Universidad de Talca
Facultad de Ingeniería
Departamento de Ciencias de la Computación

Seguridad Informática

Ensayo 3

IoT stands for Internet of Shit

Erik Regla
eregla09@alumnos.utalca.cl

17 de mayo de 2020

En los ensayos anteriores siempre hemos hablado al respecto de la seguridad, la confidencialidad y como nosotros ocmo individuos tenemos que hacernos cargo de esos aspectos de la seguridad por medio de algo tan simple como la educación. Sin embargo, esto es aplicable en el contexto que nosotros somos personas que tenemos control sobre lo que estamos usando. Por ejemplo, sabemos que no tenemos que entregar el código de validación de nuestra tarjeta de crédito porque podríamos ser víctimas de un fraude, pero claro nosotros estamos en control de nuestra tarjeta de crédito.

Sin embargo, nosotros estamos en un mundo en que no solo las personas (nosotros) estamos conectados al mundo a través de internet, también estamos conectados por medio de las herramientas que utilizamos a diario, nuestros dispositivos.

El internet de las cosas se refiere a los dispositivos -que simples no son- que se conectan a la red con tal de obtener capacidades gracias a esta[1]. Pero es más bien como que llevan tus datos a la nube para poder dejar los calculos en algún lugar donde no sea tan pesado para algo energizado con una pila de 1.5v. Pero todos sabemos que en realidad es para quedarse con estos datos. Y así podemos seguir todo el día.

Hay muchas tecnologías amarradas a esta y no todas conectadas a dispositivos físicos como uno podría pensar. Por ejemplo si bien es natural atribuirle este fenomeno a al acceso a componentes de bajo costo y baja potencia como *Bluetooth Low Energy Profile*[2] y el acceso a la conectividad, también las plataformas de computación distribuida en la nube y herramientas de machine learning de fácil acceso han ayudado a poder hacer que dispositivos pequeños puedan usar sus capacidades de forma remota.

Por ejemplo, cuando utilizas Google Assistant, no es tu teléfono el cual interpreta las instrucciones, tu voz es enviada a la nube de Google para determinar que fue lo que dijiste, tu teléfono solo ejecutó la orden. Y tu voz de paso sirve para alimentar de forma anómina -supuestamente- la maquinaria detrás para que mas personas puedan disfrutar del servicio y también tu puedas tener

[1] https://www.oracle.com/cl/internet-of-things/what-is-iot.html
[2] https://es.wikipedia.org/wiki/Bluetooth_de_baja_energía

un mejor acceso.[3]

Quizás el mejor aspecto de todo esto es que la tecnología para poder desarrollar soluciones IoT es tan accesible en estos días, que cualquier persona con conocimientos básicos de computación puede crear sus propios dispositivos utilizando herramientas como *PlatformIO*[4] y SoCs *Xtensa* [5].

Hay bastantes casos emblemáticos si nos queremos reir de esto, siendo personalmente *Internet Of Shit*[6] la mejor fuente de risas al respecto. Y no lo digo de mala manera, simplemente no podemos estar conectando todo lo que se nos antoja a internet. O sea, ¿Quién pensó que ponerle una camara al indoro para poder identificar gente por medio de la forma del ano era una buena idea?[7] Ahora si, si quieres detectar enfermedades está bien, ¿Pero a dónde van a parar esas imágenes?

Otro caso es el de el mug que se calienta solo de acuerdo a su contenido. Está bien, justificamos su uso porque es conveniente, pero tener que actualizar el mug si no no puedes usarlo es un problema. Lo mismo ocurre con nuestros televisores, estas viendo un programa y no puedes continuar porque hay que actualizarlo. Las personas no son tan pacientes, entonces la opción es, dejémoslo para después. De todas formas que puede haber en nuestro televisor que sea importante, que esté conectado a intenet no es un gran problema.

Justamente eso ocurrió con *Mirai Botnet*[8] el cual es un malware que se aprovechaba de que muchos routers (que como podrán imaginar, están directamente expuestos a la red) para ejecutar attaques de denegación de servicio masivos contra servidores de registro de dominio. Su funcionamento es bastante simple, dado que muchos dispositivos tenían su seguridad configurada por defecto, su explotación es simple, de hecho, ¿A quién le interesa cambiar la contraseña del router en estos días?

Los usuarios son flojos, pero también los desarrolladores de hardware. Es algo que pasa en todas las familias, grandes o pequeñas, antiguas y nuevas. Por ejemplo, hace unos meses OralB liberó al publico una nueva línea de cepillos dentales los cuales comparten información por medio de la red para tener estadisticas de los cepillados y demases. Entonces el usuario de Twitter `@imduffy15` capturó la información propagada por bluetooth del cepillo para transformarlo en un control remoto[9]. Algo que puede ser muy inocente al comienzo, sin embargo tal y como menciona Ian, *"[...]una vez un dispositivo es conectado, puede volverse un gatillante para cualquier cosa[...]"*.

