D. G. Rosado, E. Fernandez-Medina, and J. Lopez, "Hacia una Arquitectura de Servicios de Seguridad para entornos Grid móviles", *V Congreso Iberoamericano de Seguridad Informática (CIBSI09)*, pp. 409-423, 2009.
NICS Lab. Publications: https://www.nics.uma.es/publications

Hacia una Arquitectura de Servicios de Seguridad para entornos Grid Móviles

David G. Rosado[1], Eduardo Fernández-Medina[1] y Javier López[2]

[1] Universidad de Castilla-La Mancha. Grupo Alarcos – Instituto de Tecnologías y Sistemas de Información. Dep. de Tecnologías y Sistemas de Información – Escuela Superior de Informática, Paseo de la Universidad 4, 13071 Ciudad Real
{David.GRosado, Eduardo.FdezMedina}@uclm.es
[2] Departamento de Lenguajes y Ciencias de la Computación. Universidad de Málaga, jlm@lcc.uma.es

Resumen. Grid móvil incluye las características de los sistemas Grid junto con las peculiaridades de la computación móvil, añadiendo la propiedad de soportar usuarios y recursos móviles de forma homogénea, transparente, segura y eficiente. La seguridad de estos sistemas, debido a su naturaleza abierta y distribuida, es un tema de gran interés. Una arquitectura de seguridad basada en SOA proporciona una arquitectura distribuida diseñada para interoperabilidad de servicios, fácil integración, y acceso seguro, simple y extensible. Por tanto, una arquitectura orientada a servicios de seguridad es construida para entornos Grid móviles, ofreciendo servicios de seguridad a usuarios móviles quienes usan servicios Grid y recursos para ejecutar sus trabajos y tareas. Esta arquitectura es integrada con otras arquitecturas existentes proporcionando mayor seguridad y permitiendo que los usuarios móviles puedan acceder a servicios Grid existentes ofreciendo nuevos y necesarios servicios de seguridad para Grid móviles. Hemos definido un conjunto de servicios de seguridad, que junto a protocolos, políticas y estándares de seguridad forman una arquitectura de seguridad orientada a servicios para entornos Grid móviles. Esta arquitectura es abierta, escalable, dinámica, interoperable y flexible.

Palabras claves: Arquitectura Seguridad, Servicios de Seguridad, computación Grid, computación Móvil, Seguridad.

1 Introducción

La idea del Grid está enfocada fundamentalmente en el acceso remoto a recursos computacionales, solventando el problema de coordinar los recursos compartidos entre las organizaciones virtuales multi-institucionales y dinámicas [1]. Grid móvil, unión de Grid y computación móvil, es un completo heredero del Grid con la característica de dar soporte a los usuarios y recursos móviles de forma transparente, segura y eficiente [2-4]. Grids y Grids móvil pueden ser la solución ideal para muchas aplicaciones a gran escala que son de naturaleza dinámica y que requieren transparencia para los usuarios.

Hay dos posibles roles a la hora de incorporar los dispositivos móviles al grid. Primero, los dispositivos móviles pueden ser usados como interfaces para el grid. Así, un dispositivo móvil puede iniciar el uso de recursos grid, monitorear los trabajos que son ejecutados remotamente, y tomar cualquier resultado desde el grid. Segundo y más interesante, los dispositivos móviles pueden asumir participar en un grid como proveedores de recursos de computación, no sólo como receptores de servicios. Nosotros creemos que el reciente avance de tecnología en dispositivos móviles y comunicaciones wireless hacen este escenario más factible.

La seguridad es un aspecto central en la computación Grid desde el principio, y ha sido considerado como el cambio más significativo de la computación Grid [5, 6]. La seguridad en entornos móviles es más crítica debido a la naturaleza abierta de las redes wireless. Además, la seguridad es más difícil de implementar dentro de una plataforma móvil debido a las limitaciones de recursos de los dispositivos móviles [7].

Debido a la dificultad de incorporar dispositivos móviles dentro de un entorno grid [3, 4, 8, 9], y sumado a la aparición de una nueva tecnología donde la seguridad es fundamental y los avances que la computación móvil ha experimentado en los últimos años, aparece la necesidad de definir, considerar y desarrollar una metodología o proceso de desarrollo en el cual, dentro de todo el ciclo de vida software [10, 11], se analizan e integran todos los requisitos y aspectos de seguridad relacionados con los sistemas Grid móviles, obteniendo como resultado un sistemas Grid móvil seguro, robusto y escalable.

En este artículo, se presenta una visión general sobre la arquitectura de servicios de seguridad que sirva de referencia para cualquier sistema Grid móvil. Esta arquitectura debe ofrecer servicios que soporten y cumplan con todos los requisitos de seguridad identificados y analizados en la actividad de análisis de nuestra metodología, y debe dar soporte a todos los algoritmos, mecanismos, y tecnologías de la actual arquitectura grid.

El resto del artículo está organizado como sigue: en la sección 2 describimos el trabajo relacionado sobre las diferentes arquitecturas de seguridad; en la sección 3 explicamos brevemente nuestra metodología de desarrollo para sistemas Grid móviles seguros; en la sección 4 presentamos la actividad de diseño de nuestra metodología donde definimos la arquitectura de servicios de seguridad para los sistemas Grid considerando la incorporación de dispositivos móviles, e identificamos los servicios de seguridad que forman parte de la arquitectura; finalmente proponemos las conclusiones y el trabajo futuro.

