RIC

Estándar, seguridad, vulnerabilidades y riesgos para la automatización del hogar

Standard, safety, vulnerabilities and risksfor home automation

Cindy Carrizo-Díaz[1] & Miguel Vargas-Lombardo[2*]

[1]Licenciatura en Ingeniería de Sistemas y Computación – Facultad de Ingeniería en Sistemas Computacionales – Universidad Tecnológica de Panamá

[2]CIDITIC-GISES – Universidad Tecnológica de Panamá

Resumen Este artículo busca ampliar conocimientos sobre las vulnerabilidades y riesgos que trae consigo la automatización del hogar. Para lograr este objetivo, se analizaron diferentes elementos del estándar ZigBee: el funcionamiento de ZigBee como estándar de comunicación, la topología de red, la seguridad en el estándar (llaves criptográficas y manejo de las llaves), algunas de las vulnerabilidades que pueden ser encontradas en cada una de las capas del estándar, así como vulnerabilidades específicas propias del estándar.

Palabras claves Automatización, seguridad, riesgos, vulnerabilidades, ZigBee.

Abstract This article seeks to expand knowledge about the vulnerabilities and risks that comes with home automation. To achieve this goal, we analyzed different elements of the ZigBee standard: the ZigBee operation as communication standard, network topology, security in the standard (cryptographic keys and key management), some of the vulnerabilities that can be found In each of the layers of the standard, as well as specific vulnerabilities specific to the standard.

Keywords Automation, security, risks, vulnerabilities, ZigBee.

*** Corresponding author:** miguel.vargas@utp.ac.pa

1. Introducción

Es importante mencionar que la proliferación de las comunicaciones inalámbricas y tecnologías de la información actual han alterado el estilo de vida y las interacciones sociales de los seres humanos [2].

Esta alteración se puede considerar tanto de manera positiva como negativa. Lo que nos lleva a destacar que la Tecnología trae consigo muchos beneficios, pero es importante conocer también que existen ciertos riesgos y vulnerabilidades a las que estamos expuestos si no manejamos adecuadamente la seguridad, sobre todo en dispositivos inteligentes relacionados con la automatización del hogar.

En muchas ocasiones, las implementaciones de comunicaciones en el hogar son normalmente de bajo costo y generalmente sin supervisión, lo que puede exponernos a una serie de ataques potenciales. Estos podrían ser ataques físicos, credenciales comprometidas, ataques de configuración o ataques a la red del hogar [3].

Esta investigación se agrupa en 5 secciones, en la sección 2 se realiza una breve descripción de los hogares inteligentes, seguidamente se presenta el estándar Zigbee caracterizado a los hogares inteligentes, luego se presentan las vulnerabilidades encontradas en el estándar mencionado anteriormente y finalmente, las conclusiones de esta investigación.

2. Hogares inteligentes

Un concepto que surgió desde el año 2004 es el de hogares inteligentes.

La definición de este término demuestra que los seres humanos nos adaptamos cada día más rápido al cambio y al ritmo de la tecnología [4].

Los hogares inteligentes se pueden definir como la introducción de la tecnología en el hogar para mejorar la calidad de vida de sus ocupantes, a través de la prestación de diferentes servicios, tales como la tele-salud, entretenimiento multimedia y la conservación de energía.

Para la realización de esta automatización, se define el estándar ZigBee. A continuación, se definen algunas características de este estándar.

3. ZigBee como estándar de comunicación

ZigBee es un estándar de comunicación inalámbrica, establecido por casi 200 compañías de gran renombre, con el objetivo de unificar tecnologías que permitan entre otras cosas la automatización del hogar. ZigBee fue construido bajo la norma estándar IEEE 802.15.4.

Los campos principales para los que se aplica este estándar son: control remoto, dispositivos de entrada, automatización de edificios, cuidado de la salud, servicios de telecomunicaciones, energía inteligente y automatización del hogar [5].

El estándar ZigBee está compuesto por 4 capas [6]: capa física (PHY), capa de control de acceso medio (MAC), capa de red (NWK), capa de aplicación (APL). La figura 1, muestra la división de las capas de este estándar.

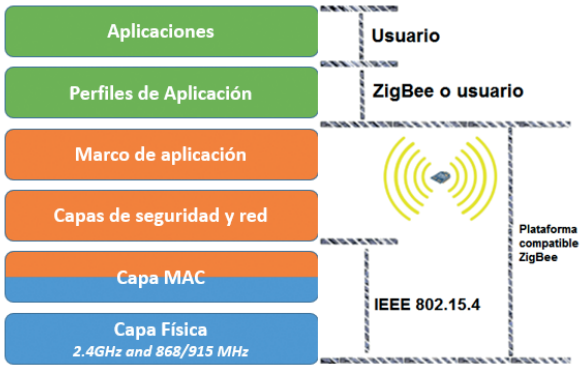

Figura 1. División de las capas del estándar ZigBee [1].