En el mundo del desarrollo de hardware es común que los desarrolladores -reconozco yo también haber pecado al comienzo de lo mismo- piensen que por estar trabajando directamente con hardware ya es una gran barrera de entradas a posibles intrusiones en el sistema, en especial si estas son desarrolladas de manera física. Porque claro que con Mirai ya quedó claro que tienes que cambiar la contraseña del router y actualizar tu televisor, pero no mucho puedes hacer si como en el caso del cepillo esta información es propagada directamente sobre el aire.

Normalmente en un sistema robusto una persona no debería poder tener acceso a uso de los

[3] https://developers.google.com/assistant/smarthome/overview
[4] https://platformio.org/
[5] https://www.espressif.com/en/products/socs/esp8266ex/overview
[6] https://twitter.com/internetofshit
[7] https://med.stanford.edu/news/all-news/2020/04/smart-toilet-monitors-for-signs-of-disease.html
[8] https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/
[9] https://twitter.com/imduffy15/status/1256954852996939777

datos a ese nivel, mucho menos poder interferir la comunicación entre estos dispositivos, pero dado que la comunicación entre el cepillo y su hub no estaba cifrada ni mucho menos protegida de alguna manera, ahora ese cepillo puede ser utilizado para cualquier cosa.

Un caso similar y más preocupante fue el de un desarrolo de ingeneríoa inversa sobre el firmware para IoT utilizado en cámaras Xiaomi[10] en el cual uno de los descubrimientos fue que las credenciales son filtradas directamente en la comunicación entre dispositivos Zigbee debido a que el firmware utilizado en la radio no estaba debidamente limpiado previo a su despliegue. Este es un error comun de los desarrolladores de hardware que al momento de integrar componentes en el sistema si funcionan directo sacandolos de la caja se olvidan que pueden venir precargados con bootloaders u otro programa el cual altera el funcionamiento original o esperado.

Recuerdo que hace mucho tiempo cuando logré tener en mis manos una de las muestras de ingenería de un ESP8266 -no pregunten como la obtuve, solo me llegó a la casa-, el SDK que venía con este tenía una particularidad. Para ser una pequeña pieza de hardware tenías acceso al stack completo de instrucciones para controlar la radio que viene incorporada.

Entre esos, estaba disponible un método `wifi_send_pkt_freedom`, el cual te permitía liberar paquetes al aire saltandote todo el stack de 802.11. Ok, ningún problema con esto, total siempre que te comunicas utilizando algun medio inalámbrico *liberas paquetes al aire*, sin embargo, nada impide que puedas fabricar tus propios paquetes de deautenticación en el proceso y por qué no, leer paquetes *desde el aire*[11] para obtener la dirección MAC de los dispositivos en el radio y enviar paquetes para deautenticar su conexión.[12].

En estos días cualquier cosa puede ser un armamento digital, como lo demostró Gene Bransfield en la DEF CON 22 con la aparación del *War Kitteh* y el *Denial of Service Dog*[13] y si no has visto este video te recomiendo verlo. Es la demostración de como un entusiasta sin experiencia desarrollando firmware puede usar un gato para obtener información georeferenciada de APs sin seguridad en un barrio y de como las confian lo que ven a su alrededor permitiendo la entrada a posibles atacantes.

Es mucho más complicado explicar a los usuarios acerca de los riesgos de no ser *responsable* con el uso de dispositivos, mucho mas que entiendan como prevenir intrusiones o ataques. No es como el computador de la casa que si tienes un malware que esté minando criptomonedas te das cuenta de inmediato por el consumo de CPU, acá no tienes una interfaz, no sabes que está ocurriendo detrás.

Los desarrolladores de hardware tenemos una responsabilidad enorme al respecto, sin embargo muchos deciden hacer oidos sordos o ignorar el problema, porque mientras nadie se de cuenta de este, el problema no existe. Y además tenemos una obsesión por conectar todo a internet, nuestra lavadora, el refrigerador, los televisores, incluso hasta los huevos dentro del mismo refrigerador pueden estar siendo monitoreados desde la comodidad de tu sillón para saber cuando se vencen.[14]

Total ¿Qué importa? Tu cocina conectada a internet es solo una cocina, no puede encenderse por si sola, no puede encender el horno cuando no estás y mucho menos saber cuando estás en casa o cuando no. ¿Qué tan peligroso puede ser conectarla a internet?

[10] https://hackaday.com/2019/10/24/reverse-engineering-xiaomi-iot-firmware/
[11] https://bbs.espressif.com/viewtopic.php?t=1357
[12] https://github.com/pulkin/esp8266-injection-example/issues/1
[13] https://www.youtube.com/watch?v=DMNSvHswljM
[14] https://iot.do/devices/egg-minder