

“Estudio comparativo de políticas de revocación de certificados: OCSP vs. Overissued-CRL”

José Luis Muñoz, Juan Carlos Castro, Jordi Forné Muñoz
Departament d'Enginyeria Telemàtica. Universitat Politècnica de Catalunya.
Jordi Girona 1 y 3. Campus Nord, Mód C3, UPC. 08034 Barcelona
E-mail: {jlmunoz, jcastro, jforne}@mat.upc.es

Abstract. *The emergent applications of electronic commerce require security services. The authentication is the most difficult to archive, and the employment of public key infrastructures (PKI) is required. The revocation of the certificates is the major cost in the whole PKI. Up to the date, different revocation policies have been proposed. In this paper we evaluate two of the main proposed policies: OCSP and Overissued-CRL.*

1 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).

Para proporcionar los servicios de seguridad básicos, necesarios para la construcción de aplicaciones seguras para los usuarios finales, en el entorno que estamos tratando, 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.

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.

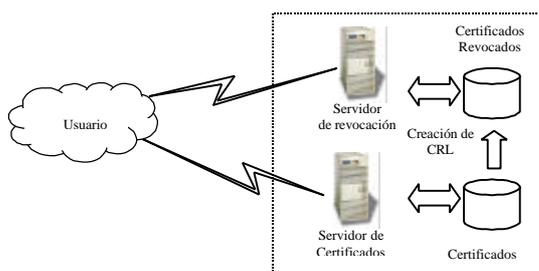


Figura 1 Esquema general de una AC

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.

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]. 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 públicas 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. 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 [19]. Cada uno de estos estudios propone una política de revocación diferente, aunque no proporcionan un modelo general para evaluar dichas políticas. En este artículo se presenta un estudio comparativo de las dos principales políticas de revocación. Para poder evaluar políticas de revocación en primer lugar se define y se justifica que parámetros son

considerados relevantes y finalmente se evalúan dichos parámetros en las políticas estudiadas. El principal parámetro evaluado es la velocidad de transmisión necesaria.

2 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 dividir en dos grandes grupos:

Políticas de revocación basadas en distribución de listas. 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 cada vez que desee emplear un certificado para verificar si el certificado dado ha caducado. El contenido de la CRL consta de diferentes campos: Versión, Emisor de la lista, Algoritmo empleado para firmar la CRL, Fecha de expiración de CRL, Información de los certificados revocados etc. 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 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 a destacar es el Sistema de Revocación de Certificados (CRS) la cual fue propuesta en 1996 por Silvio Micali [17]. 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), este método asigna a cada usuario un conjunto de cadenas Hash en lugar de una sola.

La siguiente política fue la propuesta hecha por Paul Kocher [15] en la cual presenta un modelo de Arbol de Certificados Revocados (CRT). Posteriormente 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], actualmente se encuentra en discusión una nueva propuesta [19], dicha propuesta expira Agosto 2001. Mediante este protocolo el usuario recibe el estado del certificado o grupo de certificados que necesita. En [10] Fox y La Macchia presentan una alternativa a OCSP basada en 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.

3 Evaluación de políticas de revocación

Se han mencionado diferentes técnicas de revocación de certificados en las secciones anteriores, dichas técnicas se pueden agrupar en consultas Off-Line y consultas On-Line [10]. 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 donde 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.

3.1 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, por lo que los parámetros de evaluación que vamos a considerar serán parámetros del servidor de revocación. En 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:

B	Velocidad binaria de transmisión de salida del servidor
$T_{\text{validación}}$	Tiempo medio de validación de certificado.
T_{cpu}	Tiempo de procesador que consume una validación de certificado.

Tabla 1 Parámetros críticos en el diseño del servidor de revocación

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

- 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 esta directamente relacionada con el ancho de banda necesario para poder realizar la transmisión, por lo que en adelante se utilizará indistintamente velocidad de transmisión o ancho de banda necesario.
- El $T_{\text{validación}}$ 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 $T_{\text{validación}}$ muy elevado es posible que se puedan perder consultas por temporización de conexiones TCP o que los usuarios abandonen la consulta.
- El valor de T_{cpu} 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.

