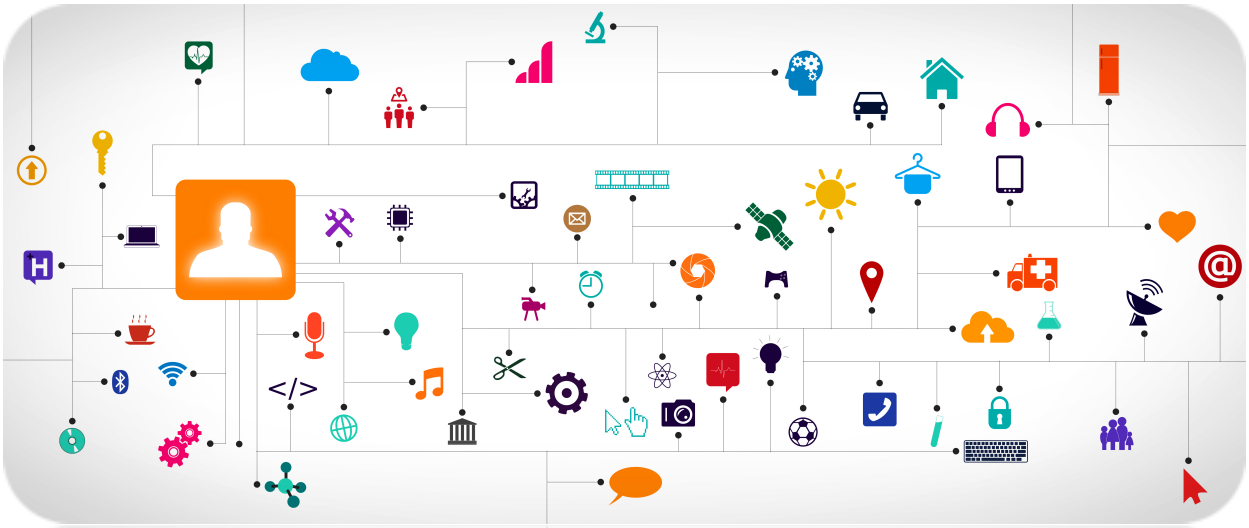
IoT Funcionalidades y Seguridad.

Universidad Mariano Gálvez de Guatemala



Alvaro Antonio Arana Vásquez
Guatemala, octubre del 2016

6,4 billion IoT's will be connected to the internet according to Gartner Inc. the technological advantage of the IoT has surpassed the expectations of its initial design and has nowadays become one of the most consumed products, since the SmartTV, smart refrigerators and the most popular Smartphone. In Guatemala there are at least over 5 million IoT's connected to the internet, according to one of the last data of the Super Intendencia de Telecomunicaciones de Guatemala (Super Administration of Telecommunications of Guatemala), one user has at least 2.5 smart devises.

Definiciones.

IoT: Internet of the things, la definición dada a todos los equipos electrónicos que están conectados a una red de datos *(internet).* IoT es más que conexiones de internet a equipos domésticos, es el alcance de un rendimiento muy potente de al menos el 90% de equipos que utilizamos a diario; relojes, teléfonos celulares, monitores para bebes, estufas, refrigeradores, cámaras de vigilancia, etc.
Es unificar todo lo que podemos utilizar en nuestro día a día en un solo punto de acceso: Internet.

DNS: Domain Name System, según sus siglas en ingles. Es el encargado de gestionar todos los nombres relacionados en una red privada o bien en internet, interpreta los nombres de dominios o host a sus respectivas direcciones IP.

Dirección IP: Es el numero que identifica lógicamente a un dispositivo dentro de una red privada o publica (internet)

Malware: Malicious Software, según sus siglas en ingles. Es el software mal intencionado diseñado para infiltrarse en sistemas operativos y poder tomar el control del mismo o bien dañar su sistema de archivos.

Ethernet: Interfaz de comunicación basada en protocolos TCP/IP.

Sistema Operativo: Lenguaje de programación de alto y bajo nivel que abstrae las propiedades del hardware.

