DESAFÍOS DE PRIVACIDAD Y SEGURIDAD IoT PARA ENTORNOS DOMÉSTICOS INTELIGENTES

Ing. Flores Montaño Luis Alberto
Estudiante de Maestría en Informática SEPI UPIICSA
Email: luisfloresmontano@hotmail.com

Lic. Aline Militzin Rojas Perea
Estudiante de Maestría en Doncencia ALIAT
Email: alinerojasp@hotmail.com

Dr. Álvarez Cedillo Jesús Antonio
Profesor de Maestría en Informática SEPI UPIICSA
Email: jaalvarez@ipn.mx

Resumen/Abstract

A menudo, Internet of Things (IoT) se considera como un único dominio de problemas, con soluciones propuestas destinadas a ser aplicadas en una amplia gama de aplicaciones. Sin embargo, las necesidades de privacidad y seguridad de la infraestructura de ingeniería crítica y las operaciones comerciales sensibles son muy diferentes a las necesidades de un entorno doméstico inteligente. Además, los recursos financieros y humanos disponibles para implementar la seguridad y la privacidad varían mucho entre los dominios de la aplicación. En entornos domésticos, los problemas humanos pueden ser tan importantes como los problemas técnicos. Examinando las soluciones existentes para mejorar la seguridad de IoT, el documento identifica los requisitos futuros clave para los sistemas de una "Smart Home" o Casas Inteligentes confiables. Para esto, se selecciona una arquitectura de puerta de enlace, adecuada para dispositivos con recursos limitados y para una alta disponibilidad del sistema. Se identifican dos tecnologías clave para ayudar a la administración automática del sistema. En primero es la compatibilidad con la configuración automática del sistema, el cual, mejorará la seguridad de este. Y el segundo es acerca de la actualización automática del software y firmware del sistema, para lo cual es necesario mantener el funcionamiento seguro del sistema en curso.

I Introducción

El Internet ha pasado de ser una herramienta de investigación útil para las universidades a tener una utilidad fundamental, tan importante como la electricidad, el agua o el gas. Así, donde quiera que haya un recurso valioso, también existe el crimen que busca obtener valor del uso ilícito de esa tecnología, o negar el uso de ese recurso a otros.

La naturaleza interconectada de Internet significa que los recursos de Internet pueden ser atacados desde cualquier lugar del mundo, y esto hace que la ciberseguridad sea un tema clave, este último término gira en torno a tres temas principales, confidencialidad, autenticación y acceso.

Por otro lado, actualmente la siguiente faceta del internet está orientada a controladores conectados a esta., conocidos como "El Internet de las cosas" o por su término en inglés

"Internet of Things" (IoT), dichos dispositivos han obtenido relevancia en los últimos años como un término para describir la conexión de dispositivos no tradicionales, como maquinaria de fábrica, equipos médicos o electrodomésticos, al Internet. En las últimas décadas, el uso de controladores basados en microprocesadores en aplicaciones desde tostadoras hasta aviones se ha vuelto omnipresente en la sociedad.

Como dato importante, la Comisión Europea reconoce que IoT será responsable de futuras tecnologías disruptivas. Y en el 2008, el Consejo de Inteligencia Nacional de EE. UU. Enumeró el Internet of Things como una de las "seis tecnologías con posibles impactos en los intereses de EE. UU. Hasta 2025" (Yu, Lu, Zhu, 2012).

Por lo que ahora, que el Internet se ha convertido en un componente de misión crítica de las empresas modernas, la ciberseguridad se ha convertido en un componente indispensable de los sistemas de información. Sin embargo, a medida que se mejora la ciberseguridad, el cibercrimen está evolucionando para ser más extenso, más destructivo y más sofisticado.

