UN ACERCAMIENTO A POLÍTICAS DE SEGURIDAD EN AMBIENTES GRID DADAS POR AUTORIDADES CERTIFICADORAS (AC)

C. A. Rodríguez Sánchez[1]

CARLOS ALBERTO RODRÍGUEZ S.[1]

Docente investigador, candidato a Magister en ciencias de la información y las comunicaciones de la Universidad Distrital "Francisco José de Caldas", candidato a Magister en Dirección e Ingeniería de Sitios Web de la Universidad Internacional de la Rioja en España, Especialista en Auditoria de sistemas de la Universidad Antonio Nariño, profesional en Ingeniería de Sistemas de la Universidad Antonio Nariño.

RESUMEN

Este artículo presenta una visión global teórica acerca de los principales estándares para la seguridad en la computación Grid. Las Grid computacionales han emergido con la finalidad de mejorar el rendimiento del sistema en su disponibilidad, escalabilidad, confiabilidad y seguridad mediante la integración de recursos heterogéneos compartidos. Se describe además políticas de seguridad que permitan de manera dinámica, escalable, la protección de los recursos, los datos almacenados y las salidas de los trabajos enviados por los usuarios.

PALABRAS CLAVE: Autoridad certificadora, Clave Publica, Clave privada, Computación grid

RESUMEN

This paper shows an overview about security standards for grid computing. The computational grids have emerged with the aim of improving system performance in availability, scalability, reliability and security through the integration of heterogeneous resources sharing. It also describes security policies that enable a dynamic, scalable protection of resources, stored data and the output of the work submitted by users.

KEY WORDS: Certificate authority, Public key, Private Key, Grid computing

1. INTRODUCCIÓN

Ya sea para agregar recursos o trabajar de forma integrada; en el entorno de red deben existir componentes de seguridad fuertes involucrados en cada uno de los procesos se lleven a cabo, la razón fundamental es la necesidad de prevenir cualquier uso malintencionado que podría interferir con la prestación o utilización de estos recursos.

Estas precauciones incluyen la certificación de los usuarios y recursos (por ejemplo servidores y aplicaciones). Estar certificado significa tener un tipo de visado, pasaporte o autorización que garantiza a todos en la red que el individuo, equipo o aplicación que está realizando una transmisión de datos es válida, confiable y comprobable, es decir quién o lo que dice es fiable (que certifique el emisor) [1].

Hay muchas comunidades, grupos y foros para crear esfuerzos y políticas acerca de la seguridad, el principal grupo en esta propuesta se conoce como Global Grid Forum (GGF). Esta comunidad ha desarrollado una política de certificado para Grid Computing que reducen el costo y el tiempo necesario para crear una infraestructura Grid de clave pública (PKI) y la política de aumento y la interoperabilidad técnica en la comunidad Grid.

2. EL CRECIMIENTO DE PKI GRID

Una Grid Computacional es una forma de computación distribuida que comprende: Coordinar y compartir recursos, aplicaciones, datos, almacenamiento o recursos de red entre organizaciones dinámicas y geográficamente distribuidas. Por lo general, los recursos Grid son proporcionados por diversas organizaciones y son utilizados por personas de diversas áreas de las organizaciones. Una Grid puede ser de apoyo (o definir) una organización virtual única, o puede ser utilizado por más de una organización virtual. Los equipos de hardware pueden ser usados en más de una Grid, y las personas pueden ser miembros de más de una organización virtual.

Los diferentes recursos en una Grid pueden tener diferentes políticas de acceso, incluyendo cómo se autentican y como los usuarios se registran. Así, en este trabajo vamos a suponer que para cualquier conjunto de recursos hay algunas autenticaciones generales o los procedimientos de autorización específicos. Así como en cualquier otro sistema en el mundo, la seguridad es un aspecto vital de los sistemas Grid. Las tres características más importantes de seguridad que el Grid debe proveer son: Login, Autenticación, Autorización. La primera significa que un usuario es capaz de registrarse haciendo uso de sus credenciales de seguridad [usuario y contraseña] y tener acceso a los servicios del Grid por un cierto periodo de tiempo. Autenticación significa ser capaz de crear una identidad, como por ejemplo cuando hay login en la cuenta de mail para autenticarse con el servidor dando usuario y contraseña. Autorización es el proceso de gestionar y controlar los privilegios de los usuarios[2].