3.2 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

Figura 2 se muestra el esquema general del modelo de servidor de revocación que vamos a utilizar.

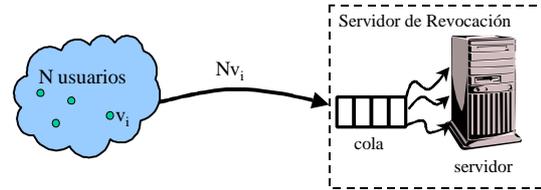


Figura 2 Modelo basado en teoría de colas para el servidor de revocación

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 viene dada por $\nu e^{-\nu t}$. Donde ν 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, la del sistema sería $\nu = Nv_i$.

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 $T_s = T_{\text{tx}} + T_{\text{cpu}}$. 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 .

$$CRL = CRL_H + c \ CRL_C \quad (1)$$

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 t y de parámetros de la política de distribución de certificados que se aplique

$$M_R = f(M, t, \dots) \quad (2)$$

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

$$M_R = pM \quad 0 \leq p \leq 1 \quad (3)$$

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

$$B = \frac{CRL \text{ [bits]}}{T_{tx} \text{ [s]}} \text{ [bps]} \quad (4)$$

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 r como la carga del servidor de revocación mediante la siguiente expresión $r = vT_s$. De (1) y (4) se obtiene una expresión general para la velocidad binaria de transmisión B

$$B = \frac{CRL_H + c CRL_C}{\frac{r}{Nv_i} - T_{cpu}} \quad (5)$$

Finalmente el tiempo de validación se puede hallar según la siguiente expresión

$$T_{validacion} = \frac{T_s(2 - vT_s)}{2(1 - vT_s)} \quad (6)$$

Substituyendo T_s por las expresiones en (4) se obtiene una expresión para (6) en función del tamaño de los datos CRL, de B y del tiempo de CPU consumido

$$T_{validacion} = \frac{\left(\frac{CRL}{B} + T_{cpu}\right) \left[2 - v\left(\frac{CRL}{B} + T_{cpu}\right)\right]}{2 \left[1 - v\left(\frac{CRL}{B} + T_{cpu}\right)\right]} \quad (7)$$

3.3 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, 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 3.2 para evaluar la bondad de dos de las principales políticas de revocación de certificados:

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

3.3.1. Aplicación a la política OCSP

La aplicación del modelo a OCSP, es directa, únicamente determinar los parámetros concretos de la misma. En primer lugar la tasa de peticiones será la que nos proporciona la ecuación $v = Nv_i$.

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

$$B = \frac{CRL_H + CRL_C}{\frac{r}{v} - T_{cpu}} \quad (8)$$

Los valores de CRLH y CRLC para certificados X.509 se hallaron 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

3.3.2. Política *Overissued-CRL*

Overissued-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 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 pico de peticiones de validación hacia el servidor de revocación igual a:

$v_{pico} = v = Nv_i$. 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 (*Overissued-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 definimos 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

$$v_{pico} = \frac{Nv_i}{(O-1)(1 - e^{-\frac{v_i T_{exp}}{O}}) + 1} \quad (9)$$

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

$$\lim_{O \rightarrow \infty} v_{pico}^{min} = \frac{Nv_i}{v_i T_{exp} + 1} \leq v \quad (10)$$

La tasa de pico hacia el servidor depende del número de intervalos de sobreemisión O . Para simplificar la ecuación (9), podemos expresarla en función de un parámetro F , el cual denominaremos factor de sobreemisión y que nos indicará lo próxima o lejana que está la v_{pico} que estamos manejando respecto al mínimo teórico

$$v_{pico} = F v_{pico}^{min} = \frac{Nv_i(1+F)}{1 + v_i T_{exp}} \quad (11)$$

Donde F

$$F = f(O) \text{ y } 0 \leq F \leq v_i T_{exp} \quad (12)$$

Finalmente, considerando que el tiempo de preparación de la CRL para ser enviada T_{cpu} es despreciable para esta política (firma *Off-Line* y datos en RAM) podemos obtener una expresión para B aplicando a la expresión (5) la expresión

$$B = \frac{(CRL_H + pN CRL_C)(Nv_i)(1+F)}{r(v_i T_{exp} + 1)} \quad (13)$$

Los valores de CRLH y CRLC 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 de CRL para distribución de listas

