GESTIÓN DE LA SEGURIDAD EN EL INTERNET DE LAS COSAS

Luis Alberto Zabala Jaramillo, e-mail: zabalajaramillo@gmail.com
Junio 2016

***Abstract*—**This document will describe, in a brief summary, the latent security threats that are on the Internet of things. Are described the current status and most common threats on platforms of technologies that are based on this concept and recommendations on how mitigate these risks, where the main drawback is the number of devices that are connected globally.

***Resumen*—** En este documento se describen, por medio de un breve resumen, las amenazas de seguridad latentes que se encuentran en el *Internet de las Cosas*. Se describe el estado actual y las amenazas comunes sobre las plataformas de tecnología que se basan en este concepto. También se tratan las recomendaciones sobre cómo se pueden mitigar estos riesgos, en donde el principal inconveniente es la cantidad de dispositivos que se encuentran conectados a nivel global.

***Keywords*—** Security, Internet of things, Internet, standardization, secure development, hacking, education.

***Palabras clave*—** Seguridad, Internet de las Cosas, Internet, estandarización, desarrollo seguro, hacking, educación.

1. INTRODUCCIÓN

En las últimas tres décadas se ha visto un auge en lo relacionado a la digitalización de la información y la posibilidad de tener la misma al alcance de la mano: de forma rápida y sencilla. El Internet, que originalmente era usado por entidades militares y educativas, fue evolucionando para, posteriormente, convertirse en una herramienta fundamental del funcionamiento de grandes compañías y finalmente entró a ser parte del día a día de las personas en casi todas sus actividades (desde las herramientas de trabajo hasta la creación de relaciones interpersonales por medio de las redes sociales). El Internet vive una nueva revolución que está cambiando la forma en que se conecta el mundo.

Esta revolución se basa en un concepto denominado como IoT (Internet of Things) o *Internet de las Cosas*, donde su idea principal es poder tener información de casi cualquier elemento que nos rodea en tiempo real por medio de diferentes tipos de tecnologías.

IoT se encuentra definido como "Una infraestructura global interconectada con capacidades de autoconfiguración basados en estándares de interoperabilidad y protocolos de comunicación en donde elementos físicos y virtuales tienen identidades, atributos físicos y personalidades virtuales además de interfaces inteligentes las cuales son integradas a redes conectadas en donde se comunican constantemente los datos asociados con los diferentes usuarios y ambientes" [1].

Internet de las Cosas es un concepto que está evolucionando a pasos avanzados y ya se encuentra instalado en varios sectores como:

- Automatización de Hogares: inteligencia en la administración de los elementos que confirman un hogar (Smart lighting, Smart Appliances), detección de intrusos, detectores de gas/humo entre otros.

- Ciudades Inteligentes: el objetivo de las ciudades inteligentes es automatizar tareas que pueden generar degradación en la calidad de vida de las personas. Varias áreas a cubrir por el *Internet de las Cosas* son: parqueaderos inteligentes, alumbrado público inteligente, carreteras inteligentes, vigilancia, respuesta a emergencias.

- Medio ambiente: al igual que en el caso de las ciudades inteligentes, el *Internet de las Cosas* aplicado en el medio ambiente está orientado a mejorar la calidad de vida de las personas y tratar de mitigar el huella ecológica de cada individuo. Algunas de las áreas en donde se puede implementar este modelo son: monitoreo de clima, de polución de aire, de polución de ruido, detección de incendios forestales, y de desborde de ríos.

- Energía: desarrollado para generar modelos de producción energética más eficiente como lo son las *Smart Grids* y los sistemas de energía renovable.

- Retail: en el área de la industrial *Retail*, el *Internet de las Cosas* se orienta hacia lograr un aumento de ventas por medio de la optimización de procesos como la administración de inventarios, pagos inteligentes y máquinas expendedoras inteligentes.

