PRIVILEGE DELEGATION: PATH VALIDATION vs. CERTIFICATE REVOCATION

DELEGACIÓN PRIVILEGIADA: VALIDACION vs. REVOCACION

Cristina Satizábal[1,2], Rafael Páez[1], Jordi Forné[1]

[1] **Universidad Politécnica de Catalunya**, Departamento de Ingeniería Telemática.
C/Jordi Girona 1-3 C3, 08034 Barcelona, España.
{isabelcs, rpaez, jforne}@entel.upc.es
[2] **Universidad de Pamplona**, Facultad de Ingenierías y Arquitectura
Pamplona, Colombia

Abstract: One of the challenges of the current delegation systems is the efficient management of the delegation paths. In this paper, we determine the computational cost of the cryptographic operations that a privilege verifier carries out during the validation of a delegation path, as the path length is increased. Also, we analyze the influence of the revocation mechanisms, CRL and OCSP, in such cost. Our goal is to show the complexity of the delegation path validation process and to motivate the search of new alternatives that lead to simplify this process.

Resumen: Uno de los retos del sistema de delegación actual es la administración eficiente de los caminos de la delegación. Este articulo, determinamos el costo computacional de las operaciones de criptografía que un verificador de privilegio lleva a cabo durante la validación de un camino de delegación, cuando la longitud del camino se aumenta. También, se analiza la influencia de los mecanismos de revocación, CRL y OCSP, y sus costos. Nuestro objetivo es mostrar la complejidad del proceso de validación del camino de la delegación y motivar las búsquedas de nuevas alternativas que puedan conducir a simplificar este proceso.

Keywords: Privilege Management Infrastructure (PMI), Delegation Path Validation, CRL (Certificate Revocation List), OCSP (Online Certificate Status Protocol).

1. INTRODUCCIÓN

Hoy en día, los sistemas computacionales se encuentran altamente distribuidos, componiéndose de varias organizaciones, cada una con sus correspondientes políticas de seguridad. Por ello, es importante la delegación de privilegios entre las distintas entidades de un sistema.

La herramienta básica para realizar esta operación son los certificados digitales, especialmente los certificados de atributo (ACs) (ITU-T 2000), que vinculan un conjunto de permisos o privilegios con una entidad.

Uno de los retos de los sistemas de delegación actuales es la gestión eficiente de los caminos de delegación. Un camino de delegación es un grupo de certificados mediante el cual cierto conjunto de permisos va propagándose de unas entidades a otras. Las decisiones de autorización basadas en caminos largos pueden ser complejas, tanto desde el punto de vista computacional como considerando el conjunto de recursos que se necesita para almacenarlos, obtenerlos desde directorios y verificarlos.

En este artículo, se determina el coste computacional de las operaciones criptográficas realizadas por un verificador de privilegios, durante la validación de un camino de delegación. Para ello, en la sección 2 se explica en que consiste la validación de caminos de delegación y se describen los mecanismos de revocación CRL y OCSP. Posteriormente en la sección 3, se determina el número de operaciones criptográficas que realiza el verificador de privilegios para validar un camino de delegación, sin y con revocación. En la sección 4, se calcula el coste computacional de las operaciones criptográficas especificadas en la sección 3. Finalmente, la sección 5 contiene las conclusiones de este estudio.

2. ESTADO DEL ARTE

2.1 PMI y validación de caminos de delegación

En la revisión del año 2000 de la recomendación X.509 (ITU-T 2000), la ITU-T definió formalmente el marco de certificados de atributo, que proporciona las bases para construir una Infraestructura de Gestión de Privilegios (PMI). En PMI, la SOA (Fuente de Autoridad) es responsable de la asignación inicial de privilegios. La SOA puede autorizar a otra entidad para que actúe como Autoridad de Atributo (AA) delegándole un conjunto de privilegios. Esta AA, puede también delegar todos o parte de esos privilegios que posee a otra AA, o bien delegarlos directamente a entidades finales, según sus derechos se lo permitan. Con ello se forma un *Camino de Delegación* que es una lista de ACs, enlazados por los nombres de sus emisores y propietarios. El verificador de privilegios deberá validar dicho camino comprobando que cada AA tiene los privilegios y la autorización suficiente para la delegación. Así, la validación de un camino de delegación incluye:

- Establecer un camino de delegación confiable.
- Verificar la firma digital de cada certificado de atributo (AC) en el camino de delegación.
- Verificar que los ACs no están caducados o han sido revocados por sus emisores.
- Asegurar que cada emisor estaba autorizado a delegar los privilegios.
- Asegurar que los privilegios en el certificado AC son suficientes cuando se les compara con la política de control de acceso (PCA).
- Autenticar a las entidades que hacen parte del camino de delegación. Para ello se puede usar el servicio de autenticación de una PKI (Infraestructura de Clave Pública) (ITU-T 2000). La autenticación consiste en establecer un camino de certificación, y verificar la firma y validez de los certificados de clave pública (PKCs) que hacen parte de dicho camino.

2.2 Mecanismos de revocación

Revocar es anular el vínculo de una clave pública o privilegio y una identidad antes de la expiración del certificado que establece dicho vínculo. Un certificado puede ser revocado por la pérdida o compromiso de la clave privada asociada, por un cambio en los derechos de acceso del propietario, etc. Los mecanismos de revocación estándar son CRL (ITU-T 2000) y OCSP(Myers, Ankney et al. 1999).

CRL (Certificate Revocation List). Las CRLs fueron introducidas en 1988 por ITU-T en la recomendación X.509 (ITU-T 2000). Una CRL es una lista, firmada digitalmente por una autoridad, que contiene los números seriales de los certificados revocados junto con su fecha y razón de revocación. Estas listas son actualizadas periódicamente y publicadas en repositorios no confiables. Para conocer el estado de revocación de un certificado, el verificador debe recuperar la CRL donde se encuentra la información de revocación de dicho certificado y verificar su firma. Luego, debe buscar el número serial del certificado dentro de la lista. Si lo encuentra, el certificado ha sido revocado.

OCSP (Online Certificate Status Protocol). Fue adoptado por IETF en 1999(Myers, Ankney et al. 1999). Sirve para determinar la validez de un certificado en línea. Para conocer el estado de revocación de uno o más certificados, el verificador envía su solicitud a una entidad confiable llamada responder OCSP. Esta solicitud contiene: la versión del protocolo OCSP utilizado, el tipo de servicio requerido y uno o más identificadores de certificados. Un identificador de certificado contiene a su vez el hash sobre el DN (Distinguished Name)(Kille 1995) del emisor del certificado, el hash sobre la clave pública del mismo emisor y el número de serie del certificado. El responder OCSP le devuelve al verificador el estado de revocación de estos certificados, junto con sus respectivos identificadores y el intervalo de validez de dicha respuesta. Esta respuesta va firmada digitalmente por el responder OCSP. El estado *good* significa que el certificado no ha sido revocado, pero puede no haber sido expedido todavía o que la respuesta se expidió fuera de su período de validez. El estado *revoked* significa que el certificado se ha revocado y el estado *unknown* significa que el responder no tiene información sobre el certificado requerido.

3. NÚMERO DE OPERACIONES CRIPTOGRÁFICAS

Durante la validación de un camino de delegación se llevan a cabo diversos tipos de operaciones: operaciones criptográficas, operaciones de búsqueda en listas, operaciones de transmisión de información. Sin embargo, debido a su complejidad, las operaciones criptográficas son quizás las que requieren mayor tiempo de procesamiento.

En esta sección se determina el número de operaciones criptográficas que realiza un verificador durante la validación de un camino de delegación, sin y con revocación. Son operaciones criptográficas las de hash y las exponenciaciones modulares utilizadas para cifrado/descifrado. Se denota como L_d la longitud del camino de delegación y se supone que todos los caminos de certificación, involucrados en la validación del camino de delegación, tienen la misma longitud L_c. La Tabla 1 muestra la notación utilizada en este artículo.

