Modelo de seguridad para entornos colaborativos de nueva generación

Jasone Astorga, Jon Matias, Puri Saiz, Eduardo Jacob

Departamento de Electrónica y Telecomunicaciones.
Universidad del País Vasco / Euskal Herriko Unibertsitatea.
Escuela Superior de Ingenieros. Alameda de Urquijo s/n. 48013 – Bilbao
Teléfono: 94 601 40 36 Fax: 94 601 42 59
E-mail:{jasone.astorga, jon.matias, puri.saiz, eduardo.jacob}@ehu.es

***Abstract* — Today, collaboration is considered a way of improving efficiency and quality of work, and in order to exploit this concept the organisation of NGCWEs (Next Generation Collaborative Working Environments) has emerged. Such working environments try to integrate the experiences of the workers into the system, for which they make use of sensors and low capacity mobile devices. In this paper we take into account all the special features of NGCWEs to propose a security model which best fits its requirements. Therefore, we have developed a solution based on private key cryptology and a centralized authorization system, which allows the minimization of the load of the security solution over the final systems.**

I. INTRODUCCIÓN

Actualmente la colaboración se percibe como una herramienta para aumentar la efectividad organizacional en un gran número de contextos de trabajo. Por este motivo, las organizaciones están invirtiendo numerosos esfuerzos en el desarrollo de entornos NGCWE (Next Generation Collaborative Working Environments) [1], los cuales se definen como potentes entornos de trabajo en colaboración que permiten elevar la productividad, creatividad y la calidad del trabajo. A grandes rasgos, los entornos NGCWE están compuestos por una serie de elementos básicos y un conjunto de herramientas colaborativas o middleware. Los primeros son los componentes cruciales individuales asociados a las funcionalidades de los distintos entornos, es decir, son las piezas básicas que construirán los CWE. Por su parte, las herramientas colaborativas se definen como un sistema que integra los componentes individuales del mismo. Estas herramientas permiten obtener sinergias entre los distintos elementos básicos consiguiendo un resultado muy superior a la suma de las funcionalidades individuales, es decir, se consigue la creación de aplicaciones colaborativas de alto nivel bajo demanda y de forma dinámica.

Uno de los aspectos fundamentales de este tipo de entornos se basa en conseguir integrar la experiencia propia del trabajador en la creación de los mismos, para lo cual normalmente se hace uso de sensores o dispositivos portátiles, con escasa capacidad de procesamiento y almacenamiento, dependencia de baterías para su operativa y comunicaciones a través de enlaces inalámbricos de baja capacidad y coste relativamente alto. Estas características serán de especial relevancia, y muy a tener en cuenta, en las investigaciones a realizar y sobre todo en el modelo a plantear.

El objetivo de este trabajo es proponer una solución a las necesidades de seguridad de los usuarios de entornos NGCWE, de forma que estos puedan establecer relaciones de confianza para el intercambio seguro de datos, garantizando tanto la confidencialidad e integridad de los datos transmitidos, así como el no repudio de los mismos. Entre las tecnologías existentes hoy en día, se distinguen dos enfoques básicos: la utilización de infraestructuras de clave pública, como son las PKIs [2], o los sistemas basados en secretos compartidos, entre los cuales destaca el protocolo Kerberos [3].

La implementación de sistemas basados en PKIs en entornos con unas características tan especiales como las de los NGCWEs presenta grandes retos debidos a la complejidad derivada de la obtención de las claves y los certificados, la comprobación de las listas de revocación, el establecimiento de relaciones de confianza entre dominios heterogéneos, etc [4]. En este tipo de entornos, que destacan por la utilización de dispositivos con escasas capacidades de procesamiento, se consideran más eficientes las tecnologías basadas en secretos compartidos [5]. Por lo tanto, en este artículo se propone un sistema de seguridad basado en la utilización del protocolo Kerberos.