- Logística: en el área de logística la mejora de procesos permite tiempos de entrega más efectivos; para esto se optimizan tareas como la generación de rutas de envío y horarios de entregas, rastreo de los envíos, monitoreo de los vehículos de entrega.

- Agricultura: en la agricultura se optimizan procesos como riego inteligente o control de plagas con lo cual se pueden tener mejores cosechas.

- Industria: en la industria se pueden desarrollar mejoras en el proceso de manufactura como en los elementos desarrollados por las mismas.

- Salud: para el área de la salud, el *Internet de las Cosas* permite un constante monitoreo de los pacientes por medio de ropa inteligente, monitores de salud y de estado físico.

En la **figura 1** se puede encontrar la topología genérica de una infraestructura del *Internet de las Cosas*. Básicamente se pueden observar los diferentes sensores distribuidos en la capa de adquisición de datos: el hardware que recolecta la información y la transmite hacia un punto único de recolección de la misma en la capa de equipos IoT; un elemento denominado Gateway que recibe todos los datos; y, la plataforma de análisis de información, encargada de procesar los datos de acuerdo a parámetros previamente establecidos: esta plataforma de análisis de datos se puede encontrar instalada en plataformas *cloud* (públicas, privadas o híbridas) o entornos orientados al análisis de grandes cantidades de datos (*Big Data*); finalmente, la última capa de este modelo, la capa de las aplicaciones que muestran a los usuarios finales los datos ya procesados.

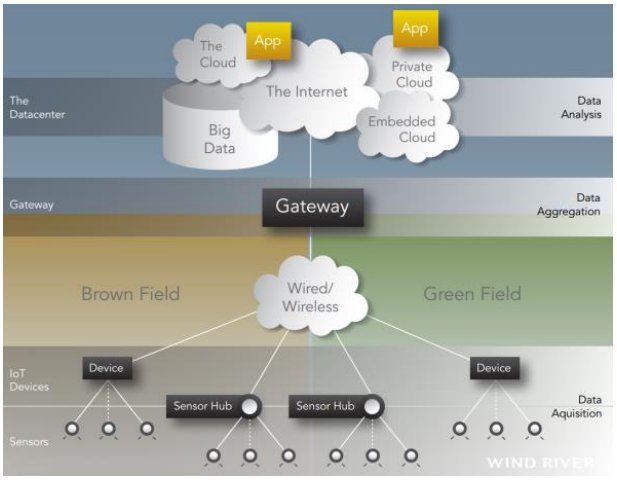

Figura 1. [2] Topología genérica de infraestructura de internet de las cosas

Esta gran red de infraestructura se encuentra globalmente interconectada el método más sencillo y módico de lograr esta comunicación: el Internet, un medio económico que brinda diferentes tipos de acceso. Por esta razón, todas las comunicaciones que se produzcan dentro de esta red son de dominio público y personas inescrupulosas pueden aprovecharse de vulnerabilidades existentes.

2. ANTECEDENTES

Como se explicó anteriormente el concepto de *Internet de las Cosas* se encuentra distribuido en casi todos los sectores y su aplicación crece de forma exponencial año tras año. "*El Internet de las Cosas* se compone de una amplia diversidad de equipos –desde grandes a diminutos, como desde simples a complejos, desde gadgets para clientes de consumo masivo hasta sofisticados sistemas de recolección de información" [3].

La diversidad de elementos y sistemas utilizados en el *Internet de las Cosas* genera una preocupación creciente a los expertos en seguridad: la falta de estandarización y el desarrollo de nuevas tecnologías.

Primero se debe entender que los elementos de hardware y software usados para realizar la recolección de datos no son los elementos tradicionales como equipos de escritorio, computadores portátiles, servidores, teléfonos inteligentes, etc. Estos son microcontroladores, elementos de hardware desarrollados por el propio fabricante, equipos de cómputo portátil modificado y demás; por esto los parámetros que se encuentran en la industria de seguridad para la protección de estos dispositivos no se encuentran desarrollados de una forma efectiva para los mismos.

