Aspectos de Seguridad en Internet de las Cosas

Alicia Castro[1], Eduardo Casanovas[3], Veronica Gil-Costa[1,2],

[1] Universidad Nacional de San Luis, San Luis Argentina
[2] CONICET, Consejo Nacional de Investigaciones Científicas y Técnicas
[3] Instituto Universitario Aeronáutico
adcastro@unsl.edu.ar; ecasanovas@iua.edu.ar; gvcosta@unsl.edu.ar

Resumen. Actualmente, los ataques contra la ciberseguridad han producido efectos económicos adversos, afectando no sólo a compañías privadas, sino también a estados gubernamentales y a las personas en sus hogares. La diversidad de ataques que se producen continuamente alrededor del mundo y la diversidad de dispositivos – en la mayoría dispositivos de IoT - con las que se utilizan, hace casi imposible generar un único protocolo o framework de seguridad que sea aplicable en todos los casos. Más aún, estadísticamente se ha reportado que la mayoría de los casos de ataques se producen por la falta de protección básica (como cambios en claves de seguridad) que los usuarios finales deberían proveer a sus dispositivos. En este trabajo se clasifican los dispositivos IoT y las vulnerabilidades. Se realiza un análisis de los protocolos, modelos y arquitecturas de seguridad existentes.

Keywords: Internet de las cosas. Seguridad. Privacidad. Smart Cities. IoT. Arquitecturas de Seguridad IoT. Ciberseguridad.

1 Introducción

En la actualidad encontramos Internet de las Cosas (Internet of Things - IoT) que permite conectar enorme cantidad de dispositivos y brindar servicios en distintos ámbitos de la vida diaria, obteniendo y distribuyendo información por la web, incrementando la apertura y complejidad de las redes, lo que lleva a nuevos desafíos de seguridad. Gartner.Inc estima que habrá más de 20 millones de dispositivos conectados para el 2020 [1].

Los dispositivos IoT pueden ser utilizados en distintos ambientes: industria, ciudades inteligentes (Smart Cities), agricultura inteligente, edificios inteligentes, Salud, finanzas, etc. De acuerdo a la utilización que se dé a estos dispositivos, se pueden categorizar en [1]: dispositivos para consumidores finales, dispositivos utilizados en el área de salud, dispositivos de uso en infraestructuras industriales (IIoT) y dispositivos utilizados en Smart Cities. Dentro de la primera categoría encontramos todos los electrodomésticos inteligentes, que si bien resultan útiles para controlar tareas rutinarias del día a día, también ofrecen a los ciberdelincuentes una nueva puerta de entrada. Respecto a los dispositivos de uso en el área de salud, se pueden observar que su uso se incrementa día a día, desde instrumentación médica con conexión inalámbrica (Estetoscopio inalámbrico, termómetro, monitor de

glucosa), productos farmacológicos (caja de pastillas inteligentes), herramientas de diagnóstico (Diabetes, Azoi), hasta dispositivos IoT implantables (desfibrilador, marcapasos). Los dispositivos de IoT utilizados en ciudades inteligentes (Smart City - SC) se utilizan en distintos entornos, geográficamente dispersos, algunos de ellos continuamente en movimiento. Se podría decir que una SC está conformada por una grilla inteligente de "cosas vulnerables" conectadas que colaboran en el funcionamiento de una sociedad moderna. En sistemas industriales, los dispositivos utilizados ayudan a automatizar la transmisión de datos entre dispositivos mecánicos o eléctricos.

Existen distintos factores que contribuyen a que los dispositivos IoT sean vulnerables: mezcla de malos diseños, entornos no regulados o regulados ineficientemente, entre otros. Los atacantes pueden usar las vulnerabilidades de estos dispositivos para obtener acceso permanente a estos equipos y a la infraestructura de red por la cual están conectados. Durante el año 2017, se han realizado nuevos ataques que utilizan distintos tipos de dispositivos, que ponen en riesgo la seguridad y privacidad de los dispositivos. Un informe brindado por Ponemon Institute y el Shared Assessments Program [2], indica que el 63% de los ataques registrados fueron dirigidos en contra de cámaras IP o grabadores digitales de vídeo y el 20% estuvieron dirigidos a dispositivos de red como módems DSL, routers y equipos similares, afectando a naciones como: China (17%), Vietnam (15%), Rusia (8%) y en un 7% a Taiwán, Turquía y Brasil.