2 Trabajo Relacionado

La actual arquitectura Grid no tienen en cuenta los entornos de computación móvil debido a que los dispositivos móviles no han sido considerados como recursos de computación válidos o interfaces en la comunidad Grid. Es actualmente cuando se está prestando más atención de integrar estas dos tecnologías emergentes, computación Grid y computación móvil, como muestran algunos trabajos en [12, 13], aunque ninguno elabora la forma de incorporar los dispositivos móviles en la actual arquitectura Grid.

El proyecto Legion, desarrollado en la Universidad de Virginia, es un intento de proporcionar servicios Grid creando la ilusión de una máquina virtual. Esta máquina virtual dirige cuestiones Grid claves tales como la escalabilidad, la facilidad de programación, tolerancia a fallos, la seguridad y la autonomía del sitio. En general, el objetivo fundamental para la arquitectura de seguridad Legion [14-16] es permitir que los participantes en un sistema Grid expongan sus recursos de forma complaciente con sus políticas locales. Sin embargo Legion no se ocupa de la replicación de objetos dinámicos, e introduce un mayor nivel en el diseño de la seguridad, acentuando la flexibilidad y extensibilidad, pero menos la arquitectura y protocolos.

Globe (Global Object Based Environment) es un sistema distribuido de área amplia, el cual fue desarrollado para constituir un nivel intermedio entre el sistema operativo y el nivel de aplicación, tal y como hace Legion. Las principales características del sistema Globe son [17]: es un modelo uniforme para soportar sistemas distribuidos, soporta un marco de implementación flexible, y es altamente escalable. La arquitectura de Seguridad de Globe se basa en criptografía de clave pública y certificados digitales con el fin de abordar las cuestiones antes mencionadas.

CRISIS [18] es la arquitectura de seguridad para WebOS. WebOS proporciona un simple y tradicional sistema de ficheros y una interfaz para la creación de procesos remotos autenticados. CRISIS define cuidadosa y eficazmente las políticas de seguridad para estos servicios básicos. Sin embargo, la solución CRISIS no proporciona un medio fácil para el desarrollo de las políticas de seguridad para los nuevos mecanismos que se añaden a WebOS, ni provee un medio para modificar las políticas de seguridad soportadas para los servicios existentes.

Ninguna de las arquitecturas descritas anteriormente tiene en cuenta dispositivos móviles como recursos del Grid, y no dan soporte de seguridad para que los dispositivos móviles puedan ser integrados y manejados por el propio Grid como un recurso más. Nuestra arquitectura de seguridad es construida para un entorno móvil y orientada a servicios, y muchas de las desventajas o características no contempladas en las anteriores arquitecturas serán corregidas en nuestra arquitectura para dar soporte a los dispositivos móviles y asegurar dichos entornos Grid Móviles.

3 Resumen de la metodología

Nuestro objetivo es proporcionar a los desarrolladores, primero, una metodología o proceso sistemático de desarrollo que incluirá el desarrollo completo de sistemas Grid móviles de cualquier complejidad y magnitud, y segundo, una arquitectura de seguridad que ayude a desarrollar un sistema Grid móvil seguro de forma sistemática y ordenada. El proceso sistemático de desarrollo es un proceso iterativo, incremental y reutilizable. Un enfoque iterativo propone una comprensión incremental del problema a través de refinamientos sucesivos, un crecimiento incremental de una solución efectiva a través de varias versiones, y técnica reutilizable para construir componentes desde elementos existentes y probados.

La estructura de la metodología sigue el ciclo clásico, donde tenemos una etapa de planificación, una de desarrollo que incluye análisis, diseño y construcción, y finalmente, de una etapa de mantenimiento, sin embargo, está especialmente diseñada

para este tipo de sistemas, con características tan particulares. Detalle sobre las actividades y tareas de la metodología pueden encontrarse en [19-21]. En la Fig. 1 podemos ver la estructura de la metodología usando SPEM (Software & Systems Process Engineering Metamodel) versión 2.0 [22].

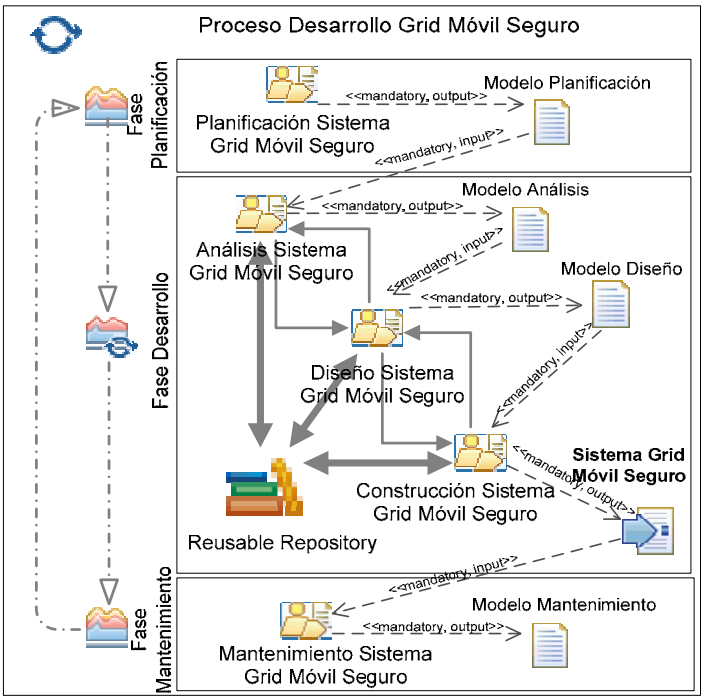

Fig. 1. Metodología de desarrollo para sistemas Grid móviles seguros

En este artículo nos centraremos en la actividad de Diseño y más concretamente, en la definición de una arquitectura de seguridad que sirva de referencia para el desarrollo de cualquier sistema Grid móvil seguro.

