Evaluación de políticas de revocación de certificados

Juan Carlos Castro Chávez, Jordi Forné Muñoz, José Luis Muñoz Tapia

Resumen

La autenticación es el servicio de seguridad más difícil de conseguir para las aplicaciones de comercio electrónico, y requiere el empleo de infraestructuras de clave pública (PKI). El elemento más costoso de toda la infraestructura PKI es la revocación de certificados. Hasta la fecha, existen diferentes propuestas de políticas de revocación de certificados. En este artículo se presenta un modelo para evaluar las diferentes políticas propuestas, y algunos de los resultados obtenidos al aplicar este modelo.

Palabras clave— Autenticación, PKI, Revocación de certificados, CRL, OCSP

Introducción

En los entornos de interconexión de usuarios abiertos, tal y como es Internet, se necesita una forma eficaz de proporcionar los servicios básicos de seguridad como son la autenticación de usuarios, la confidencialidad, la integridad de la información transmitida y no repudio (irrenunciabilidad). Mediante la aplicación de los servicios de seguridad básicos, se pueden implementar aplicaciones seguras para usuarios finales, como por ejemplo aplicaciones para comercio electrónico (business-to-business o business-to-consumer), redes privadas virtuales (VPN), correo electrónico seguro, etc.

Para proporcionar los servicios de seguridad básicos, necesarios para la construcción de aplicaciones seguras para los usuarios finales, es necesario el empleo de criptografía de clave pública. Los orígenes de la criptografía de clave pública se remontan al estudio realizado por Whitfield Diffie y Martin Hellman en 1976 [7], donde se propuso por primera vez el uso de una pareja de claves, una pública (conocida) y otra privada, para la realización de las operaciones criptográficas. De esta forma, un mensaje puede ser cifrado por cualquier persona usando la clave pública y sólo el poseedor de la clave privada podrá descifrarlo. Recíprocamente, un mensaje cifrado con la clave privada sólo puede ser cifrado por su poseedor, mientras que puede ser descifrado por cualquiera que conozca la clave pública.

Para la distribución de las claves públicas en entorno abierto, la solución que más ampliamente se ha adoptado, consiste en recurrir a una tercera parte confiable, llamada autoridad de certificación (AC), propuesta por primera vez en 1978 por Kohnfelder [16]. Las funciones de una AC consisten en verificar la identidad de los solicitantes de certificados, crear los certificados y proporcionar los mecanismos necesarios para comprobar la validez de los certificados emitidos. En la Figura 1 se muestra un esquema general de la AC. La AC se divide en dos partes: servidor de certificados, es el encargado de generar y administrar los certificados digitales, y el servidor de revocación, encargado de proporcionar la información del estado de los certificados.

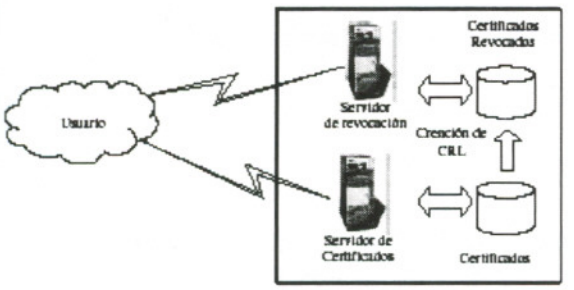

Figura 1 Esquema general de una AC

El formato y las funciones de un certificado digital se encuentran definidas en el estándar X.509 definido por la ITU [12] y [13], dicho estándar se basa en el conjunto de entradas de directorio X.500 [4] y contiene de forma estructurada información acerca de la identidad de su titular, su clave pública y la AC que lo emitió.

