Modelo de Seguridad IoT

Monzon German, Todt Carolina Mariana, Bolatti Diego Angelo, Gramajo Sergio, Scappini Reinaldo

Universidad Tecnológica Nacional, Facultad Regional Resistencia,
Centro de Investigación Aplicada en Tecnologías de la Información y la Comunicación (CInApTIC)
French 414 – Resistencia (3500) Chaco - Argentina
{ german.monzon.95, carolinatodt, diegobolatti, sergiogramajo, rscappini}@gmail.com

Abstract. El Internet de las cosas (IoT) no solo conectará computadoras y dispositivos móviles, sino que también interconectará edificios, hogares y ciudades inteligentes, así como redes eléctricas, redes de agua y gas, automóviles, aviones, etc. IoT liderará al desarrollo de una amplia gama de servicios de información avanzados que deben procesarse en tiempo real. Sin embargo, las infraestructuras y servicios de IoT presentan grandes desafíos de seguridad debido al aumento significativo de la superficie de ataque, la complejidad, la heterogeneidad y la cantidad de recursos. En este documento, presentamos un marco de seguridad de IoT para infraestructuras inteligentes como Smart Homes, Smart Grid, Smart Connected Health y otras aplicaciones basadas en IoT.

Keywords: IoT, Ciudades Inteligentes, Seguridad.

1 Introducción

El internet de las cosas (IoT) actualmente vive una fuerte expansión, convirtiéndose en una tendencia irreversible, esto se refleja en la conexión diaria a Internet de miles de dispositivos, sensores y chips los cuales obtienen y distribuyen información por la web para brindar servicios en distintos ámbitos de la vida diaria.

Esta poderosa tecnología, capaz de recolectar y distribuir gran cantidad de información trae asociados nuevos riesgos los cuales podrían amenazar la seguridad de los datos, generando graves consecuencias.

El gran desafío es la complejidad del ecosistema IoT, que impide que la mayoría de las empresas elaboren un marco de seguridad y privacidad. A diferencia de los equipos de TI, los dispositivos conectados no son diseñados pensando en la seguridad, y muchos de ellos no poseen capacidades esenciales de encriptación o autenticación.

La seguridad es una necesidad para los sistemas de IoT para proteger los datos confidenciales e infraestructuras físicas críticas [1]. Sin un buen nivel de protección, los usuarios no pueden adoptar muchos sistemas y aplicaciones de IoT. La seguridad en los sistemas de red tradicionales sigue siendo un desafío, mientras que los sistemas de IoT plantean muchos más desafíos para los investigadores debido a varias

características especiales de estos sistemas. Un análisis profundo es esencial para desarrollar nuevas soluciones de seguridad y sus aplicaciones a sistemas.

En el presente trabajo exploramos cómo mejorar la seguridad en IoT a través de la implementación de un modelo de seguridad. A lo largo del desarrollo de este modelo vamos a considerar la integración con el mundo físico, los dispositivos y las comunicaciones heterogéneas, las restricciones de recursos, la privacidad, la gran escala, la gestión de confianza, el diseño de la seguridad de los dispositivos y las redes en sí mismas.

Este informe se estructura de la siguiente manera, en la sección 2, se hace una breve descripción de la arquitectura de seguridad de IoT. En la sección 3 se presentan las principales amenazas que afectan a el IoT. En la sección 4 se da paso a la presentación del modelo de seguridad de IoT propuesto, y finalmente, en la sección 5 se presentan las conclusiones.

2 Arquitectura de Seguridad de IoT

Como hemos mencionado anteriormente, los dispositivos de IoT se están volviendo omnipresentes, esto crea nuevos tipos de problemas y preocupaciones de seguridad más complejos. Si esos problemas de seguridad no pueden abordarse adecuadamente, se dificultará en gran medida una adopción más amplia de las aplicaciones de la IoT.