En este trabajo presentamos un análisis y clasificación de los dispositivos utilizados en IoT y sus vulnerabilidades. En particular, nos enfocamos en el aspecto de la comunicación entre los dispositivos para detectar las características que deben ser consideradas en diferentes niveles o capas de seguridad. Para ello, en la Sección 2 presentamos las características de los dispositivos IoT y su arquitectura. En la Sección 3 se muestran las características referentes a la seguridad informática. La sección 4 presenta las conclusiones y trabajos futuros.

2 Características de los dispositivos IoT

Los dispositivos IoT son minicomputadoras. Cuyo hardware, son procesadores (microcontroladores) y plaquetas para uso específico, por lo cual existen diferentes fabricantes y diversidad de modelos. Con respecto al software, algunos disponen de firmware, otros de Sistema Operativo (Google tv, WebOS, Android Things, Tizen, Zephyr) y de aplicaciones de propósito específico.

Existe una gran cantidad de dispositivos IoT que no son interoperables, aunque existe soluciones de software para lograr interoperabilidad entre dispositivos de diferentes fabricantes con distintos sistemas operativos. Por ejemplo, AllJoyn que se utiliza en los televisores LG y en altavoces Panasonic. Se han conformado asociaciones de empresas que definen estándares comunes, uno de ellos es Open Interconnect Consortium [3], que brinda código abierto para crear un estándar común.

A nivel de comunicaciones, se pueden adquirir diferentes módulos que proveen distintos protocolos de comunicación. Se pueden distinguir entre dos grupos, según la aplicación que se pretenda dar: (1) sin restricciones o limitaciones (NTU), con enlaces de comunicación de alta velocidad, en el rango de transferencias con una tasa igual o

superior al Mbit/s y bajas latencias en el nivel de enlace, más afectadas por las congestiones en la red que por las propias características físicas de los elemento, y (2) restringidas o limitadas (NTC) con enlaces de comunicación de baja velocidad, en el rango de transferencias inferior al Mbit/s y grandes latencias, tienen tecnología a nivel físico de baja capacidad y políticas de ahorro de energía. En cuanto a los protocolos de comunicaciones en dispositivos IoT, podemos encontrar diferentes protocolos.

Gran parte de los dispositivos IoT de consumidores, utiliza el entorno web para la transmisión y visualización de los datos, por lo cual se utilizan los protocolos HTTP, websocket, XMPP. Sin embargo, han surgido alternativas a estos protocolos cuyo consumo de recursos es menor, por ejemplo, CoAP (protocolo de aplicación para redes con baja potencia y pérdida). Un ejemplo son las aplicaciones en los dispositivos móviles para monitoreo de actividades físicas que usan HTTPS para transferir comunicaciones con los servidores remotos.

Para redes Inalámbricas de Área Personal (WPAN), con capacidades limitadas en procesamiento, poca memoria, baja potencia, bajo costo y corto alcance, existen protocolos que trabajan bajo la normativa de la IEEE 802.15.4 como (a) LoWPAN, (b) 6lowPAN definido en la RFC 4944 para IPv6, (c) Zigbee, protocolo estándar en redes de sensores. También están los protocolos basados en la especificación de la IEEE 802.15.1 (Bluetooth), que facilita la interoperabilidad entre diferentes dispositivos empleando un enlace por radiofrecuencia en la banda de 2.4 GHz. Reconocido por Ericsson, Nokia, IBM, Toshiba e Intel. También se puede usar IPv6 con Bluetooth de baja potencia (BLE).