2.1 Estándares de Certificación Grid

Los usuarios y los servicios tienen que ser capaces de autenticarse en el entorno Grid. Experiencias comprobadas en el uso de GRID para los cálculos a distancia ha demostrado la necesidad de autenticación de usuarios, además de la autenticación interactiva[3]. La autenticación de los usuarios es necesaria, entre otras cuando:

Un usuario está haciendo pedidos frecuentes a los servidores remotos y no quiere escribir de forma repetida en una frase de contraseña. Cuando un trabajo de larga duración debe ser necesario autenticar a sí mismo después de que el usuario ha dejado de usarla. Servidores específicos de un solo host pueden necesitar que se inicien al arrancar el sistema y desarrollarse con su propia identidad o del host. Algunos servicios pueden necesitar que se inicien periódicamente en distintos host y ser capaces de autenticarse con una identidad conocida. Básicamente, la autenticación entre dos entidades en nodos remotos Grid significa que cada parte establece un nivel de confianza en la identidad de la otra parte. En el uso práctico de un protocolo de autenticación se establece una comunicación segura de canal entre las partes autenticadas, para que los mensajes posteriores se puedan enviar sin autenticación repetida de pasos, aunque es posible autenticar cada mensaje. La identidad de una entidad suele estar alrededor de símbolo o nombre que identifica la entidad[4].

Un AC de Grid se define como una entidad emisora que es independiente de cualquier organización y cuyo propósito es firmar certificados para las personas que pueden tener acceso a los recursos Grid, hosts o servicios que se ejecutan en un solo servidor. Por lo general, una AC Grid sólo firma los certificados de estas entidades finales y no de las AC subordinadas. Una AC Grid es sustancialmente diferente al tradicional AC organizacional, que firma los certificados sólo para los miembros de su organización y está estrechamente vinculada con la autoridad que define quiénes son los miembros[5,4]. Los certificados se utilizan para acceder a los recursos dentro de la organización. Hay dos implicaciones de esta diferencia: una en el formato de los DN y el otro en los métodos de investigación de antecedentes de identificación del usuario.

2.2 Secure Electronic Transaction (SSL)

El protocolo SSL es un sistema diseñado y propuesto por Netscape Communications Corporation[9]. Se encuentra en el modelo OSI entre los niveles de TCP/IP y de los protocolos HTTP, FTP, SMTP, etc. Proporciona sus servicios de seguridad cifrando los datos intercambiados entre el servidor y el cliente con un algoritmo de cifrado simétrico, típicamente el RC4 o IDEA, y cifrando la clave de sesión de RC4 o IDEA mediante un algoritmo de cifrado de clave pública, típicamente el RSA[6,1]. La clave de sesión es la que se utiliza para cifrar los datos que vienen del y van al servidor seguro. Se genera una clave de sesión distinta para cada transacción, lo cual permite que aunque sea saltada por un atacante en una transacción dada, no sirva para descifrar futuras transacciones.

MD5 se usa como algoritmo de hash. Proporciona cifrado de datos, autenticación de servidores, integridad de mensajes y, opcionalmente, autenticación de cliente para conexiones TCP/IP.

Cuando el cliente pide al servidor seguro una comunicación segura, el servidor abre un puerto cifrado, gestionado por un software llamado Protocolo SSL Record, situado encima de TCP. Será el software de alto nivel, Protocolo SSL Handshake, quien utilice el Protocolo SSL Record y el puerto abierto para comunicarse de forma segura con el cliente[4].

2.3 Transport Layer Security (TSL)

Es un protocolo destinado a proporcionar la privacidad e integridad de datos entre dos aplicaciones que se comunican. TLS se tiene dos capas: el TLS Handshake Protocolo y el Protocolo de TLS Record. En el protocolo TCP / IP, el TLS Record Protocolo se encuentra entre una capa de transporte confiable (lo que significa TCP y no UDP) y la capa de aplicación. Aunque el TLS Handshake Protocolo no es realmente un protocolo de aplicación, se sienta por encima del protocolo TLS Registro en la pila, sus mensajes son encapsulados por el Protocolo de TLS Record[7].

El TLS Handshake Protocolo permite que el servidor y el cliente se autentiquen mutuamente y negociar un algoritmo de cifrado y las claves criptográficas antes de que el protocolo de aplicación transmite o recibe su primer byte de datos. Así, cuando un cliente y el servidor TLS se comunican existe un principio básico y radica en que están de acuerdo en una versión del protocolo, para seleccionar los algoritmos criptográficos, opcionalmente deben autenticarse mutuamente, y hacer uso de técnicas de criptografía de clave pública para generar secretos compartidos. El TLS Handshake Protocolo establece los parámetros de seguridad negociada a la capa de Registro Protocolo[8].