Como se muestra en la figura 1, el estándar IEEE 802.15.4, se utiliza para las dos capas más bajas, la capa física (PHY) y la capa de control de acceso al medio (MAC). Las otras dos capas se definen propiamente por el protocolo ZigBee. Es importante destacar que desde una perspectiva de seguridad, la capa de red y la capa de aplicación son las de más alta relevancia [7].

Para una mejor comprensión del estándar, es importante describir el funcionamiento de las redes en las que se aplica este estándar y su topología de red.

3.1 Tipología de red utilizada por ZigBee

ZigBee permite 3 tipos de topologías de

red: malla, estrella o árbol. La automatización del hogar generalmente se desarrolla bajo la topología de malla, por tal motivo, a continuación, se explica con más detalle el funcionamiento de esta topología de red [6]:

Los fundamentos de esta topología de red se basan en que cada dispositivo se comunica con otro dispositivo dentro de la red a través de caminos de comunicación separados [7].

3.1.1 Roles de los nodos

Como se muestra en la figura 3, según su disposición, los nodos dentro de la red ZigBee, pueden asumir 3 roles o responsabilidades distintas [6]:

Coordinador: este rol tiene la responsabilidad, distribuir el tráfico a través de la red. Esto requiere que el nodo tenga suficiente memoria y gran capacidad de comunicación, debido a que actúa como centro de confianza.

Este centro de confianza representa para el resto de dispositivos, el origen de confianza encargado de realizar la distribución de las claves de seguridad utilizadas en el cifrado de las comunicaciones [7].

***Router* o enrutador:** tiene como tarea, gestionar las rutas de comunicación que existen entre los dispositivos de la red. En una red ZigBee, puede existir más de un router o enrutador.

Dispositivo final: se les llama a aquellos dispositivos que actúan únicamente como dispositivos finales, los cuales pueden comunicarse con un nodo padre (coordinador o router).

A continuación, se profundiza un poco en el modelo de seguridad que maneja ZigBee.

3.2 Modelo de seguridad en el estándar ZigBee

ZigBee fue construido bajo la norma estándar IEEE 802.15.4. Por lo tanto, implementa también su modelo de seguridad. Este modelo proporciona en su diseño tres mecanismos de seguridad muy importantes [8]:

Mecanismo de control de acceso de los dispositivos a la red (autenticación).

Mecanismo de cifrado de la información (utilizando criptografía de clave simétrica, específicamente AES).

Mecanismo de integridad, para asegurar la integridad del mensaje, esto verificando que las tramas trasmitidas no han sufrido manipulación (MIC).

A continuación, se describen las llaves criptográficas que utiliza el estándar.

3.2.1 Llaves criptográficas

Existen 3 tipos de llaves criptográficas utilizadas por el estándar ZigBee, como se muestra a continuación [7]:

Llave maestra: es la llave a través de la cual se generan diferentes llaves de enlace para que otros dispositivos se conecten a la red. Por su alta importancia, se debe tener en cuenta que la misma debe obtenerse por medios seguros (preinstalación o transporte. Más adelante, se definen se definen estos términos).

Llave de enlace: es la llave encargada de cifrar las comunicaciones punto a punto a nivel de aplicación. Parte importante de esta llave es que sólo es conocida por los dispositivos que participan en dicho enlace, y varía para cada pareja de dispositivos. La idea de esta llave, es minimizar los riesgos de seguridad que se relacionen con la distribución de la llave maestra.

Llave de red: esta llave, a diferencia de las otras dos, es utilizada a nivel de red y conocida por todos los elementos pertenecientes a la red [6].

3.2.2 Gestión y manejo de las llaves criptográficas

Los mecanismos para la gestión y manejo de las llaves criptográficas son los siguientes:

Preinstalación: este método solo es aplicable para las llaves maestras, debido a que proviene de la fábrica, donde, el fabricante del dispositivo, le incorpora una llave maestra dentro del propio dispositivo.

Transporte de llave: en este método, el dispositivo realiza una petición a un centro de confianza para que le envíe la llave. Este centro de confianza tiene dos modos de operación [9]:

- Modo comercial: en este modo, el centro de confianza es quien mantiene una lista de las llaves maestras, dispositivos, llaves de enlace y llaves de red. Un punto importante es que el espacio de memoria que se requiere para el correcto funcionamiento del centro de confianza va a depender de la cantidad de dispositivos asociados a la red.
- Modo residencial: en este modo, en el centro de confianza solo se mantiene la llave de red, quien es la responsable de controlar el acceso a la red. El resto de la información, se almacena en cada nodo. En este modo, no se realiza ningún control para verificar si algún intruso modificó el número de secuencia.

