Los nuevos retos de la seguridad y privacidad en el internet de las cosas en el hogar

Mtro. Flores Montaño Luis Alberto
Exalumno de Maestría en Informática
SEPI UPIICSA

Lic. Aline Militzin Rojas Perea
Estudiante de Maestría en Docencia ALIAT

Dr. Álvarez Cedillo Jesús Antonio
Profesor de Maestría en Informática
SEPI UPIICSA

Imagen proporcionada por el autor

Resumen

El Internet de las cosas (en inglés "Internet of Things" o IoT) es considerado una de las tecnologías más innovadoras, sin embargo, debido a su arquitectura computacional de bajo procesamiento, presenta un problema para la implementación de protocolos de seguridad. Por ello, ha generado diversas propuestas de soluciones en variadas aplicaciones que utilizan estos dispositivos, considerando que las medidas de seguridad implementadas a las aplicaciones de uso doméstico son distintas a las de operaciones comerciales, y tomando en cuenta los recursos financieros y humanos disponibles para implementar la seguridad y privacidad.

El problema en la seguridad del internet de las cosas en las casas inteligentes suele deberse, en muchas ocasiones, a error humano; no obstante, también influyen considerablemente los errores técnicos en esta tecnología. Por lo tanto, en este artículo se examinan las soluciones existentes para mejorar la seguridad en los dispositivos antes mencionados, así como la identificación de requisitos esenciales para la seguridad en los dispositivos en una "casa inteligente", conocida también como "Smart Home".

Para lograr estos objetivos, se selecciona una arquitectura de puerta de enlace adecuada para los dispositivos con un bajo poder de procesamiento; adicionalmente se identifican las tecnologías adecuadas de soporte para la administración automática del sistema. Se identifican debidamente dos principales tecnologías, la primera para la compatibilidad con la configuración automática del sistema, y la segunda para la actualización automática del firmware y software de los dispositivos que forman parte del sistema, el cual es fundamental para el funcionamiento adecuado y seguro.

Palabras clave

Casas Inteligentes, Middleware, Internet de las cosas, Nube de las cosas.

Abstract

The Internet of Things is considered one of the most innovative technologies; however, due to its low processing computing architecture, it is considered a problem for the implementation of security protocols; Therefore, it has generated various proposals for solutions in diverse applications that use these devices. Security measures implemented in applications for domestic use differ from those for commercial operations, considering financial and human resources available to implement security and privacy.

The problem in the security of the internet of things in smart homes is often due to human error; On the other hand, technical errors in this technology also influence considerably. Therefore, this article examines existing solutions to improve the security of the devices, as well as the identification of essential requirements for device security in a Smart Home.

To achieve these objectives, a gateway architecture suitable for devices with low processing power is selected; Additionally, appropriate support technologies for automatic system administration are identified. Two main technologies are duly identified, the first for compatibility with the automatic configuration of the system, and the second for the automatic update of the firmware and software of the devices that are part of the system, which is essential for proper and safe operation.

Keywords

Smart Home, Middleware, Internet of

Things, Cloud of Things.

Introducción

Hoy en día se considera a la Internet como una herramienta fundamental y necesaria para la vida diaria, tomando en cuenta su uso en casi todas las áreas de la sociedad actual; considerada también como una necesidad indispensable como lo son: el agua, gas, gasolina o la electricidad [1]. La esencialidad de este recurso provoca a su vez que exista el crimen en busca de un uso ilícito, afectando a terceros, obteniendo información ilegal, mandando virus (afectando información o diversos equipos informáticos) o simplemente negando el servicio de internet a ciertos sectores de la sociedad [3].

La interconexión de la red de internet implica que pueda ser afectada o atacada desde cualquier parte del globo, haciendo que la ciberseguridad sea algo fundamental para el uso seguro de esta tecnología, teniendo en cuenta los principios de autenticación, acceso y confidencialidad [3].

El internet se encuentra en una etapa orientada a los controladores o dispositivos conectados a esta, conocidos como el "Internet de las cosas" o por sus siglas en inglés como "IoT"; término que ha obtenido una gran relevancia en los últimos años, para describir la conexión en los dispositivos no tradicionales, como es el caso de electrodomésticos, equipos médicos, maquinaria de fábrica e incluso pequeños dispositivos que censan la información en la industria; dispositivos que ahora están presentes en básicamente todos los sectores de la sociedad [2].

Por lo tanto, diversas organizaciones importantes han fijado su atención en esta tecnología, como es el caso del Consejo de Inteligencia Nacional de los Estados Unidos, el cual considera al Internet de las Cosas como una de las "seis tecnologías con posibles impactos en los intereses de los Estados Unidos, hasta el año 2025" [4]; por otro lado, la Comisión Europea ya ha reconocido que en los años venideros el Internet de las Cosas será responsable de las tecnologías disruptivas [2].