Por lo tanto, vamos a enfocar el problema de la seguridad en base a sus aplicaciones, como ser Smart Home, Smart Grid, Smart connected health y otras aplicaciones basadas en IoT como transporte, logística, seguridad pública, video vigilancia urbana, climatología, entre otras [1].

El primer aspecto que tomaremos en cuenta es el servicio de seguridad de capa perimetral (Edge layer security service -EdgeSec). Muchos dispositivos finales como las etiquetas RFID, no tienen recursos suficientes para administrar la seguridad de extremo a extremo. En lugar de que los dispositivos finales gestionen procesos de seguridad por sí mismos, las tareas de administración de seguridad pueden ir desde dispositivos de baja capacidad hasta dispositivos de borde más potentes. En este escenario, el dispositivo final puede tener que confiar en la capa de borde y usarla como el agente de seguridad.

Las ventajas de implementar seguridad en la capa de borde están relacionadas a mayores recursos para cómputo intensivo, cifrado de datos, generación de claves y detección de intrusos, desde dispositivos finales. Además, por estar cerca de los dispositivos finales, se reducen los costos de comunicación y mejoran el rendimiento de aplicaciones en tiempo real. Y, al tener mayor capacidad de información, que los dispositivos finales, es posible implementar una administración de seguridad más optimizada en la capa Edge que puede usarse para proteger la privacidad de los dispositivos finales [2].

3 Amenazas en IoT

Según la recomendación ITU-T Y.4806 podemos clasificar las distintas amenazas hacia los dispositivos IoT según el vector de impacto, que puede provenir del entorno virtual, el entorno físico o del objeto mismo. La figura 1 muestra los distintos vectores de ataque que pueden afectar al sistema [3].

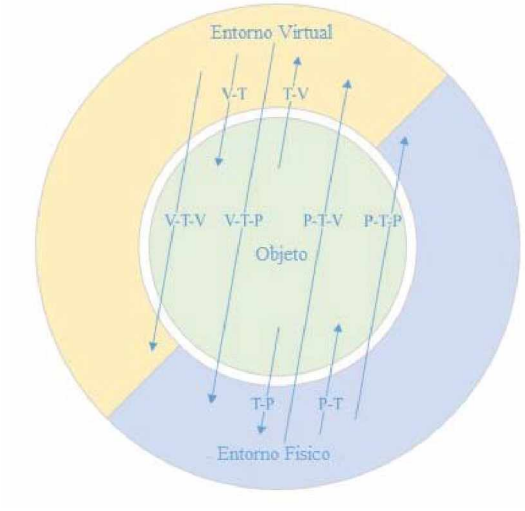

Fig. 1. Vectores de Ataque

El aspecto más importante a estudiar es el vector proveniente del entorno virtual, el cual a través del objeto afecta al entorno físico. Y los que tienen su origen en el comportamiento del objeto, debido a una mala implementación o a que pudiera estar comprometido, dando lugar a problemas de seguridad tanto en el aspecto informativo como funcional [3].

Las principales amenazas que afectan los sistemas de Internet de las Cosas son [3]:

- Manipulación intencional o eludir las restricciones establecidas por los mecanismos de seguridad.
- Desactivación de los mecanismos de seguridad separados debido a las acciones maliciosas del atacante.
- Aprovechar la falta de controles de seguridad inadecuados que, si se implementan adecuadamente, detectarán las acciones que son, o que pueden ser, engañosas (ingeniería social, solicitud de falsificación, etc.).
- La explotación de la falta de, o la aplicación inapropiada de seguridad, que fue limitado por requisitos o exigencias de seguridad relacionadas con la naturaleza de los procesos físicos y con la aplicación del objeto.
- Desactivación de los mecanismos de seguridad debido a las acciones maliciosas del atacante.

2.1 Capacidades para afrontar las amenazas

Para hacer frente a estas amenazas, vamos a recopilar las capacidades de seguridad que podrían dar soporte a la aplicación segura de Internet de las Cosas, como se menciona en la recomendación ITU-T Y.4401[3].

