IOT - EL INTERNET DE LAS COSAS Y SUS RIESGOS EN LOS PILARES DE LA SEGURIDAD DE LA INFORMACIÓN

Coy Sosa, William Andrés
williamcoy.1@gmail.com
Universidad Piloto de Colombia, *Especialicación en seguridad Informática*

Abstract - The Internet of Things IOT looking interconnect different electronic devices to separate tasks helping automate, benefiting the daily lives of users. In addition to this, it also helps to obtain and access specific information, therefore, its use makes it possible to process a lot of information, in order to predict different events and habits of those who use them. The use of IOT devices in the next four years is estimated to reach 26 million devices therefore makes during this time is an access point growing to information and therefore a new gap to consider the availability, integrity and confidentiality of information.

Resumen - El internet de las cosas busca interconectar dispositivos para que se puedan monitorizar y automatizar tareas cotidianas, para esto, es necesario realizar configuraciones de manera centralizada, por tanto, si se tiene acceso por medio de técnicas de hacking a la consola de administración de estos dispositivos es posible acceder a la información personal de los usuarios incluso que sean utilizados como botnet. En este artículo se muestran diferentes falencias que estos dispositivos pueden llegar a tener, incluso ayudar a protegerlos de posibles ataques.

Índice de Términos - Botnet, CrossSite Scripting, IDS/IPS, Hackathon, SSHowDowN Proxy, Wareable.

I. Introducción

En la actualidad el Internet de las cosas IoT, por sus siglas en inglés (Internet of Things) toma cada vez más fuerza ya que se integra a las actividades de la vida cotidiana dentro del deporte, el hogar y hasta el momento de desplazarnos en un vehículo [1]. Estos dispositivos se encargan de estar interconectados y de centralizar la información para que sea accesible y administrada desde la nube o de manera local. Deloitte hizo un estudio en el que identifica que un 55 % de los consumidores adaptan dispositivos en el hogar y un 63 % los lleva a los coches [2] ésto demuestra que IoT está presente en el día a día monitoreando diferentes actividades haciendo que los usuarios esten en pro de la adquisición de nuevos gadgets con funciones específicas que reemplacen hábitos de la vida diaria.

El patrocinio que se le está dando a IOT es tan grande que a la fecha existe un Hackathon [3] encargado de llevar Startup a hacerse realidad pues incentivan a emprendedores a crear su propia Startup que como requisito debe ser integrada en 48 horas y debe tener interacción con Big Data.

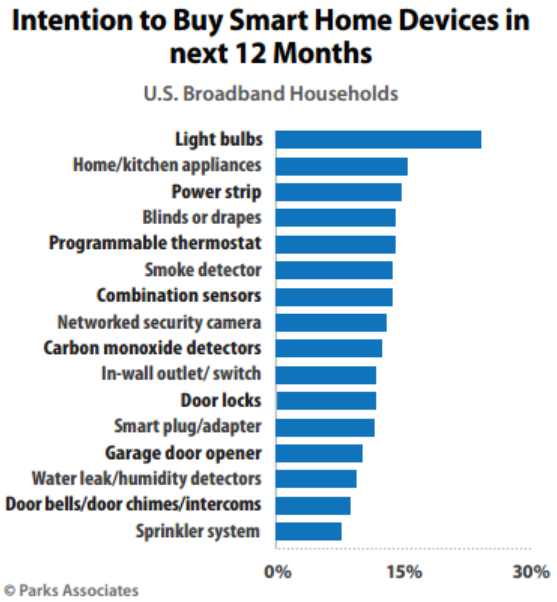

Figura 1. Intención de compra de IoT de los usuarios en los siguientes 12 meses (Parks Associates, 2015)

Según datos de IDC [4] a finales de 2013 habían más de 9.1 billones de dispositivos IoT en línea en donde cada año esta cifra crece un 17.5 % lo que se estima que para 2020 esta cifra llegue a 28.1 billones de unidades instaladas y por lo tanto se convertirá en una cuota considerable de los dispositivos que se encuentren conectados a internet transmitiendo información.

II. Adaptación de los Wearables

II-A. Actividad física

La necesidad de monitorizar la actividad física y signos vitales durante el día a día han cambiado los hábitos de estos usuarios, ya que con cada registro se puede obtener una estadística de uso, y con más datos mejor es la precisión en los resultados. Diferentes aplicaciones hacen uso de objetivos personales en donde se pueden desbloquear logros que ayudan a incentivar la actividad física desempeñada por el usuario final, esto gracias a diferentes plataformas que están enlazadas a Google Fit y Apple Health, plataformas encontradas tanto en Android como en iOS [5], estas opciones hacen que permita llevar un seguimiento en tiempo real de las actividades diarias de los usuarios, por ejemplo, los usuarios pueden monitorizar a sus familiares ya sean adultos mayores o niños con wereables

Figura 2. Recon Snow 2 (Reconinstruments 2016)

Figura 3. Interconexión en el hogar (Digicert, 2014)

que permitan enviar información de ubicación GPS o signos vitales para en caso de tener una alerta sean notificados inmediatamente y así poder tomar acciones.