Siendo así, el internet se ha convertido en un componente de misión fundamental para las empresas más modernas, por lo que la ciberseguridad se ha convertido en un componente indispensable de los sistemas de la información [2]; cabe destacar que, pese a que la ciberseguridad es mejorada con el pasar de los tiempos, lo mismo ocurre con el cibercrimen. Ambos evolucionan paralelamente, siendo ambos más sofisticados y explotando todos los recursos posibles de los sistemas de información y dispositivos.

Como muchas áreas de las ciencias computacionales, la privacidad y seguridad de la red son requisitos fundamentales para el funcionamiento adecuado y confiable en los dispositivos del Internet de las cosas [4]; sin embargo, estos últimos están enfocados únicamente a la seguridad de los sectores empresariales. No obstante, también existen tecnologías relativamente nuevas y emergentes que han sido puesto en la mira de la ciberseguridad, enfocadas a otros sectores de la sociedad [5], las cuales, han sido puestas en la mira por su vulnerabilidad, siendo así, estas son detalladas en esta investigación, específicamente para aplicaciones utilizadas en las Casas Inteligentes.

Como ya se mencionó, los sectores empresariales dedican una gran cantidad de recursos financieros y profesionales a la parte de la ciberseguridad en dispositivos y sistemas, así

como a los diseños de la arquitectura de los sistemas; por ello, esta investigación se enfoca en la tecnología utilizada en las Casas Inteligentes, la cual comúnmente no es tema de interés para la ciberseguridad [4], lo cual puede constatarse observando que los dispositivos utilizados en este sector no cuentan con recursos de gestión dedicados a la seguridad. Adicionalmente, se debe de tomar en cuenta que, en la mayoría de los casos, los usuarios de esta tecnología no cuentan con un conocimiento técnico profundo para el uso adecuado de dicha tecnología. Lo anterior evidencia los desafíos muy particulares para la privacidad y seguridad en el área; teniendo esta problemática, se presentan soluciones propuestas para este artículo que aborda las preocupaciones en la seguridad y las deficiencias en los sectores donde se deben de atender nichos en la seguridad.

Los aportes en esta investigación son dos principalmente: el primero es hacer un compendio de técnicas existentes en la red, con el propósito de que las Casas Inteligentes puedan ser protegidas de una manera más eficiente; consecuentemente, se detallan dos áreas, una en la actualización de los protocolos de seguridad y otra la configuración automática.

Contenido del artículo

Como ya se mencionó en la parte introductoria de este artículo, el Internet de las Cosas tiene un área muy amplia en diversos sectores, como es el caso del transporte público, restaurantes, entretenimiento, deporte, manufactura, telecomunicaciones, ciencias ambientales, educación, robóticas, ventas minoristas y salud. Para estas tecnologías de la Información (conocidas por sus siglas en inglés "TIC's"), existe personal especializado o en su defecto proveedores externos que garantizan la seguridad de la disponibilidad en los sistemas para las necesidades comerciales sean suficientes en los dispositivos o sistemas utilizados [5], no obstante, es común que el soporte profesional se presente continuamente en las fases de operación o en el diseño de la arquitectura de los dispositivos del Internet de las Cosas en las Casas Inteligentes. Existen estándares especializados como lo son las comunicaciones X 10 powerline-carrier, los cuales no poseen ningún tipo de seguridad, ya que fueron diseñados antes de que las redes de control domiciliario fueran conectadas a la red [4]. Sin embargo; hoy en día existen una gran cantidad de estándares en la red, los cuales, pueden usarse en las Csas Inteligentes como es el caso de las tecnologías como: Bluetooth, Zigbee Zwave, Thread Insteon, , Ethernet, Wifi, RS232, RS485, C-bus, UPB, KNX, EnOcean [5].

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 pueden ayudar a aumentar la comodidad de la vida independiente para el envejecimiento, 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. A continuación, se detallan algunas de las deficiencias que se pueden encontrar en los dispositivos de dichas casas.

Vulnerabilidades

Una vulnerabilidad es aquella deficiencia que se puede encontrar en un sistema; eso significa que el acceso del sistema en la red puede ser atacado mediante agentes ajenos o externos al mantenimiento adecuado; dichos ataques se pueden llevar a cabo de forma remota, ya sea por acceso directo a las interfaces de control en red o mediante la descarga de malware en los dispositivos [1].