Hardware: Componentes físicos que integran una computadora, IoT. En estos se incluyen la memoria RAM, CPU, Periféricos, etc.

App's: Nombre actual para las aplicaciones que conocemos actualmente. Estas tomaron el nombre debido al auge de programación a nivel de dispositivos móviles.

Introducción.

En la actualidad caminar por un centro comercial y pasar frente a las vitrinas de los enormes almacenes de tecnología me hace recordar mucho mi infancia, recordar aquella caricatura de "Los Supersónicos" *(Serie animada desarrollada por Hanna Barbera a principios de los años 60).* La serie que llevó a muchos a soñar con el futuro muy distante que permitiría tener conectado a una red global, no recuerdo haber escuchado en sus episodios algo como "La conexión a internet del televisor" simplemente veía asombrado cómo podría en un futuro poder llamar a alguien por medio de un televisor, tomando en cuenta que para mi infancia en los 80's yo solamente tenia acceso a un televisor blanco y negro. También veíamos como un robot se encargaba de todo lo necesario en casa para mantenerlo limpio y ordenado.

Quizá no más de 50 años se estrenaba aquella serie mucho más futurista "Viaje a las estrellas" o "Star Trek", vi muchos episodios con mi padre, me daba cuenta de tecnología no existente en ese momento claro está, que les permitía realizar muchas tareas, controles desde tabletas, lentes inteligentes, creo que el preferido era ver al Capitan Kirk utilizando un dispositivo de comunicación *(hoy en día lo llamamos SmartPhone)* o ver al Sr. Spock utilizando una tableta para controlar algunas funciones de la nave, etc. Eso ahora lo conocemos como internet de las cosas.

Que es el internet de las cosas?

La web y analistas definen el IoT por sus siglas en ingles *(Internet of the Things)* a la interconexión de todas las cosas que comúnmente nos rodean en una misma red *(internet).*
Muchos de los sitios web dedicados a la tecnología hablan sobre las bondades de estos, crean ese mercado que a los ojos del consumidor se vuelve atractivo y porque no decirlo, se vuelven los equipos soñados y deseados.

Ahora que hemos entendido a que se refiere el internet de las cosas, nos referiremos a ello como IoT, para mantener la abreviatura y saber identificar a que nos referimos.

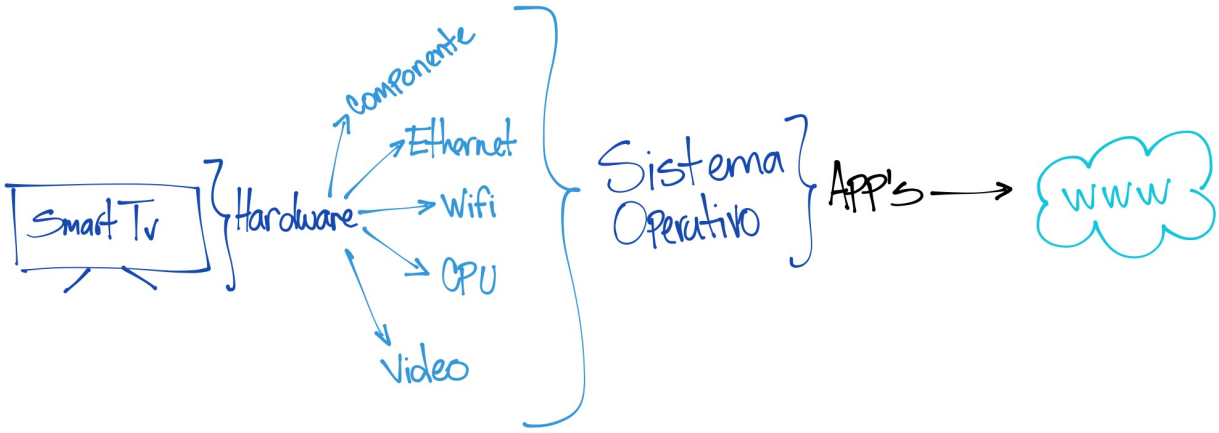
Es seguro el IoT?