Al igual que todas las áreas de la informática en red, la seguridad y la privacidad son los requisitos principales para el funcionamiento confiable del sistema en IoT. Muchos de los principios de seguridad informática son aplicados a los sistemas IoT, pero enfocados a la seguridad empresarial. Por otro lado, existe también un área emergente de interés que se investiga en este documento, esta es la aplicación de IoT aplicadas en Casas Inteligentes o "Smart Home". Se toma como tema de investigación este tipo de aplicaciones ya que, mientras que las empresas pueden dedicar recursos profesionales específicos a la seguridad del sistema y a los diseños de arquitectura del sistema; las Casas Inteligentes son a menudo un sistema relativamente sin interés, que no cuenta con recursos de gestión dedicados a la seguridad, y sin un profundo conocimiento técnico por parte del propietario. Esto presenta desafíos particulares para la seguridad y la privacidad de estas. Las soluciones propuestas en esta investigación de alguna manera abordan las preocupaciones de seguridad, sin embargo, todavía hay áreas en las que se necesita más trabajo.

Las dos principales contribuciones del documento son resumir las técnicas de red existentes que se pueden usar para proteger las Casas Inteligentes, y posteriormente presentar dos áreas una de la configuración automática del sistema y la otra de actualizaciones de seguridad.

II Contenido del artículo

La tecnología IoT está teniendo un impacto disruptivo en una amplia gama de industrias que incluyen entretenimiento, restaurantes, transporte público, deporte y fitness, telecomunicaciones, fabricación, hoteles, educación, ciencias ambientales, robótica y venta minorista. Se puede proporcionar soporte de Tecnologías de la Información (TI) especializado en el personal o de proveedores externos para garantizar que la seguridad y disponibilidad de sus sistemas sea suficiente para sus necesidades comerciales.

Sin embargo, a menudo, no hay soporte profesional continuo en las fases de diseño u operación en cuanto a la implementación de IoT en las Casas Inteligentes. Si bien existen algunos estándares de Casas Inteligentes especializados razonablemente extendidos, como las comunicaciones X.10 powerline-carrier, estos carecen de cualquier tipo de seguridad, y fueron diseñados antes de que estas redes de control domiciliario estuvieran conectadas a Internet [2]. Ahora hay una gran cantidad de estándares de red que se pueden usar en un hogar como: Zwave, Insteon, Bluetooth, Zigbee, Ethernet, Wifi, RS232, RS485, C-bus, UPB, KNX, EnOcean, Thread (Thubert,2011).

Las Casas Inteligentes potencialmente proporcionan una “comodidad” y “seguridad” adicional, así como una mayor sostenibilidad ecológica. Por ejemplo, un sistema inteligente de aire acondicionado puede usar una amplia variedad de sensores domésticos y fuentes de datos basadas en la web para tomar decisiones operativas inteligentes, en lugar de simples esquemas de control manual o de horario fijo. El sistema de aire acondicionado inteligente puede predecir la ocupación esperada de la casa mediante el seguimiento de los datos de ubicación para garantizar que el aire acondicionado alcance el nivel de comodidad deseado cuando la casa está ocupada y ahorra energía cuando no lo está.

Además, las Casas Inteligentes puede ayudar con la vida independiente para el envejecimiento para más comodidad, así como ayudar con las tareas diarias, como la limpieza, la cocina, las compras y la lavandería. Sin embargo, probablemente ninguno de estos beneficios se utilizará si el sistema la Casa Inteligente no es seguro y confiable.

Vulnerabilidades

Una vulnerabilidad significativa es el acceso al sistema en red. Debido a que los sistemas modernos de Casas Inteligentes están conectados a Internet, los ataques se pueden llevar a

cabo de forma remota, ya sea por acceso directo a las interfaces de control en red o descargando malware en los dispositivos.

La accesibilidad física del sistema también se puede considerar como una vulnerabilidad, como es el caso de los controladores de dispositivos, los cuales, han sido tradicionalmente pequeños microcontroladores de 8 bits con recursos de cómputo y almacenamiento muy limitados, lo que limita su capacidad para implementar algoritmos de seguridad complejos.

Otra vulnerabilidad en cuanto a los dispositivos viene de fábrica, con diferentes estándares de red y diferentes capacidades de actualización de software. A menudo, los dispositivos tienen poca o ninguna documentación sobre su software interno, sistemas operativos y mecanismos de seguridad instalados.

