# Handout

Ralf S. Engelschall
ApacheCon´98

Contribution to the Security Track at ApacheCon´98

Engel schall

## Security with

**The Apache Interface to SSLeay**

Title
Motivation
Solutions
Overview
Develop.
Installation
HTTPS
Use Cases

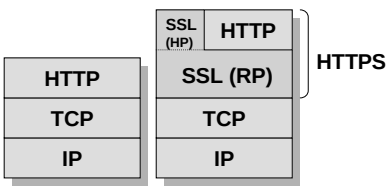
**Ralf S. Engelschall**
rse@engelschall.com
www.engelschall.com



Engel schall

## Motivation

- HyperText Transfer Protocol (HTTP) is an unsecure 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 a secure HTTP variant




Title
Motivation
Solutions
Overview
Develop.
Installation
HTTPS
Use Cases

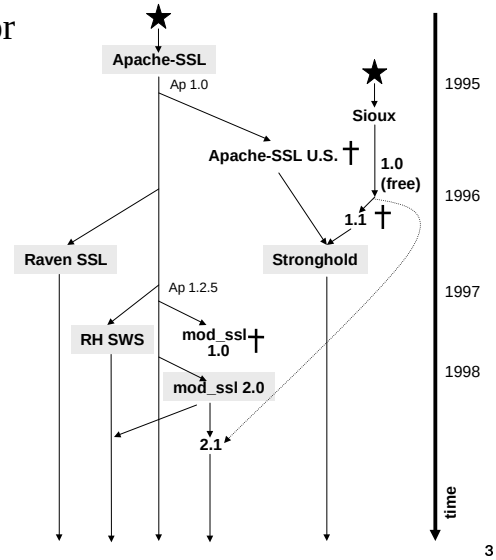


Online Version:
http://www.engelschall.com/sw/mod_ssl/docs/apachecon/

## Solutions: Overview

Engel schall

- Five SSL solutions for Apache are currently available:
  - **Apache-SSL**
    Ben Laurie, UK
    www.apache-ssl.org/
  - **mod_ssl**
    Ralf S. Engelschall, DE
    www.engelschall.com/sw/mod_ssl/
  - **Stronghold**
    C2Net, US/UK
    www.c2.net/products/stronghold/
  - **Raven SSL**
    Covalent, US
    raven.covalent.com/
  - **RH SWS**
    RedHat, US
    www.redhat.com/products/product-details.phtml?id=rhsa





Title
Motivation
Solutions
Overview
Develop.
Installation
HTTPS
Use Cases


3

## Solutions: Comparison

Engel schall

| | Apache-SSL | mod_ssl | RH SWS | Raven SSL | Stronghold |
|---|---|---|---|---|---|
| **Author** | B. Laurie | R. Engelschall | RedHat | Covalent | C2 Net |
| **Location** | UK | DE | US | US | US, UK |
| **License** | open-source | open-source | commercial | commercial | commercial |
| **Price** | $0 | $0 | $99 | $357 | $995 |
| **Distribution** | full source | full source | source (Ap.) + binary (SSL) | source (Ap.) + binary (SSL) | source (Ap.) + binary (SSL) |
| **Availability** | world-wide | world-wide | US only | US only | world-wide |
| **US Usage** | restricted | restricted | unlimited | unlimited | unlimited |
| **Support** | voluntary, always free | voluntary, always free | conceding, 90 days free | conceding, 30 days free | conceding, 30 days free |
| **SSL Engine** | SSLeay | SSLeay [+ RSAref] | SSLeay + BSAFE | SSLeay + BSAFE | SSLeay |
| **Unix** | All derivates | All derivates | RH Linux | 15 derivates | 20 derivates |
| **Win32** | no | yes | no | no | no |
| **Current Version** | 1.27 (1.3) | 2.0.13 (1.3) 2.1b6 (1.3) | 2.0 (1.3) | -- (1.3) | 2.3 (1.2) 2.4 (1.3) |

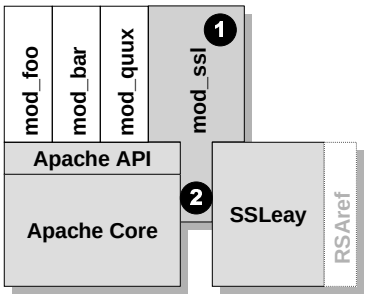

Title
Motivation
Solutions
Overview
Develop.
Installation
HTTPS
Use Cases


4

## Package Overview

Engel schall

- mod_ssl is...
  1. an Apache API conforming module (basic functionality)
  2. a source patch for the Apache API (crypto hooks)




- mod_ssl is actively developed and enhanced
- mod_ssl is maintained and distributed from Germany and Switzerland
- for easy building and installing mod_ssl uses an automated patching mechanism and is fully integrated into APACI

Title
Motivation
Solutions
Overview
Develop.
Installation
HTTPS
Use Cases

5

## Development Cycle

Engel schall

### mod_ssl 2.0

current stable version

- Complete code overhauling and cleanups
- Finally porting to Apache 1.3 (API, source config stubs)
- Fixing long-standing bugs and flaws
- Fully documenting the whole package (`INSTALL`, `mod_ssl.html`)

