Análisis de caso para formular el Modelo de prevención de fuga de información para dispositivos IoT en redes domésticas

Madelaine Nelly Velasquez Blacutt
Postgrado en Informática
Universidad Mayor de San Andrés
La Paz - Bolivia
madevelb@gmail.com

***Resumen*—El Internet de las cosas convierte el mundo físico en un entorno de información donde dispositivos IoT recolectan y envían datos generados por un usuario y su entorno. Por la creciente demanda y evolución, los fabricantes descuidaron la inclusión de medidas de seguridad de la información en los dispositivos, lo cual los convierten en blanco de atacantes que, al obtener acceso a una red comprometen la privacidad de la información del usuario. Como solución a los problemas de privacidad que exponen los dispositivos IoT, se busca proporcionar al usuario una herramienta que permita preservar la privacidad de su información, realizando el análisis de vulnerabilidades e incluyendo buenas prácticas para la implementación segura de dispositivos IoT.**

Palabras clave—Fuga de información, IoT, Internet de las cosas, redes LAN domésticas.

I. INTRODUCCIÓN

Con el Internet de las Cosas (IoT por sus siglas en inglés, *Internet of Things*), muchos dispositivos que por años tenían tareas simples a desempeñar, ahora están siendo conectados a Internet. Es así como los fabricantes, han diseñado asistentes digitales que, a través de algún tipo de aplicación, pueden realizar diversas tareas a pedido del usuario. Pero en medio de este paradigma de información, donde un hogar con dichos dispositivos se integra a Internet, no necesariamente cuenta con privacidad en sus datos.

Con el deseo de tener la última tecnología y una constante necesidad de acceso a todo tipo de información, se observa que los usuarios aceptan términos de privacidad por distintos proveedores y fabricantes, los cuales podrían estar recolectando información personal, sin que el usuario sepa para qué se utiliza la misma. Por lo que, a mayor número de dispositivos conectados y dependiendo del tipo de dispositivo, se podría introducir un mayor número de riesgos relacionados a la privacidad de la información recolectada por estos dispositivos.

De esta forma, se realiza el análisis de caso para el planteamiento de un modelo que cubra la falta de privacidad en el uso de información por dispositivos IoT, mediante la implementación de herramientas que permitan la detección de vulnerabilidades, herramientas que suplan la seguridad de la información deficiente y la aplicación de buenas prácticas para la implementación segura de los dispositivos IoT. El conjunto de estas soluciones, se convierten en un modelo de prevención de fuga de información, que permita a un usuario administrar la privacidad de su información, recolectada por dispositivos IoT.

A. Estado del arte

Respecto a la evaluación de vulnerabilidades de dispositivos IoT, el trabajo de Sicari, Rizzardi, Miorandi, & Coen-Porisini [1], proporciona el nivel de seguridad de un sistema ante posibles ataques internos y externos. De esta forma, propone una metodología de riesgo aplicable a infraestructuras IoT, que toma en cuenta componentes estáticos y dinámicos de los sistemas.

Por otro lado, Van Diermen [2], propone un modelo de seis capas, donde define las tecnologías utilizadas en cada una de estas, además de las responsabilidades de los usuarios y de los proveedores o fabricantes de los dispositivos IoT. Además, este trabajo describe riesgos y pruebas que se podrían realizar a los dispositivos IoT para la evaluación de riesgos en cada capa del modelo descrito.

El desarrollo de herramientas en dispositivos de bajo costo, como es el módulo *Single Board Computers* (SBC): Raspberry Pi. En la *propuesta Securing the Home IoT Network* de Leos [3], se atiende las deficiencias de seguridad típicas de IoT. Este trabajo propone la implementación de una puerta de enlace que pueda proporcionar solución a deficiencias de diseño o configuración de seguridad en una red doméstica.

Los trabajos descritos contribuyen a la formulación de la propuesta, a la clasificación de contenido considerado privado o sensible y da lineamientos para la evaluación de los riesgos asociados a la privacidad de la información manejada por dispositivos IoT. Una red de datos estándar no está diseñada para proporcionar seguridad de la información ante errores de diseño en dispositivos IoT, lo que expone la privacidad de la información de los usuarios. Para la elaboración del modelo, se considera una guía en el uso de SBC para la minimización de riesgos de seguridad mencionados. Así también, se incluirá en la investigación, formas de inspección y auditoría de la información recolectada por los dispositivos IoT.

B. Objetivo de la investigación

Con el entorno descrito anteriormente, se plantea el siguiente problema de investigación:

Para referenciar este artículo (IEEE):

[N] M. Velasquez, «Análisis de caso para formular el Modelo de prevención de fuga de información para dispositivos IoT en redes domésticas» *Revista PGI. Investigación, Ciencia y Tecnología en Informática,* nº 7, pp. 69-71, 2020.