Para grandes redes de pequeños dispositivos que necesitan la supervisión o el control de un servidor de back-end en Internet, se puede usar MQTT, protocolo de Telemetría de cola de mensajes muy ligero, útil en redes con bajo ancho de banda y alta latencia o poco confiables, ofrece pocas opciones de control, es eficiente en términos de ancho de banda, independiente de los datos y tiene reconocimiento de sesión continua, no está diseñado para la transferencia de dispositivo a dispositivo, ni para realizar "multidifusión" de datos a muchos receptores.

En entorno industrial, los dispositivos de IoT usan el protocolo Data Distribution Service (DDS), estándar elegido por el Industrial Internet Consortium como plataforma de comunicación para construir sistemas inteligentes en Internet Industrial. En el ámbito de empresas de servicios (energía, gas, agua), se utiliza DNP3 (Distributed Network Protocol) protocolo industrial para comunicaciones entre equipos inteligentes (IED) y estaciones controladores, componentes de sistemas SCADA. DNP3 es actualmente compatible con las especificaciones del estándar de seguridad para infraestructuras de Sistemas de Información para la energía IEC 62351-5. El estándar IEEE 1379-2000 propone una guía para la comunicación entre RTU y dispositivos electrónicos inteligentes (IED) en entornos de energía, incluyendo cifrado y una serie de prácticas que mejoran la seguridad frente a métodos intrusivos conocidos. También está el estándar TC 57, responsable del desarrollo de estándares para el intercambio de sistemas de energía y otros relacionados como SCADA y distribución de automatización y tele protección.

Para interconectar vehículos (Internet de los Vehículos IoV) se usa el protocolo de comunicaciones de corto rango dedicado (DSRC) que soporta transmisiones rápidas de mensajes entre vehículos, infraestructura y aplicaciones. Para comunicaciones internas de CPU a periféricos, existen protocolos como I2C (Inter-Integrated Circuit)

y SPI (Serial Peripheral Interface). En cualquier ámbito, a nivel de red, existen varios protocolos utilizados en IoT como IPv6 pensado para convertirse en el estándar de comunicaciones en Internet, o Thread [4] protocolo para redes inalámbrica, para interconectar dispositivos de bajo consumo de uso hogareño.

2.1 Arquitectura IoT

Existen múltiples propuestas de arquitecturas para IoT [5], algunas privadas creadas para un fin específico, y otras open source desarrolladas por un consorcio de empresas relacionadas con IoT que pretenden brindar esta arquitectura para uso general. Un ejemplo de una arquitectura global está conformada por el dispositivo final IoT sensor-actuador ("Things") conectado (generalmente de modo inalámbrico) a otro dispositivo que permite la interconexión a Internet para brindar a un usuario, servicios de terceros o interactuar con servidores Cloud. Disponer de varias arquitecturas para Sistemas IoT, hace difícil la interoperabilidad de estos sistemas y resulta complejo brindar la seguridad y privacidad a los sistemas IoT.

OpenIoT es una plataforma open source [6] que incluye funcionalidades para componer dinámicamente y bajo demanda servicios IoT. Provee la posibilidad de recolectar y procesar los datos obtenidos de cualquier sensor, incluyendo dispositivos físicos, algoritmos de procesamiento de sensor, algoritmos de procesamiento de redes sociales, herramientas para describir los datos del sensor semánticamente según las especificaciones de W3C (Semántica para Redes de Sensores), envío de datos de diferentes sensores a la infraestructura en Cloud, descubrimiento dinámico de sensores y sus datos, visualización de datos IoT en formatos apropiados (gráficos, esquemas, mapas), optimización de recursos con el middleware OpenIoT y la infraestructura Cloud.

La arquitectura abierta de IoT V3.0 [7], generada por un proyecto europeo IoT-A y patrocinado por una gran cantidad de empresas europeas, incluye distintos modelos relacionados a las propiedades de confianza, seguridad, privacidad y confiabilidad.