Sin embargo, se puede considerar que la mayor vulnerabilidad, es la falta de profesionales de seguridad dedicados a administrar las complejidades de una red de una Casa Inteligente. Por lo que, en la mayoría de los casos, los dueños de este tipo de casas no solicitan la asistencia profesional continua de administración de la red doméstica, en cambio, los dueños de hogares aficionados deben ser capaces de autogestionar sus sistemas de forma sencilla y segura.

Algunos soportes de seguridad existentes para IoT

Debido a su bajo costo, los dispositivos informáticos IoT generalmente no son tan poderosos como las computadoras de escritorio y portátiles tradicionales. Adicionalmente, la mayoría de los dispositivos IoT son de baja energía, usando un microcontrolador de gama baja y teniendo una memoria limitada. Dichos controladores están bien adaptados a los requisitos de los controladores independientes en una lavadora o aire acondicionado.

Sin embargo, estas características han hecho que el paso a los controladores de IoT en red sea más desafiante ya que los protocolos de Internet existentes generalmente no están diseñados para estos dispositivos integrados. Varios grupos de trabajo de la Fuerza de trabajo de ingeniería de Internet (IETF) se han creado para abordar estos problemas. El trabajo de estandarización de IETF en IoT ha desempeñado un papel vital en el establecimiento de los protocolos de comunicación ligeros necesarios para entornos restringidos a través de la red IP existente. Estos incluyen IPv6 sobre redes inalámbricas de área personal de baja potencia (6LoWPAN: RFC 6282) (Brandt,2010), protocolo de enrutamiento IPv6 para redes de baja potencia y pérdidas (RPL: RFC 6550) (Shelby,2014) y protocolo de aplicación restringida (CoAP: RFC 7252) (Raza,2011).

Arquitectura para la infraestructura

Esta investigación está más enfocada a la gestión del sistema de la seguridad de Casas Inteligentes, es decir, cómo instalar y mantener adecuadamente la seguridad habilitada, para esto, se involucra una adecuada arquitectura para la infraestructura de una Casa Inteligente. Existen diversas propuestas para las arquitecturas de Casas Inteligentes, las cuales tiene problemas de seguridad particulares y dificultades de instalación; tres de estas arquitecturas más importantes y populares son las siguientes:

- **Middleware -.** Esta capa de software que se encuentra entre la capa de dispositivos de bajo nivel y la capa de aplicaciones de alto nivel. Por lo general, proporciona una interfaz común y una estructura de intercambio de datos estándar para abstraer los detalles complejos y varios niveles inferiores del hardware. Cuando el middleware recibe una solicitud de una aplicación de capa superior, convierte la solicitud de acceso a recursos estandarizados de alto nivel a los métodos específicos del dispositivo correspondientes.
- **Nube-.** La nube tiene los recursos para monitorear, recopilar, almacenar y procesar datos de dispositivos IoT. Al analizar estos datos, la nube puede desencadenar acciones de acuerdo con las políticas definidas por el usuario para lograr un control complejo de la Casa Inteligente. La arquitectura basada en la nube de IoT también se conoce como la Nube de las Cosas (CoT). El DTLS es utilizado por esta arquitectura como su protocolo de seguridad para autenticación y comunicación. Este esquema emplea cifrado de clave simétrica para aplicar confidencialidad entre las comunicaciones de extremo a extremo y a cada objeto inteligente se le asigna una clave única. La solución basada en la nube elimina la necesidad de un controlador doméstico separado y proporciona una buena manera para que IoT se conecte y coopere; sin embargo, reemplaza la necesidad de computación local con una necesidad de comunicación sustancial por Internet.

- **Puerta de Enlace-.** Esta investigación maneja dos mejoras que se necesitan para una arquitectura de Casas Inteligentes basada en la puerta de enlace para que sea lo suficientemente segura para su adopción generalizada. Por lo que se presentan algunas arquitecturas generales como prototipo del sistema, el cual, es un primer paso hacia las soluciones a las problemáticas con la seguridad de las casas inteligentes.

Soporte de autoconfiguración

Como se había mencionado, esta investigación está enfocada a la gestión del sistema de la seguridad de Casas Inteligentes, una práctica para esto es una arquitectura adecuada, sin embargo, también existe el soporte de autoconfiguración, para mantener adecuadamente la seguridad habilitada.

