Webmail sécurisé

- Buts
- Solutions
- Principe
- Installation
- Démonstration

Webmail sécurisé
Buts

- Disposer d'un accès à la messagerie interne de l'Observatoire depuis n'importe quel navigateur
- A partir d' environnements à priori hostiles
- Sans installation de logiciels particuliers

Webmail sécurisé
Solution

- Sur le client : navigateur WWW avec SSL
  - Internet Explorer 4.x et 5.x
  - Netscape Navigator 4.x
  - Netscape Communicator 4.x ,6 et 7
  - Opéra 3.x et plus
  - Frontpage2000 et plus
  - WebTV Classic et plus

Webmail sécurisé
Solution

- Sur le serveur :
  - Serveur HTTP +SSL (HTTPS)
  - Scripts (CGI, Perl, PHP)
  - Clients IMAP du serveur de messagerie
  - Génération de pages HTML avec le contenu de la BAL et de des dossiers
- Solution retenue: Apache/SSL + Horde/IMP

Autres solutions

Voir http://www.cru.fr/http-mail

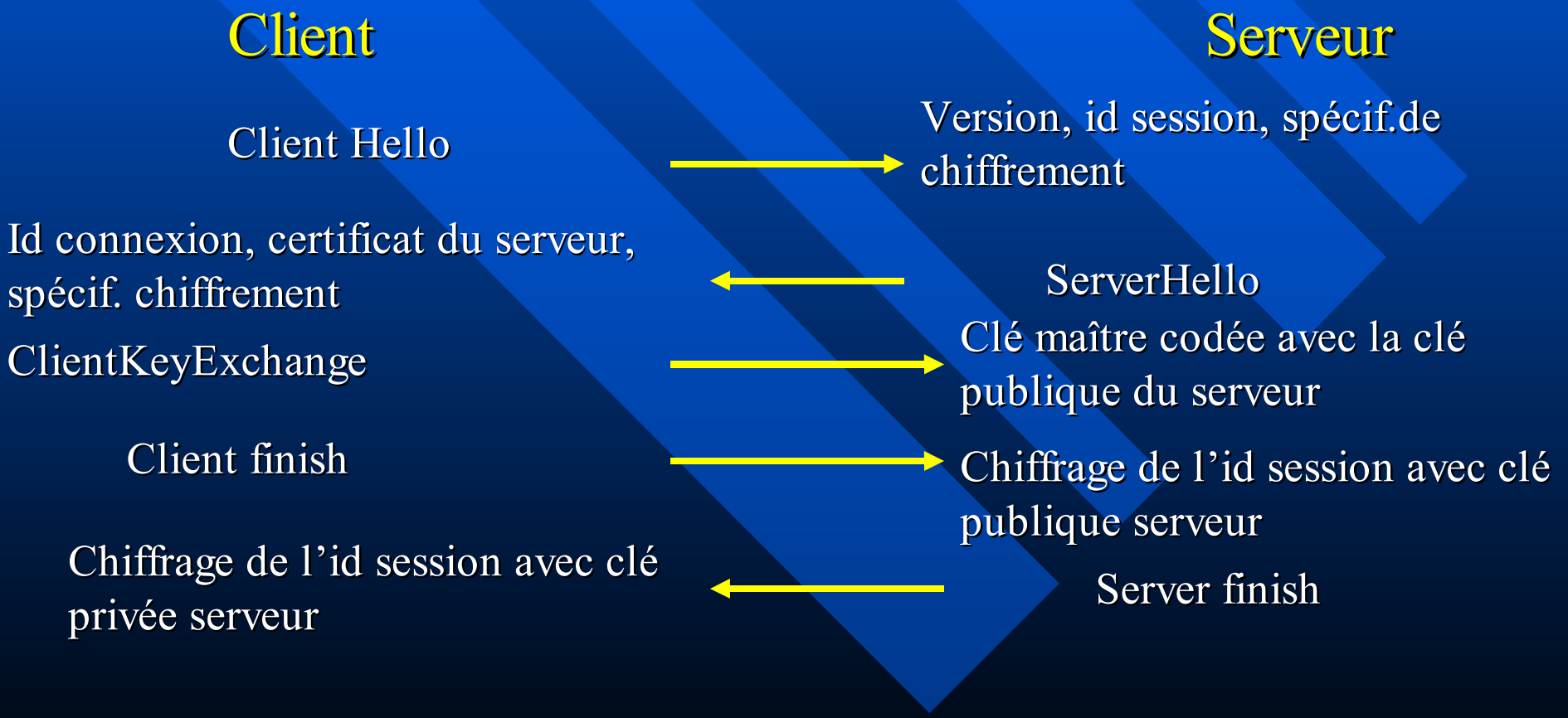
Webmail sécurisé
Objectifs :protocole SSL

- Sécuriser des protocoles existants (HTTP, SMTP, IMAP, etc.) de manière transparente
  - Confidentialité via le chiffrement
  - Intégrité via les empreintes
  - Authentification via les certificats X.509
  - Rapidité: usage de clés de session
  - Résistance aux attaques classiques