Otro ejemplo de esto, es el uso de gadgets que permiten obtener información del ambiente para las actividades deportivas, que permiten identificar velocidad o análisis de salto que permiten aumentar la experiencia en directo.

Esto también ayuda a predecir enfermedades o amenazas haciendo diagnosticos más precisos, gracias a patrones de comportamiento que es procesado en tiempo real gracias a que estos wereables están conectados a internet y extraen su información de Big Data

II-B. Hogar

En el hogar es posible tener dispositivos que permitan por ejemplo tener una temperatura personalizada, que suene una canción o disco tan pronto se ingresa a la casa, hacer una completa administración de las luces pues si se está desplazando por un pasillo o llegado a una habitación permite apagar o prender dependiendo de donde se encuentre el usuario, también al despertar es posible abrir paulatinamente las persianas puesto que entre wereables se pueden interconectar y así la información en el caso de la alarma en un dispositivo puede ser enviada a otros dentro del hogar haciendo que las labores del día puedan ser automatizadas dando la sensación de comodidad a los consumidores.

Adicionalmente , es posible agregar una capa de seguridad en el hogar, desde monitorizar cada rincón de la casa con sensores de movimiento, hasta abrir las cerraduras con solo acercar el smarthphone a las cerraduras, esto permite que la información de accesibilidad se encuentre centralizada y permita ser administrada por el propietario gracias a todas las posibilidades que la domótica utiliza en donde la información es llevada a la nube para poder ser consultada en cualquier momento y desde cualquier parte.

II-C. Seguridad

Gracias a que muchos de estos dispositivos están monitorizando constantemente la sensibilidad del ambiente en el que se encuentran ya sea en el hogar, las actividades físicas, el ritmo cardíaco entre otras, esos permiten percibir cuando existe un cambio de rutina identificando y prediciendo posibles accidentes o síntomas anómalos, alertando al momento del evento enviando la información del incidente a contactos registrados entre ellos médicos y familiares.

El uso de las cámaras de seguridad es uno de los más comunes ya que con una sola configuración permite dejarse operando sin intervención pues son capaces de determinar patrones de comportamiento y alertar en tiempo real según las reglas previamente configuradas.

II-D. Ropa Inteligente

Se están haciendo grandes avances en la introducción de tecnología en las prendas de vestir tanto para deportistas integrando sensores en diferentes partes del cuerpo junto con podómetros que se insertan en las zapatillas que permiten cuantificar la cantidad de pasos dados, tiempo de desplazamiento, así como para bebes pues ayudan a determinar los signos vitales que permiten monitorizar las diferentes actividades que está realizando quien las lleva puesta, esto hace que por ejemplo deportistas puedan hacer un seguimiento energético y potencia en diferentes partes de su cuerpo permitiendo controlar y elevar el desempeño de sus actividades, en cuanto a los bebes, controlar la temperatura corporal, respiración, o ritmo cardiaco y enviar la información directamente al Smartphone de los padres.

II-E. IoT en los alimentos

Desde el código de barras que cada alimento comprado en el supermercado se puede identificar los componentes alimenticios que cada producto contiene, así como su fecha de expiración, esta información es procesada, genera alertas y recomendaciones de consumo, haciendo que sea reconocible y se haga seguimiento a los alimentos que el usuario está tomando ayudándole a realizar dietas a gusto.

El constante monitoreo de los alimentos ha llevado a generar el concepto de *Granjas Inteligentes*

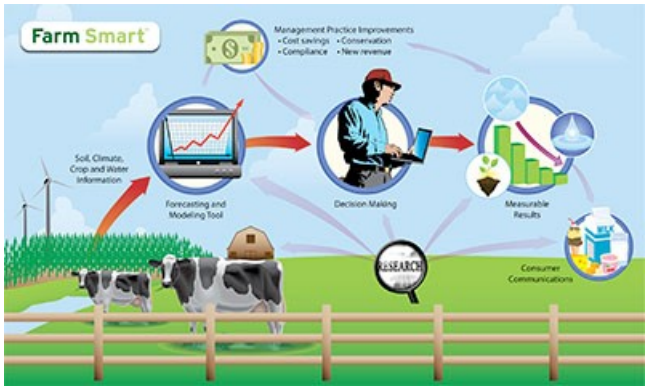

Figura 4. Ciclo de producción en granjas Inteligentes (Dairy - Farm Smart, 2014)

III. Ámbito profesional

Estos wearables dentro de sus funciones están encargados de recolectar todo tipo de información para ayudar a la automatización de tareas tanto personal como profesional. Estos dispositivos son usados como ayuda por ejemplo para recolectar información médica en hospitales de manera rápida y precisa al momento de atención de pacientes.