La actividad de análisis ha sido definida en algunos trabajos previos [20, 21, 23-25] donde las actividades y tareas son explicadas en profundidad. El análisis está centrado en construir diagramas de casos de uso y casos de uso de seguridad identificando y analizando todos los requisitos y requisitos de seguridad a partir de los casos de uso del diagrama construido para la aplicación, ayudado por los casos de uso reutilizables almacenados en el repositorio. Se construye el modelo de análisis que es la entrada a la actividad de diseño.

4 Actividad de Diseño

El objetivo de esta actividad es el diseño de una solución arquitectural donde se define la arquitectura software junto con la arquitectura de seguridad del sistema y del entorno tecnológico que le dará soporte, especificando de forma detallada todos los componentes del sistema Grid, siempre considerando el uso de dispositivos móviles. Esta arquitectura que se pretende diseñar debe ser una arquitectura de seguridad genérica que sirva de referencia para construir cualquier sistema Grid seguro, por tanto debe contemplar y dar soporte a todas las arquitecturas y tecnologías grid existentes.

Por tanto, se debe diseñar una arquitectura común para la construcción de sistemas Grid con dispositivos móviles siguiendo los requisitos y especificaciones analizadas y obtenidas en las actividades previas, y además, es necesario enriquecer la metodología con aspectos de seguridad, de tal forma que tengamos un proceso sistemático para la construcción de sistemas Grid con dispositivos móviles bajo entornos seguros.

Los dispositivos móviles son expuestos a frecuentes desconexiones desde la red, además de ser poco fiables. No es buena idea que los dispositivos móviles interactúen directamente con un sitio grid estático. Imaginemos que los dispositivos móviles se desconectan cuando estamos intercambiando datos con el sitio grid. A veces, los trabajos ejecutándose en sitios grid necesitan interactuar con el usuario móvil, pero el usuario móvil no tiene conexión. Así, un sistema fiable debe desempeñar el envío de trabajos, la monitorización, la cancelación, y la terminación del proceso por parte del usuario móvil [26].

Nuestra arquitectura se construye bajo un entorno seguro, flexible, escalable, interoperable, dinámico y abierto, por tanto, siguiendo estas metas podremos cubrir la mayoría de requisitos [27, 28], utilizando estándares que puedan ser entendidos por la gran mayoría de aplicaciones, ofreciendo protocolos de seguridad para las comunicaciones y permitiendo múltiples implementaciones dentro de la misma arquitectura y que sean capaces de cooperar entre ellas.

4.1 Definiendo Capas de Servicios de Seguridad

Considerando que la mayoría de los modelos y arquitecturas se definen mediante capas o niveles, nosotros seguiremos el mismo esquema de capas para definir nuestra arquitectura de servicios de seguridad para entornos Grid móviles. La idea de esta arquitectura de servicios es definir una arquitectura de referencia, donde se ordenan y dividen por capas los servicios de seguridad que son necesarios para la arquitectura a construir.

Cada una de las capas puede interoperar con el resto de capas adyacentes para ofrecer o beneficiarse de los servicios de las otras capas para construir nuevos servicios o mecanismos de seguridad. Podemos ver en la Fig. 2 una propuesta de 8 capas, donde se engloban todos los servicios y mecanismos de seguridad necesarios que cubren todos los requisitos de seguridad [27, 28] para los entornos Grid con dispositivos móviles.

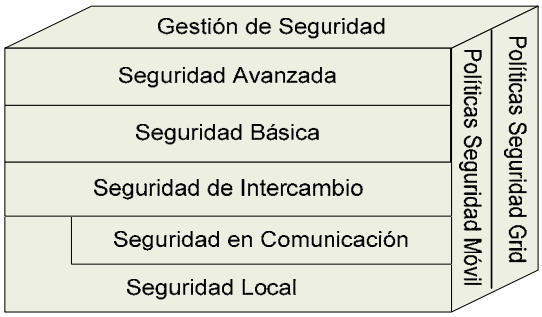

Fig. 2. Capas de Servicios de Seguridad para entornos Grid móviles.

Debemos identificar todos los servicios de seguridad que nuestra arquitectura debe soportar, y asignarlos a las capas correspondientes por su funcionalidad y la relación con otros elementos de la arquitectura.

La Tabla 1 muestra los objetivos de seguridad que debemos cumplir para cada una de las capas, y estudiar los servicios necesarios que deben estar presentes en nuestra arquitectura y que faciliten la consecución de dichos objetivos.

