Integración de la autorización basada en certificados de atributos para SSH

Integration of attribute certificate-based authorisation for SSH

Víctor Manuel Fernández Albor

Resumen

Existen una serie de necesidades que no están implementadas actualmente en el SSH como por ejemplo, los derechos de un usuario para acceder a un sistema en un momento dado, según una política de acceso que pueda tener esa organización. La gestión de políticas es una parte muy importante, ya que el propio organismo debería de tener el poder de decisión en todo momento sobre el tipo de usuario que puede acceder a los recursos disponibles.

Otra de las necesidades hoy no cubierta es la identidad de la persona, como integrante de una entidad, con un rol característico en la misma. SSH no aporta certificados de atributos asociados a certificados de usuario. Todas estas carencias están subsanadas con esta nueva versión de SSH en la que se ha desarrollado un nuevo protocolo de identificación y autenticación basado en certificados de identidad y de rol. La solución es bastante transparente y permite al proveedor aplicar políticas de acceso según el estándar XACML.

El organismo debe decidir el tipo de usuario que puede acceder a los recursos disponibles

Palabras clave: SSH, Políticas de Seguridad, XACML, Autorización, Autenticación, Certificados de Atributos, Certificados de Identidad, PKI, Certificados de identidad PMI, Autoridad de Atributos (AA), Fuente de Autoridad (SOA), Delegación de Privilegios.

Summary

There are a number of needs that are not currently covered in the SSH, such as users' rights to access a system at a given moment in accordance with whatever access policy the organisation may have. Policy management is a very important factor, since the organisation itself should have the power to decide, at any time, which kind of user can access the available resources.

Another need that is not covered at present is identity of the person, as a member of an entity, with a specific role within that entity. SSH does not provide attribute certificates associated with user certificates. All these missing elements are covered in the new version of SSH in which a new identification and authentication protocol has been developed based on identity and role certificates. The solution is quite transparent and enables the provider to apply access policies based on the XACML standard.

Keywords: SSH, Security Policies, XACML, Authorisation, Authentication, Attribute Certificates, Identity Certificates, PKI, PMI identity certificates, Attribute Authority (AA), Source of Authority (SOA), Delegation of Privileges.

Por ahora no se genera la identidad de la persona, con un rol característico como integrante de una entidad

1. Introducción

SSH (*Secure Shell*) está presente hoy día en todo tipo de entornos colaborativos, desde el entorno empresarial al académico, proporcionando una serie de servicios necesarios para la seguridad en la red.

Un paso más en este tipo de seguridad es identificar al usuario mediante sus certificados y asignarle un estatus o rol, dentro de una organización. En este contexto entran los certificados de usuario y de atributos. La integración de ambos certificados dentro de SSH ya es posible con la nueva versión desarrollada en el Cesga, esta versión ha sido desarrollada a partir de OpenSSH 5.0p1, y se ha complementado con una gestión de políticas de acceso con el estándar XACML (eXtensible Access Control Markup Language de OASIS).

Según la ITU en su revisión del año 2000 del X.509, un certificado de atributos está firmado por una

Autoridad de Atributos (AA), que es como se pasa a denominar a la autoridad habilitada para realizar la asignación de privilegios. En el caso actual nosotros usamos una SOA, que es un tipo específico de AA, y desempeña un papel análogo al de la Autoridad Raíz en las PKIs. A la SOA se le considera la responsable última en la asignación de un conjunto de privilegios. En cuanto al concepto de revocación, tenemos la Lista de Revocación de Certificados de Atributos Revocados (ACRL) con el mismo formato y administración que las típicas CRLs.

Respecto a la estructura del certificado de atributos, posee gran parecido con los certificados de identidad. Se encuentran en ella los campos habituales de versión, número de serie, algoritmo de firma, emisor, periodo de validez, e incluso los campos opcionales identificador único de emisor y de extensiones. Existen, sin embargo, otros campos nuevos, como son el campo tenedor, y el propio campo de atributos, que podrá contener información respecto a la pertenencia a grupos, identificación de cargos, valores límite de transacciones, horas de realización de ciertas operaciones, límites temporales, etc.