La siguiente gráfica muestra los servicios top en diferentes industrias en donde el internet de las cosas es de gran utilidad:

Figura 5. Iot en las empresas (netmind.es, 2015)

El enfoque del IoT a nivel empresarial está orientado al Big Data permitiendo a los negocios conocer de manera rápida y efectiva el comportamiento de diferentes actividades que se estén monitoreando, a continuación unos ejemplos de esto:

- Cantidad de vehículos que están circulando por una zona de la ciudad en particular.
- Niveles de contaminación que son recolectados por sensores de aire.
- Cantidad de bombillas que requieren ser revisadas gracias a sensores en las farolas.
- Seguimiento y control de cadena de suministros para los alimentos dando prioridad a la calidad de los alimentos ampliando su caducidad.

Gracias a la información recolectada por estos sensores es posible procesarla y determinar, horas críticas para tomar medidas de circulación, tiempo de vida en promedio que funciona una bombilla en determinado sector de la ciudad para anticipar el cambio antes de que ocasiones inconvenientes por visibilidad.

Es por esto que las empresas tienden a manejar los dispositivos IoT como activos ya que son un fuerte soporte para Big Data generando supervisión continua integrándolos a sus procesos internos.

IV. Iot y sus riesgos de seguridad

Según estudios revelados por HP son más de 25 vulnerabilidades criticas encontradas dentro de IoT dentro de los cuales se incluyen en la mayoría de estos las siguientes falencias:

Privacidad de contenido: Muchos de estos dispositivos hacen una recolección de información personal para iniciar el registro, información como, dirección de correo electrónico, fecha de nacimiento, alergias, incluso, para hacer uso de servicios con meses de gracia se solicita el ingreso de tarjetas de crédito para poder utilizarlo. Estas características aumentan su riesgo cuando la información es almacenada en la nube ya que puede empezar a ser tercerizada.

Los atacantes pueden vulnerar la misma red en la que se encuentra el dispositivo haciendo que por medio de múltiples vectores de penetración pueda capturar información sensible y manipular el dispositivo a voluntad.

Para ayudar a proteger el dispositivo, OWASP indica una serie de ítems que permite identificar posibles vectores de ataque dentro de los cuales se puede identificar lo siguiente:

- La configuración del dispositivo solo debe hacer uso de información indispensable, en lo posible no indicar información sensible en el aprovisionamiento dispuesto para su funcionamiento pues esta puede ser expuesta por mecanismos de cifrado débiles.
- Asegurarse de los datos que son recolectados no sean de naturaleza información sensible evitando introducir información confidencial.
- Asegurarse de que existan perfiles y usuarios autenticados que puedan visualizar la información controlando el acceso a ésta.
- Hacer uso de roles para la consulta y actualización de la información

Tomar estas medidas de seguridad podrá ayudaría al usuario final a evitar el robo de identidad bloqueando el acceso a que sus credenciales sean comprometidas.

Autenticación insuficiente y autorización: Unos de los métodos más prácticos y efectivos usados por los atacantes contra dispositivos IoT es el uso de autenticación débil, también, dependiendo de la plataforma y características del dispositivo, se puede hacer uso de mecanismos de recuperación inseguro para poder tener acceso al dispositivo.

La mayoría de dispositivos hacen uso de componentes móviles que no exigen una contraseña con suficiente complejidad,

Threat Agents	Attack Vectors
Application Specific	Exploitability AVERAGE
Consider anyone who has access to the device itself, the network the device is connected to, the mobile application and the cloud connection including external and internal users.	Attacker uses multiple vectors such as insufficient authentication, lack of transport encryption or insecure network services to view personal data which is not being properly protected or is being collected unnecessarily. Attack could come from external or internal users.
Security Weakness	
Prevalence COMMON	Detectability EASY
Privacy concerns generated by the collection of personal data in addition to the lack of proper protection of that data is prevalent. Privacy concerns are easy to discover by simply reviewing the data that is being collected as the user sets up and activates the device. Automated tools can also look for specific patterns of data that may indicate collection of personal data or other sensitive data.	
Technical Impacts	**Business Impacts**
Impact SEVERE	Application / Business Specific
Collection of personal data along with a lack of protection of that data can lead to compromise of a user's personal data.	Consider the business impact of personal data that is collected unnecessarily or isn't protected properly. Data could be stolen. Could your customers be harmed by having this personal data exposed?