Se espera que cada vez más electrodomésticos inteligentes se interconecten a las redes de una Casa Inteligente. La falta de soporte técnico es el mayor desafío en el entorno familiar. En la mayoría de las situaciones, los propietarios se fastidian por manuales tediosos, repetitivos por lo que están propensos a errores para agregar y administrar estos dispositivos inteligentes en su red doméstica, lo que puede representar un gran riesgo para la seguridad. Por lo tanto, para la implementación exitosa de una casa inteligente, se debe estudiar más a fondo un enfoque de autoconfiguración segura, no solo para simplificar la instalación y el mantenimiento del dispositivo en la Casa Inteligente, sino también mejorar la seguridad en el proceso de autoconfiguración.

Para la propuesta de seguridad para las Casas Inteligentes, debe existir una configuración automática, basada en dos componentes clave. El primero se implementa como un servicio basado en web. O bien el fabricante o un tercero de confianza, mantiene las últimas versiones del software y el firmware, las cuales pueden enviarse a pasarelas para ser identificadas durante el proceso de autoconfiguración. El servicio web puede distinguir entre vulnerabilidades en el sistema operativo o el código de aplicación de dispositivo específico, y puede descargar parches para cualquiera de ellos. La puerta de enlace administra el proceso de actualización localmente. La puerta de enlace puede programar automáticamente estas actualizaciones en horarios convenientes a nivel local. La puerta de enlace también puede administrar la actualización de la información de reversión si la instalación de la actualización resulta una pérdida inesperada de la funcionalidad cuando la puerta de enlace realiza pruebas automatizadas del software actualizado. La puerta de enlace también puede responder automáticamente a vulnerabilidades críticas, por ejemplo, bloqueando el acceso a la red a un dispositivo inseguro hasta que haya un parche disponible.

III. Conclusiones

El Internet de las cosas no es un único dominio de aplicación, y los enfoques de seguridad utilizados en una aplicación doméstica inteligente son bastante diferentes de los que pueden ofrecer en las aplicaciones de la industria. Un problema particular es que la seguridad de la red depende de la instalación y configuración por parte de personal. Esto hace que las políticas y los mecanismos de seguridad efectivos sean mucho más difíciles de desarrollar, implementar, cumplir y mantener, a menos que esto se pueda hacer automáticamente. Una arquitectura en la puerta de enlace para la Casa Inteligente soportada por servicios web para la configuración automática de red, dispositivos y actualizaciones automáticas del sistema es un enfoque viable para resolver problemas de seguridad.

Referencia y Recursos Electrónicos

1. Yu, L.; Lu, Y.; Zhu X; (2012). “Tecnologías civiles disruptivas, Seis Tecnologías con Potencial de Impacto en los intereses de Estados Unidos hasta el 2025”; Consejo Nacional de Inteligencia-NIC”; Washington D.C, Estados Unidos, 2008.

2. Yu, L.; Lu, Y.; Zhu X; (2012). “Tecnologías civiles disruptivas, Seis Tecnologías con Potencial de Impacto en los intereses de Estados Unidos hasta el 2025”; Consejo Nacional de Inteligencia-NIC”; Washington D.C, Estados Unidos, 2008..

3. Brandt, A.; Hui, J.; Kelsey, R.; Levis, P.; Pister, K.; Struik, R.; Vasseur, J.P.; Alexander, (2010); Protocolo de enrutamiento IPv6 para redes de baja potencia y pérdida de energía; Internet Engineering Task Force; California, Estados Unidos.

4. Shelby, Z.; Hartke, K.; Bormann, C.; (2014). El protocolo de aplicación restringido (Coap); Internet Engineering Task Force: Fremont, CA, USA.

5. Raza, S.; Duquennoy, S.; Chung, T.; Yazar, D.; Voigt, T.; Roedig, U. ; (2011), Asegurando la comunicación en 6lowpan con Ipsec comprimido ". En actas de la Conferencia Internacional de 2011 sobre Informática Distribuida en Sistemas de Sensores y Talleres, Barcelona, España.