¿Cómo una persona con conocimientos mínimos sobre seguridad de la información podría gestionar la privacidad de la información recolectada por dispositivos IoT de su red LAN doméstica?

A partir de la pregunta anterior, se plantea el siguiente objetivo de investigación:

Diseñar un modelo de prevención de fuga de información que gestione la privacidad de la información recolectada por dispositivos IoT en una red LAN doméstica, para una persona con conocimientos mínimos sobre seguridad.

II. OWASP

El Open Web Security Project, es un proyecto de código abierto que plantea determinar y solucionar causas por las que el software resulta inseguro. La fundación OWASP y su comunidad, plantea documentación y herramientas para integrar seguridad en aplicaciones, a través de apoyo y gestión de proyectos e infraestructura.

OWASP clasifica un Top 10 de vulnerabilidades para IoT [4], evaluaciones que se deben tomar en cuenta, en cuanto a la privacidad de la información.

TABLA I. OWASP PRIVACIDAD DE LA INFORMACIÓN

Característica	Descripción
Agentes de amenaza: Específica de la aplicación	Considera a cualquiera que tiene acceso al dispositivo, la red, la aplicación móvil y la conexión a la nube, usuarios externos e internos.
Vectores de ataque *Explotabilidad:* PROMEDIO	Un atacante usa múltiples vectores como: autenticación insuficiente, falta de cifrado en el transporte o servicios de red inseguros para el acceso a datos personales.
Debilidad de seguridad *Prevalencia:* COMÚN *Detectabilidad:* SENCILLA	Las preocupaciones de privacidad y la falta de protección adecuada de datos son prevalentes. Las preocupaciones de privacidad son fáciles de descubrir al revisar los datos que están siendo recolectados cuando el usuario configura y activa el dispositivo.
Impacto técnico *Impacto*: Severo	La recolección de datos personales junto con la falta de protección de esos datos puede comprometer los derechos de un usuario.
Impacto en el negocio Específico de aplicación	Considerar el impacto al negocio de datos personales recolectados sin necesidad. Los datos podrían ser robados.

De esta forma se incluye para el análisis, la privacidad de la información que manejan los dispositivos IoT, información que debe ser clasificada identificada como personal, es decir, la información que clasifica a un individuo, como ser nombre, datos biométricos o datos de tarjetas de crédito. La identificación del dispositivo conectado a la red de datos, así como el tráfico que este genera e identificación de a dónde se dirige su tráfico.

En cuanto a algunos vectores de ataque que pudieran ser explotados, se debe incluir medidas que suplan funciones que no hayan sido implementadas, de forma de brindar al usuario protección a la red doméstica que utiliza. Las medidas que pudieran incluirse dependerán del dispositivo que se utilice, en búsqueda de estandarizar una solución o alertar al usuario que el dispositivo es vulnerable a ataques.

A. Metodología

La metodología que se propone en el análisis para la obtención del modelo consta de las siguientes fases y herramientas para el desarrollo de este.

1) Fase exploratoria

Se realiza el relevamiento de información, recabando y construyendo el marco teórico de apoyo y respaldo para el trabajo. Consulta de fuentes bibliográficas.

2) Fase de planificación y diseño

Se estudia la arquitectura de las redes LAN domésticas, con una propuesta estándar para la normalización y definición del entorno de trabajo. También se considera la arquitectura típica de capas de dispositivos IoT.

a) Recolección de datos: relevamiento de infraestructura de red de datos.

b) Recolección de datos: relevamiento de arquitectura de dispositivos IoT así como los paquetes que generan.

c) Recolección de datos: sniffing de red

d) Arquitectura de objetos

e) Diseño del modelo: inclusión e interacción de herramientas para análisis y protección de datos.

f) Escaneo de información recolectada: análisis de cabeceras y carga útil a ser analizada.

3) Fase empírica

En función de la información recolectada y análisis de campos de los paquetes recolectados, se realiza el filtrado de información de interés para realizar el análisis.

a) Filtrado de datos recolectados, según parámetros específicos para análisis.

b) Búsqueda de comportamiento, o patrones de interés de la información recolectada.

c) Comportamiento de tráfico de dispositivos IoT, con herramientas implementadas.

4) Fase analítica

Evaluación de resultados, según experimentación de distintas herramientas, así como análisis de los datos de interés obtenidos para su presentación.

a) Evaluación de datos obtenidos.

b) Obtención de estadísticas para interpretación.

c) Validación, comparación de resultados según indicadores conocidos.

d) Comunicación de resultados.

e) Presentación de resultados.