Las bases se pueden dar por sentadas sobre las funciones del IoT y como mejoran la vida, pero también es la punta de lanza en este mundo tecnológico. Veremos la importancia de asegurar las comunicaciones en el IoT, como los *virus, malware, ramsonware* pueden tumbar el IoT o al menos destapar lo oculto bajo la sabana tecnológica.

Funcionalidades de IoT.

Cualquier dispositivo electrónico que utilizamos para conectarnos a internet o para automatizar actividades, mantiene una programación que se ejecuta en un hardware en especifico. Esta programación se basa en lenguajes que abstraen dicho hardware y generan una comunicación en base a instrucciones o comandos.

Nuestras computadoras, funcionan con sistemas operativos que van desde distribuciones de Linux, Unix, MacOS, Microsoft Windows, etc. Pero para los IoT es un tanto diferente pues un Smart TV ejecuta un software programado para abstraer las funciones de su hardware.



En la ilustración de arriba se describe de una manera muy sencilla como se conforma y SmartTV pasando por los componentes de hardware, abstraídos por el sistema operativo y que este por medio de las aplicaciones se conecta a internet.
Es una manera sencilla y podríamos pensar que esto es inofensivo y que no lleva mas problema para conectarse a internet.

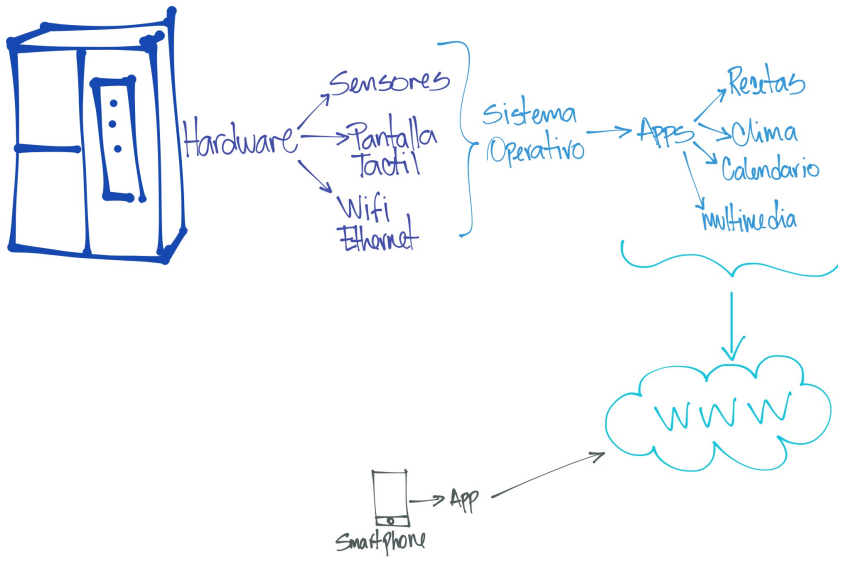
Lo mismo sucede con otros equipos que forman parte del IoT, los ejemplos pueden ir desde refrigeradores, hornos, sistemas de ventilación, automóviles, etc.

Con el ultimo ejemplo mencionado, cabe destacar los sistemas operativos diseñados para los automóviles "autónomos" o como muchos los describen, un auto inteligente. Pero como puede un auto inteligente ser funciona? Esto nuevamente me remonta a los programas de televisión de mi infancia y recordar aquella serie "Knight Rider" o como era llamada en Latinoamérica "El Auto Fantástico".
Era genial recordar esa serie y como Kitt *(Nombre del auto protagonista)* tomaba desiciones por si solo y mantenía una conexión con un centro de mando, comunicación inalámbrica, etc.