Para el uso de certificados digitales se está definiendo una infraestructura adecuada para asegurar la autenticación de las entidades involucradas en una transacción; a esta infraestructura se le conoce como PKI o Infraestructura de Clave Pública, que genéricamente se define como "el conjunto de Hardware, Software, personas, políticas y procedimientos necesarios para crear, administrar, almacenar, distribuir y revocar certificados de claves publicas basados en criptografía de clave pública" [2]. En la actualidad se ha generado una gran expectativa respecto a una nueva generación de aplicaciones que incorporen los mecanismos de seguridad necesarios para ofrecer determinados servicios que de otra forma no serían posibles (p.e. comercio electrónico). Sin embargo y a pesar de la madurez de la tecnología de clave pública, sigue sin producirse un despliegue masivo de este tipo de servicios, esto se debe en gran medida a la todavía inmadura PKI. La PKI presenta varios problemas, sobretodo cuando se quiere extender sus soluciones a una gran cantidad de usuarios, es decir, presenta problemas de escalabilidad. Entre estos problemas uno de los más graves es la revocación de certificados. A este respecto, el tema de la revocación ha sido objeto de diferentes estudios [5], [6], [15], [17] y [20]. Cada uno de estos estudios propone una política de revocación diferente, aunque no proporcionan un modelo general para evaluar dichas políticas. En este artículo presenta un modelo genérico que permita evaluar políticas de revocación. Para poder evaluar políticas de revocación en primer lugar se define y se justifica que parámetros son considerados relevantes y finalmente mediante la aplicación del modelo descrito se evalúan dos de las políticas propuestas más representativas. El principal parámetro evaluado es la velocidad de transmisión necesaria.

Políticas de revocación de certificados

Las políticas de Revocación de Certificados definen la forma en la cual un usuario puede obtener información relativa al estado de un determinado certificado digital. El análisis de la forma en la cual debe ser proporcionada dicha información al usuario se ha realizado en los estudios mencionados anteriormente, de los cuales podemos concluir que las políticas de revocación de certificados se pueden agrupar en dos grandes grupos [21]:

- Grupo de políticas de revocación basadas en distribución de listas o Off-Line: este tipo de políticas se caracteriza por el envío de una lista de certificados revocados o CRL al usuario, mediante la cual el usuario debe de verificar el estado del certificado.
- Grupo de políticas de revocación en línea o On- Line: este tipo de políticas se caracteriza por el envío de información sobre la validez de un determinado certificado o certificados que el usuario solicita en un instante en particular.

A continuación se expondrán las diferentes técnicas empleadas en cada uno de estos grupos.

La primera de estas políticas se basa en la generación de listas de revocación de certificados a la cual se irán añadiendo los certificados revocados a medida que se van produciendo [12]. Este método fue introducido en 1988 en la versión 1.0 de CRL definido en el estándar X.509, dicha lista de certificados revocados hace uso de una base de datos centralizada, a la cual cada usuario debe acceder para verificar si un certificado dado ha caducado. El contenido de la CRL consta de diferentes campos: Versión, Emisor de la lista, Algoritmo empleado para firmarla CRL, Fecha de expiración de CRL, Información de los certificados revocados etc. Un usuario solicita al servidor el envío de dicha lista cuando se va a realizar una operación que requiere el empleo de un certificado, y cada vez que necesite realizar una nueva operación ha de solicitar nuevamente la CRL. La primera mejora a emplear sobre este método es mantener la CRL en una memoria caché del usuario, de esta forma el usuario no ha de solicitar al servidor de revocación el envío de una nueva CRL si ya dispone de una CRL no caducada en su caché. Como principal problema de esta política tenemos que todos los usuarios tienen el mismo tiempo de expiración para las CRL almacenadas en sus caches, esto hace que todas las CRL caduquen en el mismo tiempo y que el servidor de revocación tenga una carga elevada entorno a este instante. Para solucionar este problema en [5] se propone cambiar el periodo de emisión (creación) de CRL's en el servidor de revocación. Se sugiere un valor de emisión de CRL's inferior al tiempo de expiración, de esta forma se reparte la carga hacia el servidor de revocación en el tiempo.

Otra nueva mejora es el empleo de la política basada en delta CRL, la cual fue introducida en el estándar X.509 en 1994. Esta política consiste en generar una lista de revocación de certificados base (CRL_base) y después de un periodo de tiempo delta, menor que el tiempo de expiración de la CRL_Base, se genera una nueva CRL denominada CRL_Delta que únicamente contiene las revocaciones producidas desde la emisión de la CRL_Base. Con este método el usuario ya no necesita obtener toda la CRL si dispone de una CRL_Base no caducada, sino simplemente necesita la última CRL_ Delta. De esta forma la CRL_Delta al tener un tamaño menor respecto a la CRL_Base, disminuye los costes de transmisión [11]. Una mejora a esta política se propone en [6].