Figura 6. Privacidad de contenido (Owasp 2014)

Threat Agents	Attack Vectors
Application Specific	Exploitability AVERAGE
Consider anyone who has access to the web interface, mobile interface or cloud interface including internal and external users.	Attacker uses weak passwords, insecure password recovery mechanisms, poorly protected credentials or lack of granular access control to access a particular interface. Attack could come from external or internal users.
Security Weakness	
Prevalence COMMON	Detectability EASY
Authentication may not be sufficient when weak passwords are used or are poorly protected. Insufficient authentication/authorization is prevalent as it is assumed that interfaces will only be exposed to users on internal networks and not to external users on other networks. Deficiencies are often found to be present across all interfaces. Many Issues with authentication/authorization are easy to discover when examining the interface manually and can also be discovered via automated testing.	
Technical Impacts	**Business Impacts**
Impact SEVERE	Application / Business Specific
Insufficient authentication/authorization can result in data loss or corruption, lack of accountability, or denial of access and can lead to complete compromise of the device and/or user accounts.	Consider the business impact of compromised user accounts and possibly devices. All data could be stolen, modified, or deleted. Could your customers be harmed?

Figura 7. Autorización/Autenticación insuficiente (OWASP 2014)

contraseñas que fácilmente pueden ser extraídas por medio de diccionario por éste motivo es recomendable hacer uso de políticas de contraseña asegurando que el dispositivo solicite que sea una con complejidad elevada en el momento de que sean seteadas. Por otra parte, es recomendado hacer una análisis de tráfico de red en donde se pueda verificar si el dispositivo transporta información en texto plano en donde se pueda visualizar de manera clara los accesos.

De igual manera que una sesión en un desktop el dispositivo debe en lo posible contar con un sistema de control de sesiones en donde permita administrar roles y privilegios de los usuarios que tienen acceso a éste limitando funcionalidades así como gestionando sus contraseñas para que puedan caducar o ser reestablecidas según las políticas de administración de usuarios.

Muchos de estos dispositivos están implementando autenticación de doble factor permitiendo fortalecer el acceso a la configuración y sus funcionalidades, por tal motivo se recomienda su uso si se encuentra disponible.

Ausencia en el cifrado de transporte: Al momento de enviar información por la red local/wireless e internet, los dispositivos no cuentan con un método de cifrado ni certificado de seguridad haciendo que la información transportada viaje de manera plana lo que permite a los atacantes por medio de técnicas de MITM puedan ver la información de acceso manera clara.

Para ayudar a encontrar debilidades en el protocolo de transporte, es posible implementar las siguientes sugerencias:

- Hacer una revisión de análisis de red en donde se pueda identificar si la información está viajando en texto plano, sin cifrar hacia las diferentes aplicaciones que el dispositivo usa, ya sea local o hacia la nube

Threat Agents	Attack Vectors
Application Specific	Exploitability AVERAGE
Consider anyone who has access to the network the device is connected to, including external and internal users.	Attacker uses the lack of transport encryption to view data being passed over the network. Attack could come from external or internal users.
Security Weakness	
Prevalence COMMON	Detectability EASY
Lack of transport encryption allows data to be viewed as it travels over local networks or the internet. Lack of transport encryption is prevalent on local networks as it is easy to assume that local network traffic will not be widely visible, however in the case of a local wireless network, misconfiguration of that wireless network can make traffic visible to anyone within range of that wireless network. Many Issues with transport encryption are easy to discover simply by viewing network traffic and searching for readable data. Automated tools can also look for proper implementation of common transport encryption such as SSL and TLS.	
Technical Impacts	**Business Impacts**
Impact SEVERE	Application / Business Specific
Lack of transport encryption can result in data loss and depending on the data exposed, could lead to complete compromise of the device or user accounts.	Consider the business impact of exposed data as it travels across various networks. Data could be stolen or modified. Could your users be harmed by having their data exposed?

Figura 8. Lack of Transport Encryption (OWASP 2014)

- Hacer una revisión de los mecanismos de cifrado que se estén usando, pues es necesario que se encuentren actualizados ya que dependiendo de la versión existen diferentes exploits que permiten vulnerarlo y tomar posición tanto del dispositivo como de la información.

Interfaces web inseguras: Seis de cada 10 dispositivos que sirvieron de guía en dicho estudio, muestran debilidades en sus propias páginas web que manejan para hacer la administración de sus funcionalidades, dentro de las debilidades que se encontraron están el uso de comandos crosssite scripting, mala gestión de sesiones y credenciales de autenticación débiles que pueden ser extraídas por medio de métodos de restablecimiento de contraseña con poca seguridad.