Tabla 1. Relación entre Capas, Objetivos y Servicios de Seguridad

Capas de Seguridad	Objetivos de seguridad	Servicios de seguridad
Seguridad Local	Seguridad del dispositivo; Seguridad hardware; Seguridad Software; Seguridad Recurso; Seguridad del Contenido; Seguridad de Claves; Protección de Datos; Protección de Password	Autorización, Protección Autenticación, Antivirus
Seguridad de Comunicación	Seguridad de transporte; Seguridad de mensajes; Seguridad inalámbrica.	Confidencialidad, Integridad, Privacidad, Conversación Segura
Seguridad de Intercambio	Intercambio políticas; Intercambio Credenciales y Privilegios; Intercambio Identidad y Claves	Intercambio; Traducción Credenciales & Identidad
Seguridad Básica	Autenticación; Autorización; Confidencialidad; Integridad; Disponibilidad; No repudio	Autenticación, Autorización, Disponibilidad, No repudio
Seguridad Avanzada	Confianza; Delegación; SSO; Logging; Audit; Contexto de Seguridad; Antivirus	Confianza; Delegación & SSO; Logging & Audit
Políticas Seguridad Grid	Definir y Manejar políticas de Integridad; Privacidad; Autorización; Autenticación; Delegación; Federación; Confianza.	Políticas Grid
Políticas seguridad dispositivos móviles	Definir y manejar políticas de Acceso a dispositivos móviles; Localización; Protección de Password; Protección tarjeta almacenamiento; Cifrado ficheros; Protección física; Protección datos; Backups; Restricciones Software.	Políticas Dispositivos móviles
Gestión de seguridad	Gestionar Claves, Usuarios, Políticas Grid, Políticas Dispositivos Móviles, Recursos, Credenciales e Identidad.	Gestión Seguridad

Ahora explicaremos cada una de las capas de seguridad consideradas y los servicios de seguridad que debemos considerar en cada capa, indicando los aspectos de seguridad más relevantes que creemos deben ser tenidos en cuenta en cada capa, considerando los aspectos y características de los entornos Grid con dispositivos móviles. Los servicios de seguridad que se desprenden de esta tabla son: Autorización, Protección, Autenticación, Antivirus, Confidencialidad, Integridad, Privacidad, Conversación Segura, Intercambio, Traducción Identidad & Credenciales, Disponibilidad, No repudio, Confianza, Delegación & SSO, Logging & Audit, Políticas Grid, Políticas Dispositivos móviles, y Gestión Seguridad.

4.1.1 Servicios de Seguridad Locales

En esta capa se agrupan los servicios de seguridad que son exclusivos de los recursos y dispositivos móviles que forman parte del Grid. Son los servicios que ofrecen cierto nivel de seguridad a los recursos (incluyendo dispositivos móviles) tanto de forma aislada como conectado al sistema Grid. Entre los servicios nos encontramos con los servicios de Protección de Datos y Passwords para los dispositivos móviles, servicio de Autenticación de usuario, servicio de Backup y Antivirus residentes en los dispositivos móviles, y el servicio de Autorización para el acceso a dicho recurso.

Los dispositivos móviles que almacenan información o sirven para conectarse a la red, deberían proteger la clave con fuertes frases de paso (passphrases/PINs). Esto previene que los ladrones entren en el dispositivo y accedan a la información almacenada en él. Para proteger contra perdida de datos, los ficheros deben ser volcados a una localización segura fuera del dispositivo (volcar regularmente los datos de un PDA a un PC para evitar daños por virus o gusanos). Es recomendable usar antivirus en los dispositivos como PDAs, ya que los escaneos a nivel de red son más efectivos y es una forma centralizada de prevenir virus y otras interrupciones asociadas con los dispositivos móviles. Las soluciones firewall son más fáciles y efectivas de controlar y manejar que soluciones similares alojadas en el operador móvil

Siempre que el dispositivo cliente se conecte a una red corporativa, el usuario y el dispositivo deben ser autorizados para hacer cualquier cambio en la red. En general, las soluciones de autenticación efectivas son aquellas que permiten acceder a la red sólo a usuarios autorizados. Las soluciones de autenticación incluyen el uso de nombres de usuario y claves, smart cards, biométricas, o PKI; o una combinación de soluciones (por ejemplo, smart cards con PKI). Cuando confiamos en nombres de usuario y claves, es importante tener políticas especificando una longitud mínima de la clave, caracteres de clave requeridos, y caducidad de claves.

4.1.2 Servicios de Seguridad de Comunicación

La seguridad de comunicación es a menudo descrita en términos de confidencialidad, integridad, autenticación y no repudio de los datos transmitidos. Estos servicios de seguridad son a su vez implementados por varios mecanismos que suelen ser de naturaleza criptográficos [29].

La confidencialidad de los datos transmitidos puede ser proporcionada cifrando la información entre las partes que se comunican, bien end-to-end o en alguna de las partes implicadas. La autenticación de los datos transmitidos es un servicio

asimétrico, queriendo decir que cuando A y B están comunicándose, la autenticación de los datos de A en B es independiente de la autenticación de los datos de B en A. Los tipos de autenticación disponibles dependen del protocolo de seguridad utilizado. En Internet, por ejemplo, SSL permite cifrar con cuatro opciones de autenticación diferentes: 1) autenticación del servidor, 2) autenticación del cliente, o 3) autenticación tanto del servidor como el cliente, o 4) ninguna autenticación, por ejemplo, proporcionando sólo confidencialidad.

Debemos proporcionar seguridad a nivel de mensaje y de transporte. La seguridad a nivel de mensaje es alcanzada mediante tecnologías y estándar tales como WS-Security, XML-Encryption y XML-Signature. La seguridad a nivel de mensaje se basa en WS-Security y soporta la privacidad e integridad, y es un óptimo esquema si se envían pocos mensajes. También podemos establecer seguridad a nivel de mensaje mediante WS-SecureConversation que soporta delegación de credenciales, privacidad, integridad y autenticación anónima. Si se envían muchos mensajes, su rendimiento es bueno.