LG *(Compañía Sur Coreana, dedicada a la electrónica y fabricación de IoT)* Trata de alzar el vuelo montando un sistema operativo completo para sus Smart TV, este es el ***WebOS,*** ya integrados en las gamas altas y bajas de sus televisores, WebOS se muestra como uno de los fuertes contendientes en la abstracción de hardware y brindar mayor rapidez en la conexión de sus Apps hacia internet.

www.Cnet.com publica en su sitio uno de los lanzamientos mas extravagantes en cuanto al IoT se refiere. Muestra el lanzamiento del nuevo refrigerador de Samsung *(Compañía Sur Coreana, dedicada a la electrónica y fabricación de IoT)* Samsung en sus muchas innovaciones lanza un refrigerador capaz de controlar todo lo que tienes allí almacenado. Quizá te preguntarás como puede innovar un refrigerador inteligente? La respuesta es sencilla de explicar; Los refrigeradores inteligentes están diseñados para ayudarte manteniendo un inventario adecuado a una lista programada, su conectividad a internet te permite comprar lo que ya no tienes disponible en casa, todo mediante una App y la conexión a internet de tu refrigerador.
Te dejo el link para que puedas darle un vistazo. https://www.cnet.com/es/analisis/samsung-family-hub-refrigerator/primer-vistazo/

Te ilustro un poco sobre los refrigeradores inteligentes.

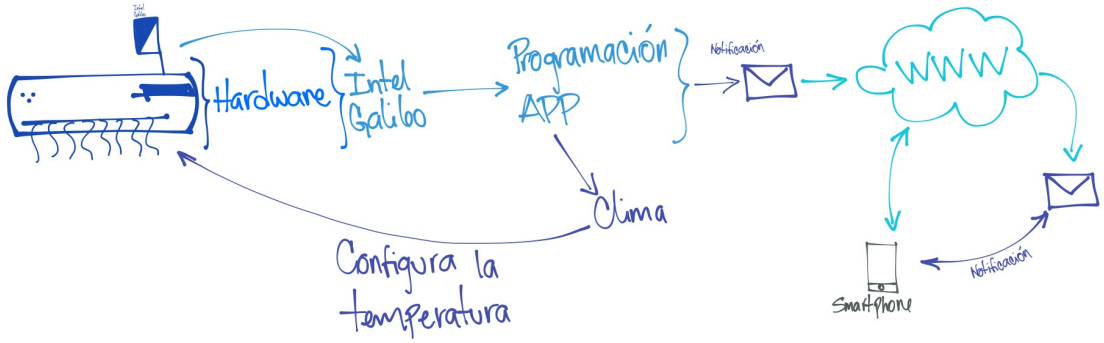


Lenguajes de programación de IoT.

Los lenguajes de programación del IoT son muy variados, y esto depende del hardware y funciones que vaya a desarrollar, los lenguajes de programación van desde C, C++, Java, Javascript, Python, Go, Rust, etc.

Por ejemplo, los sistemas de aire acondicionado realmente no son equipos inteligentes, sino que estos cuentan con micro computadoras que pueden controlar los componentes de estos.
Una de las compañías más importantes en cuanto a desarrollo de hardware es Intel *(Compañía Norte Americana dedicada al diseño y fabricación de procesadores, software y hardware)*. Intel ha realizado una alianza con Arduino *(Compañía Norte Americana dedicada a la fabricación de software y hardware libre)* y han creado el Intel Galileo.

Intel Galileo es una placa desarrollada para ser programada y gestionar aplicaciones e integraciones a otros equipos, por ejemplo podrías integrarlo a un sistema de aire acondicionado el cual será accesible desde una aplicación instalada en un smartphone o tableta. Imagina la capacidad de configurar tu placa de Intel Galileo para que controle el clima de toda tu casa en base al estado del tiempo de tu ciudad, eso seria genial, tomando en cuenta nuestro cambio climático... Sabrías que si has pasado un día de invierno demasiado frío, el sistema de aire acondicionado de tu casa estará en la temperatura perfecta, pues ya ha tenido conexión a internet y te ha notificado por medio de un email.



Intel Galileo puede ser programada en varios lenguajes como C, C++, C#, G++, y tiene como base de fabrica una imagen basada en Python. Existen otras placas en el mercado, como Arduino, Raspberry Pi que están enmarcadas en los micro computadores de bajo costo.