El fortalecimiento de las interfaces Web ayudan a que no se usen estos dispositivos como vectores de ataque que puedan ser usados para uno aún más grande.

Para ayudar a configurar y proteger la interface web de la administración del dispositivo se pueden implementar los siguientes ítems:

- Durante la configuración inicial del dispositivo y antes de ajustar las diferentes opciones y funcionalidades, se recomienda hacer una validación de usuarios para identificar las credenciales del administrador/root, verificando que sea posible cambiar la contraeña evitando dejar configurada la que se encuentra por defecto.
- Validar si es posible y puede ser habilitada la opción de bloquear una cuenta de usuario después de x números de intentos fallidos al tratar de iniciar sesión
- Hacer un test de análisis de seguridad (caja negra y caja blanca) al sitio web de administración del dispositivo validando que no tenga problemas de crosssite scripting, sql injection entre otros.
- Hacer una análisis de vulnerabilidades al sitio, validando que no tenga problemas de vulnerabilidades reportadas y que sean explotables
- Hacer uso de políticas de contraseña que eviten usarlas con nivel de fortaleza débil
- Garantizar que los mecanismos de recuperación de contraseña sean robustos y que al momento de hacer una recuperación no le indique al atacante información sensible que permita hacer uso de otras t écnicas como ingeniería social.

Software y Firmware Inseguros: En muchos de los casos el firmware no contaba con hash para validar si se contaba con una versión original firmada de fábrica lo que se identificó que muchos de estos fueron interceptados y manipulados permitiendo que se pueda inyectar código malicioso los binarios descargados.

Una de las recomendaciones en cuanto al software del dispositivo a tener en cuenta al momento de investigar una adquisición es que cuente con la capacidad de que se pueda actualizar y que los parches sean lanzados con regularidad, así evitando que nuevas brechas de seguridad que son expuestas sean cerradas tan pronto son descubiertas.

La comunicación con el servidor de actualizaciones debe ser en lo posible cifrada así como el servidor no debe contar con vulnerabilidades reportadas, esto asegura que la versión que se está descargando para ser implementada no ha sido alterada.

Si es posible, hacer uso de booteo seguro después de aplicar una actualización de firmware validando las funcionalidades que se cargan en el arranque del dispositivo.

Según análisis realizados por Gartner [6] para el año 2020 se estima que se encuentren disponibles y habilitados más de 26 Billones de unidades para el internet de las cosas, lo que se volvería un nuevo mecanismo para realizar ataques distribuidos si no se toman las medidas de seguridad apropiadas para fortalecerlos.

Recientes investigaciones proporcionadas por Akamai Technologies, Inc. [21] han identificado amenazas que ocurren a partir de dispositivos del internet de las cosas para generar tráfico y ataques de remotamente haciendo uso de una vulnerabilidad de más de 10 años llamada SSHowDowN Proxy

Threat Agents	Attack Vectors
Application Specific	Exploitability EASY
Consider anyone who has access to the web interface including internal and external users.	Attacker uses weak credentials, captures plain-text credentials or enumerates accounts to access the web interface. Attack could come from external or internal users.
Security Weakness	
Prevalence COMMON	Detectability EASY
An insecure web interface can be present when issues such as account enumeration, lack of account lockout or weak credenitals are present. Insecure web interfaces are prevalent as the intent is to have these interfaces exposed only on internal networks, however threats from the internal users can be just as significant as threats from external users. Issues with the web interface are easy to discover when examining the interface manually along with automated testing tools to identify other issues such as cross-site scripting.	
Technical Impacts	**Business Impacts**
Impact SEVERE	Application / Business Specific
Insecure web interfaces can result in data loss or corruption, lack of accountability, or denial of access and can lead to complete device takeover.	Consider the business impact of poorly secured web interfaces that could lead to compromised devices along with compromised customers. Could your customers be harmed? Could your brand be harmed?

Figura 9. Insecure Web Interface (OWASP 2014)

incluida en OpenSSH, dentro de los dispositivos usaros para estos ataques se encuentran:

- Circuitos cerrados de televisión (CCTV), grabadoras de vídeo en red (NVR) y grabadoras de vídeo digital (DVR).
- Equipos de antenas de satélites.
- Dispositivos de red (por ejemplo, routers, puntos de acceso, WiMax, módems por cable y ADSL, etc.).
- Dispositivos NAS (almacenamiento conectado a la red) conectados a Internet.

Estos dispositivos comprometidos se han utilizado para el siguiente fin:

- Dirigir ataques DDos contra objetivos y servicios en Internet por medio de protocolos HTTP/HTTPS, SMTP y escaneos de puertos.
- Uso de ataques a la red interna por medio de los dispositivos que allí se encuentran conectados.