Sin embargo, Kerberos únicamente garantiza la identidad del usuario, pero no se encarga de validar los derechos que dicho usuario pueda tener sobre las aplicaciones finales, lo que se denomina proceso de autorización o control de acceso, dejando en manos de los proveedores de servicio la implementación de los mecanismos necesarios. Tal y como se ha explicado previamente, en los NGCWEs los elementos básicos se interconectan de forma dinámica para constituir aplicaciones colaborativas de alto nivel, pudiendo variar de una aplicación a otra las relaciones de confianza entre los distintos componentes. En este caso, no resulta viable que cada elemento básico mantenga y gestione su propia información de autorización, ya que sino, estos elementos básicos dejarían de ser neutrales e independientes de las aplicaciones colaborativas de nivel superior. Como solución a este problema, se propone la implementación de un sistema que gestione la autorización de forma centralizada, liberando así a las aplicaciones finales de la necesidad de implementar sus propios controles de acceso.

II. Fase de autenticación

Tal y como se ha adelantado, en el modelo de seguridad propuesto la autenticación de los usuarios se basa en la utilización del protocolo Kerberos. Este protocolo, basado en criptografía simétrica, presenta una ventaja importante con respecto a la mayoría de los sistemas de autenticación existentes hoy en día, y es que el protocolo es seguro en sí mismo, con lo que no necesita del establecimiento de un canal seguro sobre el que transportarse. La robustez de este protocolo se debe a que la contraseña del usuario nunca viaja por la red, con lo que no existe el riesgo de que un atacante pueda interceptarla.

La arquitectura propuesta se basa en la utilización de un servidor Kerberos, en el cual estarán registradas todas las entidades que quieran participar en el sistema, tanto usuarios como servidores, junto con sus correspondientes claves. A continuación se describe brevemente el funcionamiento de este protocolo y en la figura 1 se muestran las interacciones básicas del mismo.

El servidor Kerberos proporciona de forma centralizada las funcionalidades necesarias para autenticar a los usuarios frente a los servidores a los que quieran acceder y viceversa, todo ello en base a la utilización de *tickets maestros* y *tickets de servicio*. Para ello, el servidor autentica a cada una de las entidades de forma individual, y se encarga de generar y distribuir las claves secretas compartidas que cada par cliente/servidor necesita para proteger las comunicaciones entre ambos.

Cuando una entidad se autentica contra el servidor Kerberos, éste le proporciona un *ticket maestro*, que no es más que una serie de datos cifrados con una clave conocida únicamente por el propio servidor Kerberos. Este ticket le permitirá al usuario identificarse posteriormente como un usuario autenticado dentro del sistema y obtener así los *tickets de servicio* necesarios sin necesidad de volver a autenticarse. Los tickets de servicio son emitidos también por el servidor Kerberos y se construyen para garantizar la identidad de un determinado usuario frente a un servicio concreto. Para ello, contienen información relativa al usuario cifrada con una clave secreta compartida entre el servicio al que el usuario quiere acceder y el servidor Kerberos, de forma que al recibir el ticket, el servicio pueda descifrarlo y estar seguro de que la información que contiene es verídica, ya que está cifrada con una clave conocida únicamente por él mismo y un servidor Kerberos en el que confía.