3 Seguridad en IoT

En esta sección, presentamos un análisis y clasificación de los dispositivos utilizados en IoT y sus vulnerabilidades. Actualmente, es necesario repensar enfoques, ajustar herramientas, métodos y procedimientos para mejorar la seguridad en sistemas IoT.

La diversidad de hardware, de software y de protocolos de comunicación, implica mayor análisis y compromete en mayor medida la seguridad en los sistemas y dispositivos IoT. Muchos dispositivos IoT tienen sistemas operativos portables sin configurar, a menudo con un conjunto de utilidades utilizadas en el ámbito de desarrollo, pero que no deberían estar disponibles en sistemas de producción, por ejemplo, acceso por Shell. En muchos desarrollos de sistemas IoT se usan componentes de software de tercero (como librerías), que pueden incorporar vulnerabilidades. La violación a la seguridad de los dispositivos IoT, puede radicar en: (1) Los dispositivos IoT como víctimas y (2) los dispositivos IoT como herramientas de ataques.

Actualmente, surgen interrogantes sobre quien tiene la responsabilidad de resolver los problemas de seguridad de los dispositivos de IoT conectados a Internet ¿le corresponde al fabricante, al vendedor, al usuario?, ¿debe ser regulado por los gobiernos? No siempre queda claro quién es responsable de las decisiones de seguridad: una compañía diseña un dispositivo, otra provee el software, otra opera la red en la que se lo integra y otra pone a disposición el equipo. No existen normas y estándares aceptados a nivel internacional.

Un estudio [2], reveló que el 94% de los expertos considera firmemente que los dispositivos del IoT que no estén debidamente protegidos podrían detonar un incidente de seguridad "catastrófico". El 76% piensa que cualquier momento en los próximos dos años se producirá un ataque DDoS (Distributed Denial of Service) a través de IoT. El 77% admite que no considera el riesgo de IoT al desplegarlos, ya que delega este tema en las terceras partes involucradas. Además, el 67% no evalúa las prácticas seguridad y privacidad de las terceras partes antes de generar una operación de negocios con ellos. Con respecto al esfuerzo de seguridad, el 94% lo direcciona a un firewall de red tradicional para manejar las amenazas de IoT.

3.1 Amenazas en IoT

En el informe de la empresa Karsperky de junio del 2017, indica que han detectado 7.000 tipos distintos de malware que atacan a dispositivos IoT, de los cuales el 50% han sido desarrollados en 2017 y tienen como objetivo el espionaje, extorsión y chantaje [8]. El malware Mirai, tiene tres componentes principales: un módulo de comando y control que establece la comunicación; un escáner de redes, que permite infectar otros dispositivos de la IoT desde un equipo de retransmisión; y un módulo de ataque, que permite hacer uso y abuso del tráfico legítimo de las redes.. El malware Hajime [9] surgió para evitar que el dispositivo sea infectado por el malware Mirai cerrando los puertos utilizados en los ataques de DDoS. Tiene un módulo de propagación, se expande usando redes P2P descentralizadas (en vez de servidores de control y comando) y utiliza diferentes técnicas para ingresar al dispositivo e infectarlo. Si bien surgió como un software con fines benéficos para la seguridad informática, en abril del 2017 se conocieron ataques empleando este malware.
La Tabla 1 muestra algunas amenazas del procesamiento, comunicación y almacenamiento de la información, presente en cualquiera de las categorías de dispositivos IoT [1] [5].

Tabla 1: Clasificación de las amenazas en IoT

Clasificación	Descripción
Suplantación de identidad	Un atacante obtiene la clave del dispositivo, a nivel hardware o software.
Denegación de servicio	Dejar sin funcionar un dispositivo, impedir la comunicación, o brindar un servicio.
Manipulación de la información	Manipulación o reemplazo de los componentes del sistema operativo. Lectura de datos desde el almacenamiento de información. Manipulación de datos de telemetría, de datos de control de comandos en cola o en la memoria caché, de paquetes de actualización de configuración o firmware