Threat Agents	Attack Vectors
Application Specific	Exploitability DIFFICULT
Consider anyone who has access to the device and/or the network the device resides on. Also consider anyone who could gain access to the update server.	Attacker uses multiple vectors such as capturing update files via unencrypted connections, the update file itself is not encrypted or they are able to perform their own malicious update via DNS hijacking. Depending on method of update and device configuration, attack could come from the local network or the internet.
Security Weakness	
Prevalence COMMON	Detectability EASY
The lack of ability for a device to be updated presents a security weakness on its own. Devices should have the ability to be updated when vulnerabilities are discovered and software/firmware updates can be insecure when the updated files themselves and the network connection they are delivered on are not protected. Software/Firmware can also be insecure if they contain hardcoded sensitive data such as credentials. Security issues with software/firmware are relatively easy to discover by simply inspecting the network traffic during the update to check for encryption or using a hex editor to inspect the update file itself for interesting information.	
Technical Impacts	**Business Impacts**
Impact SEVERE	Application / Business Specific
Insecure software/firmware could lead to compromise of user data, control over the device and attacks against other devices.	Consider the business impact if data can be stolen or modified and devices taken control of for the purpose of attacking other devices. Could your customers be harmed? Could other users be harmed?

Figura 10. Insecure Software/Firmware (OWASP 2014)

Esta vulnerabilidad hace que los atacantes puedan tener acceso remoto al dispositivo, en algunos casos hacer escalamiento de privilegios y allí tomar control completamente de la máquina.

Esta vulnerabilidad se da gracias a que la mayoría de los dispositivos que abarcan el internet de las cosas no reciben parches de seguridad ya que al momento de que salen de fábrica están expuestos a éstas falencias.

Vulnerability	Description
Privacy	80% raised privacy concerns regarding the collection of data such as name, email address, home address, date of birth, credit card credentials, and health information
Authorization	80% failed to require passwords of sufficient complexity and length, with most devices allowing passwords such as “1234” or “5678”
Encryption	70% did not encrypt communications to the internet and local network, while 50% of their mobile applications performed unencrypted communications to the cloud, internet or local network
Web Interface	60% raised security concerns with their user interfaces such as persistent XSS, poor session management, weak default credentials and credentials transmitted in clear text
Software	60% did not use encryption when downloading software updates—some downloads could even be intercepted, extracted and mounted, allowing the full code to be viewed or modified

Source: HP Fortify

Figura 11. Vulnerabilidades de IOT (HP Fortify 2015)

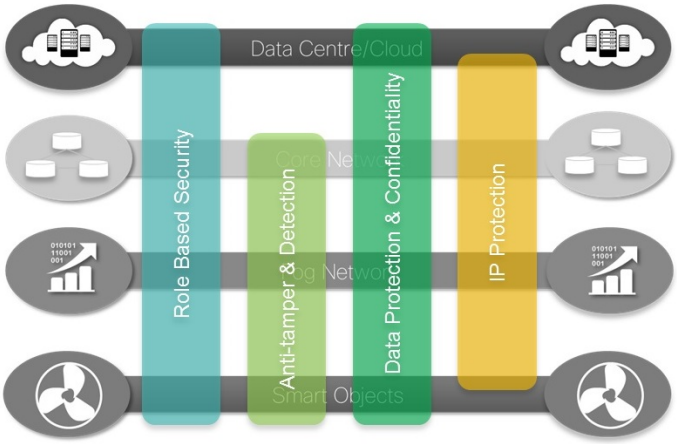

Figura 12. Proposed IoT/M2M Security Framework (Cisco 2015)

V. Aspectos a tener en cuenta en la disminución de riesgos en IoT

Algunos fabricantes ofrecen una capa de seguridad que ayuda a mitigar estas vulnerabilidades, tales como:

- Algunos dispositivos ofrecen la opción de cambiar la contraseña que viene por defecto y generar claves privadas por medio de SSH, ayudando a que se puedan modificar los valores predeterminados.
- Si los dispositivos usan el servicio SSH éste puede ser configurad para que no permita el acceso a la modificación de archivos agregando el parámetro *AllowTcp-Forwarding No* dentro del archivo de configuración sshd_config, también dentro de los archivos de llaves de cada usuario /ssh/authorized es posible agregar restricciones *no-port-forwarding* y *no-X11-forwarding*.
- O bien si el acceso SSH no es indispensable, puede desactivarse para cerrar esa puerta de acceso por medio de la consola de administración del dispositivo.

