The State of Apache & SSL

Mark J Cox

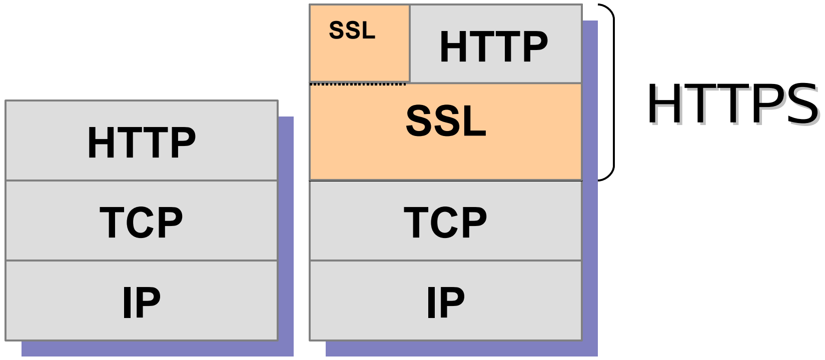
mjc@redhat.com
mjc@apache.org

This presentation

- Overview of current situation
- Historic legal issues
- History of SSL integration into Apache
- Comparison of architectures
- Apache 2.0 and SSL

SSL/TLS Protocol

- HyperText Transfer Protocol (HTTP) is an insecure application level protocol on top of TCP/IP
- HTTP lacks both peer authentication and reliable encrypted communication



- Secure Sockets Layer (SSL) is an additional transport protocol on top of TCP/IP providing communication authentication, privacy and reliability through strong cryptography techniques
- Current standards: SSLv3 (Netscape) and TLSv1 (IETF)
- HTTP Secure (HTTPS) is HTTP over SSL and thus a secure HTTP variant

SSL Versions and Standards

- Various SSL Protocol Versions exists:
  - SSLv1 (Netscape)
    - never released
  - SSLv2 (Netscape)
    - minor security flaws
  - SSLv3 (Netscape)
    - de-facto standard
  - TLSv1 (IETF)
    - cleanup of SSLv3 (so, aka SSL 3.1)
    - standardized by RFC 2246 (Jan 1999)

- RFC 2246 (TLSv1)
  - 80 page description
  - 28 cipher variants (DES, IDEA, RC4, ...)
  - 13 key exchange algorithm variants (DH, RSA, ...)
  - 3 message digest variants (NULL, MD5, SHA1, ...)
  - open structured, i.e. allows for new algorithms to be included in future

Historical Issues: RSA Patent

- Most browsers only support RSA cryptographic algorithms
- Use of these algorithms in the USA before September 2000 required a patent license
- Problems for open source
- Significant barrier to entry
- TLS 1.0 started to address this: complete transactions using non-patented algorithms

Historical Issues: Export

- USA ITAR prohibited export of "strong" encryption (more than 40 bit)
- Later allowed some 128 bit for specific end-users (banks mainly)
  - *Server Gated Cryptography*
  - *Global Server ID certificates*
- Problems for open source projects
  - *Hooks*
  - *USA Hosted projects*
- Later "certified" applications were exportable
  - *Not open-source projects*

Historical Issues: CAs

- Secure servers require a certificate signed by a trusted third party
- The list of trusted third parties is controlled by the browser manufacturer
- Main CA was unwilling to sign certificates for “unsupported” software
- Server Gated Cryptography certificates only for “export approved” software

How Apache got around this

- Crypto code was not part of main Apache
  - *Developed completely outside of the USA*
  - *No hooks in Apache*
- Patent Licensing
  - *Okay to use outside of USA*
  - *Inside USA RSA unwilling to give single licenses*
- Commercial versions for the USA
  - *C2Net, Covalent, Red Hat, IBM*

Today

- RSA patent expired September 2000
- Export laws altered for cryptography
  - *Can export to most end-users*
  - *Open source development now possible*
  - *Code is "tainted"*
- CAs liked Apache

