Evaluación y dimensionamiento de sistemas de revocación de certificados

Evaluation and Dimensioning of Certificate Revocation Systems

J. Forné y J. L. Muñoz

Hay grandes expectativas 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

Resumen

La PKI presenta actualmente varios problemas de escalabilidad, entre ellos uno de los más complejos es el de la revocación de certificados en escenarios con una gran cantidad de usuarios y tasas de validación elevadas. En este artículo revisamos los sistemas de revocación más significativos y proponemos una metodología para la evaluación y dimensionamiento de sistemas de revocación en diferentes escenarios de aplicación. Esta evaluación se lleva a cabo tanto a través de un modelo analítico como de un testbed de simulación denominado CERVANTES (CERtificate VAlidatioN TEStbed), que está siendo desarrollado en la UPC.

Palabras clave: PKI, Revocación de Certificados, X.509, CRL, OCSP

Summary

Certificate revocation is one of the hardest scalability problems of the whole PKI, specially in those scenarios with a large number of users and high validation rates. In this paper we review the main revocation systems and we propose a methodology to evaluate and dimension revocation systems in different application scenarios. This evaluation is carried out by means of both an analytical model and a simulation testbed named CERVANTES (CERtificate VAlidatioN TEStbed), which is being developed at the UPC.

Keywords: PKI, Certificate Revocation, X.509, CRL, OCSP

1.- Introducción

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, sobre todo cuando se quieren 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. Cada uno de estos estudios propone una política de revocación diferente, aunque no proporcionan un modelo general para evaluar dichas políticas. En este trabajo nos centramos en la evaluación y dimensionamiento de sistemas de revocación de certificados, tanto analíticamente como mediante la utilización de un testbed de simulación.

2.- Políticas de revocación de certificados

Las políticas de revocación de certificados definen la forma por la cual un usuario puede obtener información relativa al estado de un determinado certificado digital. El análisis de la forma en la que debe proporcionarse dicha información al usuario se ha realizado en los estudios mencionados anteriormente, de donde podemos concluir que las políticas de revocación de certificados se pueden dividir en dos grandes grupos: las basadas en distribución de listas u Off-line y las que lo están en línea.

2.1.- Grupo de políticas de revocación basadas en distribución de listas u Off-Line

Este tipo de políticas se caracteriza por el envío de una lista de certificados revocados o CRL al usuario, mediante la cual debe de verificar el estado del certificado. Generalmente los usuarios guardan la lista en su memoria caché y no es necesario realizar transacciones en línea cuando se necesita verificar el estado de un cierto certificado. Estas políticas vienen descritas en el estándar X.509 [1].

Las políticas de revocación basadas en distribución de listas se caracteriza por el envío de una lista de certificados revocados o CRL al usuario, mediante la cual debe de verificar el estado del certificado

La más simple de estas políticas se denomina Traditional-CRL (Certificate Revocation List), es además más madura y forma parte del estándar X.509 desde la versión 1. En Traditional-CRL, la información de revocación es una colección digitalmente firmada de los números de serie de los certificados revocados y no expirados junto con información acerca de la versión, número de serie de la CRL, emisor, algoritmo utilizado para la firma, firma, fecha de emisión (not-valid-before), fecha de expiración (not-valid-after) y algunos campos opcionales denominados extensiones. Una vez la CRL ha sido emitida, la CA la envía a los repositorios. Una mejora para evitar picos de petición en los instantes de expiración se conoce como Overissued-CRL [2], y consiste en emitir una nueva CRL antes de que la CRL anterior haya expirado.

En 1994 se presentó Delta-CRL. Se trata de una pequeña CRL que proporciona información acerca de los certificados cuyo estado ha cambiado desde la emisión de una lista completa llamada Base-CRL. El periodo de emisión de una Delta-CRL es mucho menor que el de una Base-CRL, de tal forma que el usuario puede bajarse la última Delta-CRL en lugar de bajarse una Base-CRL, la cual tiene un tamaño mucho mayor. Otra política que puede ser combinada con las anteriores es CRL-Distribution-Points, donde cada CRL contiene los certificados revocados de un cierto grupo. Los criterios para crear estos grupos pueden ser geográficos, por nivel de importancia, tipo de uso, razón de revocación, etc.

2.2.- Grupo de políticas de revocación en línea u 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 concreto.

El protocolo de estado de certificados en línea (OCSP) [3] ha sido propuesto por el grupo PKIX del IETF, y proporciona el estado de uno o varios certificados a través de un servidor de confianza denominado OCSP Responder. OCSP se basa en mecanismos de solicitud/respuesta que pueden encapsularse en múltiples protocolos de comunicaciones, aunque el más utilizado es HTTP.

Por último, se han propuesto en la literatura una serie de políticas basadas en árboles de funciones de hash, como CRT [4], o los diccionarios autenticados [5]. Incluso se han hecho propuestas en las que la validación viene implícita, como el SCVP [6]. Sin embargo hasta la fecha sólo CRL y OCSP han sido ampliamente utilizadas.

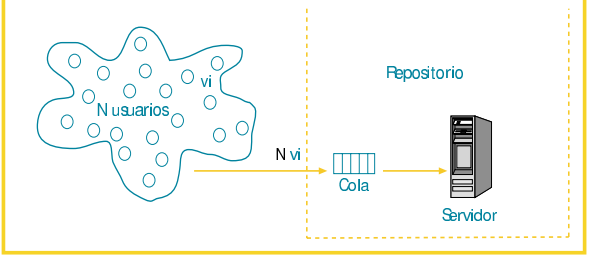
3.- Evaluación de sistemas de revocación de certificados

Entre los parámetros a evaluar se consideran: la seguridad, el ancho de banda necesario y la carga computacional (tanto de lado cliente como servidor).