Otra mejora que se puede aplicar en general a todas las políticas es la utilización de diferentes puntos de distribución de CRL, este método se introdujo en 1997 [12] para X.509 V.3, cada CRL contiene las revocaciones de un determinado grupo de certificados. Los criterios para crear estos grupos pueden ser: geográficos, de nivel de importancia, de ámbito de uso, de motivo de revocación.

Políticas de revocación On-Line

En este tipo de este tipo de políticas se caracteriza por el envío de información de un determinado certificado o certificados que el usuario solicita en un instante en particular, la primera política de la que hablaremos es el Sistema de Revocación de Certificados (CRS) la cual fue propuesta en 1996 por Silvio Micali. Esta política se basa en un sistema de firmas Off Line/On Line [8]. Una mejora a este sistema, propuesta por Aiello en 1998 [1], fue denominada Sistema de Certificados Revocados Jerárquicos (HCRS).

La siguiente política fue la propuesta hecha por Paul Kocher [15] en la cual presenta un modelo de Arbol de Certificados Revocados (CRT). Moni Naor y Kobi Nissim presentaron un modelo [20], basado en el árbol de certificados revocados presentado por Kocher [15].

El grupo de trabajo del IETF (Internet Engineering Task Force) ha desarrollado una propuesta para emitir el estado de certificados llamada On Line Certificate Status Protocol (OCSP). Este protocolo nació con la base de dos borradores propuestos [3] y [18]. La idea general de OCSP es olvidarse del uso de las Listas de

Certificados Revocados (CRL) y centrarse en lo que sucede a un certificado; el usuario recibe el estado del certificado o grupo de certificados que necesita, actualmente se encuentra en discusión una nueva propuesta [19], dicha propuesta expira Septiembre 2001. Fox y La Macchia [10] presentaron una alternativa a OCSP ellos proponen la emisión de un nuevo certificado X.509 como respuesta a las solicitudes del estado de un certificado dado, dicho certificado indicara si el certificado en cuestión se encuentra revocado o no.

Evaluación de políticas de revocación

Se han descrito diferentes técnicas de revocación de certificados en las secciones anteriores, dichas técnicas se pueden agrupar en consultas Off-Line y consultas On-Line [21]. En la presente sección se expondrá un modelo de evaluación basado en teoría de colas que nos permitirá encontrar las diferentes características que presentan dichas técnicas. Un primer modelo se puede encontrar en [9], en dicho modelo se hace un análisis de una Autoridad de Certificación sin el empleo de CRL observando la relación existente entre el número de usuarios y tiempo de servicio del servidor de revocación.

Parámetros de evaluación

En este apartado se determinan justificadamente los parámetros que se van a utilizar para la evaluación de las diferentes políticas de revocación. La parte crítica del sistema de revocación es el servidor de revocación, así pues los parámetros de evaluación que vamos a considerar serán parámetros del servidor de revocación, aunque para un estudio más exhaustivo habría que tener en cuenta también parámetros de evaluación en los usuarios (como costes de caché) y en la entidad emisora de certificados (coste de emisión de un certificado). En la Tabla 1 podemos encontrar los parámetros que consideramos relevantes en la evaluación del servidor de revocación:

A continuación se justifica porque cada uno de estos parámetros se considera crítico:

B	Velocidad binaria de transmisión de salida del servidor
$T_{validación}$	Tiempo medio de validación de certificado. Es el tiempo transcurrido desde que el servidor recibe una consulta hasta que acaba de transmitir la respuesta a esa consulta. Incluye el tiempo de proceso más tiempo de espera en cola
T_{cpu}	Tiempo de procesador que consume una validación de certificado.