Según esta recomendación, podemos dividir las capacidades de seguridad en 6 grupos [3]:

- **Seguridad en la comunicación**
  - Validación de entradas, control de fuentes, protocolos y flujos.
  - Resistencia a la sobrecarga del canal y denegaciones de servicio.
  - Protocolos de encriptación de datos.
- **Seguridad en la gestión de datos**
  - Control de los comandos para las aplicaciones IoT, de los parámetros y la semántica.
  - Encriptación de datos de aplicación, sumas de comprobación y firmas digitales.
- **Seguridad en la provisión de servicios**
  - Mecanismos de monitoreo, aislamiento de los datos obtenidos y análisis de los componentes, mecanismos de alarmas, aislamiento del monitoreo.
- **Integración de la seguridad**
  - Integración de las reglas y políticas para la validación de entradas en diferentes capas.
- **Autenticación y Autorización mutua**
  - Autenticar y autorizar los sujetos antes de que intenten gestionar y controlar los mecanismos de protección.
- **Auditoría de la seguridad**
  - Monitorear los intentos de gestión y control de los mecanismos de protección.
  - Capacidad de detectar ataques.
  - Monitorear la carga del equipamiento y los canales de comunicación.
  - Detectar ataques en la capacidad de recuperación y respuesta a incidentes.

4 Modelo de Seguridad Propuesto

A continuación, vamos a proponer un modelo de seguridad para redes y dispositivos de Internet de las Cosas, para ello tomamos como base las recomendaciones de la IoT Security Foundation (Fundación de Seguridad IoT), que propone un marco de referencia para cubrir los aspectos de seguridad de los dispositivos IoT.

Este marco de referencia incluye, además de la seguridad del software de los dispositivos, a la seguridad misma del "objeto", y los procesos de negocio que podrían ocasionar problemas en cuestiones de seguridad, y aspectos relacionados a los

puntos de agregación como Gateway(puertas de enlace) que, si bien no son dispositivos IoT, forman parte de la red por la cual éstos se comunican, y, desde este punto de vista, también incluiremos el cableado y las conexiones inalámbricas de los dispositivos[4].

La Fundación resalta 6 puntos claves para la seguridad en IoT: Gestión Responsable de la seguridad, Diseñado para la seguridad, Ajustado para la criptografía, Asegurar los frameworks de redes y aplicaciones, Asegurar los procesos de producción y la cadena de suministros, y Seguridad para los consumidores [4].

Si bien, este enfoque está orientado a las empresas industriales que proveen productos dentro del rubro de Internet de las Cosas, podemos extraer varios puntos importantes comparando con la recomendación anterior:

- **La gestión de la seguridad:** Desde el punto de vista de los recursos humanos, se recomienda tener personal dedicado especialmente a gestionar y controlar la seguridad de los dispositivos y sus aplicaciones.
- **Seguridad en las redes de comunicación:** Se debe prestar especial atención en que los canales de comunicación, así como las interfaces de red que se utilicen, apliquen respectivamente las medidas de seguridad necesarias para mitigar las amenazas mencionadas anteriormente.
- **Integración de los procesos de seguridad:** el hardware y el software deben estar diseñados para cumplimentar las medidas de seguridad establecidas, en caso contrario, exploraremos la posibilidad de extraer esos requerimientos a una capa de red diferente.

El proceso para determinar los requerimientos de seguridad depende no solo de la naturaleza de los dispositivos IoT que se vayan a utilizar, sino también del entorno objetivo para su implementación.

Como primera medida, se deben determinar los potenciales riesgos que afectarían la seguridad tanto de la información, como de las características físicas en las cuales los dispositivos puedan estar implicados.

Una vez determinada la lista de riesgos, se procede a asignar una probabilidad y un costo en caso de ocurrencia, para obtener un factor de riesgo, y de esta forma poder priorizarlos. Luego estudiaremos los riesgos de un caso de aplicación particular para nuestro proyecto.