4.1.3 Servicios de Intercambio de Seguridad

Es posible que este servicio sea necesario cuando trabajamos con identidades de distinta naturaleza y bajo distintos dominios de aplicación. Una identidad que es válida para el Grid puede no ser válida para los dominios porque trabajan con otro tipo de identidad. Es por ello que se debe mapear la identidad para el dominio local cuando se quiera acceder a un recurso, y viceversa si queremos acceder al Grid. Las identidades globales que maneja el Grid no son aceptadas en muchos dominios locales, que obligan a hacer una traducción de identidad en su dominio local y asignarle los derechos locales correspondientes con la identidad local. Por ello, cuando una petición accede al recurso, se debe hacer un mapeo de identidad global a local para que el servicio de autorización local trabaje con dicha identidad local.

Cada dominio local tiene sus propios mecanismos y políticas de seguridad para proteger al recurso. Es tarea de la arquitectura ofrecer los servicios necesarios para poder comunicarse con las políticas de seguridad locales de forma que puedan comunicarse y enviar peticiones de acceso a recursos e intercambio de información. Esto significa que es posible que se requiera un servicio de conversión de formatos, de credenciales o de protocolos para comunicarse con la infraestructura de seguridad local de cada dominio.

4.1.4 Servicios de Seguridad Básicos

Los servicios básicos que consideramos son los servicios básicos de seguridad para entornos abiertos genéricos, y que son igualmente importantes para entornos Grid. Estos servicios son: Autenticación, Autorización, Non-repudio, privacidad, integridad y confidencialidad. A partir de estos servicios básicos, ampliándolos, modificándolos o combinándolos podemos crear nuevos servicios (servicios de seguridad avanzados) que son necesarios para construir una arquitectura de seguridad para sistemas Grid con dispositivos móviles.

Algunos de estos servicios de seguridad que consideramos básicos, ya han sido asignados a la capa de comunicación (Integridad, Privacidad, Confidencialidad), por lo que en esta capa se definen el resto de servicios básicos, Autenticación,

Autorización y No-repudio. Nosotros añadimos el servicio de Disponibilidad que se refiere a la capacidad de las partes autorizadas a obtener acceso a la información cuando sea necesario.

Una función importante de una arquitectura de descubrimiento/entrega de servicio es reaccionar rápidamente a fallos. Un servicio, por ejemplo, podría no estar disponible más debido a un fallo del servidor o a la movilidad, por ejemplo. La disponibilidad puede ser definida como la propiedad de un sistema que siempre cumple con peticiones legítimas por entidades autorizadas. Es violada cuando un atacante consigue denegar el servicio a los usuarios legítimos (por ejemplo, utilizando todos los recursos disponibles).

La protección contra ataques y amenazas a la seguridad es importante, ya que está fuertemente vinculada a la disponibilidad de la red y, por tanto, a todos los servicios y funcionalidades que una red móvil ofrece a los usuarios y diversas organizaciones. Los ataques de denegación del servicio (DoS, Denial-of-service) han llegado a ser una de las más obvias amenazas que pueden tener un efecto severo en la disponibilidad, rendimiento y calidad de los servicios en una red móvil. Las soluciones de seguridad de redes móviles deben proporcionar protección contra una variedad de amenazas existentes y trabajar para asegurar la disponibilidad de los recursos de red [30].

El no repudio es similar a la autenticación en que es un servicio de seguridad asimétrico. Un simple ejemplo para describir la diferencia entre autenticación y no repudio es que con la autenticación el destinatario está seguro del origen del mensaje pero no sería capaz de convencer a nadie más sobre ésto, sin embargo, con el no repudio, el destinatario sería capaz de convencer a terceras partes del origen del mensaje. La firma digital es el mecanismo usado para el no repudio. Hay que controlar las acciones que tienen lugar, los solicitantes y receptores de las acciones, para proteger de las falsas negaciones. Algunas técnicas comunes para proporcionar no repudio son la autenticación combinadas con el logging y firmando el contenido de la comunicación con claves privadas.

Para los servicios básicos de seguridad, debemos emplear todos los estándares existentes para crear una arquitectura abierta y que pueda inter-operar con múltiples servicios de otras arquitecturas existentes. Así por ejemplo, para la autenticación, el protocolo basado en TLS es usado para llevar a cabo la autenticación y proporcionar protección del mensaje (cifrado y prueba de integridad). La infraestructura de clave pública (PKI) junto con certificados X.509 son frecuentemente utilizados.

4.1.5 Servicios de Seguridad Avanzados

Uno de los requisitos importantes de los entornos Grid es que un usuario pueda tener acceso a un gran número de recursos distribuidos autenticándose una sola vez. Esto es referido como single sign-on, que lo consideramos como un servicio avanzado donde interviene el servicio de autenticación de la capa de seguridad básica. Para permitir compartir grandes cantidades de datos y recursos computacionales a través de comunidades de usuarios altamente distribuidas de forma eficiente y efectiva, es esencial permitir la delegación. Uno de los factores característicos de una infraestructura Grid es la necesidad de delegar derechos de entidad a otras entidades dentro del Grid.

