Sistema de Autenticación, Autorización y Registro para aplicaciones basadas en Servicios Web XML

Por Ing. Karel Gómez Velázquez, Jefe Dpto. Sistemas de Gestión Hospitalaria (CESIM); Ing. Annia Arencibia Morales, Analista Ppal. Dpto. Sistemas de Apoyo a la Salud (CESIM); Ing. Danisbel Rojas Ríos, Esp. Centro de Consultoría; e Ing. Héctor Manuel Solis Mulet, Prof. Facultad 7, Universidad de las Ciencias Informáticas (UCI)
kgomez@uci.cu, aarencibia@uci.cu, drojas@uci.cu, hmsolis@uci.cu

1 Introducción

A través del Programa para Informatizar la Sociedad, el estado cubano ha experimentado un incremento en la utilización de las tecnologías de la información en los últimos años, con el fin de alcanzar un mejoramiento en la infraestructura tecnológica para satisfacer las necesidades de almacenamiento y acceso, además de la utilización de la información tanto en la esfera socioeconómica como política.

La informatización del Sistema Nacional de Salud (SNS) está apoyada en estrategias y políticas trazadas por la dirección del país y el MINSAP. Esta es una tarea de vital y prioritaria importancia. Con este proceso, se pretende crear una infraestructura informática para el sector, al que se integrarán todos los productos o servicios, respondiendo a una Arquitectura Orientada a Servicios - Arquitectura Basada en Componentes —del inglés, *Service Oriented Architecture - Component Based Architecture* (SOA-CBA)—. Esta infraestructura integradora permitirá que todas las unidades de salud del país alcancen un nivel de informatización elevado en las actividades que realicen y que influya, directamente, en el aumento gradual de la eficiencia del personal de salud y en la calidad de los servicios que se brinden a la población.

Actualmente la informatización del SNS no ofrece un mecanismo único para la integración. Las instituciones de Salud Pública poseen un conjunto de aplicaciones que ofrecen solución a determinados problemas; pero estos se comportan como islas de información al no poder interactuar entre sí para obtener un flujo lógico y coherente de la información clínica relacionada con los pacientes.

En este sentido, el problema a resolver por el sistema es: ¿cómo fortalecer los procesos de Autenticación, Autorización y Registro en los productos desarrollados para la informatización del Sistema Nacional de Salud cubano? Para resolver esta dificultad se propone desarrollar un Sistema de Seguridad que estandarice estos procesos.

2 Metodología

Un sistema o componente, con el objetivo de gestionar los requerimientos de seguridad en aplicaciones Web, debe apoyarse en algunos elementos esenciales para lograr el propósito de su implementación. Estos elementos consisten, básicamente, en el control de acceso de los diferentes usuarios a las aplicaciones, el cual constituye una poderosa herramienta para proteger la entrada a un sistema completo o sólo a ciertos directorios concretos e, incluso, a ficheros o programas individuales. Este control consta generalmente de dos pasos:

- **Autenticación:** es el proceso de verificación de la identidad digital de un remitente de una comunicación que hace una petición para conectarse a un sistema. El remitente puede ser una persona que usa una computadora u otro medio electrónico, una computadora por sí misma o un programa. En otras palabras, es un modo de asegurar que los usuarios son realmente quiénes dicen ser y que tienen la autorización para realizar funciones en el sistema.

◆ **Autorización:** proceso por el cual se autoriza al usuario identificado a acceder a determinados recursos del sistema, es decir, se comprueba que los usuarios con identidad válida solo tengan acceso a aquellos recursos sobre los cuales tienen privilegios.

Precisamente teniendo en cuenta estas razones, el Sistema de Seguridad implementa una fuerte política de **Registro** gracias a la cual se registran todos los accesos y peticiones realizadas por los usuarios y, además, siempre quedan almacenados un conjunto de datos como: usuario, servicio que consume, componente y dirección IP desde el cual accede, fecha, hora, tipo de traza que genera y una descripción que permite aumentar el nivel de detalles acerca de las acciones de los usuarios. De esta forma, facilita el proceso de análisis de las trazas.

También se pueden realizar búsquedas avanzadas de las mismas. Para ello, el sistema brinda la posibilidad de utilizar varios parámetros para ir filtrando la información, por ejemplo: nombre del organismo al cual pertenece el usuario, nombre del componente, usuario, tipos de traza, periodo de tiempo y rangos de direcciones IP; estos tienen como objetivo hacer más flexible y eficiente la búsqueda. Otra funcionalidad es la creación de reportes en formato PDF que permite imprimir la información y facilita el proceso de registro del sistema, aún cuando no se dispone de una computadora.

Las bases de datos de trazas tienden a crecer con mucha rapidez. Como una vía alternativa para solventar esta realidad, el sistema brinda la posibilidad de eliminar las trazas de los usuarios. Cuando se elimina una, pasa a formar parte de otra base de datos donde se registra con el mismo formato pero bajo la categoría de traza histórica. En caso de ser eliminada, nunca se pierde el control sobre la misma, debido a que es guardada en un fichero en el servidor, lo cual facilita su persistencia futura mediante el uso de dispositivos de almacenamiento externo —CD, DVD o discos extraíbles—. Para complementar este proceso, el Sistema de Seguridad permite recuperar las trazas que una vez fueron eliminadas y que constituyen una porción de información importante en un momento determinado.

2.1 Materiales y métodos

2.1.1 Patrones de arquitectura y diseño

Los patrones arquitectónicos y de diseño utilizados para el desarrollo del Sistema de Seguridad son: Modelo-Vista-Controlador —del inglés, *Model-View-Controller* (MVC)—, Arquitectura en tres capas, Arquitectura Orientada a Servicios y Basada en Componentes [1-2].

2.1.2 Tecnología Servicios Web XML

Teniendo en cuenta la heterogeneidad tecnológica y la diferente distribución física de los sistemas, se definió implementar la arquitectura SOA mediante Servicios Web XML. Los Servicios Web usan SOAP —*Simple Object Access Protocol*— como protocolo para invocar llamadas remotas debido a su simplicidad, se puede identificar un mensaje SOAP como un documento XML conformado por una envoltura obligatoria, un encabezamiento opcional y un cuerpo también obligatorio. Este permite la comunicación entre aplicaciones heterogéneas, de modo que usuarios de diferentes plataformas o lenguajes de programación pueden comunicarse entre sí de manera satisfactoria [3].

Alrededor de los Servicios Web existen protocolos y mecanismos adicionales para facilitar tareas como el descubrimiento de servicios distribuidos a lo largo de la red o UDDI —*Universal Description, Discovery and Integration*—, una descripción del contenido de los mensajes o WSLD —*Web Services Description Language*— el cual describe la forma de comunicación, es decir, los requerimientos del protocolo y los formatos de los mensajes necesarios para interactuar con los servicios listados en su catálogo. Además se utiliza el protocolo HTTP —*Hypertext Transfer Protocol*— para el transporte de la mensajería, utilizando el puerto 80 porque el mismo siempre se encuentra accesible [4].

2.1.3 Single Sign On (SSO)

Los usuarios para identificarse ante varias aplicaciones informáticas son forzados a recordar numerosas contraseñas por lo que en la mayoría de los casos eligen contraseñas sencillas poniendo potencialmente en riesgo la seguridad del sistema. La utilización de una arquitectura SOA tiene como objetivo dar acceso a los usuarios a múltiples servicios Web o aplicaciones. En la mayoría de los casos, se encuentra que cada uno de los servicios o aplicaciones cuenta con su propio componente o mecanismo de seguridad, lo que puede comprometer la seguridad de todo el sistema. El nivel de seguridad de todo un sistema es igual al nivel de seguridad del componente más inseguro que lo integra.

No es más que es un proceso de autenticación de sesión/usuario que permite, mediante un solo conjunto de credenciales, acceder a diferentes aplicaciones. Esto es utilizado, principalmente, en ambientes distribuidos. El proceso autentica al usuario para todas las aplicaciones, al que le ha dado derechos, y elimina todos los mensajes de autenticación que se generan cuando se cambia de interfaz durante una sesión particular.

Este es un elemento de mucha importancia que se tuvo en cuenta en el proceso de desarrollo del Sistema de Seguridad, sobre todo, porque permite el encapsulamiento de la infraestructura de seguridad subyacente y la posibilidad de que los procesos de implementación, despliegue y mantenimiento sean más

fáciles. Ninguna de las partes comunicantes en el sistema distribuido, necesita implementar individualmente todos los mecanismos de seguridad. Este tipo de proceso permite a los desarrolladores y a las organizaciones centrarse en el desarrollo de la lógica de negocio asociada a un componente en particular, obviando los mecanismos de seguridad, debido a que estos serán proporcionados de manera automática por el Sistema de Seguridad en el momento de la integración y el despliegue [5].

2.1.4 Lenguajes utilizados

El sistema se desarrolló utilizando el lenguaje de *script* PHP 5.2.5, particularmente mediante el *framework Symfony* 1.0.8 para garantizar la validación de los datos del lado del usuario *javascript*. Para obtener una interfaz visual moderna y de utilización intuitiva, se empleó la librería de componentes visuales Yahoo User Interface YUI 2.5.0, la cual se integra, fácilmente, con el conjunto de tecnologías AJAX garantizando, de esta manera, una rapidez en la obtención de las respuestas originadas desde el servidor.

2.1.5 Otros elementos utilizados

Teniendo en consideración el volumen de datos que se genera y manipula por un sistema como este, se utilizó como sistema de gestión de bases de datos PostgreSQL 8.3. Uno de los elementos más significativos en este sistema es que está desarrollado sobre tecnologías no propietarias donde los componentes reutilizados poseen licencia de software BSD —*Berkeley Software Distribution*—. De este modo, se garantiza su implantación en cualquier entorno sin costo alguno. El proceso de desarrollo estuvo basado en la metodología RUP —*Rational Unified Process*— y los artefactos generados fueron modelados visualmente mediante UML 2.0 —*Unified Modeling Language* / Lenguaje Unificado de Modelado— en la herramienta CASE Enterprise Architect 7; para ello, se consideran los estereotipos para el modelado de aplicaciones Web [6].

3 Resultados

El Sistema de Seguridad contiene un conjunto de definiciones identificadas que permiten un mayor entendimiento del ejercicio del mismo, siendo estas:

Administrador General: actor que, en dependencia de su nivel de acceso sobre un organismo cuyos requerimientos de seguridad son gestionados por el Sistema, tiene los permisos necesarios para gestionar la información de los usuarios que, en la estructura jerárquica de niveles definada por su organismo, posean un nivel igual o inferior al suyo. Esta gestión incluye crear usuarios, modificar sus datos y privilegios, eliminarlos y realizar búsquedas a partir de diferentes parámetros. Por otra parte, puede realizar un registro estricto a través de las trazas almacenadas por el Sistema, que le permite conocer qué usuario ha participado en cada transacción.

Administrador Configuración: actor que tiene permiso total sobre la configuración del sistema. Único encargado de la gestión de organismos, niveles, ubicaciones, componentes, servicios y roles.

Usuario: actor que interactúa directamente con el Sistema de Seguridad una vez que se hayan superado las fases de desarrollo correspondientes con el objeto de consultar, modificar o eliminar la información gestionada por él.

Componente: es una unidad ejecutable que representa el núcleo de la aplicación, la cual puede ser implantada independientemente y ser a la vez sujeto de composición de terceras partes, es decir, se puede tomar el componente y agregarlo a otro componente en desarrollo o simplemente consumir algunos de los servicios que brinda.

Certificado: conjunto de datos y privilegios de un usuario determinado que se crea de forma automática durante los procesos de autenticación y autorización. El mismo posee un identificador único de treinta y dos caracteres que se genera de manera aleatoria, contiene el nivel de acceso del usuario, el identificador del nivel de acceso y un listado de los componentes a los que tiene derecho de acceso, así como los privilegios de ejecución correspondientes en estos componentes.

Nivel de Actividad: clasificación del usuario que permite diferenciar entre un usuario activo —que está autorizado a utilizar el sistema dentro de un período de tiempo determinado— y uno de tipo inactivo —contrarresta la definición anterior—.

Traza: historial donde se almacenan todos los eventos realizados por el usuario al interactuar con la información perteneciente al Sistema.

Rol: papel que cumple un usuario dentro de un componente y que limita el conjunto de funcionalidades que puede desempeñar en ese ámbito dentro del Sistema.

Servicio: operación proporcionada por un componente determinado.

Organismo: conjunto de dependencias, oficinas o empleos que cumplen con determinadas leyes, usos y costumbres y que, a la vez, forman una institución social.

Nivel: concepto asociado a las diferentes instancias de dirección administrativa de un organismo determinado.

Ubicación: recoge la ubicación exacta del usuario en cada uno de los niveles en que se desempeñe.

Grupo de Nivel: especifica los diferentes niveles que tiene cada uno de los organismos.

Grupo de Rol: se recogen todos los roles que pertenecen a cada organismo.

Período de Actividad: es el tiempo durante el cual el usuario va a estar

en estado activo dentro de la aplicación.

Historial de Traza: se especifican los tipos de trazas definidos que pueden dejar los usuarios.

4 Discusión

Seguridad en las comunicaciones: desde la concepción inicial del Sistema de Seguridad se identificó la necesidad de contar con un canal seguro de comunicación, debido a la importancia de la información que el mismo gestiona y a las consecuencias nefastas que se podrían originar en caso de no tomar las precauciones necesarias para garantizar la seguridad de la información que viaja entre el servidor Web y el usuario. En caso de no tener presente este aspecto, el sistema podría ser víctima de un ataque electrónico que permitiría interceptar el contenido de las comunicaciones TCP/IP comprometiendo la seguridad de las aplicaciones Web que utilicen los servicios que brinda el Sistema de Seguridad.

Por esta razón, se requiere la utilización de protocolos seguros de comunicación como el HTTPS —*Hypertext Transfer Protocol Secure*—. Este protocolo no forma parte del proceso de elaboración propio del Sistema de Seguridad, sino que debe configurarse en el servidor Web donde va a ser instalado el sistema una vez que haya rebasado sus fases de construcción.

Integración con servidores LDAP —*Lightweight Directory Access Protocol*—: generalmente los organismos o instituciones tienen su propia red informática para la comunicación de los diferentes servicios que pudieran brindar o consumir, así como sus propios usuarios ya establecidos con una estructura jerárquica definida. Para acceder a los datos de los usuarios utilizan un servidor LDAP, que puede ser empleado desde distintas plataformas, debido a que su implementación está basada en estándares internacionales y hace que los procesos de búsqueda y de autenticación sean mucho más rápidos y eficientes que un SGBD —Sistemas de Gestión de Bases de Datos— convencional [7].

Teniendo en cuenta estas características, el Sistema de Seguridad, para la gestión de la información de sus usuarios, brinda de forma adicional la posibilidad de conectarse a servidores LDAP, esto permite la reutilización de la información en beneficio de las ventajas que proporciona el uso del protocolo LDAP.

Para la conexión a servidores LDAP, se especifican una serie de parámetros de entrada, que permiten la comunicación estándar independientemente del lugar y estructura del servidor que provee la información. Estos parámetros son [8]:

- Dirección IP donde se encuentra el servidor.
- Puerto por el cual se va a establecer la conexión.
- Versión del LDAP.
- Base DN —del inglés, *Distinguished Name* / Nombre Distinguido—: estructura en forma de árbol jerárquico que define la concatenación de los DNS —*Domain Name System* / Sistema de Nombres de Dominio— relativos de las entradas "padre" hasta llegar a la entrada "raíz" del árbol. Un ejemplo de DN pudiera ser —cn=Pedro Pérez, ou= UCI Domain Users, o=uci ,c=cu—
- Usuario y Contraseña registrados en el LDAP para establecer la conexión.
- Filtro de conexión: filtro que permite restringir la búsqueda de una persona en el directorio.

Luego de haber establecido la conexión con el servidor LDAP, se obtiene una serie de parámetros de salida estándares, lo cuales pueden ser utilizados en dependencia de las necesidades del usuario o sistema que consulta el Servidor LDAP. Algunos de estos parámetros son:

- givenname: devuelve el nombre del usuario.
- sn: apellidos del usuario.
- cn: nombre completo del usuario.
- mail: dirección de correo electrónico del usuario.
- mailnickname: nombre de usuario

Publicación de Servicios Web: la implementación de Servicios Web juega un papel protagónico en el Sistema de Seguridad, debido a que ofrece la posibilidad, a componentes externos, de consumir algunas de sus principales funcionalidades independientemente de la plataforma o lenguaje en el que hayan sido desarrollados.

Para publicar un Servicio Web se agrupan las funcionalidades que se deseen brindar como servicios en una o varias clases contenedoras, posteriormente, se especifica la descripción para cada tipo de datos, tanto de entrada como de salida de cada función. Luego utilizando el IDE —del inglés, *Integrated Development Environment* / Entorno de Desarrollo Integrado— para PHP —*Hypertext Preprocessor*—, ZendStudio, se especifica la dirección del fichero donde se encuentran las clases contenedoras, a continuación se selecciona la clase que contiene las funciones que se desean publicar y, finalmente, se describe el servicio en un fichero .wsdl que es la interfaz entre el Servicio Web y los sistemas o usuarios que necesitan consumir alguno de los servicios publicados.

El Sistema de Seguridad brinda los Servicios Web: Autenticar, Autorizar, Búsqueda de Usuarios, Búsqueda de Componentes, Adicionar Traza, Búsqueda de Traza. Seguidamente se muestran datos de los servicios Autenticar, Búsqueda de Usuarios y Adicionar Traza respectivamente, entre los que se incluyen: una breve descripción, parámetros de

entrada y salida, ejemplos sobre cómo consumirlos así como la estructura de la información que devuelven.

5 Beneficios

En sentido general el desarrollo del Sistema de Seguridad proporciona un grupo de beneficios para cualquier aplicación que utilice la arquitectura anteriormente descrita. Entre ellos pueden mencionarse los siguientes:

- Gestión eficiente de requerimientos de seguridad para todos los sistemas informáticos que consuman sus servicios de Autenticación, Autorización y Registro. Ofrece facilidades de mantenimiento a estos sistemas y permite la agilización del proceso de construcción de las aplicaciones. Los desarrolladores podrán obviar los mecanismos de seguridad que serán suministrados, de manera automática, por el Sistema de Seguridad en el momento de la integración.
- Aumento de los niveles de integración entre los diferentes sistemas, al evitar que cada uno posea, de forma aislada, la administración de sus usuarios, esta información será almacenada y gestionada de modo centralizado. De igual manera, permitirá organizar los módulos por grupos que facilita la unificación de componentes heterogéneos de acuerdo con su negocio.
- Perfeccionamiento de los procesos de gestión de usuarios y asignación de privilegios.
- Gestión eficiente del proceso de Registro de los productos integrados a él, lo que admite hacer reportes de las trazas históricas en relación con los diferentes parámetros y controlar la acumulación de información de esta naturaleza en las bases de datos.
- Permite la integración con servidores LDAP al facilitar la reutilización de los datos de usuarios de un organismo determinado y evitar, así, la duplicación de la información en la base de datos.

Este Sistema de Seguridad está desarrollado en forma de producto. Su funcionamiento no está limitado a un determinado ambiente de desarrollo, por el contrario, puede ser perfectamente escalable ante cualquier conjunto de tecnologías y requerimientos de software.

Considerando los beneficios generales expuestos, el Sistema Nacional de Salud se favorecerá directamente, pues las aplicaciones desarrolladas para automatizar sus procesos funcionarán en forma integrada, en ese sentido, la atención a los pacientes será rápida y eficiente. También, se garantizará una protección estricta de la información manejada por los sistemas médicos, sobre la base de que la información clínica es muy sensible y no puede ser accedida o divulgada por cualquier persona que interactúe con este tipo de aplicaciones. Igualmente sus usuarios, con un mismo conjunto de credenciales, podrán acceder a cualquiera de ellas debido a que funcionarán como un gran sistema de información en salud integrado tanto para sus usuarios como sus beneficiarios.

6 Conclusiones

Se implementó una solución de software integrada a las diferentes soluciones existentes para la informatización del Sistema Nacional de Salud Cubano que estandariza los requerimientos de seguridad asociados a los procesos de Autenticación, Autorización y Registro. La solución propuesta garantiza una protección estricta de los diferentes niveles de información, de modo que sólo sea accedida por aquellos usuarios a quienes se les hayan asignados las credenciales de acceso necesarias para la gestión de dicha información.

7 Referencias bibliográficas

[1] Aruquipa Chambi, Marcelo G. y Márquez Granado, Edwin P. "Desarrollo de software basado en componentes". Postgrado en Informática - Maestría en Ingeniería del Software, Universidad Mayor de San Andrés, La Paz, Bolivia. 2007. http://www.postgradoinformatica.edu.bo/enlaces/investigacion/pdf/INGSW3_23.pdf. (acceso noviembre 8, 2008).

[2] Jacobson, Ivar, Booch, Grady y Rumbaugh, James. *El proceso unificado de desarrollo de software*. La Habana, Cuba: Editorial Félix Varela., 2004, págs. 4, 5, 6 y 7.

[3] Gudiño Fleites, Pedro. *Tutorial de Sistemas Distribuidos I*. México: Departamento de Sistemas y Computación, Instituto Tecnológico de Colima, 2004. http://www.itcolima.edu.mx/profesores/tutoriales/sistemas_distribuidos_I/sd_u1_1.htm. (acceso noviembre 10, 2008).

[4] Gómez, Karel, González, Leonardo, y Arencibia, Annia. "Centro de Control para el Sistema de Información para la Salud". Trabajo de Diploma para optar por el título de Ingeniero Informático, Universidad de las Ciencias Informáticas, La Habana, Cuba, junio de 2007, pág. 26.

[5] Gómez, Karel, González, Leonardo, y Arencibia, Annia. "Centro de Control para el Sistema de Información para la Salud". Trabajo de Diploma para optar por el título de Ingeniero Informático, Universidad de las Ciencias Informáticas, La Habana, Cuba, junio de 2007, pág. 29.

[6] Navarro Franco, Ángel José. *UML en acción. Modelando aplicaciones Web*. La Habana, Cuba: Instituto Superior Politécnico "José Antonio Echeverría", mayo 2005.

[7] "Sistemas ¿Qué es LDAP?". En *Manual de OpenLDAP en español*. (10/12/2004). http://www.ldap-es.org/contenido/04/12/1.-%C2%BFque-es-ldap%3F. (acceso noviembre 11, 2008).

[8] Rojas, Danisbel, Solis, Héctor M., y Centeno, Karina. "Componente de Seguridad para aplicaciones del Área Temática Sistemas de Apoyo a la Salud". Trabajo de Diploma para optar por el título de Ingeniero en Ciencias Informáticas, Universidad de las Ciencias Informáticas, La Habana, Cuba, junio de 2008, págs. 87, 88 y 89.

8 Anexo

Página principal del sistema para el Administrador de Configuración