Igualmente el desarrollo de todas las aplicaciones que se usan en el *Internet de las Cosas* es realizado principalmente por empresas nuevas, las cuales están intentando ingresar a un mercado competitivo y su presupuesto (y/o conocimiento) en temas de seguridad es muy limitado. Estos dos factores influyen en que no se tengan estándares de desarrollo seguro al momento de implementar una aplicación o que los recursos invertidos para el desarrollo y el aseguramiento del software sean los mínimos, pues están orientados a disminuir los costos de producción.

Otro fallo en la implementación de seguridad en los diferentes dispositivos usados es la capacidad de hardware. Dentro de la gran variedad de elementos utilizados para la recolección de datos, muchas veces los requerimientos de hardware y software necesarios son los mínimos. Por lo tanto, las empresas, al desarrollar estos dispositivos, los diseñan y configuran para cumplir una única función (generalmente envío de datos a un Gateway). Por ello, si se desea implementar algún tipo de característica de seguridad, resultaría imposible ya que el equipo se encuentra al tope en consumo de recursos.

Estas malas prácticas de desarrollo por parte de fabricantes y la funcionalidad de los equipos, crean retos que se deben tener en cuenta al desplegar una infraestructura basada en el *Internet de las Cosas* como se muestra en la **Tabla 1**.

Función Crítica	Los elementos del *Internet de las Cosas* no solo manejan la automatización de hogares, infraestructura de transporte y sistemas de comunicación global, además pueden sufrir ataques con consecuencias catastróficas.
Replicación	Los dispositivos recolectores de datos se fabrican en masa, por lo tanto un error en el diseño de un elemento se replica a gran escala.
Presunciones de seguridad	Los desarrolladores y fabricantes asumen que dispositivos no especializados se encuentran fuera del rango de ataque por parte de hackers.
No fácilmente actualizables	La mayoría de los elementos no se pueden actualizar a nivel, siempre ejecutará la misma versión de software desarrollada al salir de la fábrica de producción.
Ciclo de vida extensos	Los ciclos de vida de dispositivos especializados son muchos más largos que los equipos tradicionales, por sus vulnerabilidades estarán expuestas más tiempo y serán más fáciles de atacar.
Desarrollos propietarios	Mucho fabricantes desarrollan sus propios protocolos de comunicación, lo que dificulta el uso de herramientas de seguridad y la estandarización de los mismos.
Instalados fuera del perímetro de la empresa	Es común encontrar que las empresas cuentan con algún tipo de protección en su red, pero al instalar dispositivos del *Internet de las Cosas* fuera de la red segura, muchas veces no se tienen en cuenta las medidas de seguridad.

Tabla 1. [3] Retos de implementación de arquitectura de IoT.

Bajo este escenario de vulnerabilidades latentes existen cinco temas que generan preocupación en los expertos de seguridad de la información. A continuación su resumen:

Privacidad: los datos que manejan los diferentes dispositivos no se encuentran almacenados de forma segura, lo cual permite que ante un fallo de

seguridad el atacante pueda acceder a los mismos sin ningún inconveniente.
Protocolos de autenticación: la mayoría de las arquitecturas del *Internet de las Cosas* no cuentan con protocolos de autenticación y/o autorización al enviar o recibir la información. Por lo mismo cualquier atacante podrá acceder a la misma sin mayores problemas.

Transporte de la información: la información viaja por medios inseguros sin ningún tipo de cifrado o protocolo de seguridad.

Web Interface: muchas aplicaciones del *Internet de las Cosas* constan de interfaces Web de administración y/o acceso a la información. Muchas veces estas interfaces no están configuradas con protocolos de acceso seguro (Certificados SSL).

Software Inseguro: ésta es la principal falla de los diferentes fabricantes, el desarrollo de software sin seguir parámetros de desarrollo seguro con el fin de mitigar riesgos.