Es conveniente resaltar que, a diferencia de lo que ocurre en el certificado de identidad, es posible no dejar explícita la identificación del usuario en el certificado de atributos, sino que utiliza el campo tenedor para enlazar este certificado con el correspondiente certificado de identidad del usuario, mediante la utilización en el campo tenedor del número de serie del certificado de identidad del usuario sobre el que se expresan los atributos o privilegios. De esta forma, la PKI autentica a aquellos usuarios de quien la PMI emite certificados de atributos.

Hay que identificar al usuario mediante sus certificados y asignarle un rol

El desarrollo de SSH con la integración de la autorización basada en certificados de atributos se engloba dentro del Proyecto de Infraestructura de Firma Electrónica Cualificada (IFeC Código de proyecto: FIT-360000-2007-14) objeto de la ayuda concedida a las Entidades ALDABA servicios profesionales, Centro de Supercomputación de Galicia, ALDABA soluciones y proyectos, Escuela Técnica Superior de Ingeniería en Telecomunicación de la Universidad de Vigo dentro del Programa de Fomento de la Investigación Técnica, Convocatorias Año 2007, (Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información) e ISEC (Código de proyecto: 07SIN012CT), dentro del programa Innovación Ciencia e Tecnoloxía I.n.c.i.t.e. de la Xunta de Galicia.

2. Análisis y módulos del nuevo SSH con certificados

Existen dos módulos básicos a tener en cuenta, en primer lugar el módulo SSH desde donde un sistema cliente se intenta conectar a un sistema servidor, utilizando para ello OpenSSH y los certificados de usuario y atributos. En segundo lugar el módulo de la función de decisión encargado de decidir desde la verificación de los certificados hasta el acceso, según la política definida por una organización.

Es posible no dejar explícita la identificación del usuario en el certificado de atributos

2.1. Función de decisión

En este módulo se han estudiado algunos de los diversos tipos de políticas de acceso:

- SAML, estándar XML para el intercambio de información de autenticación y autorización a través de dominios. Tiene las denominadas aserciones, que mejoran la comprensión de la política de acceso.

- XACML, otra política de acceso estudiada, cuya versión 3.0, añade funcionalidades entre los distintos roles dentro de las organizaciones, interesante para las características de certificados de atributos.

Se han probado herramientas de escritura XACML, por ejemplo UMU XACML Publisher, fácilmente integrable en aplicaciones web. Así como herramientas como Reva-v1.1, herramienta proporcionada por Oasis, con políticas de ejemplo, que muestran el uso de certificados de usuario.

Se han analizado las siguientes bibliotecas para el desarrollo del sistema:

- La solución Parthenon-xacml(1), que es un conjunto de componentes cuya característica principal es que se basan fielmente en el estándar XACML 1.1, pero por contra no es de libre distribución.

- La API para Sun solución XACML(2), que tiene todas las solicitudes estándar XACML, de libre distribución, realizado en Java, y fácil de transportar a todos los tipos de arquitecturas.

2.2 Caso práctico de uso: Acceso SSH

Se han analizado las siguientes bibliotecas para el desarrollo del sistema: Pathernon-xacml y Sun solución XACML

Se han probado parches y herramientas que tratan de imitar el proyecto propuesto, contactar a través de SSH con certificados de usuario y de rol, y una política de acceso, en la que se evalúen permisos de utilización de un recurso. Específicamente se analizaron:

- OpenSSH(3) implementación libre del protocolo SSH, realizado en código C, que proporciona una amplia funcionalidad y grupos de discusión acerca de su funcionamiento, una característica notable de esta distribución de SSH es que se usa en la mayoría de los sistemas actuales, como clientes y principalmente como servidores de este protocolo.