Confianza o Trust puede generalmente ser definida como tener la confianza que una parte se comporta de una manera esperada a pesar de la falta de capacidad para

supervisar o controlar la otra parte. En un entorno donde se describe la política de acceso en términos de identidad de usuarios o de atributos requeridos, la gestión de la confianza consiste en definir las fuentes de autoridades para la identificación del usuario, la asignación de atributos y, posiblemente, la creación de política. En un sistema donde los usuarios pueden delegar algunas o la totalidad de sus derechos a otros usuarios, el control de dicha delegación es parte de la gestión de confianza [5]. El Grid debe establecer confianza entre los distintos dominios para asegurar que las peticiones, los mensajes y los datos que son manejados en el Grid, proceden de dominios de confianza, que han sido protegidos de ataques, y han seguido las políticas de seguridad que garanticen su seguridad.

Hay que registrar todo lo que vaya sucediendo en el sistema, los trabajos enviados, la memoria, la utilización de recursos, estado de los trabajos, resultados obtenidos, etc. Hay que considerar que los ficheros logs pueden residir en diferentes dominios administrativos, por lo que el acceso seguro a los ficheros logs es una tarea compleja. Los logs deben ser asegurados y a prueba de manipulación, y capacitado para asegurar la integridad del mensaje.

El servicio de Auditoría es conducida por política y responsable de registrar los eventos relevantes de seguridad. Este servicio es típicamente usado por los administradores de seguridad dentro de una VO para comprobar la adherencia a las políticas de control de acceso y autenticación. La auditoría requiere que los eventos sean registrados de forma segura.

4.1.6 Servicios de Política Grid

En esta capa se definen todas las políticas de seguridad que definirán el comportamiento de los servicios de seguridad, de las comunicaciones y de las transacciones que se realicen en el sistema. Tendremos que definir las políticas de integridad, de autorización, de intercambio de políticas, etc. Debemos definir una política de seguridad, un conjunto de roles que definen los sujetos de seguridad (usuarios), los objetivos de seguridad (recursos) y las relaciones entre ellos. Esta capa debe estar en contacto directo con cada una de las capas anteriores para asegurar que cada servicio en cada capa tenga acceso a sus respectivas políticas de seguridad de forma directa y segura.

Las políticas de seguridad son un conjunto de reglas que gobiernan el sistema y que lo protegen de ataques y amenazas. Todas las acciones, peticiones y transacciones deben llevarse siguiendo alguna política de seguridad. La política de seguridad se refiere al conjunto de reglas, leyes y prácticas que regulan cómo una organización gestiona, protege y distribuye la información delicada. Una política de seguridad debe especificar los objetivos de seguridad que el sistema debe cumplir y las amenazas que deben resistir. Esto implica que una política de seguridad debe determinar el tipo de comunicación requerida para las diversas transacciones, el tipo de autenticación, los procedimientos de auditoría, técnicas de recuperación y control de acceso, que es una parte importante de la política de seguridad. En general, la política de control de acceso especifica quién puede acceder a determinados recursos y qué operaciones se permiten en esos recursos.

Se pueden emplear las especificaciones SAML y XACML para expresar las políticas de control de acceso, sentencias de autorización, y protocolos de autorización. La especificación XACML establece el mecanismo de política de

recurso a cada recurso o servicio. SAML también tiene un mecanismo de política pero está muy limitado para el Grid, mientras que XACML proporciona un mecanismo mucho más flexible que puede ser aplicado a cualquier tipo de recurso.

4.1.7 Servicios de Política Móvil

Es conveniente crear políticas de seguridad específicas para el uso de dispositivos móviles, así por ejemplo, si queremos minimizar el impacto por la pérdida de un dispositivo, debemos proteger con contraseñas todos los dispositivos, cifrar los documentos sensibles en el dispositivo, y no usar scripts automáticos para el acceso a VPN. Las políticas de seguridad del dispositivo móvil deben incluir también un acceso mínimo a fuentes limitadas utilizando cortafuegos.

Las empresas deben tratar la seguridad móvil como una tarea independiente, y como tal, las políticas de seguridad específicas para el uso móvil deben ser creadas e implementadas. Un análisis de riesgo global de los posibles riesgos de seguridad asociados con el uso de dispositivos móviles debe ser el primer paso hacia la creación de la política de seguridad de dispositivos móviles.

El primer paso, entonces, es desarrollar las políticas de seguridad razonables para gobernar el uso de dispositivos móviles en el Grid. La organización debe disponer de políticas que son específicas para los dispositivos móviles, no sólo tratar de aplicar las políticas generales de seguridad. También es importante educar a los usuarios del dispositivo móvil sobre las cuestiones de seguridad, incluida la seguridad física. Algunas políticas de seguridad pueden ser aplicadas tecnológicamente, pero otras dependen del cumplimiento del usuario.

4.1.8 Servicios de Gestión de Seguridad

El modelo de seguridad Grid agrupa todas las funciones de gestión de seguridad aplicables a los diversos aspectos de vinculación, política y federación. Éstos incluyen gestión de claves para funciones criptográficas, gestión de registro de usuarios, gestión de dispositivos, autorización, privacidad y gestión de política de confianza, y gestión de reglas de mapeos que permite la federación. También puede incluir la gestión de detección de intrusos, servicios de antivirus y garantía de servicio de información que permita a los solicitantes de servicios descubrir lo que pueden ofrecer los mecanismos de seguridad de un entorno de alojamiento o host. Abordar la gestión de diversos aspectos de la infraestructura de seguridad satisface los requisitos de manejabilidad en el entorno Grid [31].