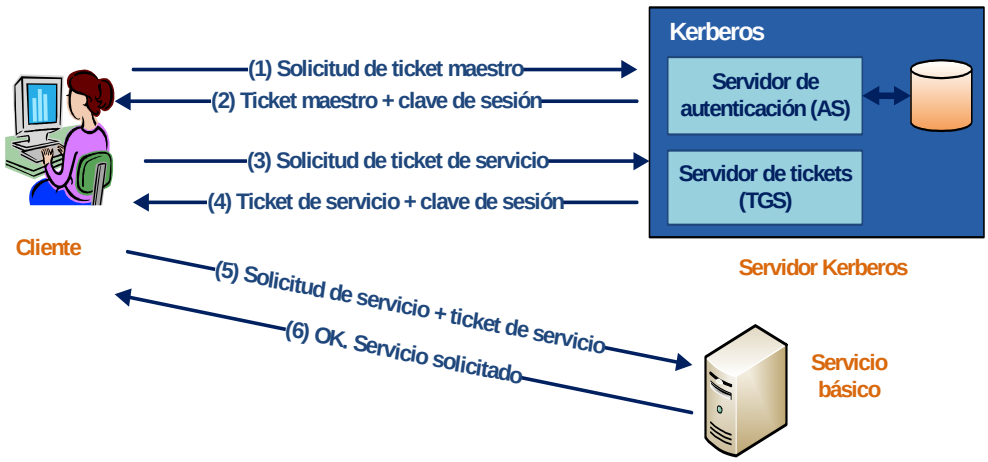

Fig. 1. Esquema genérico de las interacciones necesarias con el servidor Kerberos para la obtención del ticket maestro y ticket de servicio durante la fase de autenticación

No obstante, una de las limitaciones del protocolo Kerberos es que únicamente alcanza a garantizar a las aplicaciones finales la identidad de los usuarios, pero no proporciona ninguna información a cerca de los permisos de dichos usuarios. Con el objetivo de hacer frente a esta limitación, se ha desarrollado un sistema de autorización centralizado que permita completar las funcionalidades ofrecidas por el protocolo Kerberos para ofrecer una solución de seguridad completa e independiente de las aplicaciones finales.

III. Fase de autorización

El problema de la autenticación en sistemas distribuidos ha recibido mucha atención en los últimos años por parte de la comunidad investigadora, sin embargo, la autenticación es sólo un paso en el proceso de garantizar que cada usuario acceda únicamente a aquellos datos o servicios para los cuales tenga permiso. A pesar de que los problemas de autenticación y de autorización en sistemas distribuidos están fuertemente ligados, el esfuerzo invertido en desarrollar mecanismos de autorización seguros para este tipo de entornos no ha sido tan significativo como en el caso de los mecanismos de autenticación.

En este sentido, cabe mencionar que la mayoría de las soluciones de autenticación y autorización existentes hoy en día tienden a implementar las funcionalidades de autorización de forma local en los sistemas finales. Sin embargo, en entornos

como los NGCWEs no es posible para los sistemas finales mantener información de autorización actualizada a cerca de todos los posibles usuarios participantes en el entorno colaborativo, ya que requieren la interacción entre usuarios y servicios que no se conozcan previamente.

En este tipo de entornos es necesario centralizar los procesos de autorización en un único elemento que dé servicio al resto de los participantes en el sistema, descargando de esta forma a los sistemas finales de la necesidad de mantener información de autorización relativa a cada una de las entidades participantes, así como de la carga de gestión derivada del mantenimiento de dicha información.

Tal y como se explicará más adelante, el escenario para el que se ha diseñado la solución de seguridad está compuesto por múltiples entidades con funcionalidades básicas coordinadas por un elemento central, para formar aplicaciones colaborativas de alto nivel. En este caso, el servicio de autorización centralizado se integrará en el sistema como una más de las entidades básicas que lo componen. Por lo tanto, las funcionalidades de autorización se implementarán mediante un elemento de bajo nivel que se encargará de proporcionar servicios de autorización al resto de entidades del sistema. Esto implica que todas las entidades que participen en el entorno colaborativo delegarán sus decisiones de control de acceso en un elemento externo, el cual llegarán a conocer gracias a la información facilitada por el elemento de gestión centralizado. Así, la securización de este elemento y de las comunicaciones entre el mismo y el resto de las entidades del sistema cobra vital importancia.

Cada vez que un servidor final reciba una petición de un usuario, validará su identidad mediante el procedimiento de autenticación descrito en el apartado anterior. Una vez que el servidor haya obtenido garantías de la identidad del usuario solicitante, tendrá que comprobar si dicho usuario está autorizado a acceder al servicio o datos solicitados, para lo cual hará uso del procedimiento de autorización aquí descrito.