- Path Nutmay(4) es un parche para la distribución de OpenSSH, que implementa el acceso con los certificados de atributos. Pero su desarrollo se ha detenido en una fase temprana del proyecto, y no posee todo lo concerniente a políticas de acceso.

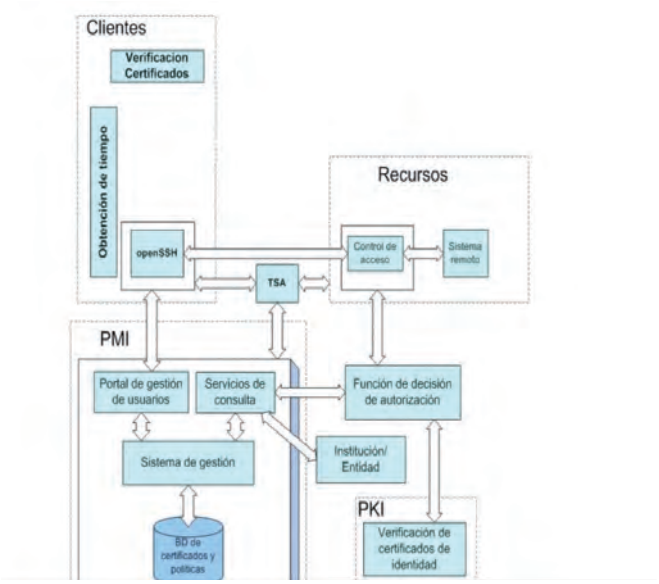
- Path SSH con Certificados(5) es un parche para la distribución gratuita de OpenSSH, que implementa el acceso con certificados de usuario. Las versiones son estables y se actualizan con frecuencia en función de las versiones nuevas de distribución de OpenSSH. Por contra, no mencionan el uso de certificados de atributos o políticas de acceso.

3. PMI como servicio de autorización

Se han probado herramientas que tratan de contactar a través de SSH con certificados de usuario y de rol

Para la creación y verificación de los certificados de atributos se necesita toda una infraestructura, desde la PKI (OpenCA en nuestro caso junto con OpenSSL), para la creación de certificados de usuario, hasta la PMI para la creación de certificados de atributos. El diseño global del sistema es completo, así como varios servicios específicos. El sistema ha sido desarrollado en Java, con el mayor número de posibles modelos, para una mayor compatibilidad y un desacoplamiento entre los diversos componentes, con el fin de que se puedan organizar como desee el usuario. Por lo tanto, las comunicaciones entre los bloques se realiza mediante Servicios Web. La PMI, junto con los sistemas de acceso SSH puede ser dividida en 3 bloques principales:

FIGURA 1



Con el punto de acceso SSH se rechaza o se permite a un usuario acceder a un sistema

- *El punto de acceso SSH*: es el punto en el cual a un usuario se le rechaza o permite el acceso a un sistema y se controla la recepción de los certificados de atributos y de identidad. El proceso principal es la presentación de los certificados de atributos a la función de la decisión que puede decidir sobre la concesión del acceso o no.

- *Función de autorización de decisión*: el punto donde se comprueba si un conjunto de certificados de atributos son válidos y los atributos que contienen permiten realizar una acción basada en una política de control de acceso definido para la organización. Basado en el uso de las bibliotecas de la gestión de XACML (estándar XML para la definición de políticas).

La función de decisión comprueba si un conjunto de certificados de atributos son válidos

- *Sistema de gestión*: una base de datos controlada por un motor que proporciona la información a un portal de Internet y las funciones de autorización. Puede ser dividido en dos secciones:

    - *Back-end:* la aplicación principal consta de una base de datos donde se almacena la información acerca de los usuarios, las organizaciones, los atributos, las solicitudes de renovación de Revocación y mantiene la consistencia de datos mediante el uso de Java Persistence.
    - *Front-end:* El portal para usuarios y administradores para administrar sus licencias y de la institución. Realizado utilizando el FrameWork Apache Cocoon, el acceso de usuario se basa en SSL con autenticación mutua para que el sistema muestre un ambiente personalizado según la organización a la que pertenece. Las acciones, y la información a la que el usuario tiene acceso, va a depender de la organización.