3. PROBLEMA

La falta de estandarización en el desarrollo de los diferentes dispositivos, imposibilita la generación de una guía de mejores prácticas para cubrir esta falencia. Lamentablemente lograr una parametrización de desarrollo es una tarea titánica ya que, debido a la gran industria, los desarrolladores muchas veces eligen la opción más fácil que es desarrollar sus propios protocolos. Estos modelos de desarrollo propietario, generan varios inconvenientes a nivel de seguridad; algunos aplicativos no se basan en desarrollos seguros, otros no brindan las actualizaciones necesarias con el fin de corregir errores y otros no ofrecen integración con plataformas de seguridad de terceros.

"El cambio es lo único constante y los usuarios se esfuerzan en desarrollar diferentes tipos de tecnología para suplir sus necesidades. La evolución de las amenazas ha causado un incremento en las medidas de seguridad que se deben tomar en consideración y bajo este modelo los modelos tradicionales de prevención de amenazas y sistemas de recuperación (DRP) no pueden ser usados" [7].

Hay varios tipos de ataques que pueden ser ejecutados hacia la infraestructura que soporta el *Internet de las Cosas.* Éstos son:

- Ataques externos.
- Ataque Whormhole.
- Ataque Fordwarding selectivo.
- Ataque Sinkhole.
- Ataque Sewage pool.
- Ataque Witch.
- Ataque HELLO flood.
- Spoofing dirección IP de los diferentes dispositivos.
- Denegación de servicio distribuido
- Flash crowd.

Al ser el *Internet de las Cosas* una plataforma que corre bajo un ambiente público, como lo es Internet, los tipos de ataques se pueden ejecutar sin mayor esfuerzo por parte de terceros. Adicional a las amenazas públicas expuestas, también existen falencias propias de la arquitectura del *Internet de las Cosas* que pueden ser explotadas.

Una de las razones más importantes por la que la gestión de seguridad en el *Internet de las Cosas* es un problema muy serio, es el usuario final. El concepto de IoT se ha movido rápidamente al mercado masivo en donde personas, sin conocimientos técnicos, pueden usar diferentes módulos en donde su proceso de instalación se realiza basado en las configuraciones por defecto que contiene cada dispositivo, permitiendo que las vulnerabilidades sean explotadas.

Al día de hoy, las mayores explosiones de datos generado por el *Internet de las Cosas* son productos orientados a consumo masivo: televisores inteligentes, cámaras IP, elementos para un hogar automatizado, etc., en donde su factor común es una comunicación con ambientes *cloud*, como se puede ver en la **figura 2**. Incluso para elementos situados en el mismo lugar físicamente.

Figura 2. [4] Elementos básicos de automatización de hogares

En un estudio realizado por Sarthak Grover [4] y Nick Feamster de la Universidad de Princeton, se realizó una serie de pruebas a diferentes elementos usados en la automatización de hogares. Estas pruebas se orientaron a conocer cómo los bajos estándares de programación por parte de los fabricantes y la mala configuración por parte de los usuarios, podían generar vulnerabilidades fácilmente aprovechables por terceros.

Uno de los elementos analizados fue un Marco digital de fotos. Éste toma diferentes fotografías del usuario en un perfil en la nube y las presenta en el Marco digital. En este análisis se pudieron observar todas las peticiones de tráfico y actualizaciones (RSS) en texto claro por medio del puerto 80, peticiones de DNS, correo electrónico de usuario, toda la información proveniente del Marco Digital. En la **figura 3** se puede ver la información obtenida por medio de un analizador de tráfico.

Figura 3. [4] Información obtenida por medio de un analizador de tráfico de Marco digital de fotos.

Igualmente se realizó el mismo análisis sobre una cámara IP, en donde se podían observar fallos de seguridad similares al elemento anterior. Tráfico enviado por la cámara IP en texto claro por medio del puerto 80 (Incluso credenciales de acceso). Los videos y fotografías eran enviados a un servidor FTP (**Figura 4**) sin cifrar y requerimientos DNS.