Tabla 1. Parámetros críticos en el diseño del servidor de revocación

- La velocidad binaria de transmisión de salida del servidor B es un parámetro primordial ya que determinará el caudal del flujo de salida de datos mínimo que ha de tener el servidor de revocación hacia los usuarios, ya que la velocidad de transmisión sentido usuario-servidor es menos crítica. La velocidad de transmisión está directamente relacionada con el ancho de banda, por lo que en adelante se utilizará indistintamente velocidad de transmisión o ancho de banda necesario.
- El Tvalidación es un parámetro a tener en cuenta por lo que respecta a los *timeouts* de las conexiones TCP establecidas para realizar la consulta. Normalmente los protocolos de consulta suelen ser LDAP o http que son protocolos de aplicación sobre TCP. Si el servidor de revocación nos proporciona un Tvalidación muy elevado es posible que se puedan perder consultas por temporización de conexiones TCP o que los usuarios abandonen la consulta.
- El valor de Tcpu tiene mayor o menor importancia dependiendo de la política de revocación, ya que hay políticas que han de firmar los resultados en el mismo instante de la validación con lo que se puede convertir en un parámetro crítico.

Modelo de evaluación

En este apartado se hallarán los parámetros de evaluación que han sido considerados relevantes en el apartado anterior para el servidor de revocación. Para ello se va a emplear un modelo basado en teoría de colas. En la Figura 2 se muestra el esquema general del modelo de servidor de revocación que vamos a utilizar.

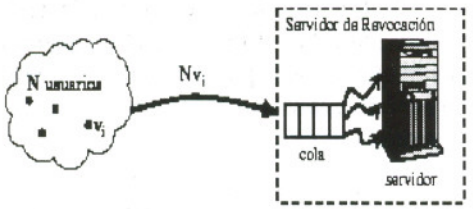

Figura 2 Modelo basado en teoría de colas para el servidor de revocación

N es el número de usuarios de la población que maneja el modelo. Suponiendo N relativamente grande y por las características del servicio de validación de certificados, podemos aproximar el tiempo entre peticiones de validación de certificados que genera la población del modelo mediante una estadística exponencial, tal y como hacen otros modelos de tráfico, como por ejemplo los modelos de tráfico para las redes de voz.

La expresión de la densidad de probabilidad del tiempo entre peticiones consecutivas para la estadística exponencial sigue la siguiente expresión

$$ve^{-vt} \qquad (1)$$

donde v es la tasa agregada media de peticiones de validación al servidor de revocación de la población del modelo. Si v_i es la tasa de peticiones de validación de uno de los miembros de la población, entonces

$$v = Nv_i \qquad (2)$$

En segundo lugar aproximaremos el tiempo de servicio T_s de una petición de validación por un valor constante (determinista), es decir, todas las consultas una vez en el servidor tardan el mismo tiempo en procesarse. En general T_s se puede expresar como

$$T_S = T_{tx} + T_{cpu} \qquad (3)$$

Donde T_{tx} es el tiempo de transmisión de los datos de la validación y T_{cpu} es el tiempo que precisa la CPU del servidor de revocación para preparar los datos de la validación. Los datos a transmitir como resultado de una petición de validación los denominaremos genéricamente como CRL (lista de certificados revocados), aunque un caso particular es que la lista este compuesta por un solo certificado.

En general el tamaño de la CRL se puede expresar como la suma de una cabecera CRL_H más cierta información correspondiente a cada certificado revocado CRL_C.

$$CRL = CRL_H + cCRL_C \qquad (4)$$

En la CRL_H se puede encontrar dependiendo de la política de revocación parte o la totalidad de la siguiente información :

- Versión de la CRL.
- Algoritmo de firma.
- Firma digital.
- Fecha de emisión.
- Fecha de actualización.
- Extensión de X.509 para la política de validación.

En la CRL_C (información de cada certificado revocado) se puede encontrar parte o la totalidad de la siguiente información:

- Número de serie del certificado revocado.
- Fecha en la que fue revocado el certificado.
- Extensión de entrada de CRL.

Definiremos M como el número total de certificados emitidos por la entidad certificadora, si consideramos que cada

usuario perteneciente a la población que puede realizar peticiones de validación dispone de un certificado tendremos que M = N.