En la figura 1 se presenta un modelo basado en teoría de colas que nos permite evaluar la política de revocación más adecuada en cada escenario en concreto, así como dimensionar tanto la capacidad de cálculo de los servidores como el ancho de banda del que deben disponer. Para una justificación profunda del modelo utilizado consultar [7].

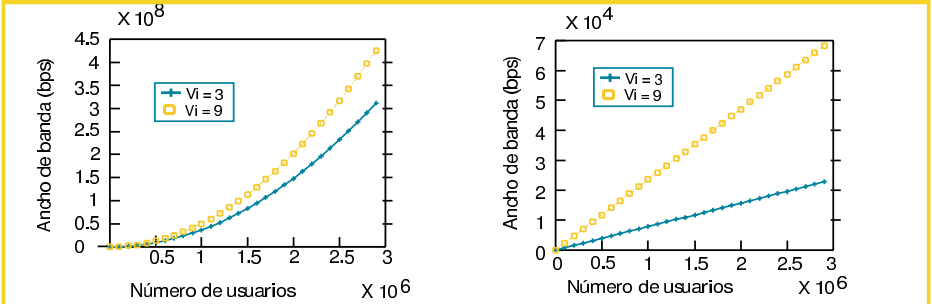
El modelo propuesto permite evaluar el comportamiento de diferentes políticas de revocación en distintos escenarios de aplicación

FIGURA 1: MODELO DE EVALUACIÓN



La aplicación de este modelo en diferentes entornos nos permite elegir la política de revocación y los parámetros más adecuados para cada escenario. En la figura 2 puede verse un ejemplo de los resultados obtenidos mediante la aplicación de este modelo a un escenario de correo electrónico seguro. En la figura se muestra el ancho de banda necesario del servidor de revocación en función del número de usuarios, para las políticas Overissued-CRL (izda.) y OCSP (dcha.). Se ha considerado un tiempo de expiración de la CRL de 12 horas. Vi es el número medio de consultas por día.

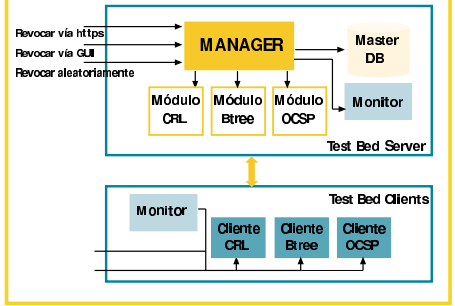
FIGURA 2: APLICACIÓN DEL MODELO A UN ESCENARIO DE CORREO ELECTRÓNICO SEGURO



4.- CERVANTES

El modelo propuesto permite evaluar el comportamiento de diferentes políticas de revocación en distintos escenarios de aplicación, facilitando la elección de la política más adecuada y el dimensionamiento de los elementos del sistema de revocación (capacidad computacional de los servidores OCSP, ancho de banda de los repositorios, ancho de banda necesario para los clientes, etc.).

FIGURA 3: ARQUITECTURA DE CERVANTES



Para la evaluación de las políticas basadas en árboles y propuesta de nuevas políticas, así como para la integración de distintos sistemas de revocación, el modelo analítico se torna complejo y por ello estamos desarrollando un testbed de revocación (CERVANTES).

La figura 3 muestra la arquitectura de CERVANTES. El sistema está compuesto por dos módulos fundamentales: un testbed servidor, que implementa las principales políticas de revocación propuestas, así como nuevas propuestas para ser evaluadas; y un testbed de cliente, que implementa simuladores de clientes de los protocolos mencionados. El lector puede obtener información adicional sobre el estado del proyecto CERVANTES en [8].

5.- Referencias

[1] ITU/ISO Recommendation. X.509 Information Technology Open Systems Interconnection - The Directory: Autentication Frameworks, 2000. Technical Corrigendum.

[2] D.A. Cooper. A model of certificate revocation. In *Fifteenth Annual Computer Security Applications Conference*, pp. 256-264, 1999.

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

[4] P.C. Kocher. On certificate revocation and validation. In *International Conference on Financial Cryptography (FC98). Lecture Notes in Computer Science*, number 1465, pp. 172-177, February 1998.

[5] M. Naor and K. Nissim. Certificate Revocation and Certificate Update. *IEEE Journal on Selected Areas in Communications*, 18(4):561-560, 2000.

[6] A. Malpani, P. Hoffman, P. Housley, and T. Freeman. Simple Certification Validation Protocol (SCVP), 2001. Internet Draft: draft-ietf-pkix-scvp-08.txt.

[7] J.L. Muñoz and J. Forné. Evaluation of Certificate Revocation Policies: OCSP vs. Overissued CRL. In *Database and Expert Systems Applications 2002 (DEXA 02)*, pp. 511-515. IEEE Computer Society, September 2002

[8] http://isg.upc.es/cervantes

Jordi Forné
jordi.forne@entel.upc.es
José Luis Muñoz
jose.munoz@entel.upc.es
Dpto. de Ingeniería Telemática - UPC