Tabla 1. Notación

Notación	Significado
L_d	Longitud del camino de delegación
L_c	Longitud de un camino de certificación
R_d	Número de repositorios/responders consultados para verificar el estado de revocación de los certificados que hacen parte del camino de delegación.
R_c	Número de repositorios/responders consultados para verificar el estado de revocación de los certificados que hacen parte de un camino de certificación.
OP_{hash}	Número de operaciones de hash
OP_{pub}	Número de operaciones de cifrado con clave pública
T_{hash}	Tiempo de ejecución de una operación de hash
T_{pub}	Tiempo de ejecución de una operación de cifrado con clave pública.
size	Tamaño de la información sobre la que se realiza una operación de hash [bytes].
$size_{CRL}$	Tamaño del contenido de una CRL [bytes].
$size_{OCSP}$	Tamaño del contenido de una respuesta OCSP [bytes]
COST	Coste computacional
N	Número de certificados emitidos por una autoridad.

3.1 Primer Caso: Sin Revocación

En este caso, las operaciones criptográficas que realiza el verificador de privilegios son:

- Verificación de la firma digital de cada AC en el camino de delegación: L_d operaciones de hash, L_d operaciones de cifrado con clave pública.
- Verificación de la firma digital de los PKCs que hacen parte del camino de certificación de las entidades que conforman el camino de delegación: L_dL_c operaciones de hash y L_dL_c operaciones de cifrado con clave pública.

El número total de operaciones criptográficas que realiza el verificador en este caso se especifica en la Tabla 2.

Tabla 2. Operaciones criptográficas sin revocación

TIPO DE OPERACIÓN	NÚMERO DE VERIFICACIONES
OP_{hash}	$L_d + L_d L_c$
OP_{pub}	$L_d + L_d L_c$

3.2 *Segundo Caso: Con Revocación*

Revocación con CRL. Además de las operaciones criptográficas consideradas en el caso anterior, el verificador de privilegios valida la firma de las CRLs que contienen el estado de revocación de los certificados que hacen parte tanto del camino de delegación como de los caminos de certificación involucrados. En el mejor de los casos, el estado de revocación de todos los certificados que hacen parte de un camino estará en una misma CRL descargada previamente por el verificador, por lo que no es necesario verificar su firma durante este proceso. En el peor de los casos, se descargará una CRL por cada certificado en el camino, ya sea porque los certificados pertenecen a dominios de certificación diferentes o porque existen distintos puntos de distribución. Por tanto, el número de operaciones criptográficas dependerá de los repositorios R_d y R_c que deba consultar el verificador para obtener la información de revocación de todos los certificados en los diferentes caminos, donde: $0 \leq R_d \leq L_d$ y $0 \leq R_c \leq L_c$. El número mínimo y máximo de operaciones de hash y de cifrado con clave pública que realiza el verificador en este caso se especifica en la Tabla 3.

Tabla 3. Operaciones criptográficas con CRL

TIPO DE OPERACIÓN	NÚMERO DE VERIFICACIONES	
	Mínimo $R_d = R_c = 0$	**Máximo** $R_d = L_d$, $R_c = L_c$
OP_{hash}	$L_d + L_d L_c$	$2L_d + 2L_d L_c$
OP_{pub}	$L_d + L_d L_c$	$2L_d + 2L_d L_c$

Revocación con OCSP. Además de las operaciones criptográficas consideradas en el primer caso, para formar una solicitud OCSP, el verificador realiza dos operaciones de hash por certificado (sobre el DN y sobre la clave pública del emisor). Ya que la firma de estas solicitudes es opcional, se supone que no van firmadas. En el mejor de los casos, el verificador hará una solicitud OCSP por todos los certificados en el camino, y en el peor de los casos, tendrá que hacer una solicitud OCSP por cada certificado, es decir, $1 \leq R_d \leq L_d$ y $1 \leq R_c \leq L_c$, donde R_d y R_c es el número de responders consultados para verificar el estado de revocación de los certificados en el camino de delegación y en los caminos de certificación respectivamente. El verificador comprueba luego la firma de las respuestas OCSP que recibe.

El número mínimo y máximo de operaciones criptográficas que realiza el verificador en este caso se especifica en la Tabla 4.