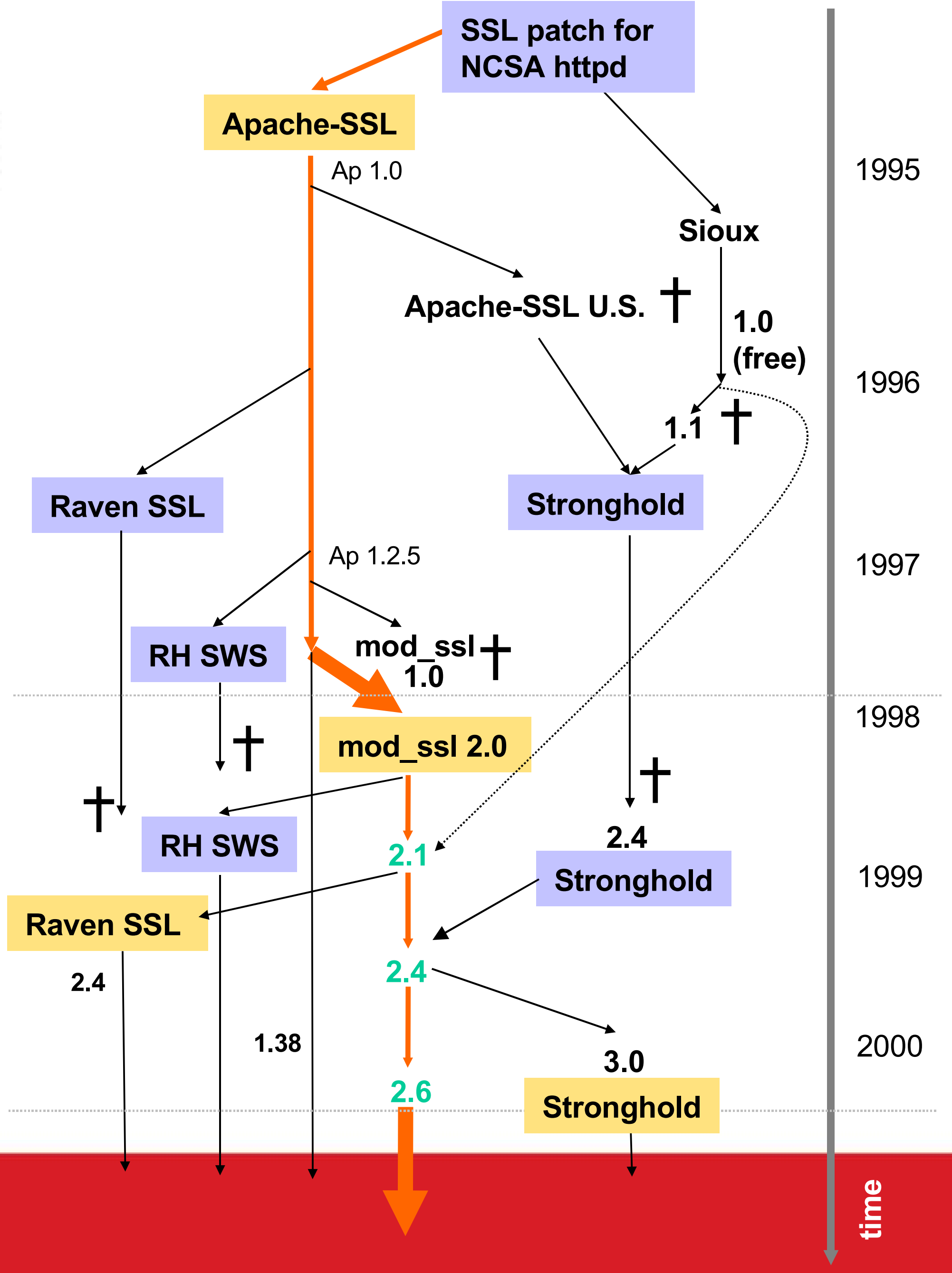
Architecture

- Apache 1.3
- Crypto library that can do SSL
  - *OpenSSL*
  - *RSA-C*
- Module and linking patches for Apache
  - *Apache-SSL*
  - *mod_ssl*

Package Source Size Overview:

Apache:	*80,000 LoC,*	*6 MB*
mod_ssl:	*11,000 LoC,*	*3 MB*
OpenSSL:	*180,000 LoC,*	*12 MB*

Evolution



SSL patch for NCSA httpd

Apache-SSL

Ap 1.0

Sioux

Apache-SSL U.S. †

1.0 (free)

1.1 †

Raven SSL

Stronghold

Ap 1.2.5

RH SWS

mod_ssl 1.0 †

mod_ssl 2.0

†

†

†

RH SWS

2.1

2.4

Stronghold

Raven SSL

2.4

2.4

1.38

3.0

2.6

Stronghold

1995

1996

1997

1998

1999

2000

time

mod_ssl or Apache-SSL?