### mod_ssl 2.1

current development version

- New pass phrase handling
- New session cache
- New SSL engine logging (levels, error dup, annotat.)
- New „`make certificate`“
- Internal „Mutex“
- HTTPS support for Proxy module
- RSAref support
- Port to Win32

### mod_ssl 2.2

forthcoming version

- Integrated real CA/client cert. management
- Certificate Revocation List (CRL) support
- LDAP support for authentication
- IPC Shared Memory support for session cache

Title
Motivation
Solutions
Overview
Develop.
Installation
HTTPS
Use Cases

6

## Installation Illustration

Engel schall

Title
Motivation
Solutions
Overview
Develop.
Installation
HTTPS
Use Cases

```
$ gunzip <apache_1.3.3.tar.gz | tar xf -
$ gunzip <mod_ssl-2.1b6-1.3.3.tar.gz | tar xf -
$ gunzip <SSLeay-0.9.0b.tar.gz | tar xf -

$ cd SSLeay-0.9.0b
$ make -f Makefile.ssl links
$ perl ./Configure gcc
$ make

$ cd ../mod_ssl-2.1b6-1.3.3
$ ./configure --with-apache=../apache_1.3.3
              --with-ssleay=../SSLeay-0.9.0b
              --prefix=/usr/local/apache

$ cd ../apache_1.3.3
$ make all
$ make certificate
$ make install

$ /usr/local/apache/sbin/httpd -DSSL
$ netscape https://localhost/
```

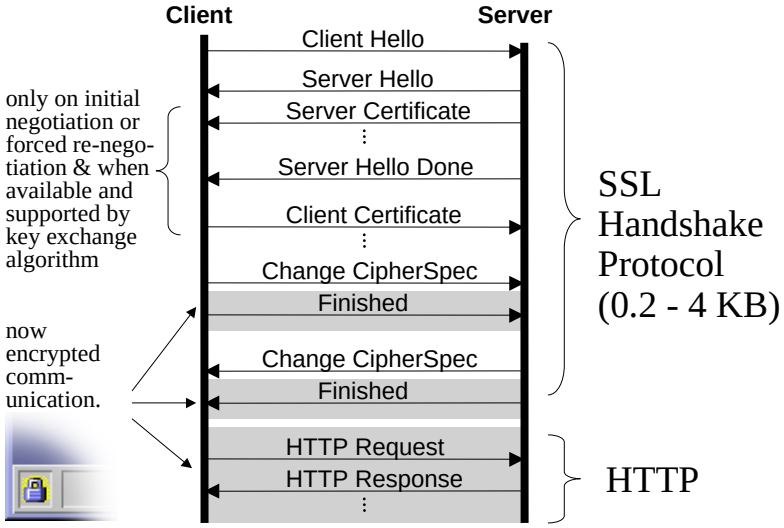
1. extract sources
2. build SSLeay
3. apply mod_ssl to the Apache source tree
4. build and install Apache
5. test the server!

7

## HTTPS Communication

Engel schall

Title
Motivation
Solutions
Overview
Develop.
Installation
HTTPS
Use Cases




8

Engel schall

## Use Cases (1)

- Standard Setup:
  - HTTP on port 80
  - HTTPS on port 443
- Startup:
  - HTTP only:
    `$ httpd`
  - HTTP and HTTPS:
    `$ httpd -DSSL`

```
# httpd.conf
  :
Port 80
  :

<IfDefine SSL>
Listen 80
Listen 443

SSLSessionCache dbm:/var/run/ssl.scache
SSLMutex        file:/var/run/ssl.mutex
SSLLog          /var/log/ssl.log

<VirtualHost _default_:443>
SSLEngine             on
SSLCertificateFile    /etc/ssl.server.crt
SSLCertificateKeyFile /etc/ssl.server.key
SSLVerifyClient       none
</VirtualHost>
</IfDefine>
   :
```

Title
Motivation
Solutions
Overview
Develop.
Installation
HTTPS
Use Cases

9

Engel schall

## Use Cases (2)

- Access Control with „Basic Auth“ through the Subject-DN of the X.509 certificate

```
# /etc/ssl.passwd.foo

/C=DE/L=Munich/CN=Foo:xxj31ZMTZzkVA
/C=US/L=S.F./CN=Bar:xxj31ZMTZzkVA
/C=US/L=L.A./CN=Quux:xxj31ZMTZzkVA
```

```
# httpd.conf
    :
AllowOverride FileInfo AuthConfig
    :
<VirtualHost _default_:443>
    :
SSLCACertificatePath /path/ssl.ca/
SSLVerifyClient      require
SSLVerifyDepth       10
SSLFakeBasicAuth
    :
</VirtualHost>
    :
```

```
# .htaccess

    :
<Files foo.html>
SSLRequireSSL
AuthType      Basic
AuthName      "foo"
AuthUserFile  /etc/ssl.passwd.foo
require       valid-user
</Files>
    :
```

Title
Motivation
Solutions
Overview
Develop.
Installation
HTTPS
Use Cases

10

Engel schall

# Use Cases (3)

- Access Control with „SSLRequire“ through arbitrary boolean expressions

```
# httpd.conf
    :
<VirtualHost _default_:443>
    :
SSLCACertificatePath /path/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/^192\.76\.162\.[0-9]+$/
    :
</VirtualHost>
    :
```

Title
Motivation
Solutions
Overview
Develop.
Installation
HTTPS
Use Cases

11