Establecimiento de llave sin comunicación: este es un método que se utiliza localmente para generar llaves de enlace a partir de la llave maestra para dos dispositivos sin la necesidad de comunicarlos. Para esto, ZigBee se basa en el protocolo SKKE (Symmetric-Key Key Establishment). El único requisito es que ambos dispositivos involucrados en la comunicación, deben tener la llave maestra, la cual debió ser obtenida por los métodos antes mencionados (preinstalación o transporte de llave).

4. Vulnerabilidades encontradas

A continuación, se describen las vulnerabilidades encontradas en cada una de las capas.

4.1 Capa física

4.4.1 Acceso no autorizado a las etiquetas

Debido a la falta de mecanismos de autenticación correcta en un gran número de sistemas de RFID, las etiquetas pueden ser accedidas por algún atacante sin autorización. El atacante no puede leer los datos, pero los datos pueden ser modificados o incluso eliminados [10].

4.4.2 Clonación de etiquetas

Dado que las etiquetas se implementan en diferentes objetos que son visibles, sus datos pueden ser leídos y modificados con algunas técnicas de hacking. Por lo tanto, pueden ser fácilmente capturados por cualquier atacante que puede crear una réplica de la etiqueta y confundir al lector, debido a que no puede distinguir entre el original y la etiqueta clonada o comprometida [11].

4.4.3 Espionaje

Debido a las características inalámbricas del RFID, se hace muy fácil para el atacante ver donde se encuentra la información confidencial, como contraseñas o cualquier otro dato que se derivan de la etiqueta [12].

4.4.4 *Spoofing*

Se habla de este ataque cuando un atacante difunde información falsa en los sistemas RFID y la hace ver como de la fuente original. De esta manera, el atacante tiene acceso completo al sistema, lo que lo hace vulnerable [13].

4.2 Capa de control de acceso medio

4.2.1 Acceso no autorizado

La capa de control de acceso proporciona diferentes interfaces para las aplicaciones y las instalaciones de almacenamiento de datos [14]. El atacante puede fácilmente causar daños en el sistema mediante la prohibición del acceso a los servicios relacionados con la automatización, mediante la supresión de los datos existentes. Así que un acceso no autorizado, podría ser fatal para el sistema.

4.2.2 Ataque DDOS

Este ataque consiste en saturar el sistema a través de peticiones. La idea final del ataque es apagar el sistema. Esto da como resultado, la falta de disponibilidad de los servicios.

4.3 Capa de red

4.3.1 Ataque de privación del sueño

Los nodos de sensores en la red de sensores inalámbricos son alimentados con baterías con no tan buen ciclo de vida, por lo que los nodos están obligados a seguir las rutinas de

sueño para extender su vida útil. La privación del sueño es el tipo de ataque que mantiene los nodos despiertos, lo que resulta en un mayor consumo de la batería y, como consecuencia la duración de la batería se reduce al mínimo [15].

4.3.2 Inyección de código malicioso

Este es un tipo grave de ataque en el que un atacante compromete un nodo para inyectar código malicioso en el sistema que incluso podría dar lugar a un cierre completo de la red o en el peor de los casos, el atacante puede obtener un control completo de la red [16].

4.3.3 Ataque de hombre en el medio

Esta es una forma de escucha ilegal que tiene como objetivo de ataque interceptar el canal de comunicación, sin que ninguna de las dos partes se dé cuenta que el canal ha sido violado o interceptado [17].

4.4 Capa de aplicación

4.4.1 Inyección de código malicioso

Este ataque consiste en inyectar código malicioso a través de técnicas de hacking y de esta forma, utilizando el usuario final del sistema como entrada, robar información confidencial o incluso, datos del usuario [18].

4.4.2 Ataque de denegación de servicios

Los ataques de denegación de hoy en día, son más sofisticados. Ofrecen al atacante una cortina de humo para llevar a cabo ataques para romper el sistema defensivo y los datos de privacidad del usuario, mientras que engañan a la víctima haciéndole creer que el ataque real está sucediendo en otro lugar [7].

4.4.3 Ataque de *phishing*

Se trata de un ataque de suplantación de correo electrónico en el que la víctima, generalmente un alto cargo, es inducido a abrir el correo electrónico a través del cual el atacante gana acceso a las credenciales de la víctima y luego a información más sensible [14].

4.4.4 Ataque de *sniffing*

Un atacante puede forzar un ataque contra el sistema mediante la introducción de una aplicación sniffer en el sistema, lo que podría obtener información de la red que da como resultado, la corrupción del sistema [19].