	durante el almacenamiento en caché o en la cola local.
Divulgación de información	Cuando un dispositivo ejecuta un software manipulado que proporciona datos a partes no autorizadas.
Elevación de privilegios	Se puede forzar a un dispositivo que realiza una función específica a realizar otra función.
Suplantación, revelación de información	Los dispositivos tienen a menudo funciones de seguridad, como PIN o contraseña, o se basan totalmente en confiar en la red, lo que significa que concederán acceso a la información cuando un dispositivo se encuentre en la misma red y con frecuencia dicha red sólo esté protegida por una clave compartida.
Alteración	Un atacante puede interceptar o invalidar parcialmente la difusión y enviar información falsa.

A continuación, se muestran los riesgos por categorías de dispositivos IoT. [5]

Dispositivos IoT de Consumidores: Obtener acceso al dispositivo para beneficio personal. Acosadores puede usar la información de localización. Identificación de patrones. A modo de ejemplo se mencionan amenazas detectadas: a) En junio 2016 [10] se detectó un malware tipo ransomware conocido como "flocker" que afectó a Smart TV LG con S.O. Android, con el objetivo de obtener datos, encriptarlos y bloquear la pantalla para pedir "rescate" de dinero para su desbloqueo. b) En Marzo del 2017 [11], la empresa Oneconsult ha logrado emitir un malware capaz de tomar el control del televisor emitido por la frecuencia de TDT (Televisión digital Terrestre). Esto no solo afectaría a los TVs sino a cualquier dispositivo en el rango de acción de la antena. Probado en Smart TV Samsung. c) La empresa Slashgear [12] reporta una vulnerabilidad presente en varios Smart TV's que podría permitir a atacantes vulnerar cientos de dispositivos al mismo tiempo.
Dispositivos IoT para la Salud: Violación a la vida (causar daño a pacientes VIP). Pérdida de privacidad (brindar información confidencial de los pacientes). Diagnóstico no confiable debido a fallas en software o hardware. Modificación de información, generando toma de decisiones nocivas para la salud. Efectos nocivos para el cuerpo humano por ingesta incorrecta de medicamentos
Dispositivos utilizados en Infraestructura Industrial: Destrucción o daño físico causado por el ciber o eco-terrorismo. Interrupción de operaciones por broma o "hacktivismo". Robo de productos a ser entregados por el drone y/o robo del propio dispositivo en sistemas aéreos sin tripulación.
Dispositivos IoT utilizados en Smart Cities. Daños o destrucción física causados por Ciber-terrorismo.

3.2 Vulnerabilidades

Existe un conjunto amplio de vulnerabilidades en los dispositivos IoT [13] como son: Comunicaciones locales y remotas sin encriptar, almacenamiento sin cifrar, acceso remoto por Shell, cuentas ocultas, acceso a través de las interfaces UART (Universal Asynchronous receiver transmitter) y JTAG, entre otros.

Las redes radio cognitivas [14], cuyo acceso al espectro es dinámico, son extremadamente vulnerables a ataques maliciosos, particularmente porque los

usuarios secundarios no son propietarios del espectro. Al tener una red con alto dinamismo se hace difícil aplicar medidas de seguridad, por lo que los métodos para asegurar un espectro compartido son críticos. La amenaza más crítica es impedir comunicaciones de usuarios secundarios.

A continuación, se mencionan algunas vulnerabilidades reportadas por distintas empresas del ámbito de seguridad Informática.

Vulnerabilidades de monitores de bebé de diferentes marcas, detectadas por la empresa Rapid7 [13] en septiembre del 2015. Presenta problemas de acceso físico al dispositivo, acceso desde una LAN y desde Internet, por ejemplo: a)La vulnerabilidad CVE-2015-2886 permite que cualquier usuario autenticado en el sitio ibabycloud.com puede observar la cámara y los registros de video de otro usuario debido a la vulnerabilidad de referencia de objetos directos. b) La vulnerabilidad CVE-2015-2887, muestra cómo se puede acceder por telnet o UART al dispositivo accediendo con usuario común (admin) hardcodeados en su código. c) La vulnerabilidad CVE-2015-2883, muestra como el servicio web para crear sesiones remotas de streaming es vulnerables a ataques XSS y Session hijacking.