Por otra parte, el número de certificados revocados M_R es en general una función de M, del tiempo y de parámetros de la política de distribución de certificados que se aplique

$$M_R = f(M, t, ...) \quad (5)$$

Para nuestro modelo utilizaremos una fórmula sencilla para M_R, suponiendo que es proporcional a M y que no varia con el tiempo

$$M_R = pM \qquad 0 \le p \le 1 \quad (6)$$

$$B = \frac{CRL\,[bits]}{T_{tx}} \quad [=]\,bps \quad (7)$$

Por otra parte, la velocidad binaria de transmisión de salida del servidor de revocación se puede expresar como

Por último supondremos que el servidor dispone de una cola lo suficientemente grande como para poderla considerar infinita, de esta forma podemos aplicar al servidor de revocaciones un modelo clásico de teoría de colas [14] M/D/1. Se ha justificado poder aplicar un modelo de teoría de colas, ya que éste permite la obtención del valor de los parámetros de evaluación sin necesidad de realizar simulaciones, puesto que disponemos de expresiones analíticas para dichos parámetros.

Por último supondremos que el servidor dispone de una cola lo suficientemente grande como para poderla considerar infinita, de esta forma podemos aplicar al servidor de revocaciones un modelo clásico de teoría de colas [14] M/D/1. Se ha justificado poder aplicar un modelo de teoría de colas, ya que éste permite la obtención del valor de los parámetros de evaluación sin necesidad de realizar simulaciones, puesto que disponemos de expresiones analíticas para dichos parámetros.

Se define ρ como la carga del servidor de revocación mediante la siguiente expresión

$$\rho = vT_S \quad (8)$$

De (3), (4), (7) y (8) se obtiene una expresión general para la velocidad binaria de transmisión B:

$$B = \frac{CRL_H + cCRL_C}{\frac{\rho}{Nv_i} - T_{cpu}} \quad (9)$$

Finalmente, de acuerdo con la teoría de colas para la M/D/1 [14], el tiempo de validación se puede hallar según la siguiente expresión

$$T_{validación} = \frac{T_S(2 - vT_S)}{2(1 - vT_S)} \quad (10)$$

Substituyendo T_s por las expresiones en (3) y (7) se obtiene una expresión para (10) en función del tamaño de los datos CRL, de B y del tiempo de CPU consumido

$$T_{validación} = \frac{\left[\frac{CRL}{B} + T_{cpu}\right]\left[2 - v\left(\frac{CRL}{B} + T_{cpu}\right)\right]}{2\left[1 - v\left(\frac{CRL}{B} + T_{cpu}\right)\right]} \quad (11)$$

Aplicación del modelo de evaluación

Dependiendo del escenario en el cual se ha de aplicar el esquema de revocación de certificados, resulta adecuado el empleo de una determinada política de revocación u otra. Esto es así porque cada política intenta optimizar diferentes parámetros, como por ejemplo, las tasas de petición de validación contra el servidor de revocación, el ancho de banda de transmisión necesario, reducir el tamaño de la CRL, bajar los requerimientos en el servidor de revocación (RAM, CPU...) etc.

En este apartado se mostrará la forma de aplicar el modelo descrito en arriba para evaluar la bondad de dos de las principales políticas de revocación de certificados:

- OCSP, la principal política de tipo On-Line.
- *Over-issued* CRL, la política de distribución de listas básica.

Aplicación a la política OCSP

OCSP es un protocolo especificado por el IETF [19], este protocolo es empleado para establecer el estado de validez de un certificado de forma on-line. El protocolo es aplicado entre un cliente (OCSP cliente) y un servidor (OCSP "responder") el cual se encarga de enviar el estado del certificado a utilizar.

La aplicación del modelo a OCSP, es directa, únicamente se necesita determinar los parámetros concretos de la misma. En primer lugar la tasa de peticiones será la que nos proporciona la ecuación (2).

Por lo que respecta a T_{cpu} consideraremos que la lista de certificados revocados se encuentra almacenada al completo en la memoria RAM del servidor de revocación y que el tiempo de búsqueda de un certificado revocado es despreciable frente al tiempo de la firma de la respuesta. Se ha estimado como parámetro típico de firmado para los datos respuesta a una petición OCSP un valor de 20ms. Consideraremos que se realizan peticiones de estado de revocación para un solo certificado a la vez. Teniendo en cuenta este hecho podemos expresar B como

$$B = \frac{CRL_H + CRC_C}{\frac{\rho}{v} - T_{cpu}} \qquad (12)$$

Los valores de CRLH y CRLC para certificados X.509 se han hallado utilizando el ejemplo en [19]. Dichos valores se pueden observar en la Tabla 2.

