Modulo de validación OCSP

Introducción.

Todo el sistema se basa en los trabajos del Centro de Computación Noruego (NR - Norwegian Computing Center) sobre el modulo de apache mod_ssl.

El objetivo es dotar al servidor web Apache de la capacidad de realizar consultas OCSP para validar el estado de los certificados de los usuarios, en vez de recurrir al sistema de Listas de Certificados Revocados, que aunque viene configurado por defecto en la instalación de Apache-SSL, es menos eficiente y obliga al administrador del servidor a realizar cargas periodicas de la CRL. Para ello, evidentemente, el Apache debe estar configurado para aceptar SSLv3 con autenticación de usuarios.

El modulo SSL ya viene incorparado en Apache 2.X, pero para la serie 1.3.X, que es la que nos ocupa, es necesario instalar el paquete mod_ssl, y es en este paquete donde se han efectuado las modificaciones. Mod_SSL es un paquete se software licenciado bajo GPL, que parchea al servidor web para dotarlo de la capa SSL/TLS.

En cuanto al OCSP (Online Certificate Status Protocol), es un protocolo estandar (RFC2560) que permite realizar consultas a un servidor predeterminado sobre el estado de un certificado, en base al numero de serie y el firmante del mismo.

Instalación.

Se proporcionan los fuentes necesarios para realizar una instalación en los distintos sistemas operativos mas utilizados (Solaris, Linux, Windows, etc) , así como los binarios para las plataformas antes mencionadas.

- Ficheros fuentes.

Es necesario instalar openssl en su versión 0.9.7 (esta version lleva soporte OCSP, la serie 0.9.6 todavia no lo ha incluido). La compilación es muy sencilla, y os remito al INSTALL del propio paquete para llevarlo a cabo. Se proporciona el ultimo snapshot, ya que esta versión se encuentra en beta y la ultima release (beta3) da problemas de compilacion en plataformas win32.

La version parcheada de mod_ssl es la 2.8.12, que parchea al Apache 1.3.27, proporcionandose ambas.

Hay que descomprimir ambos paquetes en el disco y en el directorio raiz del mod_ssl realizar configure (o configure.bat si estamos en Windows) pasandolo como parametros el path de apache y el de openssl:

```
./configure --with-apache=../apache_1.3.27 --with-ssl=../openssl-0.9.7 \
 --prefix=/path/to/apache –enable-shared=ssl
```

Para Windows:

```
configure.bat --with-apache=..\apache_1.3.27 --with-ssl=C:\openssl
```

Os remito a los ficheros Install e Install.win32 del directorio raiz del mod_ssl.

Una vez parcheado, en el directorio de apache, realizamos make (o nmake si estamos en Win32).

- Binarios.

La instalación de los binarios es mucho más sencilla (también menos flexible). Sólo hay que descomprimirlos y dejarlos caer en el directorio elegido. En el caso de Linux y Solaris, se instalan ambos en /usr/local, creando ssl el directorio /usr/local/ssl y apache /usr/local/apache . En Win32 se instalan en raiz, creando \Apache-SSL. Es posible cambiar el path de instalación si somos coherentes a la hora de efectuar la configuración.

Configuración.

La configuración es exactamente la misma que en un Apache con mod_ssl normal.
En el caso de los binarios el fichero de configuración ya esta modificado para realizar las consultas OCSP y si se realiza la compilación no hay mas que añadir en la sección de SSL de httpd.conf las siguientes lineas:

```
# Configuración OCSP

SSLUseVA 1
SSLVAServiceType 1
SSLVAPath    '/'
SSLVAHost ocsp.pki.gva.es
SSLVAPort 80

# Fin Configuración OCSP
```

El servidor debe disponer de un certificado valido de la autoridad de certificación de la GVA, así como tener configurada la CAGVA y la RootCA como certificados firmantes y de los cuales se aceptan certficados de cliente.

Para ello hay que configurar los valores en httpd.conf:

```
#Certificado del Servidor
SSLCertificateFile   /usr/local/apache/conf/ssl.crt/server.crt
#Clave del Servidor
SSLCertificateKeyFile /usr/local/apache/conf/ssl.key/server.key
#Certificados Firmantes
SSLCertificateChainFile /usr/local/apache/conf/ssl.crt/ca.crt

#Certificados Reconocidos
SSLCACertificatePath /usr/local/apache/conf/ssl.crt
SSLCACertificateFile /usr/local/apache/conf/ssl.crt/ca-bundle.crt
```

Para utilizar el OCSP hay que tener una zona de acceso restingido con:

```
SSLVerifyClient require
SSLVerifyDepth  2 # Tenemos dos niveles
```

Una vez hecho esto, arrancamos el apache con:

```
/usr/local/apache/bin/apachectl startssl
```

o en windows

```
\Apache-SSL\aapache -D SSL
```