in 2011

• Exploits a (previously-known) weakness of predictable IVs for the CBC mode of operations

• Allows to decrypt communications (but not so easily), such as session tokens

• Mitigation: 1/n-1 split, TLS compression helps
Protocol Attacks
Compression Side Channels

• Old attacks known about how compression interacts with encryption (Kelsey, 2002)

• Attacks applied on TLS by Duong and Rizzo in 2012 (CRIME), improved by Be’ery in 2013 (TIME), and by Gluck et al. in 2013 (BREACH)

• Mitigation: SSL/TLS compression must die!
Protocol Attacks
Padding Oracles

• Attack invented in 2001-2002 (Vaudenay, Canvel et al.)

• Al Fardan and Paterson applied it to TLS in 2013 (Lucky13)

• Mitigation: avoid CBC cipher suites
Protocol Attacks

RC4

- Old statistical attacks against RC4 known since 2001 (Mantin and Shamir)
- Recycled against TLS by Al Fardan et al. in 2013
Protocol Attacks

POODLE

• Attack discovered by Möller, Duong and Kotowicz in 2014

• Man-in-the-middle attack taking advantage of fallback to SSL v3 and padding oracles

• Variants even work on TLS for some implementations

• Mitigation: never use SSL v3 again!
Implementation Attacks
Heartbleed

• Implementation flaw in OpenSSL discovered in August 2014

• Leak of internal memory of OpenSSL library (including private keys, passwords, etc.)

• Mitigation: patch, change private keys, etc.
Implementation Attacks

FREAK

• Announced in 2015 by several researchers, notably from INRIA

• Allows an attacker to force a downgrade to export-grade cipher suites on a TLS link

• Bug present in several libraries
In Summary…

- Following SSL/TLS security is not a « long fleuve tranquille »
- Complexity of SSL/TLS does not help, functionality is an enemy of security
- Poor implementation/review quality on (very) popular SSL/TLS libraries, mainly due to catastrophic funding of the projects
- Many, many different ways to defeat SSL/TLS!
Thank you!

@cryptopathe