El hardware del sistema en los dispositivos de las Casas Inteligentes tiene diversas vulnerabilidades, como es el caso de los controladores de estos dispositivos. Dichos controladores son comúnmente microcontroladores muy pequeños de 8 bits con recursos de cómputo, y almacenamiento muy limitados, lo cual limita la capacidad para implementar algoritmos de seguridad muy complejos; otra vulnerabilidad que tienen en los dispositivos viene desde fábrica, ya que contienen diferentes estándares de red y diferentes capacidades de actualización en el software [1].

Algo muy importante que se destaca en esta sección, es la mayor vulnerabilidad para estos dispositivos, ya que, debido a la falta de profesionalismo en la implementación de la seguridad, la complejidad de las redes carecen de protocolos básicos; debido a esto, en diversas situaciones, los propietarios de este tipo de casas no son asistidos por personas expertas en el tema para dar una administración adecuada a la red, por lo que dichos propietarios deben ser capaces de gestionar este sistemas de dispositivos de una manera más intuitiva.

Herramientas de apoyo existentes para la seguridad en el Internet de las Cosas en casas inteligentes

Debido al bajo presupuesto de los dispositivos del Internet de las Cosas, generalmente no suelen ser de un alto rendimiento en el procesamiento, como es el caso de computadoras portátiles o de escritorio; por otro lado, estos dispositivos tienen un costo de energía demasiado bajo, por lo que usan un microcontrolador de gama baja y consecuentemente, se tiene una memoria limitada. Cabe mencionar que estos controladores están muy acondicionados a los requisitos de los dispositivos utilizados en las Casas Inteligentes.

Por otro lado, las características peculiares en los controladores de estos dispositivos en red se hacen más desafiantes, ya que los protocolos de internet que existen hoy en día, por lo general no están diseñados para estos dispositivos integrados. Diversos grupos de ingenieros dedicados en la ingeniería del internet se han dedicado a crear soluciones para abordar este tipo de problemas, en especial el grupo conocido por sus siglas la IEFT (en inglés Internet Engineering Task Force); este grupo de ingenieros ha trabajado en el desempeño de los protocolos de comunicación ligeros, los cuales son necesarios para entornos restringidos a través de la red [3], con el existente protocolo IP. Adicionalmente, también incluyen a los protocolos IPv6, sobre las redes inalámbricas de área personal de baja potencia (conocido por sus siglas 6LoWPAN: RFC 6282) [2], al protocolo de enrutamiento IPv6 para redes de baja

potencia (conocido por sus siglas RPL: RFC 6550) [4] y el protocolo de aplicación restringida (conocido por sus siglas CoAP: RFC 7252) [3].

Arquitectura y diseño para la infraestructura

Para la arquitectura y el diseño de la infraestructura, esta investigación se basa en la gestión de un sistema de la seguridad de Casas Inteligentes, más específicamente, en mantener e instalar la seguridad habilitada, por lo que se involucra una arquitectura adecuada para la infraestructura de una casa inteligente; cabe mencionar que, en la actualidad existen diversas propuestas para dichas arquitecturas, que contienen diversos problemas en la seguridad y dificultades en la instalación.

Las cuatro arquitecturas en las que se basa está investigación son las más comunes e importantes, y que a continuación se especifican:

- **Middleware** -. Esta capa se encuentra entre la capa de aplicaciones de alto nivel y la de dispositivos de bajo nivel; proporciona una estructura de intercambio de datos estándar para abstraer los detalles complejos, así como diversos niveles inferiores del hardware, por otro lado, también proporciona una interfaz común. Dicha capa recibe una solicitud de una aplicación de capa superior, convirtiendo la solicitud de acceso a recursos estandarizados de alto nivel a los métodos específicos del dispositivo correspondientes. En la Figura 1 se muestra la infraestructura del software en la capa de Middleware.

Figura 1. Infraestructura del software Middleware.

- **Nube** -. Una parte importante de la arquitectura en el sistema es la nube, ya que esta contiene recursos para recopilar, procesar y monitorear datos que censan los dispositivos del Internet de las Cosas. Una vez que se analizan estos datos, la nube puede tomar acciones de acuerdo con las políticas definidas por el usuario, esto con el propósito de lograr un control complejo de una casa inteligente. Esta arquitectura también es conocida como Nube de las Cosas (en inglés Cloud of Things-CoT). La seguridad en el datagrama de transporte (en inglés Datagram Transport Layer Securit- DTLS), es utilizado por esta arquitectura como un protocolo de seguridad en la comunicación y autenticación [3]. Este esquema emplea el cifrado en una clave simétrica, con el propósito de aplicar confidencialidad entre las comunicaciones de extremo a extremo, asignando a cada dispositivo "inteligente" una clave única.