El servidor de aplicación enviará una consulta de autorización al servidor de autorización centralizado, indicándole el nombre del usuario solicitante, así como el del servicio solicitado. El servidor de autorización centralizado comprobará los permisos del usuario indicado en la petición y responderá al servidor de aplicación indicándole si el usuario está autorizado para llevar a cabo la operación solicitada o no.

Al integrarse el servidor de autorización como una entidad más del sistema distribuido, la validación de la identidad de los diferentes servidores de aplicaciones que quieran hacer uso de sus servicios se garantizará gracias al procedimiento de autenticación basado en Kerberos descrito anteriormente, tal y como se muestra en la figura 2.

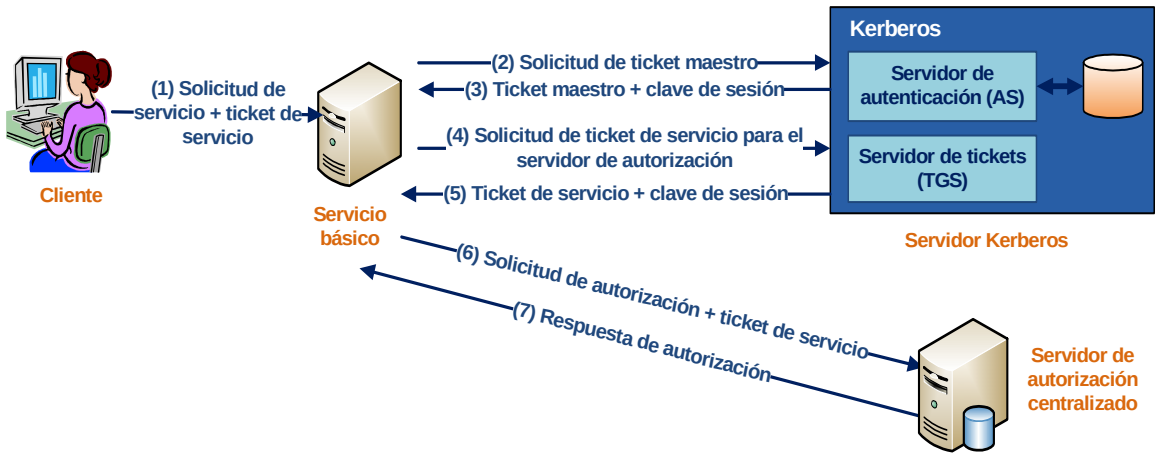

Fig. 2. Esquema genérico de las interacciones necesarias durante la fase de autorización.

Según este procedimiento, cada entidad que quiera solicitar servicios de autorización, tendrá que actuar como cliente del servidor de autorización centralizado y por lo tanto, obtener del servidor Kerberos un ticket de servicio para dicho servidor de autorización. Este ticket estará cifrado con la clave secreta del servidor de autorización, por lo que sólo él será capaz de descifrarlo, e incluirá la identidad del cliente, así como la clave compartida que tendrá que utilizar para cifrar las subsiguientes comunicaciones con dicho cliente. De esta forma se evita que el servidor de autorización centralizado pueda ser suplantado por un impostor, ya que si la petición de algún cliente llegara a un servidor de autorización fraudulento, éste no sería capaz de descifrar el ticket de servicio contenido en la petición y por lo tanto, no podría responder al cliente utilizando la clave compartida incluida en el mismo.

En definitiva, la clave compartida que cada cliente envía al servidor de autorización dentro del ticket de servicio sirve para garantizar la identidad de ambos extremos, así como para proteger la integridad y la confidencialidad de las subsiguientes comunicaciones entre los mismos, ya que será utilizada como clave de cifrado simétrica.