Uno de los fabricantes que ha creado un framework para que sea adaptado a la seguridad de IoT es Cisco [20], ellos realizaron una investigación proyectada a los próximos 5 años en donde identificaron el crecimiento que los dispositivos IoT van a ocupar en la red, identificando que el crecimiento está destinado a que se adaptaran pequeños sistemas que ejecuten múltiples tareas así como la convergencia de protocolos sobre IP adoptando IPv6. Por este motivo, adoptaron una propuesta de framework que da prioridad a los siguientes ítems:

- **Autenticación**: En este marco se verifica la identidad de quienes tienen acceso a la plataforma de administración desde que se establece el primer enlace, validando el acceso a las diferentes funcionalidades de la infraestructura con perfiles predefinidos. Los puntos de accesos pueden ser definidos por medio de credenciales humanas (Nombre de usuario, contraseña, lectores biométricos, etc.) y los permisos que son concedidos hacen uso de mecanismos electrónicos tales como certificados, direcciones mac, identificación por radiofrecuencia, entre otros.
- **Autorización**: Se establece una relación de confianza entre dispositivos para intercambiar información especifica entre ambos, en donde tan pronto sea validada la autenticidad de ambos dispositivos se procede a compartir más información relacionada. Esto genera un gran reto que es el de crear una infraestructura escalable que permita cubrir el crecimiento de IoT en los próximos años.
- **Políticas de aplicación de red**: Esta capa cubre todos los enrutadores que intervienen en el tráfico para asegurar los paquetes que envían estos dispositivos
- **Visibilidad y Control**: En esta capa intervienen todos los servicios involucrados por los que pueden interactuar los dispositivos IoT, proporcionando visibilidad y monitoreo de las actividades que estos dispositivos están realizando en tiempo real asegurando así la detección y mitigación de amenazas permitiendo tener control del funcionamiento de estos dispositivos.

De no tomar medidas de seguridad para implementar en IoT estos dispositivos pueden ser comprometidos y utilizados entro otros usos para el siguiente fin:

- Dirigir ataques DDoS contra objetivos y servicios en Internet por medio de protocolos HTTP/HTTPS, SMTP y escaneos de puertos.
- Uso de ataques a la red interna por medio de los dispositivos que allí se encuentran conectados.

Si el dispositivo IOT se encuentra dentro de un firewall en una red interna, es recomendable hacer las mismas configuraciones que usa un desktop convencional haciendo uso de los puertos únicamente indispensables, así como cambiando los usados por defecto. Adicional a esto es recomendable limitar el tráfico de salida para evitar que estos dispositivos sean usados como botnet [21]

- Antes de adquirir el dispositivo, es recomendable realizar una investigación sobre las especificaciones y medidas de seguridad que estos manejan junto con las vulnerabilidades que han sido encontradas.
- Hacer uso de las protecciones de seguridad con las que estos dispositivos vienen incluidas, no hacer uso de contraseñas débiles ni dejarlas por defecto.
- Mantener los dispositivos actualizados, es recomendable realizar una política de actualización en estos dispositivos validando si existen medidas de seguridad tomadas por fabricantes que puedan cerrar brechas de seguridad ya identificadas. Por esto es importante registrarlos en las páginas oficiales para que las notificaciones de parches y novedades sobre ellos sean enviadas.
- No es recomendable optar por la opción de menor costo pues en la mayoría de los casos esto identifica que el dispositivo tiene características reducidas, o bien el soporte a este está limitado y no se han tomado medidas de seguridad óptimas. Por esto es recomendable hacer una investigación previa para identificar las marcas que están mejorando sus dispositivos constantemente.
- Mantener al tanto la información que publica el dispositivo, si se detecta un comportamiento fuera de lo común es recomendable revisarlo para identificar si este no ha sido vulnerado.
- No siempre se recomienda hacer una adquisición de un producto tan pronto es lanzado puesto que estos pueden contener problemas de seguridad que aún no han sido encontrados ni expuestos, por esto una de las recomendaciones es esperar que los dispositivos hayan pasado por varias actualizaciones de software que cierren brechas de seguridad.
- Al hacer uso de wereables evitar compartir información personal y sensible con terceros controlando el acceso a internet que estos tengan, así se protege de fuga de información.

VI. Conclusiones

En el origen de internet no se identificó que fuera orientado para estos tipos de dispositivos por tanto se fueron desplegando con capas de seguridad débiles. Con el pasar del tiempo estos dispositivos han sido distribuidos de manera masiva haciendo que se integren medidas de seguridad a las diferentes funcionalidades que estos manejan.

Mientras las medidas de seguridad son sometidas a técnicas como hardening y metodologías como las implementadas por OWASP [7] es necesario prevenir el acceso que se tiene a ellos pues puede existe un alto riesgo de estar vulnerable de que puedan ser usadas por atacantes.