Parámetro	Valor [Bytes}
CRL_H	130
CRL_C	28

Tabla 2. Valores de CRL para OCSP

Política *Over-issued* CRL

Over-issued CRL es una política que requiere de una memoria caché en los usuarios para almacenar la CRL durante un cierto tiempo. De esta forma, el servidor de revocación emite una CRL que tiene validez desde el momento de su creación hasta su tiempo de expiración T_{exp}.

La ventaja de este tipo de política es que los usuarios realizarán una petición de validación únicamente si en su caché no tienen una CRL no caducada, produciéndose por tanto, una disminución de la tasa de peticiones al servidor de revocación.

Basándonos en [5] estudiaremos la forma de aplicar la política *Over-issued* a nuestro modelo.

Supongamos en primer lugar que el servidor de revocación crea una CRL, válida durante su periodo de expiración y que no crea otra CRL hasta que la CRL anterior deja de ser válida. Si el servidor de revocación actúa de esta forma tendremos que todas las copias en los caché de los usuarios de CRL que se habrán creado al mismo tiempo y que por tanto también expirarán en el mismo instante. Esto generará un tráfico de pico alrededor del tiempo de expiración con una tasa de pico de peticiones de validación hacia el servidor de revocación igual a

$$v_{pico} = v = Nv_i \qquad (13)$$

Esto implica que en los instantes cargados del servidor (alrededor del tiempo de expiración) se mantiene una tasa de peticiones de validación igual a la de la política OCSP, teniendo tamaños de CRL mucho mayores, por lo que sino se hace algo esta política no resulta viable. Para que el caché tenga los deseados efectos positivos sobre las peticiones de validación, se ha de aplicar una técnica de sobre-emisión o sobre-creación de CRL (O*ver-issued* CRL) en el servidor de revocación.

En síntesis se trata de repartir las peticiones de validación de los usuarios en el tiempo y evitar la concentración de tráfico. Para conseguirlo, se hace crear CRL's al servidor de revocaciones a un ritmo mayor de lo que estas listas tardan en expirar, de esta forma se consigue que los usuarios tengan copias de CRL con diferentes tiempos de expiración y por tanto

se logra repartir la carga de validación. Si empleamos la ecuación presentada por Cooper en [5], en donde se define O como el número de CRL emitidas durante el tiempo de expiración T_{exp}. Podemos expresar la nueva tasa de pico mediante la siguiente expresión

$$v_{pico} = \frac{N v_i}{[O-1]\left[1-e^{\left(\frac{v_i T_{exp}}{O}\right)}\right]+1} \quad (14)$$

Emitiendo CRL's continuamente se puede conseguir una tasa de peticiones de validación de pico de

$$\lim_{O\to\infty} v_{pico}^{min} = \frac{N v_i}{v_i T_{exp}+1} \le v \quad (15)$$

La tasa de pico hacia el servidor depende del número de intervalos de sobre emisión O. Para simplificar la ecuación (14), podemos expresarla en función de un parámetro F, que nos indicará lo próxima o lejana que está la v_{pico} que estamos manejando respecto al mínimo teórico

$$v_{pico} = F v_{pico}^{min} \frac{N v_i (1+F)}{1+v_i T_{exp}} \quad (16)$$

$$F = f(O) \quad y \quad 0 \le F \le v_i T_{exp} \quad (17)$$

Los valores de CRL_H y CRL_C para certificados X.509 se han hallado utilizando el ejemplo en [11]. Dichos valores se pueden observar en la Tabla 3.

Parámetro	Valor [Bytes}
CRL_H	170
CRL_C	17

Tabla 3. Valores CRL para distribución de listas

Escenarios y resultados

A continuación se presenta el análisis de las dos políticas descritas en el apartado anterior en base al ancho de banda necesario en el sentido servidor de revocación a usuario, para dicho análisis se hace uso de parámetros como la tasa de validación, tiempo de expiración de la lista, etc. En este cálculo no se tendrá en cuenta el coste de la memoria caché en los usuarios, ni el coste de CPU. En la evaluación no se contemplan los diferentes niveles de seguridad que las políticas proporcionan, es decir, no se pondera el riesgo de tomar un certificado como válido cuando este se encuentra en realidad revocado.