El siguiente paso es determinar el nivel de cumplimiento requerido para cada uno de los dispositivos, para esto, vamos a analizar la tríada CIA, constituyendo así 5 clases de cumplimiento [4]:

Clase de Cumplimiento	Objetivo de Seguridad		
	Confidencialidad	Integridad	Disponibilidad
Clase 0	Baja	Baja	Baja
Clase 1	Baja	Media	Media
Clase 2	Media	Media	Alta
Clase 3	Alta	Media	Alta
Clase 4	Alta	Alta	Alta

Tabla 1. Nivel de Cumplimiento

Como podemos observar en la tabla 1, para cada clase de cumplimiento se asigna un nivel de Confidencialidad, Integridad y Disponibilidad. Haciendo un análisis de

esta tabla, vemos que el factor más determinante es la Disponibilidad, ya que está directamente relacionada con la función básica de los dispositivos, que es el de generar y proveer información, y en caso de una falla, se verá afectada la seguridad tanto de las personas como del entorno en el cual están desplegados. Y como segunda medida tenemos la confidencialidad, aunque este punto dependerá de la privacidad de los datos que se están compartiendo a través de la red.

A continuación, realizaremos una descripción de cada una de las clases de cumplimiento mencionadas anteriormente [4]:

- **Clase 0:** Donde la pérdida de control sobre los dispositivos, o el compromiso de los datos, resultan en un impacto poco perceptible para los usuarios.
- **Clase 1:** Donde la pérdida del control o el compromiso de los datos resulta en un impacto limitado para los usuarios.
- **Clase 2:** En adición a la clase 1, el dispositivo está diseñado para resistir ataques que afecten la disponibilidad, que puedan tener un impacto significativo para los usuarios, por ejemplo, limitar las operaciones dentro de la infraestructura a la cual están conectados.
- **Clase 3:** En adición a la clase 2, el dispositivo está diseñado para proteger datos sensibles incluyendo datos personales de los usuarios.
- **Clase 4:** En adición a la clase 3, en estos dispositivos el compromiso con los datos generados o la pérdida de control pueden afectar críticamente la infraestructura o causar lesiones en los usuarios.

Una vez determinada la clase de cumplimiento a la que pertenece nuestro dispositivo, debemos completar la lista de requerimientos para identificar cuales se cumplen, y cuales debemos implementar, variando su característica excluyente u opcional en base a la clase a la que pertenece.

Para abordar estos requerimientos, analizaremos las características principales que se deben estudiar:

- Procesos, políticas y responsabilidades.
- Hardware del dispositivo y seguridad física, incluyendo claves de encriptación para los dispositivos.
- Software del dispositivo y Sistema Operativo.
- Interfaces cableadas e inalámbricas del dispositivo.
- Autenticación y autorización, cumpliendo las normativas de protección de datos y privacidad.
- Seguridad en la capa de aplicación, incluyendo sistemas web y móviles, así como los sistemas de red y la nube.
- La configuración de los dispositivos, así como la guía de usuario para un uso seguro de los mismos.

En este punto, vamos a incluir en nuestro estudio otras recomendaciones, para completar nuestra lista de requerimientos. Primero extenderemos la clasificación de los mismos, analizando el caso de CISCO, que propone un modelo de seguridad para Internet de las Cosas (IoT) y comunicaciones máquina a máquina (M2M), compuesto de 4 componentes: **Autenticación**, **Autorización**, **Políticas aplicadas a la red** y **Analíticas de Seguridad** [5].

Si bien los factores de autenticación y autorización han sido mencionados anteriormente, observamos que el factor de red, que se refiere a los dispositivos que transportarán el tráfico generado por nuestros dispositivos, no deja de ser un factor

sumamente importante para nuestro estudio, estos funcionarán como capa de borde para aplicar las medidas de seguridad que los dispositivos IoT no puedan cumplir.