III. DISCUSIÓN

El análisis de los datos recolectados resulta en la determinación del tráfico que los dispositivos IoT generan, tanto en la red LAN doméstica interna, como hacia Internet. En caso de la red interna se determina qué información lee el dispositivo de otros equipos conectados a la misma red LAN. Se debe determinar si el dispositivo realiza un escaneo o escucha de los datos que se intercambia en la red ya que es posible una

recolección de datos según parámetros, por ejemplo, números de tarjetas de crédito. Además, la información ya sea en la red interna y externa debe viajar cifrada, con algoritmos no vulnerados para preservar su confidencialidad.

En caso de que el tráfico generado por los dispositivos IoT, vaya hacia Internet, se determina la dirección IP destino. Por un análisis del rango de direcciones IP asignadas a cada país, se puede obtener una estadística de los países destino donde el tráfico se envía. Dependiendo de la naturaleza del dispositivo, se deben definir reglas de permitir o bloquear la salida de tráfico. Es decir, si el dispositivo realiza algún tipo de almacenamiento en la nube, se debería analizar a dónde se envía la información, así como qué información sale de la red.

El cifrado de información, puede generar un reto de análisis de datos que salen e ingresan a la red [5], sin embargo, para este tipo de casos, deben analizarse otros parámetros como la cantidad de datos generados, frecuencia de envío, destino, de forma de analizar la necesidad de este envío. Una vez identificados ciertos parámetros, será posible proponer una solución que proteja al dispositivo y a la red, que maneja la información del usuario.

Las investigaciones relacionadas obtienen resultados según su propósito [2], que realiza una clasificación de información sensible de forma de representarlo en una etiqueta que representaría el nivel de seguridad con el que un dispositivo IoT está fabricado, sin embargo, por la evolución constante de la tecnología, es necesaria la evaluación periódica de la clasificación de la privacidad de la información, así como las pruebas de penetración para evaluar las tecnologías y entornos de los dispositivos IoT.

Por otra parte, para la evaluación de vulnerabilidades, medición de la robustez de un sistema, es importante la determinación de medidas de seguridad que protejan estos sistemas. El análisis de riesgos [1], toma en cuenta características estáticas y dinámicas de forma de obtener una evaluación confiable.

Para Leos [3], la implementación de una herramienta de bajo costo para la adopción de prácticas seguras en la red, debe adoptarse según modelos donde no existe un perímetro de la red. Existen distintas herramientas que pueden ser implementadas para cubrir los huecos de seguridad que algunos dispositivos IoT presentan, sin embargo, también se debe contar con un mayor control de los mismos a través de la segmentación y separación de estos dispositivos de los demás equipos que pueden manejar información sensible.

IV. Conclusiones

El desarrollo de un modelo que realice el análisis de la información que los dispositivos IoT manejan en una red doméstica, es necesario de forma de preservar la privacidad de esta información. Con la determinación de algunos parámetros es posible determinar qué información intenta salir de la red LAN de un usuario hacia Internet, por lo cual el usuario debe poder decidir si este tráfico es permitido o denegado.

Los dispositivos IoT por lo general no cuentan con medidas de seguridad incluidas en su diseño y fabricación, lo cual ocasiona que existan potenciales vulnerabilidades que proporcionen a un atacante la entrada a la información que se maneja en una red LAN doméstica. A través de la implementación de herramientas, se busca brindar protección a estos dispositivos, de forma que no sean fácilmente vulnerados, así como brindar seguridad a través de protocolos seguros y cifrado del tráfico de la red.

Referencias

[1] Sicari, S., Rizzardi, A., Miorandi, D., & Coen-Porisini, A. “A Risk Assessment Methodology for the Internet of Things”. Computer Communications (2018). Italia, Agosto, 2018.

[2] Van Diermen, R. “The Internet of Things: a privacy label for IoT products in a consumer market”, Junio, 2018.

[3] Leos, M. “Securing the Home IoT Network”. 2017 The SANS Institute. EE.UU., Marzo, 2017.

[4] OWASP Foundation. “OWASP Internet of Things Project”. OWASP Foundation, Mayo, 2018.

[5] Apthorpe, N., Reisman, D., Sundaresan, S., Narayanan, A. & Feamster, N. “Spying on the Smart Home: Privacy Attacks and Defenses on Encrypted IoT Traffic”, Agosto, 2017.

[6] Miley, P. “Privacy and the Internet of Things”. 2017 The SANS Institute. EE.UU, Octubre, 2017.

Breve CV de la autora

Madelaine Nelly Velasquez Blacutt es Ingeniera Electrónica por la Universidad Mayor de San Andrés, Especialista en Telecomunicaciones y Sistemas. Especialista en diseño de redes de datos y seguridad informática enfocada en redes. Diplomada en Educación Superior, Docencia Universitaria. Email: madevelb@gmail.com.