Internet of Things: Seguridad y Manejo de dispositivos

Maldonado Bolaños Daniel

Instituto Tecnológico de Tijuana, Depto. De Sistemas y Computación

Tijuana, Baja California, México.

daniel.maldonado17@tectijuana.edu.mx

Abstract

IoT tiene sus principios más atrás de lo que podemos imaginar, sin ser tan bien visto en tiempos anteriores, aprendió a ganar su lugar por medio de pequeños avances que generaron un nombre y una manera de investigar y trabajar a muchos. Hablaremos un poco de lo que es la historia principal de IoT, haciendo un resumen de los acontecimientos importantes que llevaron a IoT ser reconocido hoy en día de la población. Tomando en cuenta unos de los puntos importantes dentro de IoT que es la seguridad dentro de los dispositivos, como se maneja, que problemas se puede tener, que problemas se ha tenido en el pasado, posibles causas, posibles soluciones, etc.

Introducción

La comunicación a nivel mundial ha sido siempre una prioridad, el comprender y entender que esta pasando en otro lugar. Durante a mediados de los 80's la comunicación era popular a través del teléfono, pero en cuanto más fueron pasando los años eso fue quedando atrás haciendo que ahora el internet sea la nueva y principal plataforma de comunicación. Siendo esto los conceptos principales, ahora se pensaba sobre abrir más posibilidades a través de la red y que no otra cosa sería que es IoT (Internet of Things), una técnica que combinaba recursos existentes en la Internet para tener control sobre los dispositivos. La introducción a este concepto de IoT fue propuesta en el MIT (Massachusetts Institute of Technology) a principios de los años 90's. Sin embargo, la cafetera de Trojan Room fue la primera aplicación IoT que fue desarrollada en 1999.

Imagen de la cafetera usada por Trojan.

Evolución y problemas

Hoy en día el internet ha sido una gran manera de promocionar dispositivos (Smart devices) con altas funcionalidades a través de los sensores que se incluyen en el mismo. Estos dispositivos que están conectados a través del internet generan una gran cantidad de información que requiere ser manejada con cautela, ya

que la mayoría puede incluir transacciones, datos médicos, localización, entre otros. Sobre el pasar de los años estos dispositivos iban mejorando en su rendimiento y lentamente en su seguridad, sin jamás ser considerados extremadamente seguros para su uso. En noviembre del 2016, 4 investigadores--Eyal Ronen, Colin O'Flynn, Adi Shamir, and Achi-Or Weingarten—surgieron con una interesante Proof of concept (PoC) worm que atacaba usando drones y tomando control de Philips Hue smart lights de un edificio. Incluso si el ataque fue un PoC, no es difícil pensar que podría ser un smart device ser hackeado y tomado para algún otro fin. Casi todos los smart devices han sido determinados con fallas críticas en su seguridad al igual que con problemas con la privacidad, incluyendo sistemas de smart home, monitores para bebes e incluso juguetes sexuales.(Gupta, A. 2019)

El alza de incidentes en términos de seguridad con dispositivos IoT ha hecho que se demande seguridad profesional para este tipo de dispositivos. Esto hace que las compañías creen incentivos para información sobre bugs en términos de seguridad en sus dispositivos y ser arreglados lo más antes posible. La mejor manera de aprender sobre la seguridad de estos dispositivos es ver qué ha sucedido en el pasado. Aprendiendo sobre los errores de seguridad de otros que los desarrolladores de productos hayan realizado en el pasado, podemos obtener una comprensión de qué tipo de problemas de seguridad esperar en el producto que estamos evaluando.

Caso Jeep Hack

Jeep Hack El Jeep Hack es probablemente el hack de IoT más popular de todos los tiempos. Dos investigadores de seguridad, el Dr. Charlie Miller y Chris Valasek, demostraron en 2015 cómo podían hacerse cargo y controlar de forma remota un Jeep utilizando vulnerabilidades en el sistema Uconnect de Chrysler, lo que provocó que Chrysler tuviera que retirar 1,4 millones de vehículos. El truco completo se aprovechó de muchas vulnerabilidades diferentes, incluidos los grandes esfuerzos en la ingeniería inversa de varios binarios y protocolos individuales. Una de las primeras vulnerabilidades que hizo posible el ataque fue el software Uconnect, que permitía a cualquiera conectarse de forma remota a través de una conexión celular. Se pudo acceder al puerto 6667 con la autenticación anónima habilitada y se encontró que ejecutaba D-Bus sobre IP, que se usa para comunicarse entre procesos. Después de interactuar con D-Bus y obtener una lista de servicios disponibles, se descubrió que uno de los servicios con el nombre NavTrailService tenía un método de ejecución que permitía a los investigadores ejecutar código arbitrario en el dispositivo. método que permitió a los investigadores ejecutar código arbitrario en el dispositivo.(Gupta, A. 2019)

```
#!python
import dbus
bus_obj=dbus.bus.BusConnection("tcp:host=192.168.5.1,port=6667")
proxy_object=bus_obj.get_object('com.harman.service.NavTrailService','/com/ha
rman/service/NavTrailService')
playerengine_iface=dbus.Interface(proxy_object,dbus_interface='com.harman.Ser
viceIpc')
print playerengine_iface.Invoke('execute','{"cmd":"netcat -l -p 6666 |
/bin/sh | netcat 192.168.5.109 6666"}')
```

Se muestra el código usado para controlar la unidad.

Mientras IoT pueda comunicarse entre más dispositivos, aspira a tener una mayor cantidad de ataques hacía los dispositivos centrados, lo cual genera un gran problema en donde se este implementado. Recordemos que no solo puede ser la conectividad de nuestros dispositivos en casa, hoy en día tenemos servicios médicos, ciudades inteligentes, transportación, entre muchas otras.(Mentsiev, Adam U,2020)

La información es demasiado importante para dejarse a la ligera, por lo que estos antecedentes disminuyen, tomando la importancia y la mira de las empresas como sus prioridades. No solo se busca fortalecer los

avances tecnológicos, se debe buscar ser seguro en cualquier entorno y aunque no se pueda asegurar nada, el usuario quiere un nivel de satisfacción y trato por el trabajo que esto implica.

Conclusión

No hay una solución como tal, se debe ser constante con el tipo de asunto que se trata. Un trabajo en conjunto dentro de lo que es IoT aumentando la funcionalidad o producción y reducir los riesgos operativos. Pero algo que si se puede observar es que a menudo se pasa por alto, la gestión del ciclo de vida de los componentes de seguridad en todo el espectro del dispositivo y la nube es un elemento crítico para una estrategia de seguridad digital robusta y de largo plazo. La seguridad no es una actividad puntual, sino una parte del ecosistema del IoT que está en constante evolución. El saber cómo manejar las situaciones contendrá una gran ventaja para la evolución de las cosas, aprender de ello y adaptarnos a los riesgos y necesidades de la población.

Referencias

Gupta, A. (2019). The Iot Hacker's Handbook: A Practical Guide to Hacking the Internet of Things (1st ed.). Apress.

U, A. (2020). Impact of IoT on the automation of processes in Smart Cities: security issues and world experience. Journal of Physics Conference Series. Published. https://pdf.zlibcdn.com/dtoken/0cb3113e44523cca6fd2c423d9a0c5a2/1742-6596/1515/2/022026.pdf