Vulnerabilidades en productos wearable que permiten a las personas estar conectados en todo momento. La empresa Open Effect [15] realizó una investigación mostrando cómo algunas empresas fabricantes de estos productos no tienen en cuenta la privacidad, permitiendo obtener información del dispositivo.

Vulnerabilidades en dispositivos de salud [16]: en bombas de infusión se encuentran fallas de ausencia de autenticación para las sesiones telnet, almacenamiento de claves de acceso en texto plano, trabajan con versiones de servidor web vulnerables, código de credenciales asociados a FTP hardcodeados, los dispositivos cardiacos implantables no tienen implementado una lista de comandos autorizados. En lo que respecta a la autenticación, 3 de 4 fabricantes de dispositivos de monitoreo cardiaco hogareños, tienen hardcodeadas las credenciales que permiten autenticar los pacientes en la red.

Vulnerabilidades detectadas en los televisores Smart TV: En diciembre del 2012, detectaron una falla en Smart TV Samsung led 3D, que permite obtener acceso al TV de forma remota y así modificar archivos y modificar la configuración del control remoto. En julio del 2013, se detectó la vulnerabilidad (CVE-2013-4890) en el servidor web de Smart TV Samsung PS50C7700, que permite ejecutar un exploit para resetear el televisor utilizados en un ataque DoS.

Vulnerabilidades en Cámaras IP: En junio 2017, un estudio generado por empresa de seguridad F-Secure, encontró problemas de seguridad en cámaras IP de varias empresas.

3.3 Ataques sobre Dispositivos IoT

Los dispositivos IoT pueden ser atacados por ciberdelincuentes por distintos motivos: entretenimiento, obtener información confidencial, y cibertaques utilizando el poder computacional y de comunicaciones del dispositivo y asi poder conformar una botnet para atacar a un objetivo específico y dejarlo sin servicio, lo que se conoce como Ataque de Denegación de Servicio Distribuido (DDoS). A continuación se darán algunos ejemplos de estos tipos de ataque.

Ataque de Denegación de Servicio Distribuido usando dispositivos IoT [1]
En julio de 2015, la revista Wired reveló que piratas informáticos habían alterado remotamente la conducción de velículos Jeep Cherokee. Fiat Chrysler Automóviles NV, tomó medidas de seguridad a nivel de red para evitar este tipo de manipulación remota. También programó una campaña de recuperación preventiva de 1,4 millones de automóviles y camiones equipados con radios vulnerables en los EE. UU.

El 23 de diciembre de 2015, la distribución de energía en Ucrania fue afectada por un ataque que interrumpió el servicio de una gran cantidad de usuarios durante varias horas. Los piratas informáticos usaron el troyano BlackEnergy para acceder al sistema de gestión de la distribución de energía y fueron así capaces de emitir comandos de interrupción del servicio, borrar y sobrescribir datos del sistema y realizar operaciones de apagado

En octubre del 2016, se produjo el mayor ataque de DDoS de la historia contra la compañía de hosting francesa OVH y el proveedor de DNS estadounidense Dyn, que forzó la desconexión de más de 100 sitios web (Twitter, Spotify, Netflix, Amazon, GitHub, PayPal, etc) por varias horas. El ataque se produjo utilizando una botnet conformada por dispositivos IoT infectados con el malware Mirai. Se realizaron tres ataques que involucraron a más de 10 millones de direcciones IP que generaron un tráfico superior a 1 Tbit/s.

Ataques a dispositivos para obtención de información confidencial
La empresa VTech anunció en diciembre del 2015 que sufrió una violación de seguridad exponiendo datos personales de 12 millones de personas. El ataque fue explotando una vulnerabilidad de SQL injection y servicios de registración de usuario sin encriptar (TLS) en dispositivos de juegos electrónicos de enseñanza.