2.4 X509

Un certificado X.509 es una afirmación que criptográficamente une la identidad de alguna entidad "*Por ejemplo, un nombre de usuario o una dirección IP de servidor SSL*" con una clave pública[9]. Al demostrar que están en posesión de la clave privada asociada con la clave pública contenida en el interior, el usuario puede establecer solicitud a la identidad declarada cuando presenten el certificado de alguna otra parte en el contexto de una aplicación.

Cualquier instancia puede crear un certificado para sí misma en los que puedan reclamar ninguna identidad. Los certificados sólo serán de confianza (y por ende, ofrecer valor) si la parte que confía puede avalar al emisor, y normalmente una tercera parte llamada de *confianza (trust)* se remite a una entidad emisora de certificados (AC).

La confianza entre los titulares de certificados y las partes que confían es posible gracias a la potencialidad creando relaciones de confianza de otros que existen entre las dos entidades fundamentales

y sus asociados AC. Es a través de la confianza que tienen las partes que confían de las AC que estarán dispuestos a atribuir la confianza a los temas de los certificados expedidos por las entidades emisoras de certificados.

2.5 X500

X.500 es una forma estándar para desarrollar un directorio electrónico de personas de una organización para que pueda ser parte de un directorio mundial disponible para cualquier persona del mundo con acceso a Internet. Ese directorio se llama a veces un directorio de Páginas Blancas mundial. La idea es ser capaz de mirar a la gente de una manera fácil de usar por su nombre, departamento u organización. Muchas empresas e instituciones han creado un directorio X.500. Debido a que estos directorios se organizan como parte de un directorio único y global, puede buscar por cientos de miles de personas de un solo lugar en el World Wide Web.

El directorio X.500 está organizado bajo un directorio raíz en un "árbol" de la jerarquía: país, organización, unidad organizativa, y la persona. Una entrada en cada uno de estos niveles debe tener ciertas cualidades, y algunos pueden tener los opcionales establecidos a nivel local [10]. Cada organización puede implementar un directorio a su manera, siempre que se adhiere al esquema de base o plan. El directorio global distribuida trabaja a través de un proceso de registro y uno o más lugares centrales que gestionan muchos directorios.

Proporcionar un directorio X.500 permite a una organización a hacerse conocidos y miembros seleccionados en Internet. Dos de los mayores proveedores de servicios de directorio son InterNIC, la organización que supervisa el registro de nombres de dominio en los EE.UU., y ESnet, que mantiene los datos de X.500 para todos los laboratorios nacionales de EE.UU.. ESNet similares y proveedores también ofrecen acceso a buscar nombres en el directorio global, utilizando una serie de diferentes interfaces de usuario designado como sitios web, whois, y el índice. Estas organizaciones también proporcionan ayuda a las organizaciones que están creando su propio directorio de información Tree (DIT) [2].

En X.500, cada directorio local se llama un Directorio Agente del sistema (DSA). Un DSA puede representar una organización o un grupo de organizaciones. Los DSA están interconectados desde el árbol de directorios de la Información (DIT).

El programa de interfaz de usuario para el acceso a una o más ASD es un directorio de agente de usuario (DUA). DUAs incluyen identificadores y los programas que ofrecen una interfaz gráfica de usuario. X.500 se implementa como parte de la Distributed Computing Environment (DCE) en su Servicio de Directorio Global (GDS).

La Universidad de Michigan es lider de universidades que usan X.500 como una forma para enrutar el correo electrónico, así como para proporcionar búsqueda de nombre, utilizando el Lightweight Directory Access Protocol (LDAP) [3].

3. PROCESO DE CERTIFICACION

El interesado en operar dentro del esquema establecido por la ley, deberá, una vez creado el par de claves, presentarse ante la autoridad certificante (o funcionario que ella determine) a efectos de registrar su clave pública, acreditando su identidad o cualquier otra circunstancia que le sea requerida para obtener el certificado que le permita 'firmar' el documento de que se trate. Por ejemplo, para realizar una operación financiera de importancia con un banco, éste puede requerir al interesado un certificado del que surja, además de la constatación de su identidad, el análisis de sus antecedentes criminales o financieros. Esto quiere decir que la firma digital del interesado sólo será aceptada por la otra parte si cuenta con el certificado apropiado para la operación a realizar.