Como adición a las recomendaciones analizadas anteriormente, vemos que CISCO hace foco en los controles que se realizarán sobre los datos recolectados, para poder detectar anomalías, indudablemente debemos incluir este factor en nuestro estudio[5].

Por su parte la Online Trust Alliance, propone un Marco de confianza IoT que incluye un juego de principios estratégicos necesarios para asegurar los dispositivos IoT y sus datos cuando son enviados y a través de su ciclo de vida. El marco de confianza de IoT se divide en 4 áreas clave: Principios de seguridad, Acceso y credenciales del usuario, Privacidad, divulgaciones y transparencia y Notificaciones y mejores prácticas relacionadas. De estos principios, encontramos un nuevo ítem para nuestra clasificación, las notificaciones y avisos que proporciona el dispositivo al usuario final [6].

Por su parte, el CIS (Center for Internet Security), define una serie de controles de seguridad aplicables a Internet de las Cosas, y cada uno de estos controles vamos a incluirlos en nuestra clasificación. Como así también agregaremos una sección de respuesta a incidentes [7].

Como resultado, nuestra lista de requerimientos constará de 62 recomendaciones de seguridad, que estarán subdividas en 10 áreas claves [8]:

- **Procesos, políticas y responsabilidades:** Es necesario divulgar completamente las políticas respecto de la recolección, el uso, y como se comparten los datos, además de los términos y condiciones de los parches de seguridad.
- **Hardware del dispositivo y seguridad física:** La seguridad física es probablemente más que un problema, dado que estos dispositivos suelen estar al aire libre o en ubicaciones remotas y cualquiera puede acceder físicamente a ellas.
- **Software del dispositivo y Sistema Operativo:** Es importante mantener un inventario actualizado del software autorizado como así también de los permisos de usuario sobre el sistema operativo.
- **Interfaces cableadas e inalámbricas del dispositivo:** Es necesario adoptar políticas que controlen el acceso y los servicios de red.
- **Autenticación y autorización:** adoptar mecanismos seguros para interactuar y establecer conexiones con dispositivos.
- **Seguridad en la capa de aplicación:** La capa de aplicaciones incluye a todos los dispositivos que tengan conectividad con el dispositivo IoT, lo que puede incluir las aplicaciones web locales, las basadas en la nube y las móviles.
- **Configuración de los dispositivos:** Como en casi cualquier dispositivo IoT, la principal medida de seguridad es una configuración correcta, es indispensable no dejar la configuración por defecto y utilizar usuarios y contraseñas apropiadas para evitar posibles amenazas.
- **Analíticas de Seguridad:** Es necesario contar con una recopilación, monitoreo y normalización de datos de los dispositivos IoT, como así también proveer de informes y alerta sobre actividades específicas o cuando las actividades caen fuera de las políticas establecidas.

- **Respuesta a Incidentes:** Para administrar y recuperarse de violaciones de datos y ataques a la red es necesario contar con servicios de respuestas a incidentes.
- **Notificaciones y Alertas:** Para mantener la seguridad del dispositivo es clave tener mecanismos y procesos que notifiquen rápidamente al usuario si hay una amenaza o una acción requerida.

5 Conclusiones y Trabajo Futuro

A pesar de la gran cantidad de aplicaciones potenciales de IoT y del hecho de que muchas de las tecnologías que soportan IoT ya están en uso, IoT aún no es una realidad en un sentido práctico. Esto puede atribuirse en gran medida a las preocupaciones sobre la seguridad. La naturaleza física inherente de la IoT implica que los ataques cibernéticos, donde el daño normalmente se limita a un mundo virtual, ahora puede presentar una amenaza física real. Esto podría ser una amenaza para la privacidad, una molestia o incluso una amenaza real para la seguridad personal.

En este documento, diseñamos un modelo de seguridad el cual proporciona autenticación esencial, garantiza comunicaciones seguras, admite la autorización del usuario y ofrece notificación de riesgos, satisfaciendo así las principales preocupaciones de los usuarios. El marco puede servir como base para respaldar la seguridad de las aplicaciones de IoT.