A continuación se muestran algunos resultados obtenidos para la política de revocación OCSP. Se ha tomado un escenario de aplicación con 30000 y con un porcentaje de certificados revocados del 10%. En Figura 3 se puede observar la velocidad de transmisión mínima necesaria para diferentes niveles de carga del servidor de revocación (20%, 40%, 60% y 80 %) en función de la tasa de peticiones de los usuarios v_i.

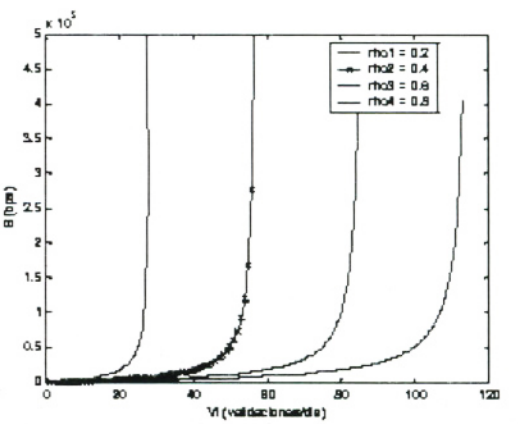

Figura 3 $B(v_i)$ para OSCP

N=30000, p=0.1

La primera conclusión relevante es que si exigimos niveles de carga más altos al servidor, requeriremos menor ancho de banda *Over-issued* para dar servicio a un mismo número de peticiones de validación. Por otra parte, como era de esperar a medida que aumentamos la tasa de validaciones aumenta el ancho de banda necesario y además lo hace de forma exponencial.

A continuación, en la siguiente figura se muestra los resultados obtenidos para la política de revocación *Overissued* CRL. Como en la política anterior en Figura 4 se puede observar B para diferentes niveles de carga del servidor de revocación en función de vi, tomando un escenario con 30000 usuarios, un porcentaje de certificados revocados del 10%, un factor F de 0.1 y un tiempo de expiración de las CRL's de 6 horas.

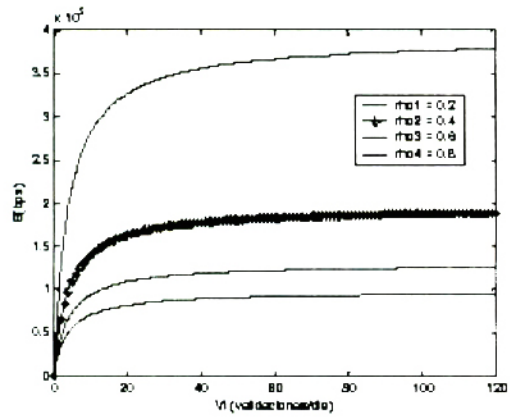

Figura 4 B(v$_i$) para *Over-issued* CRL

N=30000,p=0.1,F=0.1,Texp=6

De la figura anterior se pueden extraer prácticamente las mismas conclusiones que para la política OCSP, es decir, a más carga del servidor menos velocidad de transmisión necesaria para dar servicio a un mismo número de peticiones de validación y a medida que aumentamos la tasa de validaciones también aumenta B. Sin embargo, la forma de crecimiento de B con vi ya no es exponencial como en OCSP, sino que es lineal con vi, para vi pequeñas y tiende a un valor constante que denominaremos velocidad de transmisión umbral B_{umbral} para v_i grandes. Esta circunstancia era de esperar ya que cuando vi crece es cuando los usuarios empiezan a sacar provecho de la copia de CRL de que disponen en su memoria caché, llegando a estabilizarse el ancho de banda necesario

Conclusiones

En este artículo se ha presentado un modelo que permite la evaluación de las diferentes políticas de revocación de certificados propuestas. En particular se ha evaluado el modelo para diferentes niveles de carga del servidor de revocación, relacionando el ancho de banda necesario con la tasa de validación de usuarios. En concreto se han evaluado las políticas de validación *OCSP* y *Over-issued* CRL, alcanzándose las siguientes conclusiones:

- Se puede disminuir la velocidad de transmisión del servidor a costa de aumentar la carga del servidor (Figuras 3 y 4). Sin embargo, un aumento de la carga del servidor aumenta su tiempo de respuesta.
- Para tasas de validación por usuario altas, la política CRL requiere un menor ancho de banda, mientras que para tasas pequeñas, la política *On-line* es la que requiere un menor ancho de banda.