4. Resultados

A continuación se analizan las políticas de revocación de certificados OCSP y *Overissued-CRL* para algunos escenarios, evaluando la

influencia de parámetros como el ancho de banda, el tiempo de validación de un certificado en el servidor, el número de usuarios del escenario y el tiempo de expiración de una CRL en caché de un usuario.

4.1 Estudio del ancho de banda y tiempo de validación asociado

En primer lugar se realiza un estudio del comportamiento del ancho de banda y del tiempo de validación respecto a la tasa de peticiones de validación de los usuarios.

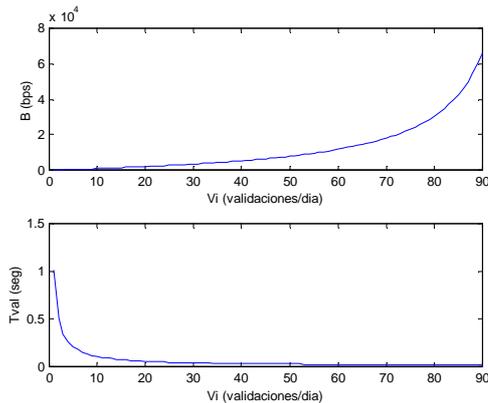


Figura 3 $B(V_i)$ y $T_{val}(V_i)$ para política OCSP. Escenario con 30,000 usuarios y una carga del 70% del servidor de revocación.

En la Figura 3 se observa un comportamiento de tipo exponencial ascendente por lo que respecta al ancho de banda necesario en función de la tasa de peticiones, a su vez el comportamiento del tiempo de validación tiene un comportamiento también exponencial pero de forma descendente. Los resultados obtenidos eran esperados, a más validaciones por usuario, manteniendo la carga del sistema, se necesitara más ancho de banda y al tener un ancho de banda mayor tendremos menos tiempo de transmisión de los datos de la consulta y por tanto menos tiempo de validación.

En la Figura 4 se muestran los resultados de un escenario semejante para la política *Overissued-CRL*.

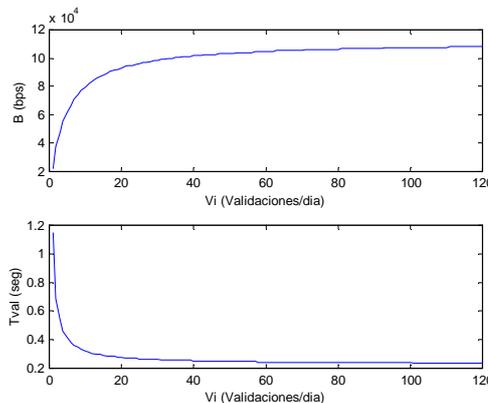


Figura 4 $B(V_i)$ y $T_{val}(V_i)$ para política *Overissued-CRL*. Escenario con 30,000 usuarios, porcentaje de

certificados revocados 10%, $F=0.1$, tiempo de expiración de CRL de 6 h y carga del servidor de revocación del 70%.

Las conclusiones en este caso son parecidas al caso de OCSP con algunos matices. A medida que aumentamos la tasa de validaciones también aumenta B y disminuye el tiempo de validación. Sin embargo, la forma de crecimiento de B con v_i ya no es exponencial como en OSCP, sino que es lineal con v_i , para v_i 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 v_i 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.

4.2 Estudio de la influencia del número de usuarios

En este apartado se realiza un estudio comparativo del ancho de banda para las políticas de revocación en cuestión, para diferentes tamaños de población del modelo.