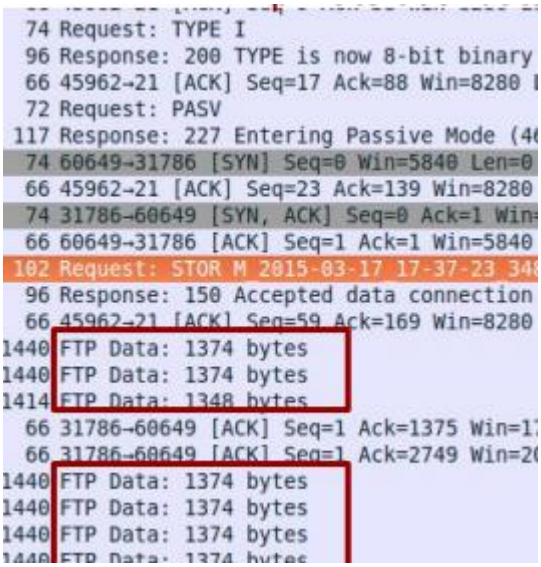

Figura 4. [4] Información obtenida por medio de un analizador de tráfico de Cámara IP.

Otro estudio realizado por el empresa *Proofpoint*, líder en seguridad informática avanzada, descubrió el primer ataque de ciberseguridad comprobado, basado en el *Internet de las Cosas* entre Diciembre 23 de 2013 y Enero 6 de 2014.

"El ataque global consistió en el envío de más de 750.000 correos electrónicos maliciosos provenientes de más de 100.000 equipos de consumo masivo como lo son Routers caseros, centros multimedia, televisores inteligentes y al menos un refrigerador, cuya seguridad fue comprometida, y fueron usados como plataforma de lanzamiento del ataque. Se espera que la cantidad de estos tipos de dispositivos conectados se incremente cuatro veces más que los equipos tradicionales de cómputo, según reportes de diferentes medios. Es la prueba de que ataques basados en IoT tienen muchas implicaciones para los dueños de los dispositivos así como para sus fabricantes." [5].

De este ataque, más del 25% de los correos enviados provenían de algún tipo de elemento no convencional que entran en la categoría de *Internet de las Cosas*. Según los estudios realizados por *Proofpoint*, desde una sola IP se enviaron solo 10 correos electrónicos. Pero el principal problema es la gran cantidad de elementos usados para realizar el ataque, lo cual

dificulta severamente un bloqueo basado en localización. Igualmente la mayoría de los accesos no autorizados se dieron por fallos en la configuración inicial de los dispositivos.

La preocupación crece cada día más porque según fuentes de IDC "se espera que para 2020 más de 200 billones de dispositivos (los cuales mueven más de $8.9 trillones de dólares) estén conectados a Internet" [5]. Dispositivos que han sido desarrollados por diferentes empresas, pequeñas *startups* y programadores novatos, en donde el hardware es limitado impidiendo la ejecución de protocolos de seguridad. Éstos se conectaran a plataformas *cloud* a nivel global.

"El *Internet de las Cosas* nos brinda la gran promesa de habilitar el control para todos los dispositivos que usamos en nuestro uso diario. También brinda una gran promesa para todos los cibercriminales quienes pueden usar nuestros *Routers* caseros, televisores, refrigerados y demás elementos conectados para lanzar un ataque distribuido a gran escala. Igualmente los elementos con Internet habilitado representan una enorme amenaza porque son fáciles de vulnerar. Los clientes tiene una intención muy baja de hacer estos elementos más seguros, crece de forma rápida la cantidad de elementos que pueden enviar contenido malicioso sin ser detectados, y pocos fabricantes están tomando medidas en contra de estas amenazas y el modelo de seguridad existente simplemente no trabaja para resolver el problema" Indica Michale Osterman, Analista principal de investigación en Osterman Research [5].