Referencias

[1] Aiello, W.; Lodha, S.; Ostrovsky, R: *"Fast Digital Revocation"*. Advances in Cryptology. Crypto 98. Lecture in Computer Science. Springer-Verlag, N° 1462. August 98. Pags. 137-152.

[2] Arsenault A.; Turner, S.; "Internet X.509 Public Key Infrastructure PKIX Roadmap". IETF Internet Draft, Octubre 1999. Draft-ietf-pkix-roadmap-04.txt

[3] Branchaud, M.; "Internet Public Key Infrastructure": Caching the Online Certificate Status Protocol", Internet Draft, 1998. draft-ietfpkix- ocsp-caching-00.txt

[4] CCITT. "Recommendation X.500: The directory-overview of concepts, models and services." 1988.

[5] Cooper, A. David. "A Model of Certificate Revocation". Proceedings of the Fifteenth Annual Computer Security

Applications Conference, December 99, Pages 256-254.

[6] Cooper, A. David. "A more efficient use of Delta-CRLs". Proceedings of the 2000 IEEE Symposium on Security and Privacy. Computer Security Division National Institute of Standards and Technology. May 2000. Pages 190-202.

[7] Diffie, W.; Hellman, M. "New directions in cryptography". IEEE Transactions on Information Theory., IT-11(6): November 1976. Pages. 1644-654.

[8] Even, S.; Goldreich, O.; Micali, S. "On-Line/Off Line Signatures". Journal of Criptology. Vol. 9. 1996, Pages. 35-67.

[9] Castro, J.C.; Forné, J.; "A Model to Evaluate Certificate Revocation"; 4th World Multiconference on Systemics, Cybernetics and Informatics (SCI2000) and the 6th International Conference on Information Systems Analysis and Synthesis (ISAS2000), Orlando (Florida). 2000.

[10] Fox, B.; LaMacchia, B; "Online Certificate Status Checking in Financial Transactions: The Case for Re-issuance". Financial Cryptography-FC 99, Lecture Notes in Computer Science, Springer- Verlag, Vol. 1648, 1999 Pages. 104-117

[11] Housley, R.; Ford, W.; Polk, W; Solo, D.; "Internet X.509 Public Key Infrastructure Certificate and CRL Profile". RFC 2459, Enero 1999.

[12] ITU /ISO "Recommendation X.509. – Information technology – Open Systems Interconnection - The Directory: Public Key and Attribute Certificate Frameworks". Agosto,1997.

[13] ITU /ISO "Recommendation X.509. – Information technology – Open Systems Interconnection - The Directory: Autentication Frameworks. Technical Corrigendum" Marzo, 2000.

[14] Kleinrock,L "Queuing Systems. Volume I: Theory". John Wiley & Sons, Inc. 1975.

[15] Kocher, Paul C, "On Certificate Revocation and Validation", Financial Cryptography-FC 98, Lecture Notes in Computer Science, Springer-Verlag, Vol. 1465, 1998 Pages. 172 – 177.

[16] Kohnfelder, L.M.; "Towards a practical public-key cryptosystem". Master's thesis, MIT Laboratory for Computer Science, May 1978.

[17] Micali, S. "Efficient Certificate Revocation". Technical Memo MIT/LCS/TM-542b Laboratory for Computer Science. Massachusetts Institute of Technology. USA.1996.

[18] Myers, M; Ankney, R.; Malpani, A.; Galperin, S.; Adams, C.; "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP". RFC 2560, June 1999.

[19] Myers, M; Ankney, R; Adams, C.; "Online Certificate Status Protocol, Version 2" September, 2000. Draft-ietf-pkix-ocspv2-00.txt

[20] Naor, M., Nissim K., "Certificate Revocation and Certificate Update", Department of Applied Mathematics and Computer Science, 7th USENIX Security Symposium, 1998.

[21] Wohlmacher, Petra; "Digital Certificates: A survey of revocation methods", Proceedings on ACM multimedia 2000. Pages 111-114.