En agosto del 2014 [17], el termostato inteligente Nest de Google, dispositivo que ayuda a aprender sobre los hábitos de calefacción y refrigeración sufrió un ataque que demostró la posibilidad de obtener el control total de Nest en segundos.

3.4 Modelos de seguridad actuales

En esta sección se mencionan algunas propuestas para brindar seguridad a sistemas IoT ya desplegados y se describen los modelos de seguridad propuestos en algunos de las arquitecturas IoT analizadas en las secciones anteriores.

Diferentes organismos gubernamentales han generado lineamientos para que los desarrolladores y usuarios introduzcan la seguridad dentro de la arquitectura. El departamento de Seguridad Nacional de Estados Unidos [18], presenta seis principios estratégicos para asegurar IoT con el objetivo de informar a usuarios, operadores y fabricantes para que tomen decisiones conscientes al trabajar con dispositivos conectados. Estos principios incluyen: (a) Incorporar la seguridad en la fase de diseño. (b) Actualizaciones de seguridad y gestión de vulnerabilidades de avanzada. (c) Construir sobre prácticas de seguridad probadas, implementar la defensa en capas, compartir información relacionada a incidentes y vulnerabilidades. (d) Priorizar las medidas de seguridad según el impacto potencial. (e) Promover la transparencia de IoT. Abarcar a todos los componentes e incluir a desarrolladores y fabricantes. (f) Proponer la implementación de "conexiones intencionales" y selectivas.

Arquitectura de seguridad para IOT.
La arquitectura de seguridad sistemática (IPM) [19], integra conciencia e interacción del mundo real, cibernético, y social dentro del modelo U2IoT, arquitectura típica de IoT compuesta por unidades IoT (redes y sensores IoT, nodos de control distribuido, gestión y centralización de centros de datos) y dispositivos IoT ubicuos (IIoT, local IoT, global IoT, nacional IoT). La arquitectura considera tres aspectos: a) El modelo de seguridad de información considera los requerimientos de seguridad básica y avanzada para tratar los sensores, red, aplicación y atribuciones sociales. b) La seguridad física incluye la infraestructura, ubicación y estado de la entidad, información de trazabilidad y condiciones del mundo real. c) La gestión de seguridad provee recomendaciones estratégicas por jerarquías clasificando escenarios con racionalidad y compatibilidad.

La arquitectura abierta de IoT (IoT-A) [7], incluye distintos modelos relacionados a las propiedades de confianza, seguridad, privacidad y confiabilidad. El modelo de confianza provee integridad de datos y confidencialidad, autenticación en puntos finales y no repudio entre dos entidades que interactúan. Incluye a) dominios de confianza, b) mecanismos de evaluación de confianza, basado en analizar información almacenada previamente del sujeto. c) políticas de comportamiento que regulan la manera en que dos sujetos con el mismo dominio de confianza interactúan; d) definición de niveles de confianza (local, global o centralizado); e) disponer de una federación de confianza que delimite las reglas de las relaciones de confianza entre los sistemas y los diferentes modelos de confianza; f) soportar M2M (Machine to machine) que permite interactuar máquinas autónomas evaluando la integridad de cada una.

Microsoft propone un modelo de seguridad [20] basándose en el modelo de riesgos. Consta de los siguientes pasos: a) Modelar la aplicación, b) Enumerar las amenazas, c) Mitigar las amenazas d) Validar las mitigaciones. Este modelo de riesgos de IoT es el utilizado en la arquitectura de referencia de IoT Microsoft Azure.

4 Conclusiones y Trabajo Futuro

En este trabajo presentamos un análisis de los aspectos de seguridad relevantes para dispositivos IoT. Conocer la forma en que un atacante podría poner en peligro un sistema ayuda a tomar las medidas pertinentes desde el principio, por lo cual es de suma importancia conocer sobre la seguridad de los sistemas y dispositivos utilizados en Internet de las cosas, conociendo cuales son las amenazas, vulnerabilidades y ataques presentes en este ámbito.

