Listas de revocación de certificados

Una lista de revocación de certificados (CRL) proporciona una lista de los certificados que han sido revocados. Una aplicación cliente, como un navegador web, puede utilizar una CRL para comprobar la autenticidad de un servidor. Una aplicación de servidor, tales como Apache o OpenVPN, puede utilizar una CRL para denegar el acceso a los clientes que ya no son de confianza.

Publique la CRL en un lugar accesible al público (por ejemplo, `http://example.com/intermediate.crl.pem`). Los terceros podrán alcanzar la CRL desde esta ubicación para comprobar si alguno de los certificados de los que dependen han sido revocadas.

```
---------------------------------------------------------------------
(¡!) Nota

Algunos proveedores de aplicaciones han desaprobado las CRL y en lugar
de usar el Online Certificate Status Protocol (OCSP).
---------------------------------------------------------------------
```

Preparar el archivo de configuración

Cuando una autoridad de certificación firma el certificado, lo habitual es que codifique la ubicación de CRL en el certificado. Añada `crlDistributionPoints` a las secciones correspondientes. En nuestro caso, añádalo a la sección `[ server_cert ]` (se refiere al archivo `/root/ca/intermediate/openssl.cnf`).

```
[ server_cert ]
# ... snipped ...
crlDistributionPoints = URI:http://example.com/intermediate.crl.pem
```

Crear la CRL

```
# cd /root/ca
# openssl ca -config intermediate/openssl.cnf \
      -gencrl -out intermediate/crl/intermediate.crl.pem



---------------------------------------------------------------------
(¡!) Nota

La sección del manual de la CA para CRL OPTIONS contiene más
información sobre cómo crear CRLs
---------------------------------------------------------------------
```

Puede comprobar el contenido de la CRL con la herramienta `crl`.

```
# openssl crl -in intermediate/crl/intermediate.crl.pem -noout -text
```

Ningún certificado ha sido revocado todavía así que la salida indicará `No Revoked Certificates`.

Debe volver a crear la CRL a intervalos regulares. Por defecto la CRL expira después de 30 días. Esto es controlado por la opción `default_crl_days` en la sección `[ CA_default ]`.

Vamos a recorrer un ejemplo. Alice está ejecutando el servidor Web Apache y tiene una carpeta privada con imágenes del lindo gatito que le tiene el corazón derritiéndose. Alice quiere conceder a su amigo, Bob, el acceso a esta colección.

Bob crea una clave privada y una solicitud de firma de certificado (CSR).

```
$ cd /home/bob
$ openssl genrsa -out bob@example.com.key.pem 2048
$ openssl req -new -key bob@example.com.key.pem \
      -out bob@example.com.csr.pem

You are about to be asked to enter information that will be incorporated
into your certificate request.
-----
Country Name [XX]:US
State or Province Name []:California
Locality Name []:San Francisco
Organization Name []:Bob Ltd
Organizational Unit Name []:
Common Name []:bob@example.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:suClave
An optional company name []:Bob Ltd.
```

Bob envía su CSR a Alice, quien lo firma.

```
# cd /root/ca
# openssl ca -config intermediate/openssl.cnf \
      -extensions usr_cert -notext -md sha256 \
      -in intermediate/csr/bob@example.com.csr.pem \
      -out intermediate/certs/bob@example.com.cert.pem \
      -subj "/CN=bob@example.com"

Sign the certificate? [y/n]: y
1 out of 1 certificate requests certified, commit? [y/n]: y
```

Alice comprueba que el certificado es válido:

```
# openssl verify -CAfile intermediate/certs/ca-chain.cert.pem \
      intermediate/certs/bob@example.com.cert.pem

bob@example.com.cert.pem: OK
```

El archivo `index.txt` debe contener una nueva entrada.

```
V 160420124740Z 1001 unknown ... /CN=bob@example.com
```

Alice envía a Bob el certificado firmado. Bob instala el certificado en su navegador web y ahora es capaz de acceder a las imágenes del gatito de Alice. ¡Viva!

Tristemente resulta que Bob se está portando mal. Bob ha publicado imágenes del gatito de Alice en Hacker News, afirmando que son propias y ganando gran popularidad. Alice lo descubre y necesita revocar su acceso inmediato.

```
# cd /root/ca
# openssl ca -config intermediate/openssl.cnf \
      -revoke intermediate/certs/bob@example.com.cert.pem

Enter pass phrase for intermediate.key.pem: secretpassword
Revoking Certificate 1001.
Data Base Updated
```

La línea en `index.txt` que se corresponde con el certificado de Bob comienza ahora con el carácter `R`. Esto significa que el certificado ha sido revocado.

```
R 160420124740Z 150411125310Z 1001 unknown ... /CN=bob@example.com
```

Después de revocar el certificado de Bob, Alice debe volver a crear la CRL.

Tras una revocación de certificado, es posible que la autoridad necesite constatar que tal cosa ha ocurrido al tiempo de una verificación de la validez posterior a la revocación. Para ello deberá rehacer la CRL y ejecutar la orden:

```
# cd /root/ca
# openssl ca -config intermediate/openssl.cnf \
      -gencrl -out intermediate/crl/intermediate.crl.pem
# openssl verify -CAfile intermediate/certs/ca-chain.cert.pem \
      -CRLfile intermediate/crl/intermediate.crl.pem -crl_check \
      intermediate/certs/bob@example.com.cert.pem
```

lo que podrucirá la siguiente respuesta:

```
CN = bob@example.com
error 23 at 0 depth lookup: certificate revoked
error intermediate/certs/bob@example.com.cert.pem: verification failed
```

en donde apreciamos que efectivamente el certificado está revocado.

El uso de la CRL del lado del servidor

En cuanto a los certificados de cliente, es una aplicación típica del lado del servidor (por ejemplo, Apache) que está haciendo la verificación. Esta aplicación necesita tener acceso local a la CRL.

En el caso de Alice, ella puede agregar la directiva `SSLCARevocationPath` a su configuración de Apache y copiar la CRL en su servidor web. La próxima vez que Bob se conecte al servidor web, Apache confrontará su certificado de cliente con la CRL y denegará el acceso.

Del mismo modo, OpenVPN tiene una directiva `crl-verify` para que pueda bloquear los clientes que han visto revocado su certificado.

El uso del lado del cliente de la CRL

Para los certificados del servidor, es una aplicación típica del lado del cliente (por ejemplo, un navegador web) que realiza la verificación. Esta solicitud tiene que tener acceso remoto a la CRL.

Si un certificado fue firmado con una extensión que incluye `crlDistributionPoints`, una aplicación del lado del cliente puede leer esta información y buscar la CRL en la ubicación especificada.

Los puntos de distribución de CRL son visibles en los detalles del certificado X509v3.

```
# openssl x509 -in cute-kitten-pictures.example.com.cert.pem -noout -text

    X509v3 CRL Distribution Points:

        Full Name:
          URI:http://example.com/intermediate.crl.pem
```