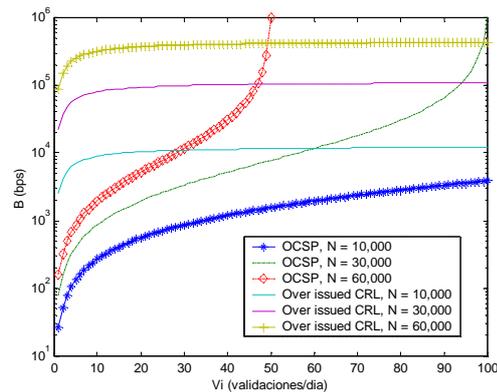


Figura 5 $B(V_i)$ para diferentes poblaciones para políticas OCSP y *Overissued-CRL*. Escenario con un porcentaje de certificados revocados de 10 %, un factor F de 0.1, un tiempo de expiración igual a 6 horas y un nivel de carga del servidor de revocación de 70 %.

En la Figura 5 se observa que la política OCSP presenta un menor ancho de banda para tasas de validación pequeñas, conforme dicha tasa aumenta el ancho de banda aumenta hasta volver al sistema inestable, esta inestabilidad se produce a tasas más bajas conforme la población crece. Por otra parte, el ancho de banda para la política *Overissued-CRL* tiende a un valor constante (B_{umbral}) para valores altos de validación. A mayor población obtenemos un mayor B_{umbral} .

4.3 Estudio de la influencia del tiempo de expiración

En la Figura 6 se observa que al aumentar el tiempo de expiración, disminuye el ancho de banda necesario, lo cual implica un compromiso entre riesgo en las operaciones con certificados y el ancho de banda utilizado.

Por otra parte, podemos apreciar que las curvas para los diferentes tiempos de expiración alcanzan el valor B_{umbral} para diferentes v_i . Esta circunstancia se explica porque para tiempos de expiración grandes con tasas bajas ya podemos sacar el máximo partido a la memoria caché y por tanto se estabiliza el ancho de banda necesario para estas tasas bajas, mientras que para tiempos de expiración pequeños son necesarias tasas v_i mayores para llegar a sacar partido de la memoria caché necesitando de esta forma una v_i mayor para llegar a B_{umbral} .

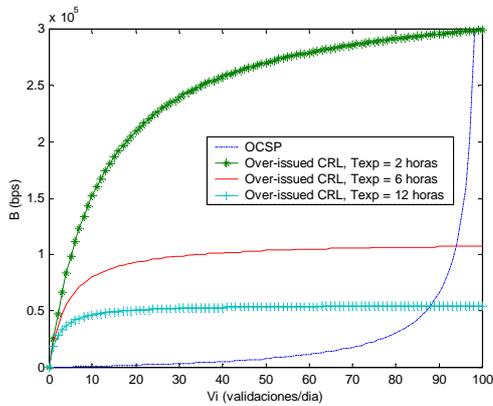


Figura 6 $B(V_i)$ para diferentes tiempos de expiración para políticas OCSF y Overissued-CRL. Escenario con un porcentaje de certificados revocados de 10 %, un factor F de 0.1 y un nivel de carga del servidor de revocación de 70 %.

A pesar de que la curva $B(v_i)$ para OCSF no depende del tiempo de expiración, se ha incluido en la Figura 6 para tomarla como referencia en la evaluación de la conveniencia de una política u otra por lo que al consumo de ancho de banda se refiere. A este respecto, se observa que conforme el tiempo de expiración se hace más restrictivo (pequeño) el cruce de ambas curvas, que nos determina cual es más conveniente, se produce a tasas de validación por usuario más altas.

4.4 Estudio de un escenario

En este apartado se va a definir un escenario concreto para el que se va a evaluar la política más conveniente en función de los parámetros que se han establecido a lo largo del presente documento.

En primer lugar se define el escenario de evaluación, vamos a suponer un escenario de tipo mediano con una población de 30,000 usuarios.