Aquí dejo el link con las especificaciones técnicas y novedades del Intel Galileo.
http://www.xataka.com/makers/intel-galileo-placa-de-desarrollo-fruto-de-la-colaboracion-entre-intel-y-arduino

Bien, ahora que entendemos como es que se desarrollan las funciones del IoT quiero entrar de lleno al tema que no se habla al momento de utilizar el IoT, *La Seguridad.*

IoT, Seguridad.

El pasado 21 de octubre del 2016 se dio uno de los más grandes ataques de seguridad, un ataque de ***Denegación de Servicios*** conocido por sus siglas en ingles ***(DDoS).*** El ataque trajo abajo muchos de los sitios en internet, sitios que funcionan para conectividad de apps que pueden usarse en el IoT, como Facebook, Twitter, Netflix, etc. Las aplicaciones estuvieron mostrando mensajes de error en la conexión, error al tratar de reproducir un contenido o bien al momento de colocar un mensaje.

WikiLeaks colocó un tweet el 21 de octubre a las 3:09 pm con el siguiente mensaje: *"El Sr. Assange sigue vivo y WikiLeaks sigue publicando. Pedimos a los simpatizantes que dejen de tomar el internet de EE. UU. Has comprobado tu punto."*

El mensaje iba en respuesta a varias amenazas que el sitio de WikiLeaks había notado, respecto a un supuesto ataque a todo internet y a sus páginas principales.

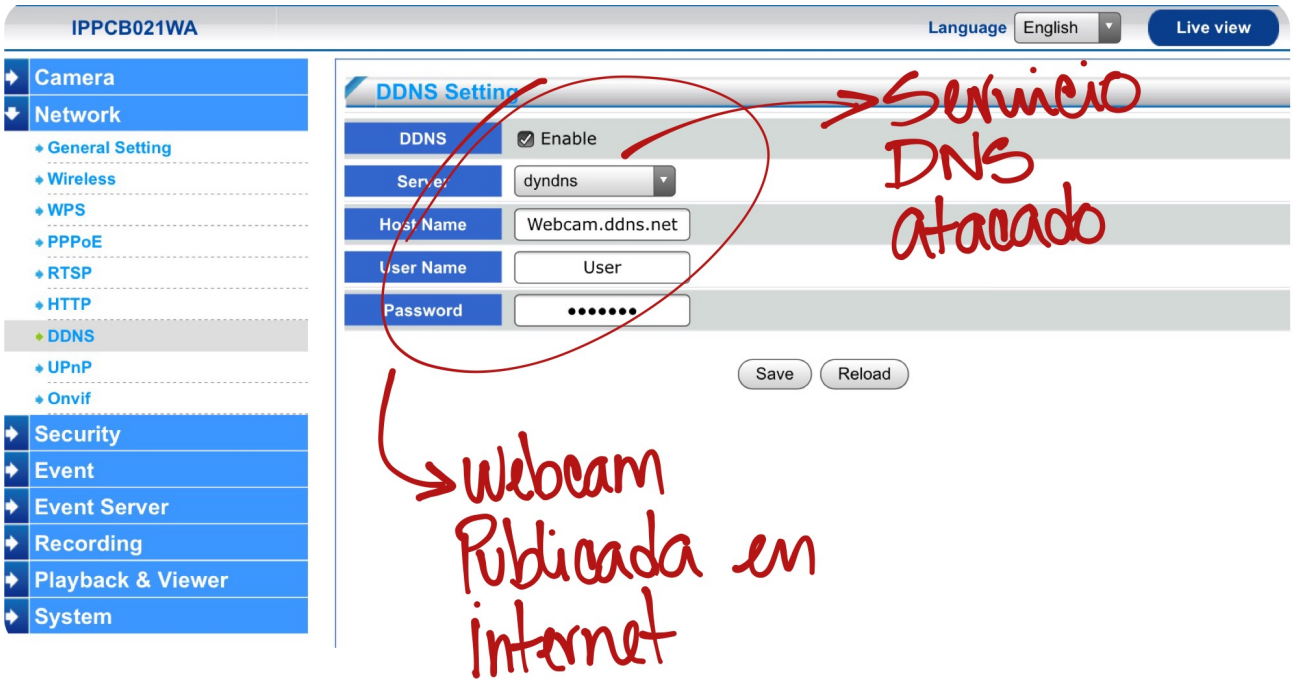
El gobierno de Estados Unidos de Norteamérica no daba aun algún tipo de sospechoso o responsable del ataque, CNN en su área de economía también publico una nota relacionada con el ataque al internet, acá coloco el link de la nota. http://money.cnn.com/2016/10/21/technology/ddos-attack-popular-sites/