Como trabajo futuro, se planea investigar y proponer un modelo de seguridad y privacidad para el diseño de los dispositivos IoT y la implantación de los mismos dentro de sistemas IoT. Considerando la integración de los diferentes protocolos de comunicación, considerando los distintos niveles o capas del sistema de comunicación y de los distintos elementos que forman parte de una arquitectura IoT, para obtener así un sistema IoT seguro. Este modelo debe incluir las propiedades de confianza, seguridad, privacidad y confiabilidad, brindando integridad de datos, confidencialidad, autenticación, disponibilidad y no repudio. Para lo cual es

importante conocer las amenazas a las que puede estar expuesto y agregar las defensas adecuadas durante el diseño de la arquitectura. Es especialmente importante diseñar productos que consideren desde el principio, un modelo de seguridad integral.

5 Referencias

1. Creación de un mundo IoT fiable y gestionado. Instituto Nacional de Ciberseguridad (INCIBE). España. (2017).
2. C. Forrest: http://www.techrepublic.com/article/94-believe-unsecured-iot-devices-could-lead-to-catastrophic-cybersecurity-attack/. (17-05-2017)
3. Open Interconnect Consortium. https://openconnectivity.org/.
4. Thread Protocol. Threads group. http://threadgroup.org/news-events/press-releases/ID/20/Introducing-Thread-A-New-Wireless-Networking-Protocol-for-the-Home.
5. Future-proofing the Connected World. Cloud Security Alliance (CSA). Report. (2016).
6. IoT Open Plataforms. http://open-platforms.eu/library/openiot-the-open-source-internet-of-things/. (05-11-2014)
7. M. Bauer, M. Boussard, N. Bui, F. Carrez, C. Jardak y J. D. Loof: Internet of Things – Architecture IoT-A – Final architectural reference model for the IoT v3.0. Report (2013).
8. Trampas para el Internet de las cosas. https://securelist.lat/honeypots-and-the-internet-of-things/85165/. (19-06-2017)
9. Hajime, the mysterious evolving botnet. https://securelist.com/hajime-the-mysterious-evolving-botnet/78160/. (25-04-2017)
10. E. Duan: http://blog.trendmicro.com/trendlabs-security-intelligence/flocker-ransomware-crosses-smart-tv/ (14-1-2016)
11. D. Goodin: https://arstechnica.com/security/2017/03/smart-tv-hack-embeds-attack-code-into-broadcast-signal-no-access-required/ (31-03-2017)
12. R. Waugh: https://www.welivesecurity.com/la-es/2014/06/10/peligro-smart-tv-vulnerabilidad-ataques-en-masa/ (10-06-2014)
13. T. B. Mark Stanislav: HACKING IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities. Rapid 7. https://goo.gl/Uh7y4e (Septiembre 2015)
14. S. Kim: Cognitive Radio Anti-Jamming Scheme for Security Provisioning IoT Communications. (2015).
15. Every Step You Fake A Comparative Analysis of Fitness Tracker Privacy and Security. Open Effect. (2016).
16. B. Rios y J. Butts: Security Evaluation of the Implantable Cardiac Device Ecosystem Architecture and Implementation Interdependencies. WhiteScope. (2017).
17. Y. Jin, G. Hernandez y D. Buentello: https://www.blackhat.com/us-14/briefings.html#smart-nest-thermostat-a-smart-spy-in-your-home (2014)
18. Strategic Principles for securing the Internet Of Things (IoT). U.S. Department of Homeland Security. Version 1.0. (15-11-2016).
19. H. L. Huansheng Ning: Cyber-Physical-Social Based Security Architecture for Future Internet of Things. Scientific Research, (2012).
20. Microsoft.com. https://docs.microsoft.com/es-es/azure/iot-suite/iot-security-architecture. (2017)
21. Privacy and Security in a Connected Life: A Study of US, European and Japanese Consumers. Ponemon Institute LLC. (Mazo 2015).