GESTIÓN DE SEGURIDAD EN ENTORNOS DE APLICACIONES BIOMÉDICAS

A Miguel, I Martínez, JM Nuez, JL Salazar, J Ruiz, J García

Grupo de Tecnologías de las Comunicaciones, Dept. IEC, CPS. Universidad de Zaragoza. España

RESUMEN

La seguridad en las redes inter-hospitalarias es un elemento crítico en el diseño de aplicaciones biomédicas. Este trabajo presenta un entorno de comunicaciones que integra un servidor web seguro, que permite autentificar el acceso y garantizar la confidencialidad de los datos clínicos, junto con un servidor de aplicaciones, que incluye acceso a bases de datos multimedia y técnicas avanzadas de análisis de señales electrocardiográficas.

1. INTRODUCCIÓN

Las redes de comunicaciones en entornos sanitarios presentan aspectos críticos en cuanto a requerimientos de fiabilidad y seguridad que es preciso proporcionar. El carácter altamente privado de la información que circula por estas redes impone la aplicación de mecanismos que incluyan desde la limitación de los accesos a la propia red, hasta la codificación y cifrado de la información de los pacientes que se almacena en las bases de datos. Los aspectos básicos que deben cumplir este tipo de sistemas son: *confidencialidad* de la información intercambiada, esté firmada o no; *integridad*, para prevenir la modificación deliberada o no de los datos firmados; a*utentificación*, para asegurar la identidad del firmante y garantizar el acceso seguro, evitando la suplantación; *no repudio*, para impedir el retracte o niegue de un documento firmado; y *auditabilidad*, para identificar y rastrear operaciones [1].

La comunicación segura de los datos médicos a través de redes telemáticas inter-hospitalarias ha demostrado ser una necesidad muy extendida y existen diversos antecedentes de diseño e implementación [2, 3]. Incluso el acceso a través de terminales inalámbricos o UVI móviles, hoy en día con cierta limitación de recursos que afecta al tiempo de procesado de datos seguros [4], con la inminente llegada de la telefonía de 3G abre nuevas posibilidades para afianzar el aspecto de la seguridad.

La información relativa al paciente no sólo requiere confidencialidad sino que presenta formatos multimedia de gran tamaño asociados a pruebas médicas. Esto implica diseños de bases de datos que incorporen una gestión de usuarios automática y adaptada a las necesidades médicas y administrativas [5]. Además se precisan sistemas de acceso a técnicas avanzadas de análisis y tratamiento digital de dichas pruebas.

2. DESCRIPCIÓN GENERAL

La estructura general del sistema propuesto se distribuye en dos partes principales: un servidor web de acceso seguro y un servidor de aplicaciones biomédicas con sus correspondientes bases de datos (ver figura 1).

El acceso al sistema vía intranet/internet puede realizarse mediante un navegador web instalado en el ordenador personal o mediante un micronavegador desde un dispositivo portátil o terminal móvil, incluyendo mecanismos hardware de protección, como un *firewall*.

El servidor seguro autentifica al cliente mediante la firma digital. Para ello, una autoridad de certificación expide un certificado para el servidor y otro para cada cliente. Al iniciar una comunicación, el servidor se identifica presentando su certificado y pide al cliente el suyo comprobando que la firma procede de la misma autoridad.

El servidor de aplicaciones integra el servidor de procesado de señales clínicas y los sistemas de almacenamiento: la base de datos y el sistema de ficheros. Permite la gestión de usuarios proporcionando distintas funcionalidades en base a un perfil de cliente, y facilita la implementación de las mismas del diseño del interfaz de usuario, según un modelo MVC *(Model View Controlle*r). Para el acceso a la base de datos se utiliza un *driver* JDBC *(Java DataBase Connectivit*y), mediante un gestor de conexiones *(pool)* que permite mejorar la eficiencia de la aplicación.

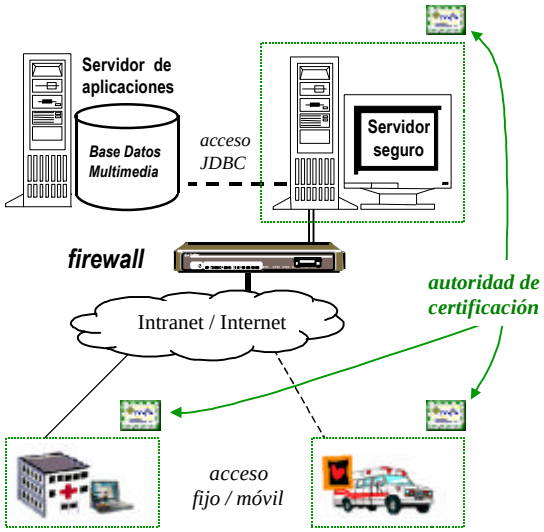


Figura 1. Descripción general del sistema

3. SERVIDOR SEGURO

El proceso de autentificación se realiza mediante una infraestructura de firma digital. La firma digital permite confiar en personas o servidores de información gracias a la confianza que se tiene en la autoridad emisora, que les avala. Así, puede crearse una red inter-hospitalaria segura sobre Internet, con integridad y confidencialidad garantizada, como si de una red local se tratara, con las ventajas de una arquitectura distribuida (ver figura 2).

En el sistema se ha implementado una infraestructura de clave pública o PKI (*Public Key Infrastructure* [6]), que define una estructura jerárquica de autoridades de certificación CA (*Certification Autority*), como se muestra en la figura 3(a). Cada una de las unidades de la red (hospitales), puede tener su propia autoridad de certificación [7], con la información pública accesible en un servidor LDAP (*Light Directory Access Protocol*) [8]. Para poder establecer comunicaciones entre distintas entidades y autoridades de certificación, se necesita un sistema de verificación y gestión de certificados cruzados. Cada autoridad de certificación firma un certificado para las demás de forma que en los árboles correspondientes quedan unidos por sus raíces, como indica la figura 3(b). En los servidores del sistema se protegen los datos para que sólo los poseedores de un certificado permitido, con la categoría adecuada puedan consultar y modificar la información.

El sistema diseñado incorpora un mecanismo propio de verificación de la seguridad de las comunicaciones. Esto está motivado por la inseguridad de los actuales navegadores web, que no actualizan en cada sesión su lista de entidades certificadoras y además suelen tener un código cerrado que oscurece una parte importante del proceso. En el diseño de la unidad de gestión inter-hospitalaria se plantea asegurar escalabilidad del sistema manteniendo la seguridad. Para ello, se proponen tres fases de implantación (ver figura 4):

- *Arquitectura 1*: Consta de una sola máquina, el servidor web seguro. El proceso de autenticación y la entrada principal a todos los servicios residen en él, mientras que los contenidos pueden estar distribuidos en otros servidores.
- *Arquitectura 2*: Consta de un servidor, en este caso trabajando como *proxy*. Se encargaría de las labores de seguridad de comprobación de certificados, pero los servicios ya no estarían centralizados.
- *Arquitectura 3*: Si el tráfico aumenta demasiado se puede optar finalmente por una arquitectura de seguridad distribuida, de forma que cada centro hospitalario tenga su servidor *proxy* seguro. Para no comprometer la seguridad de las arquitecturas anteriores, se aprovecha la evolución de los almacenes de certificados LDAP hacia un modelo distribuido (*Distributed LDAP*), que permite a todos los servidores verificar todos los caminos de certificación en un mismo LDAP virtual, formado por la unión de todos los LDAP del sistema.

4. SERVIDOR DE APLICACIONES BIOMÉDICAS

4.1. Base de datos multimedia

El usuario médico, una vez autentificado, se conecta remotamente al sistema vía intranet/internet. Desde este acceso tiene total funcionalidad para acceder a las páginas web con la información de la base de datos y del sistema de archivos. Esta aplicación sirve como conexión entre hospitales que requieran una información específica de un paciente y permite acceder a las aplicaciones biomédicas desarrolladas (como obtener, e.g. desde un centro de atención primaria, un electrocardiograma (ECG) que fue adquirido en el hospital central y procesarlo).

La aplicación que soporta la base de datos multimedia está basada en el servidor web Apache, el servidor de aplicaciones Apache Tomcat, el gestor de base de datos MySQL, un *driver* JDBC para acceso a la base de datos y un servidor de aplicaciones MATLAB, accesible a través de un CGI propietario de este servidor (ver figura 5).

El *driver* JDBC es de tipo IV ("Pure Java") que a priori ofrece un rendimiento óptimo por acceder directamente a la base de datos, a costa de perder flexibilidad en la aplicación. Un *pool* de conexiones implementado permite la reutilización de las mismas (reduciendo la carga de trabajo de la aplicación) y contrarresta la pérdida de flexibilidad debida al tipo de *driver* utilizado, ya que independiza el código de los elementos limitadores: el *driver* JDBC y la JDBC URL de acceso a la base de datos.

Las páginas web genéricas están diseñadas en código HTML *(HyperText Markup Languag*e), realizando llamadas a elementos dinámicos, enviados al contenedor para su ejecución a través del conector “mod_jk”. El diseño de las páginas dinámicas, que obtienen información actualizada de la base de datos y el sistema de archivos, está basado en lenguaje JSP (*Java Server Pages*), aplicando el modelo MVC que independiza el diseño de la lógica de la aplicación. Estas páginas JSP son ejecutadas en el contenedor Apache Tomcat y son activadas desde las páginas web genéricas que envían los parámetros necesarios para la correcta operación de las mismas. Finalmente, el usuario médico recibe los resultados en el formato adecuado como consecuencia de la lectura y consulta sobre la base de datos y la comunicación con el servidor de aplicaciones.

4.2. Aplicación de teleprocesado de ECG

En este proyecto se ha integrado un prototipo de teleprocesado remoto de señales ECG [9]. La aplicación se basa en un CGI (*Common Gateway Interface*) que envía las señales ECG y los parámetros seleccionados por el usuario al servidor de procesado, el cual los analiza y devuelve los resultados al navegador web en el formato adecuado. Las nuevas técnicas avanzadas de análisis incorporadas pueden ayudar al diagnóstico de diversas enfermedades cardiovasculares.

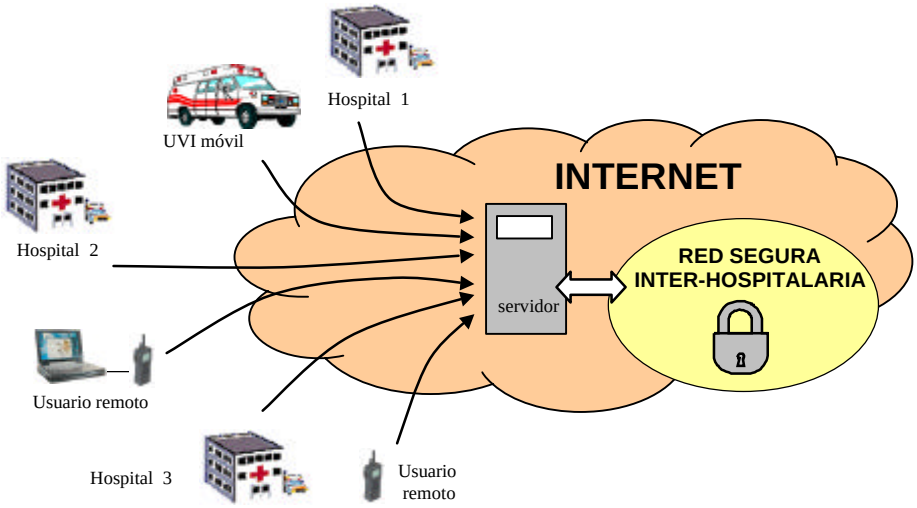
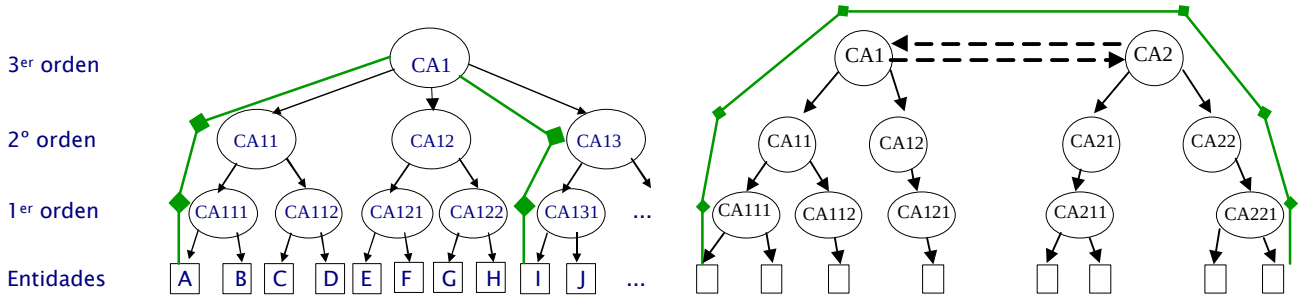


Figura 2. Esquema de red segura sobre Internet.



a) Entre dos entidades dentro de la misma CA. b) Entre dos CA´s distintas con verificación cruzada.

Figura 3. Infraestructura jerárquica PKI y caminos de autentificación.

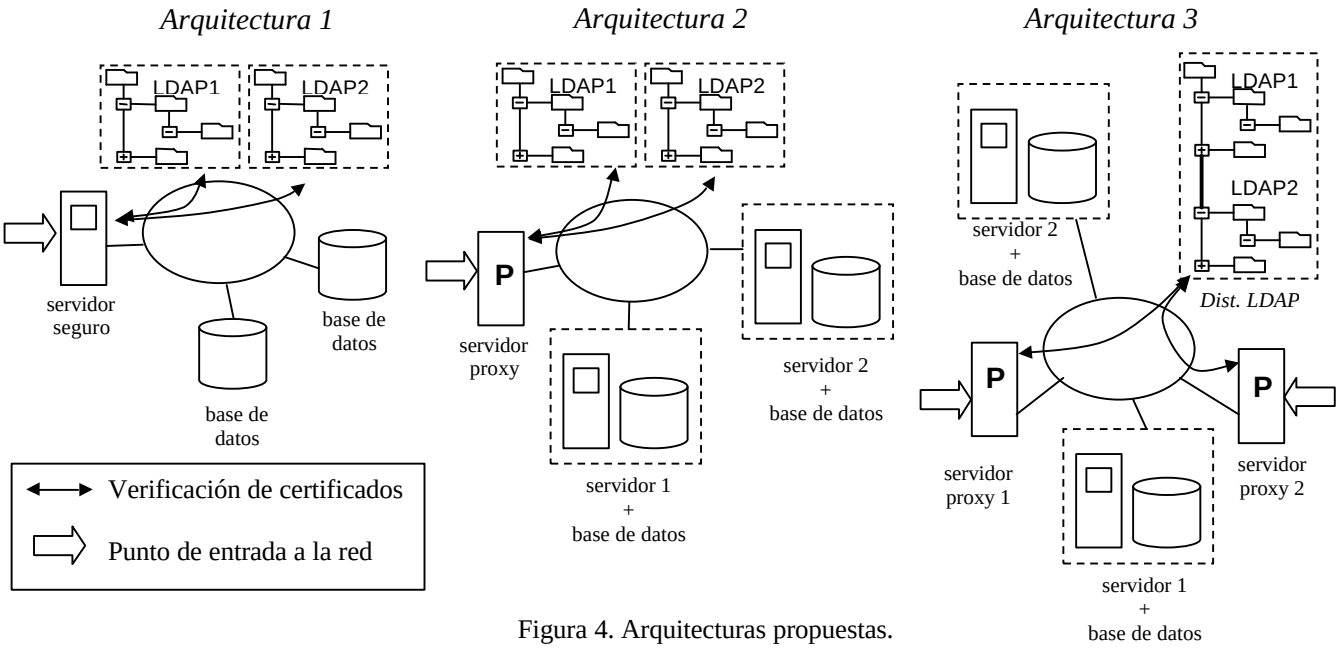


Figura 4. Arquitecturas propuestas.

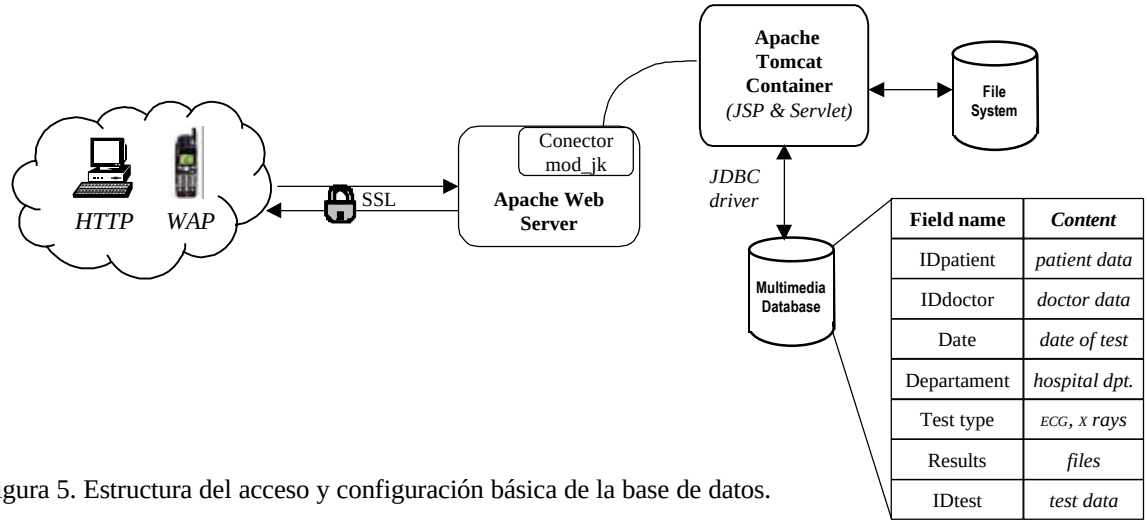


Figura 5. Estructura del acceso y configuración básica de la base de datos.

5. DISCUSIÓN Y RESULTADOS

Se ha diseñado un sistema seguro de acceso remoto conectado a una base de datos multimedia inter-hospitalaria que incluye el acceso centralizado a técnicas avanzadas de teleprocesado de la señal ECG, así como a la información clínica y administrativa de los pacientes.

El servidor seguro se ha implementado siguiendo la arquitectura 1, en la que se ha incluido una CA propia para la emisión de certificados [7]. Este sistema se ha instalado en un entorno de laboratorio donde se han efectuado pruebas de conexiones seguras desde el 'exterior' a través de un *router* y un *firewall*. Con este diseño se puede centralizar el mantenimiento, la administración y la seguridad del sistema. Sin embargo, con objeto de reducir la carga de tráfico en una misma máquina, actualmente se está poniendo a punto la arquitectura 2 (acceso mediante *proxy*). Esta solución basada en servidor *proxy* aportaría más transparencia en el acceso a las aplicaciones biomédicas y flexibilidad de diseño a través de una arquitectura distribuida, como es el caso de entornos hospitalarios.

La base de datos diseñada permite desarrollar la gestión de usuarios automatizando el proceso de transferencia, almacenamiento, gestión dinámica y actualización de la información, y obteniendo estadísticas de acceso que pueden ser de utilidad en la rutina clínica. El acceso a los contenidos a través del servidor seguro, que incorpora un proceso de autentificación y cifrado de la información, posibilita comprobar la identidad del usuario autorizado y garantizar la confidencialidad de los datos clínicos.

Los beneficios de este trabajo incluyen seguridad en el acceso a la información clínica, confidencialidad de los datos del paciente, eficiencia y automatización en el tratamiento de la información biomédica, y una importante mejora en el sistema sanitario garantizando la seguridad y evitando la redundancia de datos y la duplicidad de pruebas clínicas.

6. BIBLIOGRAFÍA

[1] J. Pastor, M.A. Sarasa, "Criptografía digital: fundamentos y aplicaciones", Colección textos docentes, Prensa Universitaria de Zaragoza, 1998.

[2] Bunz H. et al, "Secure multimedia applications and teleservices: Security requirements and protorype for health care", *Proceedings of Multimedia: Advanced teleservices high speed communcication architectures. Second international wokshop.* pp. 224-236, 1994.

[3] Green P.,"PKI: Making the dissemination of electronic healthcare data secure", *Healthcare Information Technology*, pp. 9-20, 2000.

[4] Rosser J.C. et al, "Use of mobile low-bandwidth telemedical techniques for extreme telemedicine applications", *Journal of the American College of Surgeons* , vol. 189, no. 4, pp. 397-404, 1999.

[5] J. García, A, Castaño, I. Martínez, "Acceso Remoto a Bases de Datos Clínicas", *XIX Congreso Anual de la SEIB*, pp. 57-60, 2001.

[6] S. Xenitellis, "The OpenSource PKI Book", *Open CA Team*.

[7] A. Sanz, J. Ruiz, "Diseño de un Servidor Web seguro y de una Autoridad de Certificación mediante SSL y PKI", *XV Simposium Nacional de la URSI*, pp. 671-672, 2000.

[8] http://www.openldap.org/

[9] J. García, I. Martínez, L. Sornmo, S. Olmos, A. Mur, and P. Laguna, "Remote processing server for ECG-based clinical diagnosis support", *IEEE Trans Inf Technol Biomed*, in press.

Antonio Miguel
Dept IEC. CPS. Universidad de Zaragoza
María de Luna 3. 50018 Zaragoza (Spain)
E-mail: amiguel@posta.unizar.es

Este trabajo está siendo financiado por los proyectos TIC2001-2481 y TIC2001-2167-C02-02l de CICYT.