Cada servicio, ya sea en la capa de comunicación, básica o avanzada, necesitará controlar y gestionar la información que necesita para llevar a cabo su tarea. Por eso, esta capa debe colaborar de forma directa con cada capa de la arquitectura, ofreciendo los servicios de gestión necesarios para cada servicio.

Los servicios de gestión de la seguridad se encargan de gestionar, por ejemplo los usuarios móviles que pertenecen al grid o quieren pertenecer, los derechos y privilegios para cada usuario o role, las claves generadas para cada usuario o grupo de usuarios, los recursos cedidos o eliminados de los que dispone el sistema, las identidades de cada usuario o servicio dentro del Grid, y por supuesto la gestión de las políticas de seguridad (integridad, privacidad, autorización, etc.).

5 Conclusiones

Este artículo presenta la arquitectura de seguridad para manejar diversos problemas de seguridad en el Grid. Cómo construir un sistema Grid seguro es también una tarea importante debido a la alta complejidad del sistema de computación Grid. Es difícil incorporar de forma segura dispositivos móviles existentes dentro del Grid, de manera que el impacto sea mínimo y transparente para el usuario. Esta es la razón de la necesidad de elaborar y definir una metodología de desarrollo de un sistema basado en Grid y tecnología móvil, considerando, desde las primeras etapas del desarrollo, las peculiaridades y necesidades de seguridad para este tipo de sistemas. El Grid necesita construir un sistema de seguridad unificado que soporte todas las funciones de seguridad, las cuales residen en los sistemas Grid, sea independiente de otros sistemas y tenga una buena relación de cooperación con el resto de sistemas.

Una fase importante de la metodología es el diseño de la arquitectura de seguridad que hemos propuesto con un conjunto de servicios de seguridad que cubren todos los requisitos de seguridad y usa tecnologías estándar y especificaciones de los servicios web para obtener una arquitectura de seguridad abierta, escalable e interoperable. Esta arquitectura es una arquitectura de referencia de nuestra metodología y sirve como base para construir una arquitectura específica con necesidades y requisitos especiales para los diferentes tipos de entornos Grid móvil.

Como trabajo futuro, completaremos la metodología describiendo formalmente las fases, actividades y tareas con las especificaciones SPEM. Estudiaremos en profundidad los servicios de seguridad propuestos, identificando las tecnologías de seguridad, los protocolos y mecanismos que podemos utilizar en cada servicio y relacionaremos los requisitos de seguridad con los servicios de seguridad utilizados para resolver estos requisitos. Construiremos una arquitectura orientada a servicios de seguridad desde varios puntos de vista (lógica, comunicación, implementación, servicios, red, etc.) y aplicaremos esta metodología a un caso real. Una adaptación de esta propuesta para Cloud computing, que es una tecnología que permite ofrecer servicios de computación a través de Internet, está siendo estudiada.

Agradecimientos. Esta investigación es parte de los siguientes proyectos: QUASIMODO (PAC08-0157-0668) financiado por la “Viceconsejería de Ciencia y Tecnología de la Junta de Comunidades de Castilla-La Mancha” (España), SISTEMA (PII2I09-0150-3135) financiado por FEDER y la “Consejería de Educación y Ciencia de la Junta de Comunidades de Castilla-La Mancha” (España), y ESFINGE (TIN2006-15175-C05-05) concedida por la “Dirección General de Investigación del Ministerio de Educación y Ciencia” (España).

Referencias

1. Foster, I., Kesselman, C., Tuecke, S.: The Anatomy of the Grid: Enabling Scalable Virtual Organizations. 7th International Euro-Par Conference Manchester on Parallel Processing. 15(3), 1 - 4 (2001)