Webmail sécurisé

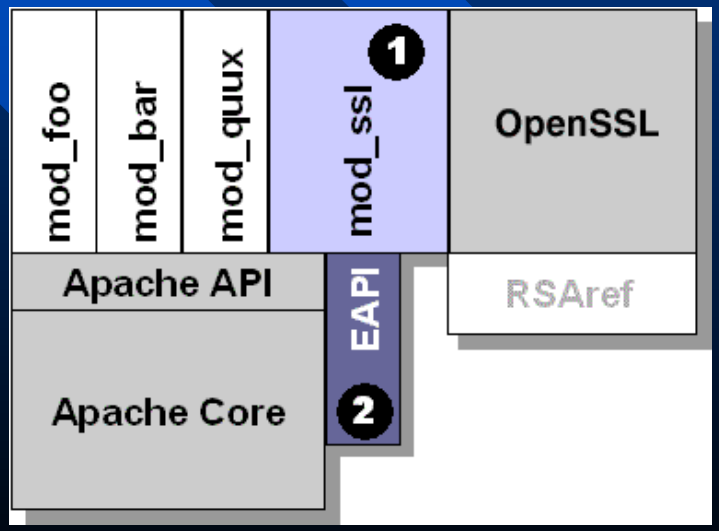
Principe SSL

Séquence d'initialisation (SSL Handshake Protocol)



Webmail sécurisé Installation

- Apache_1.3.27 (www.apache.org)
- Mod_ssl-2.8.11_1.3.27 (www.modssl.org)
- Openssl-0.9.6g (www.openssl.org)
- PHP 4.2.3 (www.php.net)



Webmail sécurisé
Installation

- PHP-4.2.3 (www.php.net)
- MySQL-3.23.39 (www.mysql.org)
- Perl-5.6.1 (www.perl.com)
- Mm1.1.3 (www.engelschall.com/sw/mm) Shared memory library nécessaire pour mod-ssh
- Horde-1.2.8 (www.horde.org)
- IMP-2.2.8 (www.horde.org/imp)
- Imap-2001.BETA.SNAP-0103131845 (www.washington.edu/imap)

Webmail sécurisé
HTTP et HTTPS

- HTTPS est le protocole HTTP porté sur une connexion sécurisée SSL
  - Utilise le port 443 par défaut et des URL particulières
- HTTP: le client envoie une requête « GET URL HTTP/1.1 »
- HTTPS: le client SSL envoie un message SSL ClientHello

  => utilisation d'URL de la forme « https://astro.u-strasbg.fr »

Webmail sécurisé
Configuration : httpd.conf (1)

```
LoadModule ssl_module /usr/lib/apache/libssl.so
AddModule mod_ssl.c

Listen 80
Listen 443

SSLSessionCache dbm:/http/logs/ssl_scache
SSLSessionCacheTimeout 300
SSLMutex                file:/http/logs/ssl_mutex
SSLRandomSeed           startup builtin
SSLRandomSeed           connect builtin
SSLLog          /http/logs/ssl_engine_log
SSLLogLevel             info
```

Webmail sécurisé
Configuration : httpd.conf (2)

```
<VirtualHost _default_:443>

DocumentRoot "/http/htdocs/horde/imp"
ServerName astro.u-strasbg.fr
ServerAdmin jyh@newb6.u-strasbg.fr
ErrorLog /http/logs/error_log
TransferLog /http/logs/access_log

SSLEngine on

SSLCipherSuite
   ALL:!ADH:!EXPORT56:RC4+RSA:+HIGH:+MEDIUM:+LOW:+
   SSLv2:+EXP:+eNULL
```

Webmail sécurisé
Configuration : httpd.conf (3)

```
#Certificat du serveur
SSLCertificateFile /http/conf/ssl.crt/server.crt

#Clé privée du serveur
SSLCertificateKeyFile /
  http/conf/ssl.key/server.key

#Certificat de l'autorité de certification
SSLCACertificatePath /http/conf/ssl.crt
SSLCACertificateFile /http/conf/ssl.crt/ca-
  bundle.crt
SSLVerifyClient none
</VirtualHost>
```

Webmail sécurisé
Configuration : httpd.conf (4)

```
<Directory "/http/htdocs/horde">
   SSLRequireSSL
      Options Indexes FollowSymLinks
       AllowOverride None
       order allow,deny
       allow from all
<IfModule mod_php4.c>
            php_admin_value include_path
   '.:/usr/local/phplib'
            php_admin_value auto_prepend_file /
   usr/local/phplib/prepend.php3
            php_admin_flag magic_quotes_gpc Off
            php_admin_flag track_vars On
       </IfModule>
   </Directory>
```

Webmail sécurisé
Configuration de Horde+IMP

- Document_root/horde/imp/config/defaults.php3

- Document_root/horde/imp/config/servers.php3

Ex :$IMAPServer[‘Aladin’] = new IMAPServer(‘Aladin’,
‘aladin.u-strasbg.fr’,
143,
‘’,
‘astro.u-strasbg.fr’);

Webmail sécurisé
Conclusions

- Outil très pratique et complémentaire aux outils SSH Client et SSH SFTC (Secure File Transfert Client)
- Il manque actuellement la partie signature et chiffrement des messages (SMIME) qui permettrait de signer des messages de façon distante.