Los Repository o Registros son la base de datos a la que el público puede acceder on-line para conocer la validez de los certificados, su vigencia o cualquier otra circunstancia que se relacione con los mismos. Dicha base de datos debe incluir, entre otras cosas, los certificados publicados en el repositorio, las notificaciones de certificados suspendidos o revocados publicadas por las autoridades certificantes acreditadas, los archivos de autoridades certificantes autorizadas y todo otro requisito exigido por la División. Para ser reconocido, el repositorio debe operar bajo la dirección de una autoridad certificante acreditada.

Las IA facilitan la confirmación de la relación existente entre una clave pública y una persona o nombre determinado. Dicha confirmación es representada por un certificado: un mensaje firmado digitalmente y emitido por una IA.

El proceso de certificación incluye servicios de registro, "naming", autenticación, emisión, revocación y suspensión de los certificados. Hay empresas que ofrecen tres niveles de servicios de certificación. Cada nivel o clase de certificados ofrece servicios específicos en cuanto a funcionalidad y seguridad. Los interesados eligen entre estos grupos de servicios el que más le conviene según sus necesidades, debiendo especificar qué clase de certificado desean.

Dependiendo de la clase de certificado requerido, los interesados pueden solicitarlos y obtenerlos electrónicamente siguiendo las instrucciones detalladamente indicadas, o deberán concurrir personalmente a una Autoridad de Registro Local o LOCAL REGISTRATION AUTHORITY (LRA), o a un delegado, que puede ser un notario. Pueden existir varias "IA" para cada uno de los distintos niveles. Cumplidos los requisitos exigidos se emite el certificado o se envía un borrador para su aceptación por el interesado, según el caso.

4. CONCLUSIONES

Los estándares descritos anteriormente permite configurar un conjunto de especificaciones técnicas dirigidas a:

- Integración con sistemas y tecnologías existentes.
- Autentificación
- Delegación y federación

• Se le debe permitir a un usuario el acceso continuo y correcto por un periodo de tiempo razonable utilizando una única autentificación
• Renovación de credenciales
• Autorización
• Confidencialidad
• Integridad de los mensajes
• Privacidad

Una de las diferencias criticas entre la seguridad en el Grid y la seguridad en los sitios o las maquinas es la autonomía de los sitios. Existe la necesidad de poner de acuerdo a una gran cantidad de personas en sitios distribuidos para establecer las políticas. Las maneras de autentificar y autorizar a las entidades dentro del grid siguen evolucionando.

5. REFERENCIAS

[1] Jinpei Pan, Mingchu Li, Weifeng Sun*, Jing Hu, A Mediated RSA-based End Entity Certificates Revocation Mechanism in Grid, 2009 Fifth International Joint Conference on INC, IMS and IDC.
[2] May Phyo Oo, Nilar Thein, Thinn Thu Naing, Grid Security Framework for Managing the Certificate, the 2006 IEEE/WIC/ACM International Conference on Web Intelligence.
[3] Sang M. Park and Soon M. Chung, Enhanced CAS Certificate for Metadata-Based Access Control in Grids, 2008 20th IEEE International Conference on Tools with Artificial Intelligence.
[4] Rachid Saadi, Jean Marc Pierson, Lionel Brunie, The Chameleon: A Pervasive Grid Security Architecture, Third International Conference on Networking and Services(ICNS'07)
[5] Randy Butler, NCSA, Tony J. Genovese, Global Grid Forum Certificate Policy Model, GFD-C.16, www.ogf.org., 2003
[6] Mary R. Thompson, Doug Olson, Robert Cowles, Shawn Mullen, Mike Helm, CA-based Trust Issues for Grid Authentication and Identity Delegation, GFD-I.17, www.ogf.org., 200.
[7] Paul Madsen, David Chadwick, Authority Recognition, GFD-I.048, www.ogf.org., 2005
[8] Robert Cowles, Tony Genovese, Michael Helm, Policy Management Authority Model Charter, GFD-C.62m www.ogf.org., 2005.
[9] David L. Groep, Michael Helm, Jens Jensen, Milan Sova, Scott Rea, Reimer Karlsen-Masur, Ursula Epting, Mike Jones, Grid Certificate Profile, GFD-C.125 www.ogf.org., 2008.
[10] Kevin Feeney, David Lewis, Patroklos Argyroudis, Keith Nolan, Declan O'Sullivan, Grouping Abstraction and Authority Control in Policy-based Spectrum Management, IEEE, 2007.