2. Litke, A., Skoutas, D., Varvarigou, T.: Mobile Grid Computing: Changes and Challenges of Resourse Management in a Mobile Grid Environment. In: 5th International Conference on Practical Aspects of Knowledge Management (PAKM 2004), (2004)
3. Guan, T., Zaluska, E., Roure, D.D.: A Grid Service Infrastructure for Mobile Devices. In: First International Conference on Semantics, Knowledge, an Grid (SKG 2005), Beijing, China (2005)
4. Jameel, H., Kalim, U., Sajjad, A., Lee, S., Jeon, T.: Mobile-To-Grid Middleware: Bridging the gap between mobile and Grid environments. In: European Grid Conference EGC 2005, pp. 932-941. Springer, Amsterdam, The Netherlands (2005)
5. Humphrey, M., Thompson, M.R., Jackson, K.R.: Security for Grids. Lawrence Berkeley National Laboratory. Paper LBNL-54853. (2005)
6. Chakrabarti, A., Damodaran, A., Sengupta, S.: Grid Computing Security: A Taxonomy. IEEE Security & Privacy. 6, 44-51 (2008)
7. Bradford, P.G., Grizzell, B.M., Jay, G.T., Jenkins, J.T.: Cap. 4. Pragmatic Security for Constrained Wireless Networks. In: Publications, A. (ed.): Security in Distributed, Grid, Mobile, and Pervasive Computing, The University of Alabama, Tuscaloosa, USA (2007) 440
8. Kwok-Yan, L., Xi-Bin, Z., Siu-Leung, C., Gu, M., Jia-Guang, S.: Enhancing Grid Security Infrastructure to Support Mobile Computing Nodes. Lecture Notes in Computer Science. 2908/2003, 42-54 (2004)
9. Sajjad, A., Jameel, H., Kalim, U., Han, S.M., Lee, Y.-K., Lee, S.: AutoMAGI - an Autonomic middleware for enabling Mobile Access to Grid Infrastructure. In: Joint International Conference on Autonomic and Autonomous Systems and International Conference on Networking and Services - (icas-icns'05), pp. 73-73. (2005)
10. Baskerville, R.: Information systems security design methods: implications for information systems development. ACM Computing Surveys. 25, 375 - 414 (1993)
11. Anderson, R.: Security Engineering - A Guide to Building Dependable Distributed Systems. John Wiley&Sons (2001)
12. Phan, T., Huang, L., Dulan, C.: Challenge: Integrating Mobile Wireless Devices Into the Computational Grid. In: 8th annual international conference on Mobile computing and networking (MobiCom'02), pp. 271 - 278. ACM Press, Atlanta, Georgia, USA (2002)
13. Clarke, B.a.M.H.: Beyond the 'Device as Portal': Meeting the Requirements of Wireless and Mobile Devices in the Legion Grid Computing System,". In: Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing at the International Parallel and Distributed Processing Symposium., IEEE Press, (2002)
14. Chapin, S., Wang, C., Wulf, W., Knabe, F., Grimshaw, A.: A New Model of Security for Metasystems. Future Generation Computer Systems. 15, 713-722 (1999)
15. Foster, I., Kesselman, C.: The Grid: Blueprint for a Future Computing Infrastructure. Morgan Kaufmann Publishers; 1ST edition, San Francisco, CA (1999)
16. Ferrari, A., Knabe, F., Humphrey, M., Chapin, S., Grimshaw, A.:: A Flexible Security System for Metacomputing Environments. In: CS-98-36, T.R. (ed.). Department of Computer Science. University of Virginia (1998)
17. van Steen, M., Homburg, P., Tanenbaum, A.S.: Globe: A Wide-Area Distributed System. IEEE Concurrency. 70-78 (1999)
18. Belani, E., A.Vahdat, Anderson, T., Dahlin., M.: CRISIS: A wide area security architecture. In: Seventh USENIX Security Symposium, (1998)
19. Rosado, D.G., Fernández-Medina, E., López, J., Piattini, M.: PSecGCM: Process for the development of Secure Grid Computing based Systems with Mobile devices. In: International Conference on Availability, Reliability and Security (ARES'08), pp. 136-142. IEEE, Barcelona, Spain (2008)

20. Rosado, D.G., Fernández-Medina, E., López, J., Piattini, M.: Engineering Process Based On Grid Use Cases For Mobile Grid Systems. In: The Third International Conference on Software and Data Technologies- ICSOFT 2008, pp. 146-151. Porto, Portugal (2008)
21. Rosado, D.G., Fernández-Medina, E., López, J.: Obtaining Security Requirements for a Mobile Grid System. International Journal of Grid and High Performance Computing. (to be published in April 1, 2009) (2009)
22. OMG: Software & Systems Process Engineering Meta-Model Specification (SPEM) 2.0. (2008) http://www.omg.org/spec/SPEM/2.0/PDF
23. Rosado, D.G., Fernández-Medina, E., López, J.: Reutilización de Casos de Uso en el Desarrollo de Sistemas Grid seguros. In: XII Conferencia Iberoamericana de Ingeniería de Requisitos y Ambientes de Software – IDEAS 2009 (accepted), Medellín, Colombia (2009)
24. Rosado, D.G., Fernández-Medina, E., López, J.: Reusable Security Use Cases for Mobile Grid environments. In: Workshop on Software Engineering for Secure Systems (SESS'09), in conjunction with the 31st International Conference on Software Engineering (ICSE 2009) Vancouver (Canadá) (2009)
25. Rosado, D.G., Fernández-Medina, E., López, J., Piattini, M.: PSecGCM: Process for the development of Secure Grid Computing based Systems with Mobile devices. In: International Conference on Availability, Reliability and Security (ARES 2008), pp. 136-142. IEEE, Barcelona, Spain (2008)
26. Park, S.-M., Ko, Y.-B., Kim, J.-H.: Disconnected Operation Service in Mobile Grid Computing. In: International Conference on Service Oriented Computing (ICSOC'2003), Trento, Italy (2003)
27. Vivas, J.L., López, J., Montenegro, J.A.: Cap. 12. Grid Security Architecture: Requirements,fundamentals, standards, and models. In: Publications, A. (ed.): Security in Distributed, Grid, Mobile, and Pervasive Computing, Tuscaloosa, USA (2007) 440
28. Trusted Computing Group Administration: Securing Mobile Devices on Converged Networks. (2006) https://www.trustedcomputinggroup.org/groups/mobile/Final_iGR_mobile_security_white_paper_sept_2006.pdf
29. Jøsang, A., Sanderud, G.: Security in Mobile Communications: Challenges and Opportunities. In: the Australasian information security workshop conference, Adelaide, Australia (2003)
30. Nokia: Mobile Device Management and Security. (2007)
31. Nagaratnam, N., Janson, P., J. Dayka, Nadalin, A., Siebenlist, F., Welch, V., Tuecke, S., Foster, I.: The Security Architecture for Open Grid Services. (2002) http://forge.gridforum.org/projects/ogsa-sec-wg/.