Si bien el marco que hemos desarrollado ayuda a cumplir con los requisitos básicos de seguridad, también nos permitió reafirmar los conceptos desarrollados durante la investigación:

- Los componentes que más nos interesan proteger son los que forman parte de las Interfaces cableadas e inalámbricas del dispositivo, ya que son el punto de acceso para establecer la comunicación con los dispositivos.
- Dentro de las interfaces, es muy importante implementar un buen mecanismo de autenticación, ya que es la forma más efectiva de evitar el acceso de usuarios maliciosos que puedan generar algún daño en el sistema.
- El segundo factor importante que se debe implementar es el de cifrado de los datos, esto se vuelve mucho más importante aún para las comunicaciones inalámbricas.
- El factor más difícil de proteger es el hardware del dispositivo, esto se debe a razones lógicas, ya que las prestaciones que ofrecen los mismos, se ven limitadas a cumplir su propósito con el menor costo en términos de fabricación e implementación.
- Aunque no podamos realizar mayores modificaciones en el hardware, este puede verse muy comprometido en el caso de que un usuario malicioso logre evadir la autenticación, y tenga acceso al software del dispositivo, este podría generar un comportamiento que afecte al componente físico del dispositivo, así como al entorno físico del mismo, incluyendo a los propios usuarios.

Vamos a analizar este último punto, si recordamos los vectores de ataque que mencionamos al inicio del documento, vemos que el caso mencionado se corresponde

con el vector V-T-P (Virtual-Thing-Physical), qué es el proveniente del entorno virtual, que, a través del acceso a las funcionalidades del dispositivo, logra afectar al entorno físico. Concluimos en que nuestra clasificación se corresponde con la información recolectada previamente.

Además, logramos descubrir dos puntos importantes en la aplicación de un modelo de seguridad para Internet de las Cosas:

- Es muy importante mantener políticas de seguridad a las cuales responden los demás requerimientos.
- Se debe notificar al usuario la mayor cantidad de información posible relacionada con eventos que afecten a la seguridad del sistema, ya que la interacción entre estos está limitada a su funcionalidad específica.

Como trabajo futuro, se planea investigar y complementar al modelo de seguridad propuesto la seguridad de las redes LoraWan, el cual es una especificación técnica de una red LPWAN (Low Power Wide Area Network) propuesta por la Lora Alliance. Esta red nace para cubrir la necesidad de comunicar dispositivos IoT o M2M, de bajo coste y bajo consumo energético a grandes distancias.

Referencias

1. N. Ekedebe, W. Yu, C. Lu, H. Song, Y. Wan. Securing transportation cyber-physical systems. Securing Cyber-Physical Systems, CRC Press, Boca Raton, pp. 163–196. 2015.
2. L. Sweeney. K-anonymity: a model for protecting privacy, Int. J. Uncertain. Fuzziness Knowl. -Based Syst. 10 (5) 557–570.2002.
3. International Telecommunication Union (ITU). (2017). Recommendation ITU-T Y.4806.
4. IoT Security Foundation. (2018). IoT Security Compliance Framework.Release 2.
5. Cisco. (2019). Securing the Internet of Things: A Proposed Framework. [online] Available at: https://www.cisco.com/c/en/us/about/security-center/secure-iot-proposed-framework.html.
6. Marco de confianza y confidencialidad de IoT v2.5 | Internet Society. (2018). Retrieved from https://www.internetsociety.org/es/resources/doc/2018/iot-trust-framework-v2-5/
7. CIS Critical Security Controls. (2015). Internet of Things Security Companion to the CIS Critical Security Controls.
8. Monzon, G., Todt, C., Bolatti, D., Gramajo, S., & Scappini, R. (2019). Modelo de Seguridad IoT. Retrieved from: http://monwatch.frre.utn.edu.ar/files/ListaDeRequerimientos