IV. Escenario de validación

El trabajo aquí presentado se ha llevado a cabo en el marco del proyecto integrado C@R "A Collaborative Platform for Working and Living in Rural Areas" del VI Programa Marco. El escenario propuesto en este proyecto se basa en un entorno distribuido compuesto por numerosas entidades que proporcionan funcionalidades básicas y que se conectan entre sí de forma dinámica para construir aplicaciones más complejas. Todas estas entidades básicas se gestionan desde una estructura centralizada donde han de registrarse antes de poder interactuar con el resto. El elemento de gestión centralizado se encarga de coordinar las conexiones entre las entidades básicas, posibilitando así la composición de aplicaciones cooperativas complejas de forma dinámica en base a módulos preescritos.

Con el fin de dotar a las entidades participantes en el sistema de las funcionalidades necesarias para poder llevar a cabo las tareas relativas a la solución de seguridad planteada, se ha desarrollado un módulo software genérico situado entre las capas de transporte y aplicación, donde se engloban todas estas funcionalidades, y que permite a los desarrolladores de las entidades básicas abstraerse de los protocolos de seguridad subyacentes. El esquema de este módulo es el que se muestra en la figura 3.

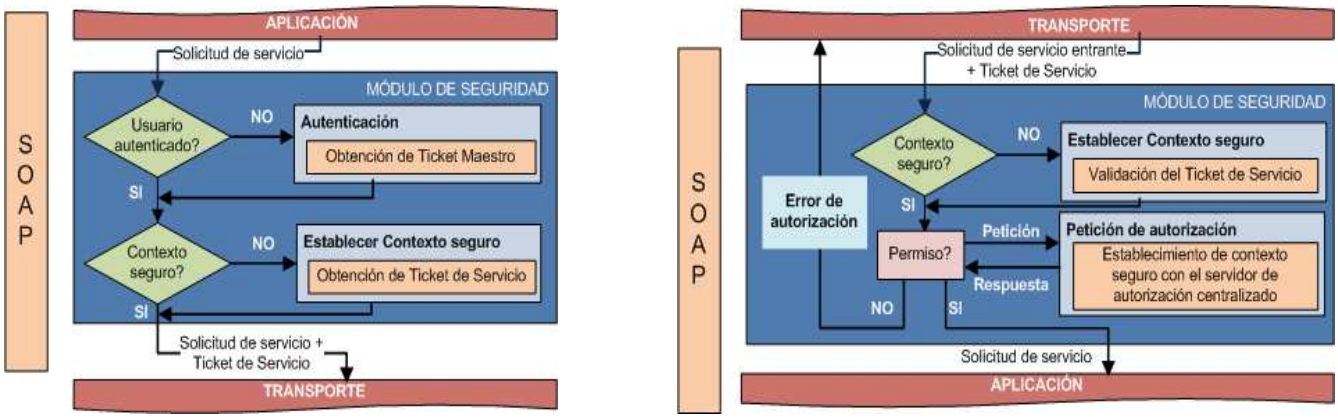

Fig. 3. Arquitectura del módulo de seguridad desarrollado: izquierda, procesado en entidad cliente que envía petición de servicio; derecha, procesado en entidad servidora que recibe la petición de servicio enviada por el cliente.

El desarrollo actual de este módulo cuenta con interfaces basadas en servicios web con el objeto de permitir la comunicación con las aplicaciones de nivel superior. Los servicios web son una tecnología que se basa en el intercambio de mensajes XML sobre SOAP y su principal ventaja es que permite la comunicación de forma sencilla entre diferentes aplicaciones, independientemente de la tecnología en la que estén implementadas cada una de ellas. El módulo de seguridad desarrollado consiste básicamente en una implementación del estándar WS-Security (Web Services Security) [6] de OASIS extendido para soportar funcionalidades adicionales, como por ejemplo, la autorización centralizada.

V. Conclusiones

En este trabajo se ha presentado una arquitectura de seguridad especialmente adaptada a entornos distribuidos en los que se integran elementos de prestaciones reducidas. Un caso típico de este tipo de entornos son los denominados NGCWE, los cuales se basan en promover la colaboración como medio para aumentar la eficiencia y la calidad del trabajo, y que en muchos casos pueden requerir de los trabajadores el uso de sensores que recojan ciertas variables, o de dispositivos móviles de tamaño reducido.