5. Conclusiones

A lo largo del desarrollo de esta revisión, se pudo entender más a fondo el funcionamiento del estándar ZigBee, descubriendo así, las vulnerabilidades y riesgos a los que se enfrenta. Algunos de los puntos importantes a resaltar con la culminación de esta investigación son los siguientes:

- Las redes ZigBee, enfocadas específicamente para la automatización, utilizan la topología de red de malla. En esta topología, cada uno de los nodos puede realizar cualquiera de estos tres roles: coordinador, enrutador o dispositivo final.
- ZigBee, en cuanto a seguridad de la información, utiliza tres llaves criptográficas: llave maestra, llave de enlace y llave de red. Estas llaves pueden ser adquiridas a través de una preinstalación, transporte de llaves o el establecimiento de llaves sin comunicación.
- ZigBee se encuentra dividido en 4 capas: capa física, capa de control de acceso medio, capa de red y capa de aplicación. Cada una de estas capas posee ciertas vulnerabilidades específicas, que pueden ser aprovechadas por los atacantes. Es por esta razón que parte importante de la seguridad en este estándar se basa en la forma de configuración de la red.

REFERENCIAS

[1] B. Yang, "Study on Security of Wireless Sensor Network Based on ZigBee Standard," in International Conference on Computational Intelligence and Security, Estados Unidos, 2009, pp. 426-430.

[2] P. Kumar, A. Gurtov, J. Iinatti, M. Ylianttila, and M. Sain, "Lightweight and Secure Session-Key Establishment Scheme in Smart Home Environments," IEEE Sensors Journal, vol. 16, pp. 254-264, 1 septiembre 2016.

[3] Y. Zhang, R. Yu, S. Xie, W. Yao, Y. Xiao, and M. Guizani, "Home M2M networks: architectures, standards, and QoS improvement," IEEE Communications Magazine, vol. 49, pp. 44-52, 2011.

[4] M. Corporation. (2016, 25 de octubre). The home of the future is finally here. Available: https://news.microsoft.com/stories/people/easydom.html

[5] Richardson, "ZigBee White Paper," AMX, Ed., ed, 2006, p. 9.

[6] I. N. d. Ciberseguridad. (2016, 27 de octubre). Seguridad en comunicaciones ZigBee. Available: https://www.certsi.es/blog/seguridad-comunicaciones-zigbee

[7] T. Zillner and S. Strobl, "ZigBee Exploited–The good, the bad and the ugly," Proceedings of the DeepSec Conferences, p. 6, 2015.

[8] S. Choudhury, P. Kuchhal, and R. Singh, "ZigBee and Bluetooth network based sensory data acquisition system," Procedia Computer Science, vol. 48, pp. 367-372, 2015.

[9] L. World. (2014, octubre 2016). Security in 802.15.4 and ZigBee networks. Available: http://www.libelium.com/security-802-15-4-zigbee/

[10] M. R. Uttarkar and R. Kulkarni, "Internet of Things: Architecture and Security," International Journal of Computer Application vol. 3, pp. 12-19, 2014.

[11] M. Burmester and B. De Medeiros, "RFID security: attacks, countermeasures and challenges," in The 5th RFID Academic Convocation, The RFID Journal Conference, Orlando , Florida, 2007.

[12] B. Khoo, "RFID as an Enabler of the Internet of Things: Issues of Security and Privacy," in Internet of Things (iThings/CPSCom), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing, Dalian, China, 2011, pp. 709-712.

[13] A. Mitrokotsa, M. R. Rieback, and A. S. Tanenbaum, "Classification of RFID attacks," Gen, vol. 15693, p. 14443, 2010.

[14] M. Farooq, M. Waseem, A. Khairi, and S. Mazhar, "A critical analysis on the security concerns of internet of things (IoT)," International Journal of Computer Applications, vol. 111, p. 6, 2015.

[15] T. Bhattasali, R. Chaki, and S. Sanyal, "Sleep deprivation attack detection in wireless sensor network," arXiv preprint arXiv:1203.0231, 2012.

[16] P. S. Fulare and N. Chavhan, "False data detection in wireless sensor network with secure communication," International Journal of Smart Sensors and AdHoc Networks (IJSSAN), vol. 1, pp. 66-71, 2011.

[17] R. P. Padhy, M. R. Patra, and S. C. Satapathy, "Cloud computing: security issues and research challenges," International Journal of Computer Science and Information Technology & Security (IJCSITS), vol. 1, pp. 136-146, 2011.

[18] S. Majoul, M. Richard-Foy, A. Agirre, A. Pérez, and A. Kung, "Enforcing trust in home automation platforms," in Emerging Technologies and Factory Automation (ETFA), 2010 IEEE Conference on, 2010, pp. 1-6.

[19] J. Suomalainen, S. Moloney, J. Koivisto, and K. Keinänen, "OpenHouse: a secure platform for distributed home services," in Privacy, Security and Trust, 2008. PST'08. Sixth Annual Conference on, 2008, pp. 15-23.