4. Verificación y control de acceso mediante XACML dentro de la función de decisión

La función de decisión tiene la responsabilidad de comprobar si un conjunto de certificados de atributos es válido y le permiten realizar una acción basada en una política de control de acceso definido para la organización, basándose en el uso de las bibliotecas de gestión de XACML. Se realiza completamente en Java utilizando Webservices para la comunicación con los diversos módulos existentes. Se utilizaron paquetes de software como Bouncy Castle, un conjunto de librerías criptográficas, SunXACML para el desarrollo de la política de XACML o JAX-WS para Servicios Web.

En el siguiente diagrama de secuencia se explica más detalladamente el proceso para la verificación de certificados, que se realiza dentro del módulo de la función de decisión, para el caso de petición de acceso a una máquina a través de SSH.

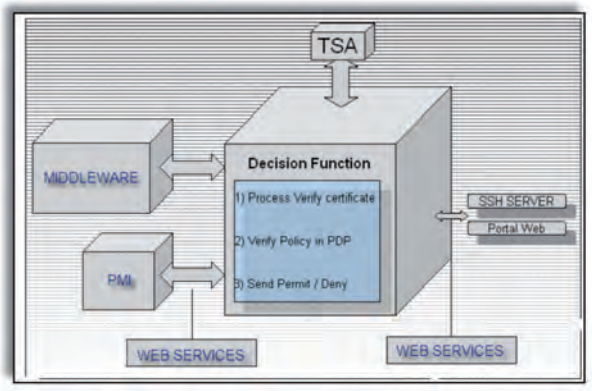
La función de decisión comprueba si un conjunto de certificados de atributos es válido

El proceso para la verificación de certificados, que se realiza dentro del módulo de la "Función de Decisión", para el caso de petición de acceso a una máquina a través de SSH, se realiza con la siguiente secuencia. Primero obtenemos toda la información posible de la PMI a través de WebServices, Certificado de SOA, Política de la organización y por último la cadena de la SOA. Una vez obtenemos la información necesaria, pasamos a validar todas las cadenas mediante OCSP y CRL, y posteriormente verificamos los certificados de atributos con el OCSP o CRL contra los WebServices de la PMI. El proceso continúa con la validación de las fechas de todos los certificados y de sus respectivas cadenas. Finalmente quedaría ver si confiamos en alguna CA, o certificado intermedio, y por último verificar la política.

Al final de la validación, se comprueba si la política escrita por la organización, permite el acceso a los recursos para un usuario particular que lo solicita. Esto se define en el PDP (Policy Decision Point), donde la política y la petición, se comparan, y se obtiene una decisión de autorización o denegación de acceso a los recursos. El diagrama de bloques sobre el funcionamiento de la función de decisión es el siguiente:

El PDP compara la política y la petición y obtiene una decisión de autorización o denegación de acceso

FIGURA 2



5. La conexión segura a sistema remoto con certificados

Se ha basado todo en la versión libre de SSH, OpenSSH, más concretamente, el Openssh_5.1p1. OpenSSH está desarrollado en ANSI-C, la parte que transmite los certificados, es la parte del cliente. La parte del servidor, respeta la política de seguridad existente en esta solución en todo momento, en lo que se refiere al diseño interno de la solución. El servidor SSH se conecta con el módulo desarrollado en Java, que es responsable de transferir la información a través de servicios web a la función de decisión, y esperar la respuesta para devolvérsela al servidor SSH.

El cliente Java Web Services, además de recibir los certificados, extrae una serie de información, que envía al PEP (Policy Enforcement Point), una parte importante en el diseño de una aplicación basada en políticas XACML, ya que es responsable de crear una solicitud de petición XACML, que se enviará junto con los certificados para compararla con la política almacenada en la PMI de la SOA correspondiente a los certificados de atributos.