Tabla 4. Operaciones criptográficas con OCSP

TIPO DE OPERACIÓN	NÚMERO DE VERIFICACIONES	
	Mínimo $R_d = R_c = 1$	**Máximo** $R_d = L_d$, $R_c = L_c$
OP_{hash}	$4L_d + 3L_d L_c + 1$	$4L_d + 4L_d L_c$
OP_{pub}	$2L_d + L_d L_c + 1$	$2L_d + 2L_d L_c$

4. COSTE COMPUTACIONAL DEL VERIFICADOR

En esta sección, se calcula el coste computacional del verificador de privilegios, considerado como el tiempo de CPU necesario para realizar las operaciones criptográficas involucradas en el proceso de validación de un camino de delegación. La ecuación (1) especifica como se calcula este coste computacional. En la Tabla 1 se encuentra el significado de sus variables.

$$COST = (OP_{hash} * size * T_{hash}) + (OP_{pub} * T_{pub}) \qquad (1)$$

Como se observa en (1), el tiempo necesario para realizar una operación de hash, depende del tamaño *size* de la información sobre la cual se aplica dicha operación.

Se va a utilizar SHA-1 como función de hash y RSA-1024 como algoritmo de clave pública. Los tiempos de ejecución de dichas funciones se definen en la Tabla 5. Estos son valores codificados en C++ y compilados con Microsoft Visual C++ .NET 2003, en un procesador Pentium 4 a 2.1GHz bajo Windows XP SP1, obtenidos de (Dai 2004).

Tabla 5. Tiempos de ejecución

ALGORITMO	TIEMPO
SHA -1	$T_{hash=}$ 14,029 ns/byte
RSA-1024 Verificación	$T_{pub=}$ 0,18 ms/operación

Los cálculos van a hacerse tomando como referencia el tamaño de los campos del certificado y la CRL expuestos en los ejemplos C.2 y C.4 de (Housley, Polk et al. 2002).

4.1 *Primer Caso: Sin Revocación*

Como se especificó en la sección 3.1, se realizan L_d operaciones de hash sobre el contenido de los ACs que hacen parte del camino de delegación y L_dL_c operaciones de hash sobre el contenido de los PKCs que conforman los diferentes caminos de certificación. El tamaño del contenido de cada PKC va a ser 665 bytes, según el certificado del ejemplo C.2 en (Housley, Polk et al. 2002)

El tamaño del contenido de un AC, determinado con base en el tamaño de los campos del certificado del ejemplo C.2 en (Housley, Polk et al. 2002) y los campos que conforman un AC (ITU-T 2000), sin incluir los campos opcionales y con dos atributos de 27 bytes cada uno, es aproximadamente de 181 bytes. Utilizando (1), la información de las Tablas 2 y 5 y haciendo $L_c = 3$ se calcula el coste computacional especificado en la Tabla 6, para este caso.

4.2 *Segundo Caso: Con Revocación*

Revocación con CRL. En este caso, se adicionan las operaciones de hash y clave pública necesarias para verificar la firma de las CRLs. Se considera que las CRLs descargadas para comprobar el estado de revocación de los certificados de atributo (ACs) y los certificados de clave pública (PKCs) tienen el mismo tamaño de la CRL en el ejemplo C.4 de (Housley, Polk et al. 2002). Su contenido ocupa 140 bytes de los cuales 32 bytes corresponden a la información de revocación de un solo certificado. Si el 10% de los N certificados emitidos por una autoridad han sido revocados, el tamaño del contenido de la CRL es:

$$size_{CRL} = 108 + (32*0{,}1*N) = 108 + 3{,}2*N \qquad (2)$$

Teniendo en cuenta (1) y (2) y la información de las Tablas 3 y 5, se calcula el coste computacional del verificador con $L_c = 3$, cuando $R_d=R_c=0$ (mínimo) y cuando $R_d=L_d$, $R_c=L_c$ (máximo), como se muestra en la Tabla 6.

Revocación con OCSP. Teniendo como referencia el tamaño de los campos del certificado en el ejemplo C.2 de (Housley, Polk et al. 2002), y conociendo los campos que conforman una respuesta OCSP básica (Myers, Ankney et al. 1999), se puede establecer que el contenido de dicha respuesta, omitiendo los campos opcionales, ocupa aproximadamente 132 bytes, de los cuales 74 bytes corresponden a la información de revocación de un certificado. Por tanto, el tamaño del contenido de una respuesta OCSP con la información de revocación de L certificados es:

$$size_{OCSP} = 58 + (74*L) \qquad (3)$$

Para formar una solicitud OCSP, se realiza una operación de hash sobre el campo issuer de cada certificado, cuyo tamaño es de 42 bytes (Housley, Polk et al. 2002), y otra sobre la clave pública del emisor del certificado, que es de 128 bytes (1024 bits) para RSA-1024.