En la Figura 2 se muestra una interacción sencilla entre los dispositivos "inteligentes" conectados a la nube.

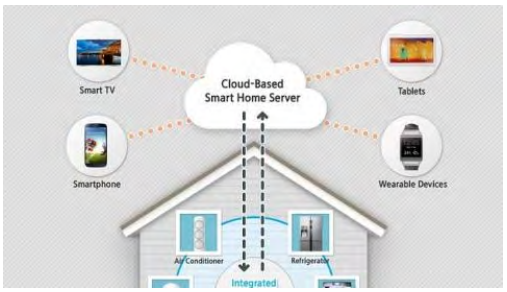

Figura 2. Infraestructura de la nube en una casa inteligente.

- **Puerta de Enlace** -. La puerta de enlace (en inglés gateway) es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación, traduciendo la información del protocolo utilizado en una red, al protocolo usado en la red de destino. En la Figura 3 se muestra la infraestructura de puerta de enlace en una casa inteligente. Posteriormente se detalla la importancia de mejoras en la puerta de enlace con el propósito de que sea suficientemente segura para su adopción en estos dispositivos en las Casas Inteligentes.

Figura 3. Infraestructura de puerta de enlace en una casa inteligente.

- **Soporte de autoconfiguración** -. Otro método para llevar a cabo una buena práctica para la gestión del sistema en la seguridad de las Casas Inteligentes es llevar cabo una arquitectura adecuada; adicionalmente, para esto existe el soporte de autoconfiguración, esto con el propósito de mantener adecuadamente la seguridad habilitada en todo momento.

Un dato importante que hay que tomar en cuenta es que en los años venideros se espera que más electrodomésticos inteligentes estén interconectados a la red de una casa inteligente. Tomando en cuenta que el soporte técnico sea el mayor desafío en un entorno familiar, poniendo a los usuarios en una situación donde pueden encontrar manuales tediosos o fastidiosos, que en su mayor parte provocan que existan errores para administrar y agregar estos dispositivos "inteligentes" a una red doméstica, presentando un riesgo en la seguridad. Por lo que la implementación de dichos dispositivos se debe estudiar a fondo con un enfoque de autoconfiguración segura, no solamente para simplificar la instalación y el mantenimiento estos dispositivos, sino también para mejorar la seguridad en la autoconfiguración.

Para hacer más segura la autoconfiguración, esta debe estar basada en dos componentes clave: uno es la implementación de un servicio basado en web, donde el fabricante o un tercero de confianza se mantienen al tanto de las últimas actualizaciones del firmware y software, las cuales pueden enviarse para ser identificadas durante el proceso de autoconfiguración. Este servicio web tiene la capacidad de distinguir las vulnerabilidades en el sistema operativo o el código de aplicación del dispositivo específico, pudiendo descargar parches para cualquiera de estos, teniendo cabida la puerta de enlace, la cual se encarga de administrar el proceso de actualización localmente.

Adicionalmente, la puerta de enlace puede programar automáticamente estas actua-

lizaciones en horarios convenientes en la hora local, también puede administrar la actualización de la información de reversión si durante la instalación de las actualizaciones resulta una perdida inesperada de funcionalidad, cuando la puerta de enlace está realizando pruebas automatizadas del software. Finalmente, la puerta de enlace también puede responder automáticamente a vulnerabilidades, teniendo como ejemplo el bloqueo de acceso en la red de un dispositivo inseguro, hasta tener un parche disponible para solucionar el problema.

Conclusiones

Los dispositivos del internet de las cosas no tienen un único dominio de aplicación, y los enfoques de seguridad utilizados en las aplicaciones para una casa inteligente son distintas en comparación de las que se ofrecen en las aplicaciones de la industria. Un problema particular que se debe tomar en cuenta es la seguridad de la red, ya que esta última depende de la instalación y configuración por parte de personal, provocando que las políticas y los mecanismos en cuestión de seguridad sean mucho más difíciles de desarrollar, implementar, cumplir y mantener, a menos que todo lo anterior se pueda hacer de manera automática. Finalmente, la adecuada organización en la arquitectura de la puerta de enlace soportada por servicios web para la configuración automática de red, dispositivos y actualizaciones automáticas del sistema se considera un enfoque viable para resolver problemas de seguridad.

Referencias y Recursos Electrónicos

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

2. Raza, S., Duquennoy, S., Chung, T., Yazar, D., Voigt, T., Roedig, U., 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, 2011.

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

4. Thubert, P., Formato de compresión para redes basadas en datagramas Ipv6,, Internet Engineering Task Force, California, Estados Unidos, 2011.

5. Yu, L., Lu, Y., Zhu X, "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.