El modelo de seguridad propuesto está principalmente condicionado por las características de los entornos en los que se pretende implantar y se basa en la utilización de criptografía simétrica o de clave privada, y más concretamente del protocolo Kerberos, para posibilitar la autenticación de los usuarios que quieran participar en el entorno colaborativo. La elección de este protocolo se debe a que su eficiencia es mayor que la de las soluciones basadas en infraestructura de clave pública y por lo tanto, se considera este protocolo el más adecuado para ser implementado en sistemas cuya principal característica es su baja capacidad de cómputo y su limitación de recursos.

Sin embargo el protocolo Kerberos no cubre todas las necesidades de este tipo de entornos, ya que no proporciona ninguna solución que haga frente a la gestión de los privilegios de los usuarios autenticados sobre los sistemas finales, obligando a estos últimos a implementar y gestionar sus propios mecanismos de control. En entornos como los NGCWE, compuestos por módulos básicos que se reutilizan para formar aplicaciones colaborativas de forma dinámica, no es posible que las entidades

básicas mantengan información de autorización, ya que una de las características de estos módulos es que sean neutrales e independientes de las aplicaciones de nivel superior. En este trabajo se ha propuesto una solución basada en un servidor de autorización centralizado que da respuesta a la necesidad planteada, y se ha explicado cómo securizar las interacciones del resto de elementos del sistema distribuido con el servidor de autorización centralizado mediante el reaprovechamiento de la solución utilizada para llevar a cabo la autenticación.

Por lo tanto, se ha planteado una solución de seguridad cuyo principal objetivo es descargar a las aplicaciones finales de la necesidad de mantener y gestionar información relativa a los mecanismos de seguridad, e incluso de conocer los protocolos de autenticación y autorización subyacentes. Esto supone un gran ahorro de tiempo y esfuerzos en la gestión de usuarios por parte de los servidores finales, ya que tanto la autorización como la autenticación se llevan a cabo de forma centralizada. Para ello, se ha diseñado un módulo software situado entre la capa de transporte y de aplicación en el que se han implementado todas las funcionalidades de seguridad necesarias y que permite gestionar la autenticación y autorización de los usuarios de forma transparente para las aplicaciones finales.

Por ultimo, hemos de decir también que una ventaja adicional proporcionada por el sistema de seguridad propuesto es que permite implementar soluciones de Single Sign-On, ya que una vez que los usuarios se han autenticado contra el servidor Kerberos y han obtenido un ticket maestro, pueden conseguir todos los tickets de servicio que quieran sin necesidad de volver a autenticarse. De cara al usuario esto supone una gran comodidad, ya que no tiene que introducir su contraseña constantemente, pero además implica también un incremento en la seguridad del sistema completo, ya que si los usuarios han de recordar una única contraseña es más probable que se preocupen de protegerla y almacenarla de forma segura.

AGRADECIMIENTOS

Parte de este trabajo ha sido financiado por el proyecto integrado C@R “A Collaborative Platform for Working and Living in Rural Areas” (FP6-2004-IST-5 IP) del VI Programa Marco.

REFERENCIAS

[1] I. Laso-Ballesteros, “Collaboration@work. At the crossroad of old technology and new IT trends”, *14th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprise,* pp. 55-65, June 2005.
[2] IETF RFC 3280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
[3] IETF RFC 1510 – The Kerberos Network Authentication Service (V5).
[4] W. Stallings, *Network and internetwork security: principles and practice,* pp. 107-136, New Jersey: Prentice-Hall, Inc. 1995.
[5] M.T. EI-Hadidi, N. H. Hegazi, H. K. Aslan, “Performance analysis of the Kerberos protocol in a distributed environment”, *Proceedings, Second IEEE Symposium on Computers and Communications,* pp. 235-239, July 1997.
[6] WS Security Kerberos Token Profile, http://www.oasisopen.org/committees/download.php/16788/wss-v1.1-spec-os-KerberosTokenProfile.pdf.