4. PROCEDIMIENTOS DE MITIGACIÓN

Comenzando a entender esta gran amenaza se pueden tomar los pasos correctivos para lograr su mitigación como se muestra en la **figura 3**, pero esta tarea no es solo de fabricantes o usuarios, es una tarea en conjunto que ayudaría a mejorar la calidad de vida y dar el uso adecuado al concepto de *Internet de las Cosas*.

Como se explicó en este documento, la infraestructura usada por el *Internet de las Cosas* para lograr su funcionamiento hace uso de diferentes tecnologías que deben ser tomadas en cuenta al momento de realizar el correcto aseguramiento al funcionar y la información que manejan.

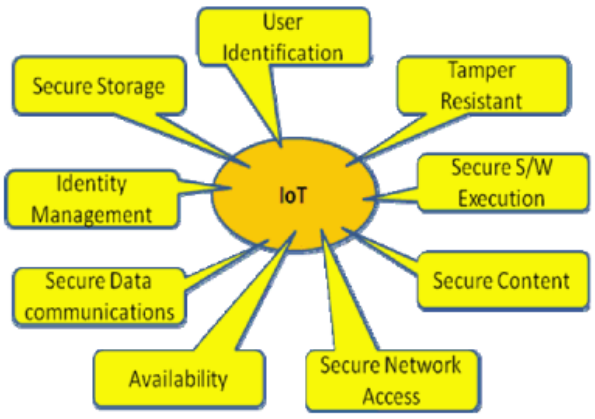

Figura 5. Requerimientos de arquitectura de seguridad IoT de alto nivel [6]

A nivel de comunicaciones se entiende que es imposible, por costos, tener canales cifrados de comunicación, canales dedicados, redes MPLS y demás entre todos los dispositivos que pueden conformar una plataforma IoT.

Para cerciorarse de su funcionamiento seguro, se plantean soluciones de autenticación segura por parte de los diferentes factores externos que quieren interactuar con cualquier dispositivo. Esta autenticación se debería realizar basada en procesos cifrados y deben ser en sentido dispositivo –casa matriz y viceversa–. En lo posible se deben usar múltiples factores de autenticación y tratar de eliminar las claves, ya que los usuarios, por falta de conocimiento o pereza, usan claves que no cumplen con los protocolos mínimos de seguridad.

Las empresas deben centrar sus esfuerzos en el desarrollo de un código seguro, aunque esto puede incrementar sus costos; si tenemos en cuenta que estos dispositivos llegan a un mercado masivo, los valores adicionales se pueden amortizar de una forma más efectiva.

Cualquier código que se quiera ejecutar en el dispositivo solo se podrá hacer si este está firmado por el fabricante, igualmente se recomienda cifrar código, sistema operativo y *firmware* con el fin de evitar modificaciones no autorizadas que puedan ser usadas para tareas diferentes a las previamente establecidas.

De la mano de desarrollo de código seguro también se deben crear planes de actualización de los diferentes dispositivos a nivel de software. Las empresas fabricantes no pueden dejar a la deriva los dispositivos una vez que estos son vendidos.

Estas actualizaciones deberían estar orientadas a la resolución de problema críticos y aplicación de parches de seguridad y actualizaciones.

Debido a la gran cantidad de fabricantes que existen, cada uno de éstos crea ecosistemas cerrados que no se adaptan de forma adecuada a sistemas de terceros y menos sistemas de seguridad. Este inconveniente representa dos grandes retos. El primero es una estandarización de los parámetros de desarrollo de tecnologías IoT por parte de algún ente regulador que permita una integración más sencilla entre todos los componentes y diferentes plataformas de seguridad. Pero al ser un mercado de billones de dispositivo esta tarea puede llegar a ser compleja. El segundo reto es la implementación de protocolos y complementos de seguridad por parte de los fabricantes pero se debe tener un compromiso grande de parte de los mismos en realizar revisiones periódicas y actualizaciones cuando se encuentren vulnerabilidades.