El coste computacional de las operaciones criptográficas, teniendo en cuenta (1) y (3) y la información de las Tablas 4 y 5, con $L_c = 3$, cuando $R_d=R_c=1$ (mínimo) y cuando $R_d=L_d$, $R_c=L_c$ (máximo) se especifica en la Tabla 6

Tabla 6. Coste computacional

MECANISMO REVOCACIÓN	**COSTE COMPUTACIONAL**	
	Mínimo	**Máximo**
Ninguno	$0{,}75*10^{-3}*L_d$	$0{,}75*10^{-3}*L_d$
CRL	$0{,}75*10^{-3}*L_d$	$1{,}48*10^{-3}*L_d + 0{,}18*10^{-6}*N*L_d$
OCSP	$0{,}94*10^{-3}*L_d + 0{,}18*10^{-3}$	$1{,}49*10^{-3}*L_d$

La Tabla 7 muestra el coste computacional sin y con revocación a medida que aumenta la longitud L_d del camino de delegación, lo que se grafica en Fig. 1 y 2 para el caso mínimo y máximo respectivamente.

Tabla 7. Coste computacional variando L_d

L_d	**COST (ms)**					
	Sin Rev	**Con CRL**			**Con OCSP**	
		Mín	**Máx** N=500	**Máx** N=10^4	**Mín**	**Máx**
1	0,75	0,75	1,57	3,28	1,12	1,49
2	1,5	1,5	3,14	6,56	2,06	2,98
3	2,25	2,25	4,71	9,84	3	4,47
4	3	3	6,28	13,12	3,94	5,96
5	3,75	3,75	7,85	16,4	4,88	7,45
6	4,5	4,5	9,42	19,68	5,82	8,94
7	5,25	5,25	10,99	22,96	6,76	10,43
8	6	6	12,56	26,24	7,7	11,92
9	6,75	6,75	14,13	29,52	8,64	13,41
10	7,5	7,5	15,7	32,8	9,58	14,9

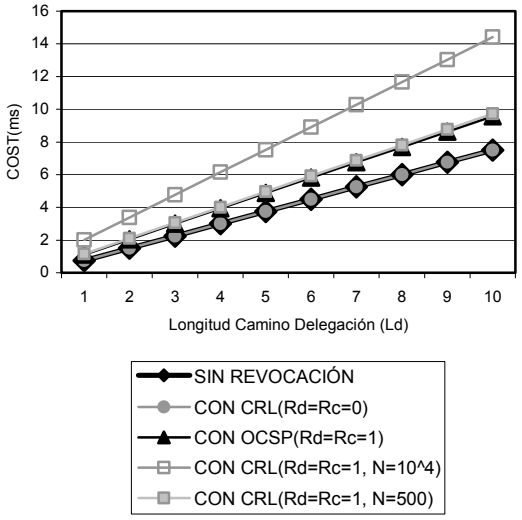

Fig. 1 Coste computacional mínimo sin y con revocación

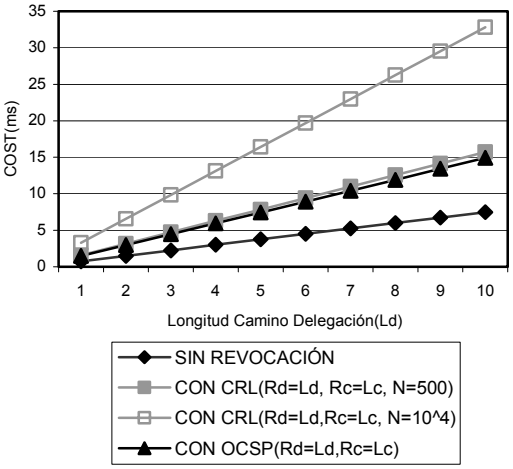

Fig. 2 Coste computacional máximo sin y con revocación

5. CONCLUSIONES

1. El proceso de validación de un camino de delegación le demanda al verificador de privilegios gran cantidad de tiempo y recursos. Por ello, uno de los retos de los sistemas de delegación actuales es la gestión eficiente de este tipo de caminos.