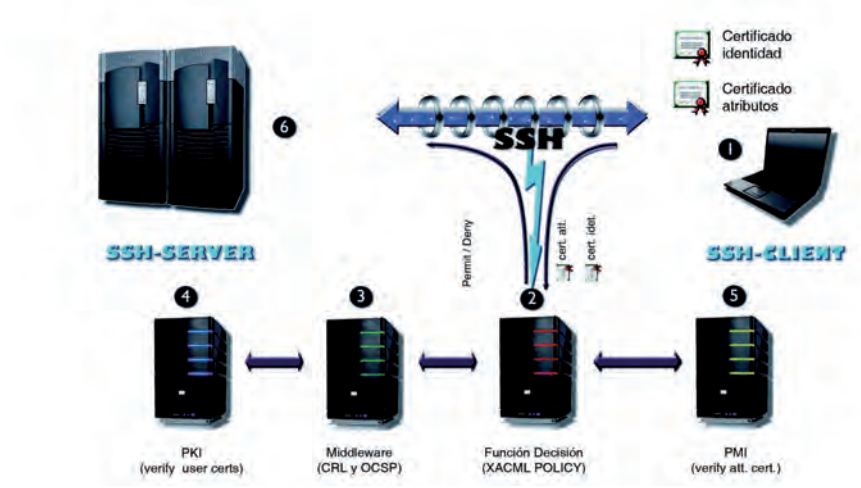
Un módulo desarrollado en Java transfiere la información a través de servicios web a la función de decisión

Una vez que los certificados y la Solicitud XACML llegan a la función de decisión, ésta sigue todo un proceso de verificación de certificados, de conformidad con las normas incluidas en rfc3281 (un certificado de atribución de Internet, perfil de la autorización), y RFC2459 (Internet X.509 Public Infraestructura de Clave, Certificado y Perfil CRL). Si la parte de verificación es correcta, accede al PDP para comprobar que en la Solicitud XACML enviada por un usuario con un determinado rol, pertenece a una organización y se le permite el acceso al recurso o por contra se le deniega.

Una vez definida una respuesta, Permit o Deny del PDP, se enviará al cliente Java, y esto se transmite al SSH-Server, que sería el último encargado en esta larga cadena, de permitir o denegar el acceso seguro al recurso.

En el siguiente diagrama se describe todo el proceso:

FIGURA 3



El proceso de verificación de certificados se hace de acuerdo a las normas incluidas en rfc3281 y RFC2459

Referencias

OSSH, The Secure Shell: The Definitive Guide
By Daniel BARRETT, DANIEL J. y SILVERMAN, RICHARD E. y BYRNES, ROBERT G.
Publisher: O'Reilly Media
Released: 2005

OASIS eXtensible Access Control Markup Language
http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

Sun's XACML Implementation
http://sunxacml.sourceforge.net/guide.html

XACML Project, Web Services Profile of XACML (WS-XACML)
http://research.sun.com/projects/xacml/

OpenSSH,a FREE version of the SSH connectivity
http://www.openssh.org/

GSI-OpenSSH, a modified version of OpenSSH that adds support for GSI authentication and credential forwarding *http://grid.ncsa.illinois.edu/ssh/*

Axis C/C++, a non-Java implementation of Axis for WebServices.
http://ws.apache.org/axis/cpp/index.html

RFC Attribute Certificate (AC) Policies Extension
http://tools.ietf.org/html/rfc4476

RFC Secure Shell
http://www.ietf.org/rfc/rfc4251.txt

Notas

(1) http://www.parthcomp.com/xacml_toolkit.html

(2) http://sunxacml.sourceforge.net/

(3) http://openssh.org

(4) http://nutmay.sourceforge.net

(5) http://roumenpetrow.info/openssh/

Víctor Manuel Fernández Albor
(victormanuel.fernandez@usc.es)
Universidad de Santiago de Compostela