Finalmente los entes gubernamentales debe tener conciencia de este tipo de amenazas y los daños que pueden ocasionar. Para esto, en conjunto con los fabricantes, se deben crear campañas de concientización, al igual que están haciendo algunas entidades financieras sobre el manejo de los datos de usuario con el fin de prevenir fraude, orientadas a que las personas puedan entender las consecuencias de no tener un cuidado correcto con el manejo de la tecnología.

Como complemento a todas las recomendaciones expuestas, se toma un aparte de un artículo de Alan Grau, Presidente de Iconolabs, empresa especializada en seguridad en el *Internet de las Cosas* [3], quien realizó un pequeño resumen de los factores que se deben tener en cuenta al momento de diseñar, instalar y soportar cualquier dispositivo los cuales son:

- Boot Seguro.
- Actualizaciones seguras de código.
- Seguridad de Datos.
- Autenticación.
- Comunicaciones Seguras.
- Protección en contra de ciberataques.
- Detección de intrusos y monitoreo de seguridad.
- Administración de seguridad embebida.
- Detección de tampering por defecto en cada dispositivo.

5. CONCLUSIONES

Gracias al *Internet de las Cosas* se puede obtener información en tiempo real de cualquier elemento, pero basado en su arquitectura de funcionamiento esta información es transmitida en ambientes hostiles en donde puede ser interceptada.

Los modelos tradicionales de seguridad no se adecuan a las diferentes tecnologías del *Internet de las Cosas* debido a su gran diversidad en hardware, protocolos de comunicación, desarrollos, fabricantes y demás.

El desarrollo no seguro junto a hardware limitado es el principal factor por parte de los fabricantes que generan brechas de seguridad en el *Internet de las Cosas*, ya sea por falta de conocimiento o reducción de costos por parte de las mismas.

Las empresas que desarrollan hardware/software relacionado con el *Internet de las Cosas* deben generar un plan de actualizaciones en sus productos con el fin de corregir fallos de seguridad y/o desempeño que se puedan llegar a presentar.

Los usuarios finales deben entender el riesgo que implica un uso no adecuado de los diferentes elementos que utilizan el concepto del *Internet de las Cosas* para su funcionamiento. Por ello conviene tomar las precauciones de configuración necesarias y/o recomendadas con el fin de evitar robo o exposición de información sensible.

Las acciones correctivas sobre los problemas de seguridad en los diferentes dispositivos del *Internet de las Cosas* de deben tomar en el corto plazo, debido a su gran proliferación. Cada día se conectan miles y miles de dispositivos nuevos con problemas de seguridad y se llegara a un punto en donde los ataques usando estos elementos podrán ser controlados.

6. REFERENCIAS

[1] Arshdeep Bahga, Vijay Madisetti (2014). Internet of things: A Hands-On Approach. 1ra Edición

[2] Wind (2015). Security in the internet of things: Lessons from the past for the connected future [Online]. Disponible en: http://www.windriver.com/whitepapers/security-

in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf

[3] Alan Grau (2015). Internet of secure things [Online]. Disponible en: http://www.iconlabs.com/prod/internet-secure-things-%E2%80%93-what-really-needed-secure-internet-things

[4] Sarthak Grover & Nick Feamster (2016). The Internet of unpatched things [Online]. https://www.cs.princeton.edu/~sgrover/sgrover_files/papers/privacycon2016-grover.pdf

[5] Larry Dignan (2013). Internet of things: $8.9 trillion market in 2020, 212 billion connected things [Online] http://www.zdnet.com/article/internet-of-things-8-9-trillion-market-in-2020-212-billion-connected-things/

[6] Natarajan Meghanathan, Selma Boumerdassi, Nabendu Chaki & Dhinaharan Nagamali (2010). Recent Trends in Network Security and Applications. 1ra Edición.

[7] Fei Hu (2916). Security and Privacy in Internet of things (IoTs): Models, Algorithms and Implementations. 1ra Edición.