Se tomará un porcentaje de certificados revocados del 10%. En el caso de la política *Overissued-CRL* se considera un factor de sobreemisión de 0.1. Por otra parte, usualmente en los sistemas prácticos, normalmente el ancho de banda disponible, es un parámetro fijado. Además, se va a evaluar la política más conveniente en dos supuestos, asumiendo que el servidor posee un ancho de banda de bajada hacia los usuarios de 50Kbps y 100Kbps respectivamente.

Política	B [Kbps]	V_i^{MAX} [val/día]	T_{exp}^{MIN} [h-m]	T_{val} [ms]
OCSF	50	124	0''	12
	100	133	0''	11
Overissued CRL	50	∞	9h23'	512
	100	∞	4h41'	512

Tabla 4 Parámetros de evaluación escenario

En la Tabla 4 se observan los diferentes parámetros¹ de evaluación (tasa de peticiones de validación por usuario y día máxima, tiempo de expiración mínimo y tiempo de validación medio) que nos proporciona cada política, para el escenario propuesto.

En función de los datos proporcionados por la Tabla 4, el administrador del servicio de revocación puede elegir la política a emplear en cada caso. Por ejemplo, para el caso del ancho de banda de 50Kbps, si tenemos tasas de validación inferiores a 120 validaciones por día y usuario, la política más conveniente es OCSF, ya que el tiempo de expiración es nulo, no necesitamos ningún tipo de memoria caché en los usuarios y los tiempos de validación medios son un orden de magnitud menor que en el caso de la otra política. Sin embargo, si la tasa de validaciones comienza a incrementarse por encima de 120, el servidor de revocación se vuelve inestable para OCSF, en ese caso es más adecuada la política *Overissued-CRL*. Se ha de recordar que para utilizar esta política es necesario utilizar memoria caché en los usuarios y tenemos un cierto tiempo de expiración, por lo que no podemos estar seguros de la validez de un certificado en tiempo real. Análogas conclusiones se pueden observar para el caso del ancho de banda de 100Kbps.

Conclusiones

En este artículo se presenta un estudio de las políticas de revocación *OCSF* y *Overissued-CRL*,

¹ Servidor de revocación trabajando al 100% de su capacidad.

observando para cada una de estas el comportamiento de los parámetros considerados críticos para la entrega del estado de revocación de un certificado. Los principales parámetros de evaluación son el Ancho de Banda, Tiempo de Validación, Tiempo de Expiración y Tasa de Validación Máxima para una población dada. Se ha estudiado el efecto de cada uno de estos parámetros individualmente y en conjunto para un escenario particular. Finalmente se han alcanzado las siguientes conclusiones:

- En general, para tasas de validación altas el sistema necesita anchos de banda elevados. En el caso de OCSP, el sistema se satura alcanzando un valor de ancho de banda infinito; mientras que el Overissued-CRL el sistema alcanza un valor umbral de ancho de banda, por lo que el sistema es capaz de soportar tasas de validación infinitas, debido a que las tasas de validación reales son constantes.
- A más validaciones por usuario, manteniendo la carga del sistema, se necesitara más ancho de banda y al tener un ancho de banda mayor, tendremos menos tiempo de transmisión de los datos de la consulta y por tanto menos tiempo de validación (Figuras 3 y 4).
- En CRL el ancho de banda necesario es proporcional al cuadrado del tamaño de la población (Figura 5).
- En CRL existe un compromiso entre ancho de banda y el nivel de riesgo. Un nivel de riesgo alto (tiempo de expiración grande), exige un ancho de banda pequeño y a la inversa (Figura 6).
- Para tasas de validación por usuario altas, la política CRL parece ser la más adecuada, mientras que para tasas pequeñas, parece más apropiada la política OCSP (Figura 6 y Tabla 4).

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] Arsenaull 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-ietf-pkix-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 256-264.
- [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. 1644-1654.
- [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.; Ankney, R.; Adams, C.; Farrell, S.; Covey, C.; "Online Certificate Status Protocol, Version 2". March, 2001. Draft-ietf-pkix-ocspv2-02.txt
- [20] Naor, M., Nissim K., "Certificate Revocation and Certificate Update", Department of Applied Mathematics and Computer Science, 7th USENIX Security Symposium, 1998.