2. De las operaciones que se realizan durante dicho proceso, las criptográficas son las que le exigen al verificador una mayor capacidad de cálculo. Por esa razón, se ha determinado el coste computacional de estas operaciones en la validación de la un camino de delegación, utilizando lo mecanismos de revocación CRL y OCSP.

3. Las Tablas 2 y 3 muestran que sin revocación y con CRL, el número de operaciones de hash es igual al número de operaciones de cifrado con clave pública. Esto se debe a que sólo se realizan operaciones criptográficas cuando se verifica la firma de los certificados y las CRLs, y cada verificación de firma involucra una operación de hash y una de cifrado con clave pública.

4. Con OCSP en cambio (Tabla 4), el número de operaciones de hash es mayor que el número de operaciones de cifrado con clave pública, ya que una solicitud OCSP involucra dos operaciones de hash por cada certificado. Sin embargo, el mayor número de operaciones de hash no es un gran inconveniente para OCSP pues el tiempo de ejecución de estas operaciones es mucho menor que el de una operación de cifrado con clave pública (Tabla 5). Además, el tiempo en realizar una operación de hash depende del tamaño de la información sobre la cual se aplique dicha función, y el tamaño del contenido de las respuestas OCSP (3) es menor que el de una CRL pues depende sólo del número de certificados cuyo estado de revocación se este consultando, mientras el tamaño del contenido de una CRL (2) depende del número de certificados revocados, lo que implica no sólo un mayor tiempo de ejecución de las operaciones de hash sino también la necesidad de una mayor capacidad de almacenamiento.

4. En la sección 4, se ha tratado de simplificar el cálculo del coste computacional suponiendo que c ada uno de los caminos de certificación verificados consta de 3 certificados (L_c=3). De esta manera, el coste computacional calculado ha quedado en función de la longitud del camino de delegación L_d, y en el caso de CRL también en función de N, considerando que el número de certificados revocados es el 10% de N. En Fig. 1 se observa que el coste

computacional con OCSP, para un PC con las características indicadas en (Dai 2004), es mayor que el coste con CRL cuando R_d y R_c toman su valor mínimo, debido a las operaciones criptográficas involucradas en la construcción de una solicitud OCSP y la verificación de la firma de su respectiva respuesta. Sin embargo, cuando R_d=R_c=1 y N=500, el coste con CRL es casi igual al coste con OCSP. Además, el coste con CRL sufre un incremento notorio cuando aumenta el número de certificados emitidos ($N=10^4$). Igualmente, Fig. 2 y la Tabla 6 muestran que el coste computacional máximo con OCSP y CRL es muy similar cuando N=500. Pero un incremento de $N=10^4$ hace que el coste computacional con CRL sea mayor que con OCSP. Lo mismo ocurre si se incrementa el porcentaje de certificados revocados. Por tanto, OCSP es la mejor alternativa cuando el porcentaje de certificados revocados es alto y/o el número de certificados emitidos es grande. Sin embargo, los costes obtenidos en todos los casos son bastante razonables para el PC considerado(Dai 2004).

5. En trabajos futuros se evaluarán otros aspectos de la validación de caminos de delegación como el coste de comunicaciones y la capacidad de almacenamiento que necesitan las diferentes entidades que hacen parte del proceso. El objetivo es proponer nuevas alternativas que conduzcan a la simplificación del proceso de validación de caminos de delegación y que requieran el uso de menos recursos.

REFERENCIAS

Dai, W. (2004). Crypto ++ 5.2.1 Benchmarks, http://www.eskimo.com/~weidai/benchmarks.

Housley, R., W. Polk, et al. (2002). RFC3280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

ITU-T (2000). "Recommendation X.509: Information Processing Systems - Open Systems Interconnection - The Directory - Authentication Framework (Technical Corrigendum)."

Kille, S. (1995). RFC 1779 - A String Representation of Distinguished Names, ISODE Consortium.

Myers, M., R. Ankney, et al. (1999). RFC2560 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP.