Gestión del control de acceso con tecnología open source en proyectos de domótica.

Mariano Emanuel Alejandro López
Departamento de Informática, Facultad de Ciencias Exactas y Naturales y Agrimensura, Universidad Nacional del Nordeste, Corrientes, Argentina.
Asignatura Redes de Datos, carrera LSI.
m_villa@hotmail.com

Leopoldo José Rios
Departamento de Informática, Facultad de Ciencias Exactas y Naturales y Agrimensura, Universidad Nacional del Nordeste, Corrientes, Argentina.
Asignatura Redes de Datos, carrera LSI.
ljr@comunidad.unne.edu.ar

Resumen

Esta línea de trabajo aborda el estudio y despliegue de un sistema domótico gestionado por software, a ser incorporado al Laboratorio LRDTBD del Departamento de Informática de la Facultad como parte de sus estrategias de investigación. Se pretende desarrollar sistemas de control de acceso para instituciones públicas y privadas de la región Nordeste, por ser uno de los problemas más complejos en las administraciones públicas, por diferentes motivos.

En sistemas como el que se propone, es imprescindible el control de acceso y la transferencia de servicios a consumir, para ello es necesario el despliegue de infraestructuras como Active Directory (administración segura de usuarios centralizada), API REST (transferencia de servicios web) y "JWT" (autenticación vía JSON Web Tokens), que resultan atractivas para resolver los problemas mencionados.

El proceso de autenticación utilizado en aplicaciones web, además de ser un aspecto sencillo de desplegar, ha seguido por buen tiempo un patrón común: usuario-contraseña-cookie, sin embargo, esto ha cambiado por motivos relacionados con la forma en que se construyen y distribuyen las aplicaciones modernas. Se busca que el inicio de sesión de usuarios sea realizado por una infraestructura de identidad sólida, de inicio de sesión único, con soporte para redes sociales y soporte corporativo (LDAP).

Palabras clave: Domótica, RBAC, JWT, LDAP, API REST.

Contexto

La línea de Investigación y Desarrollo presentada en este trabajo corresponde al proyecto PI-F17-2017 "Análisis e implementación de tecnologías emergentes en sistemas computacionales de aplicación regional.", denominado Grupo de Investigación en Innovación en Software y Sistemas Computacionales (GIISSC), acreditado por la Secretaría de Ciencia y Técnica de la Universidad Nacional del Nordeste (UNNE) para el periodo 2018-2021, en vinculación al Laboratorio LRDTBD del Departamento de Informática, de la FaCENA. Se pretende dotar al Laboratorio con nuevas y variadas tecnologías informáticas, y lograr la integración de soluciones de hardware, software existente.

Un primer estudio realizado, determinó la factibilidad de poder dar uso a microcontroladores (en este caso Intel Galileo 2.0) en la gestión de software y comunicación de resultados a través de una red de datos [1].

El presente trabajo, será impulsado como parte de sus actividades, por el responsable y adscriptos a la asignatura Redes de Datos del cuarto año de la carrera de Licenciatura en Sistemas de Información (LSI). El enfoque propuesto es dotar al Laboratorio de nuevos y variados servicios informáticos, buscando que las mismas se integren y aporten armonía para su correcto funcionamiento.

I. Introducción

Los aspectos a desarrollar en este trabajo son:

• Domótica. Definida por [2] como la integración de la tecnología en el diseño

inteligente de un recinto cerrado, o mejor aún como el uso simultáneo de electricidad, electrónica, informática y comunicaciones aplicadas a la gestión de las viviendas. Los componentes generales de un sistema domótico a estudiar son: el controlador, el sensor, el actuador y las interfaces.

• Red de datos. Se hace necesario para el despliegue, establecer mecanismos para lograr comunicación entre el controlador mencionado y las distintas aplicaciones de software, los cuales requieren estar enlazados por un determinado medio físico y utilizar un mismo protocolo de comunicación, para lugar a la denominada red de datos [3].

• Protocolos de red. En otro nivel, se requiere la aplicación de protocolos livianos con gestión de infraestructura, como Lightweight Directory Access Protocol o LDAP, conjunto de protocolos abiertos que se utilizan para acceder a la información almacenada de manera segura dentro de una red. Actualmente, LDAP se usa más dentro de organizaciones individuales, como universidades, departamentos gubernamentales y empresas privadas. El servidor de LDAP puede usar una variedad de bases de datos para guardar los directorios, cada uno optimizado para operaciones de lecturas rápidas y reiterativas. La principal ventaja de LDAP es que la información de toda una organización se puede consolidar en un repositorio central [4].

• Control y gestión de acceso. En el nivel de la aplicación informática, se debe garantizar que sólo las personas autorizadas tengan acceso a la información, que la información se mantenga intacta y disponible. El propósito es evitar el uso de la información de manera no autorizada, permitir el uso y modificación de la información por los usuarios autorizados, y preservar la consistencia interna y externa de los datos. La norma ISO 27002 describe varias áreas donde la gestión de acceso a los usuarios debe ser considerada: registro del usuario, gestión de privilegios, administración de contraseñas de usuario y revisión de los derechos de acceso de los usuarios [5].

• Control de acceso basado en roles (RBAC, Role Based Access Control). Técnica que simplifica la gestión de autorización y permisos en diferentes ambientes. Se desea dar reemplazo a sistemas de permisos de acceso que se conceden directamente al usuario, por sistemas de control de acceso basado en roles. Los roles permanecen estables en comparación a los usuarios. El rol de hecho es asociado con un conjunto de opciones de permisos en particular. Cuando los usuarios cambian, los roles solo necesitan ser retirados y reasignados [6].

• Autenticación en aplicaciones. Las aplicaciones web modernas presentan interrogantes a la hora de resolver el proceso de autenticación, al intentar hacerlo con métodos y herramientas convencionales. Las razones tienen que ver con las formas que actualmente se crean las aplicaciones y el entorno en el que se localizan y distribuyen.
El despliegue de las aplicaciones actuales se hace sobre numerosos servidores, localizados en diferentes sitios por motivos de alta disponibilidad y distribución de cargas; se busca aumentar el tiempo de actividad y mitigar situaciones de alta latencia. El efecto secundario que surge es, cuando un usuario accede a una aplicación, ya no se garantiza que siempre esté accediendo al mismo servidor, dado que el usuario puede haber iniciado sesión en un servidor, pero no en los otros en los que se distribuye la aplicación. Queda en este sentido, resolver:

- Autenticación basada en cookies: ha sido el método predeterminado y comprobado para manejar la autenticación de usuarios durante mucho tiempo, la misma es “con estado”. Esto significa que un registro o sesión de autenticación debe mantenerse tanto en el servidor como en el lado del cliente. El servidor necesita realizar un seguimiento de las sesiones activas en una base de datos, mientras que en el front-end se crea una cookie que contiene un identificador de sesión [6].

- Autenticación basada en token: trata de un método "sin estado", el servidor no mantiene registro de qué usuarios están conectados o de la emisión de token. En cambio, cada solicitud al servidor va acompañada de un token que el servidor utiliza para verificar la autenticidad [7].

• Comunicación entre aplicaciones de software. Las aplicaciones single-page, tienden a utilizar técnicas para recuperar y consumir datos JSON de una API REST "Transferencia de Estado Representacional", refiere a un método de transferencia de servicios web que permite a diferentes equipos acceder y manipular representaciones textuales de recursos web mediante un set uniforme y predefinido de operaciones sin estado" [8].
Cuando los datos a comunicar son proporcionados por una API, presenta varias ventajas, una de ellas es que los datos se utilicen en más de una aplicación [9].

II. Líneas de investigación y desarrollo.

En la línea de Ingeniería de Software se proponen las siguientes actividades:

- Utilizar Microsoft Active Directory [10] como repositorio centralizado de usuarios con control de acceso basado en roles.
- Analizar los diferentes productos hardware para desarrollos de domótica.
- Estudiar el set de herramientas necesarias para el desarrollo de software.
- Desarrollar una API REST para la gestionar los actuadores.
- Utilizar JWT [11] para autenticar a los usuarios.
- Desarrollar la interfaz o front-end inicial de la aplicación móvil.
- Configurar una red WiFi para soportar la conexión de dispositivos de usuario.
- Establecer mecanismos de log de todos los procedimientos de comunicación de datos y las formas de monitoreo.
- Proponer formas de reporte de información acerca de las personas que acceden, tiempo de permanencia, entre otros aspectos.

III. Resultados.

Resultados obtenidos. El trabajo presentado en JAIIO 45 [1], determinó la factibilidad técnica de poder gestionar un sistema informático instalado en microcontroladores, y que, en base a mecanismos de comunicación de datos, fue posible la transmisión de información para su posterior gestión. Trabajos previos desarrollados en el curso de la asignatura del año 2017, determinaron:

- la factibilidad de utilizar Raspberry pi 3 [12] como controlador del sistema de domótica,
- el uso del lenguaje de programación Kotlin [13] para el desarrollo del front y back end.
- el uso uso del framework Spring Boot [14] para el despliegue de la API REST.

Bajo estas determinaciones, fue posible implementar la infraestructura, en un esquema como lo muestra la Figura 1, compuesta por:

- MS Active Directory: Gestión y control de usuarios
- Raspberry pi 3: Controlador del sistema de domótica
- API REST sin estado: Transferencia de servicios web y generación de tokens "JWT"
- Interfaz: aplicación front-end Android

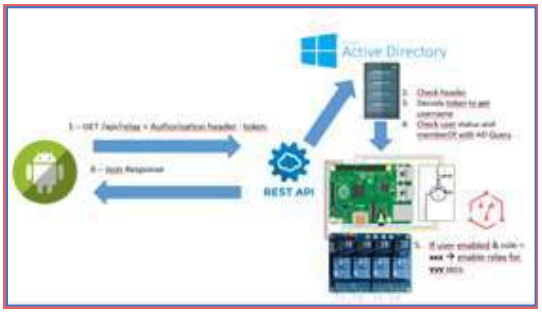

Figura 1. Esquema de funcionamiento.

Resultados esperados. Se está trabajando en la implementación en el laboratorio LRDTBD para dar continuidad a las pruebas.

- Se espera una vez implementada la solución, proponer a las autoridades de la Facultad su uso en modalidad Demo, para el análisis de funcionamiento.
- Los datos obtenidos por el monitoreo podrían ser utilizados por otras asignaturas en actividades de, por ejemplo, Data Mining, análisis estadístico, entre otros.
- Incorporar la funcionalidad de conocer el listado de personas que se encuentran en el edificio, o que hayan ingresado en algún momento determinado, como también su egreso. Si bien no está previsto incorporar el concepto de 'presencia', es decir, saber si una persona está o no en el edificio, es una funcionalidad que puede ser incorporada a futuro mediante por ejemplo la incorporación de tecnologías RfID (Identificación por radiofrecuencia)
- Conectar este sistema, con el servicio (en modalidad demo) de VoIP del Laboratorio LRDTBD, a efectos de poder, por ejemplo, contactar a las personas registradas en el edificio a través de una llamada telefónica VoIP (Voz sobre protocolo de internet).
- Incorporar cuentas de docentes y No-docentes de la Facultad, a la base de datos de usuario de Active Directory, para fortalecer y ampliar las pruebas de funcionamiento.

IV. Formación de recurso humano.

En el Grupo de Investigación en Innovación en Software y Sistemas Computacionales (GIISSC) están involucrados 4 docentes investigadores, un becario de investigación de pregrado, 1 tesista de doctorado y 3 tesistas de maestría.

Para el caso de esta línea de investigación en particular, se encuentra trabajando 1 docente investigador, y 2 Ayudantes Adscriptos (Licenciado en Sistemas de Información) a la asignatura Redes de Datos.

V. Referencias.

[1] Trabajo en 45 JAIIO. http://45jaiio.sadio.org.ar/node/55

[2] R. Hernández Balibrea, Tecnología domótica para el control de una vivienda, Cartagena: Universidad Politécnica de Cartagena, 2012.

[3] J. Kurose y R. Keith, Redes de Computadoras - Un enfoque descendente, vol. V, Pearson.

[4] M. Heslin, Integrating Red Hat Enterprise Linux 6 with Active Directory, Red Hat Inc, 2013.

[5] T. R. Peltier, «Information Security Fundamentals,» *Taylor & Frances Group,* nº 2a, 2014.

[6] J. Yang-Feng, Z. Si-Yue, H. Zhen, L. Mu-Qing, Y. Ling y N. Jing-Ping, «Access control for rural medical and health collaborative working platform,» *The Journal of Chine Universities of Posts and Telecommuni-cations,* nº 20, 2013.

[7] Auth0, «https://auth0.com/,» Auth0, 31 Mayo 2016. [En línea]. Available: https://auth0.com/blog/cookies-vs-tokens-definitive-guide/.

[8] C. Pautasso, E. Wilde y R. Alarcon, REST: Advanced Research Topics and Practical Applications, 2014.

[9] L. Richardson y M. Amundsen, RESTful Web APIs, O'Reilly Media, 2013.

[10] Microsoft, «Microsoft AD,» Microsoft, [En línea]. Available: https://support.microsoft.com/es-es/help/196464.

[11] Auth0, «JSON Web Token,» Auth0, [En línea]. Available: https://jwt.io/.

[12] Raspberry, «https://www.raspberrypi.org/,» https://www.raspberrypi.org/products/raspberry-pi-3-model-b/.
[13] Jet Brains, «https://kotlinlang.org/,» Jet Brains, [En línea]. Available: https://kotlinlang.org/.
[14] Pivotal, «spring,» Pivotal Software, [En línea]. Available: https://projects.spring.io/spring-boot/.