SWITCH

The Swiss Education & Research Network

Name-based SSL virtual hosts: how to tackle the problem

Kaspar Brand <brand@switch.ch>

2nd SWITCHpki RAO Meeting

Berne, 18 April 2007

When trying to configure Apache…

SWITCH
The Swiss Education & Research Network

This will not work as intended, actually:

```
NameVirtualHost *:443

<VirtualHost *:443>
  SSLEngine on
  ServerName server1.example.com
  SSLCertificateFile server1.example.com.crt
  SSLCertificateKeyFile server1.example.com.key
  …
</VirtualHost>

<VirtualHost *:443>
  SSLEngine on
  ServerName server2.example.com
  SSLCertificateFile server2.example.com.crt
  SSLCertificateKeyFile server2.example.com.key
  …
</VirtualHost>
```

(The client will always see **server1.example.com.crt**, only)

The SSL/TLS handshake (RFC 4346)

SWITCH
The Swiss Education & Research Network

```
Client                                               Server

ClientHello                    -------->
                                                ServerHello
                                                Certificate*
                                          ServerKeyExchange*
                                         CertificateRequest*
                               <--------      ServerHelloDone
Certificate*
ClientKeyExchange
CertificateVerify*
[ChangeCipherSpec]
Finished                       -------->
                                           [ChangeCipherSpec]
                               <--------             Finished
Application Data               <------->     Application Data
```

Basic problem: the server has to select and send the certificate to the client immediately after the ClientHello, but at this time it doesn't have any information about the requested host name (which will only follow later in the **`Host:`** HTTP header, after completion of the full handshake)

Current workaround #1

SWITCH
The Swiss Education & Research Network

Wildcard certificate: **CN=*.example.com**

will match for **server1.example.com**, **server2.example.com**, **server3.example.com** …

in Apache, specify the same certificate for each VirtualHost:

```
NameVirtualHost *:443
<VirtualHost *:443>
  ServerName server1.example.com
  SSLCertificateFile wildcard.example.com.crt
</VirtualHost>
<VirtualHost *:443>
  ServerName server2.example.com
  SSLCertificateFile wildcard.example.com.crt
</VirtualHost>
```

… or configure a single VirtualHost and use mod_rewrite:

```
RewriteCond %{HTTP_HOST} =server1.example.com
RewriteRule (.*) /document/root/for/server1/$1 [L]
RewriteCond %{HTTP_HOST} =server2.example.com
RewriteRule (.*) /document/root/for/server2/$1 [L]
```

Current workaround #1 (cont'd)

SWITCH
The Swiss Education & Research Network

Matching rules:

RFC 2595 (Using TLS with IMAP, POP3 and ACAP): *A "*" wildcard character MAY be used as the left-most name component in the certificate. For example, *.example.com would match a.example.com, foo.example.com, etc. but would not match example.com.*

RFC 2818 (HTTP Over TLS): *Names may contain the wildcard character * which is considered to match any single domain name component or component fragment. E.g., *.a.com matches foo.a.com but not bar.foo.a.com. f*.com matches foo.com but not bar.com.*

RFC 4513 (LDAP Authentication Methods): *The '*' (ASCII 42) wildcard character is allowed in subjectAltName values of type dNSName, and then only as the left-most (least significant) DNS label in that value. This wildcard matches any left-most DNS label in the server name. That is, the subject *.example.com matches the server names a.example.com and b.example.com, but does not match example.com or a.b.example.com.*

Most browsers use matching rules like these (implementation details may differ), with one notable exception: for *Mozilla, `*` simply matches everything* (i.e. a certificate with **`CN=*`** will work, though it's a pretty bad idea to trust such a certificate – can do MITM for *every* https URL)

For Internet Explorer/Windows, see also http://support.microsoft.com/kb/258858: `*` will *not* match a dot ("."), must occur in the leftmost FQDN component, can be preceeded by other characters (**`www*.example.com`**), but must be immediately followed by "." [note that some of the "accepted" examples in the referenced KB article are actually wrong – e.g. **`www.example.*`**]

Current workaround #2

SWITCH
The Swiss Education & Research Network

subjectAltName extension

- add a dNSName for every (additional) virtual host, put the default host into both the CN and the subjectAltName extension
- works with all major browsers
- Apache configuration similar to wildcard certificates
- drawback: certificate needs to be reissued whenever a new FQDN is added

Future solution: server name indication

SWITCH
The Swiss Education & Research Network

RFC 4366: Transport Layer Security (TLS) Extensions

Specifies how to extend the ClientHello, one of these extensions being the **server name indication** (SNI, the FQDN of the host the client wants to connect to)

Browser support

- currently implemented by Opera, MSIE 7 (under Vista only), and Firefox 2

Toolkits with SNI support

- GnuTLS
- OpenSSL (0.9.9 development version)
- Mozilla NSS (client-side only, currently)

Server support – currently limited to Apache

- mod_gnutls: for Apache 2.x, experimental module (http://www.outoforder.cc/projects/apache/mod_gnutls/)
- mod_ssl: experimental patch for 2.2, needs recent OpenSSL development version (http://issues.apache.org/bugzilla/show_bug.cgi?id=34607)

The Swiss Education & Research Network