Uno de los grandes retos que tienen los desarrolladores que hacen sus aplicaciones sobre IoT es que necesitan optar por implementar metodologías de seguridad para proteger la información de los usuarios que adquieren estos dispositivos aumentando la confiabilidad que los consumidores tienen sobre estos.

Gracias al crecimiento de estos dispositivos casi exponencial, la amenaza de ataque de día cero son cada vez más probables. Esto hace que implementar medidas de seguridad apropiadas sea una estrategia de protección para asegurar la protección de la información para que no sea vulnerada.

Referencias

[1] Xataca, *Que beneficios reales nos traerá en cinco años el internet de las cosas*, 2015,12, URL:http://www.xataka.com/n/que-beneficios-reales-nos-traera-en-cinco-anos-el-internet-de-las-cosas

[2] Deloitte, *Internet of things GMCS Infographic*, 2014, URL: http://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-Internet-of-things-GMCSInfographic-2015.pdf.

[3] Euskalencounter, *IOT HackAthon*, 2016, URL: http://hackathon.euskalencounter.org/es/hackathon-de-startups/.

[4] IDC, *IDC Market in a minute iot infographic*, 2014, URL:http://www.idc.com/downloads/idc_market_in_a_minute_iot_infographic.pdf

[5] Wareable, *Tech for your connected self*, 2015-04-15, URL:http://www.wareable.com/sport/google-fit-vs-apple-health

[6] Gartner, *Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020*, 2014, URL:http://www.gartner.com/newsroom/id/2636073

[7] OWASP IOT, *OWASP Internet of Things Project*, 2016, URL:https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

[8] Diario TI, *Vulnerabilidades en IOT*, 2015, URL:http://diarioti.com/atacantes-se-aprovechan-del-internet-de-las-cosas-que-no-admiten-parches/101162

[9] Diario TI, *VMWare anuncia alianzas y estrategias para internet de las cosas*, 2016-08-26, URL:http://diarioti.com/vmware-anuncia-alianzas-y-estrategias-para-internet-de-las-cosas/100145

[10] HP, *Internet of things research study*, 2015, URL:https://community.hpe.com/t5/Protect-Your-Assets/HP-Study-Reveals-70-Percent-of-Internet-of-Things-Devices/ba-p/6556284?jumpid=va_y92mxk3jtn#.WA9kRPnhCM-

[11] McAfee, *No te preocupa la seguridad para IOT puesdeberia*, 2016-07-18, URL:https://blogs.mcafee.com/languages/espanol/no-te-preocupa-la-seguridad-para-el-internet-de-las-cosas-pues-deberia/

[12] Netmind, *IOT Aportacion Big Data*, 2016-07-06, URL:http://www.netmind.es/knowledge-center/internet-of-things-iot-aportacion-big-data/

[13] OWASP, *Insufficient Authentication/Authorization*, 2014, URL:https://www.owasp.org/index.php/Top_10_2014-I2_Insufficient_Authentication/Authorization

[14] OWASP, *Privacy Concerns*, 2014, URL:https://www.owasp.org/ index.php/Top_10_2014-I5_Privacy_Concerns

[15] OWASP, *Insecure Web Interface*, 2014, URL:https://www.owasp.org/index.php/Top_10_2014-I1_Insecure_Web_Interface

[16] OWASP, *Insecure Web Interface*, 2014, URL:https://www.owasp.org/index.php/Top_10_2014-I9_Insecure_Software/Firmware

[17] Parks Associates, *ParksAssoc Connected-Consumer TopTrends in IoT 2015*, 2015, URL:http://www.parksassociates.com/bento/shop/whitepapers/files/ParksAssoc-ConnectedConsumer-TopTrends-in-IoT-2015.pdf

[18] PricewaterhouseCoopers, *The Wearable Future - PwC*, 2014-11, URL:https://www.pwc.com/mx/es/industrias/archivo/2014-11-pwc-the-wearable-future.pdf

[19] PCWorld, *Consejos para proteger sus dispositivos de IoT*, 2016-02-10, URL:http://www.pcworld.com.mx/Articulos/35613.htm

[20] Cisco, *Securing the Internet of Things: A Proposed Framework*, 2015, URL:http://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html

[21] Akamai, *Vulnerabilidad en IOT*, 2016-10-11, URL:https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/sshowdown-exploitation-of-iot-devices-for-launching-mass-scale-attack-campaigns.pdf

Autor

William Andrés Coy Sosa Estudiante de Especialización en Seguridad Informática de la Universidad Piloto de Colombia, Ingeniero de Sistemas de la Fundación Universitaria San

Martín, con experiencia en el ámbito laboral en tecnologías de la información de más de 6 años, labora actualmente en el campo de las comunicaciones, infraestructura tecnológica y seguridad de la información.