- Most widely used
  - *150,000 domains*
- Used by commercial vendors
- Many powerful features
- Easy to install/DSO
- EAPI standard

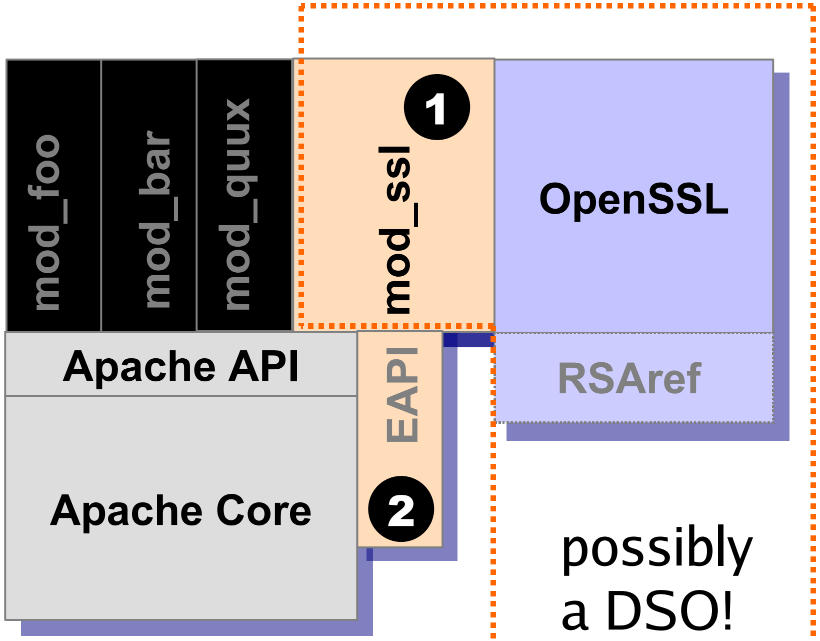
Ralf Engelschall, Germany

- Original module
  - *30,000 domains*
- Aims for stability
- “Spread” session cache
- Less code (<50%)

Ben Laurie, England

mod_ssl Architecture

- mod_ssl is...
  1. *an Apache 1.3 API conforming module (basic functionality)*
  2. *a source patch for the Extended API (additional hooks)*
- mod_ssl is linked against...
  - *OpenSSL (always)*
  - *RSAref (in U.S. only)*
- mod_ssl+OpenSSL+RSAref can be also built as a DSO



mod_ssl example

- Use of boolean expressions to perform fine-grained client certificate based access authentication

```
# httpd.conf
    :
<VirtualHost _default_:443>
    :
SSLCACertificatePath /path/to/ssl.ca/
SSLVerifyClient      optional
SSLVerifyDepth       10
SSLRequireSSL
SSLRequire (    %{SSL_CIPHER} !~ m/^(EXP|NULL)-/                 \
            and %{SSL_CLIENT_S_DN_O} eq "Snake Oil, Ltd."        \
            and %{SSL_CLIENT_S_DN_OU} in { "Staff", "CA", "Dev“} \
            and %{TIME_WDAY} >= 1 and %{TIME_WDAY} <= 5          \
            and %{TIME_HOUR} >= 8 and %{TIME_HOUR} <= 20     ) \
           or %{REMOTE_ADDR} =~ m/^141\.1\.129\.[0-9]+$/
    :
</VirtualHost>
    :
```

Future of Apache and SSL

- Apache 1.3
  - *Continues to be updated to fix major bugs*
  - *No plans to integrate EAPI or other features*
- Apache 2.0
  - *Significant changes to internals*
  - *SSL is made much easier*
  - *2.0 first beta expected very shortly*
  - *2.0 acceptance by end of 2001?*
  - *No SSL module currently available*

The State of Apache & SSL

Mark J Cox

mjc@apache.org
mjc@redhat.com

Some slide contents and graphics used with permission from Ralf Engelschall, www.engelschall.com