Realmente tumbaron las páginas de internet?

Durante el ataque a todos estos sitios, muchos notamos la falta de servicio de las aplicaciones en nuestros IoT, la conexión a Netflix no funcionaba, no podía cargar Facebook y el resto de apps de mi Smart TV, tras la aparente caída de los sitios de internet traté de conectarme a una app instalada hacia algunos días atrás *"Claro Video" Link de referencia* http://www.claro.com.gt/portal/gt/sc/personas/tv/clarovideo/ lo agradable fue notar que el streaming funcionaba sin problemas, no presté mayor atención en ese momento.

El sentido de la caída de los servicios tomo forma luego de leer un reporte post-ataque publicado por el sitio www.es.gizmodo.com en su link http://es.gizmodo.com/confirmado-el-ataque-ddos-que-tumbo-la-red-en-eeuu-sur-1788100823 el post hace referencia a que el ataque perpetrado el pasado 21 de octubre tuvo como herramienta el IoT bajo el control del Malware Mirai... *¿Como puede ser posible que el mismo IoT pueda ser capaz de tumbar los servicios que necesita?* La respuesta a simple vista puede ser compleja de responder, pero analizando el caso presentado, realmente no fueron las páginas las que cayeron, sino los servicios de DNS que identifican estos sitios.

Los servidores DNS son aquellos encargados de identificar todos los sitios existentes en internet, una forma fácil de poder describirlos es poniendo un ejemplo sencillo a bajo nivel.
Pensemos que internet es un país, y que cada habitante de este país es un sitio web o servicio, los ciudadanos se identifican por un numero único e irrepetible, ese numero es el equivalente a la dirección IP de los sitios web, pero cómo podríamos memorizar ese numero de identificación único? Aquí es donde entra en juego el servicio de DNS. Los DNS son los encargados de traducir los nombres de los ciudadanos a sus números de identificación. Puede ser tan claro que al escribir www.eset-la.com yo no sabría a primera mano la dirección IP sobre la cual está registrada, pero el DNS si.



Esto aun sigue sin responder la pregunta antes planteada *¿Como puede ser posible que el mismo IoT pueda ser capaz de tumbar los servicios que necesita?* No estamos hablando de un tipo de canibalismo a nivel del IoT donde él mismo puede tumbar los servicios que necesita para funcionar.

Estamos hablando de que el IoT es vulnerable por muchas razones y esto puede ser tan peligroso que lo visto el 21 de octubre pasado solo puede ser un ejemplo de los grandes problemas que se avecinan.
Arriba podemos ver un ejemplo de configuración de un IoT, es la configuración de DDNS para una webcam de bajo costo y en área residencial. DynDNS es una de las principales compañías encargadas en el manejo de registros DNS para grandes compañías como Netflix, Twitter, Facebook, etc.

Como se pudo manipular el IoT con Mirai? Wikipedia da una muy clara referencia *del Malware* ***"Mirai es un malware que transforma los sistemas computarizados de la familia GNU/Linux en botnets controlados remotamente, y así poder ser utilizados en ataques web de gran escala. Principalmente apunta a dispositivos que conforman la IoT."***
https://es.m.wikipedia.org/wiki/Mirai_(malware)

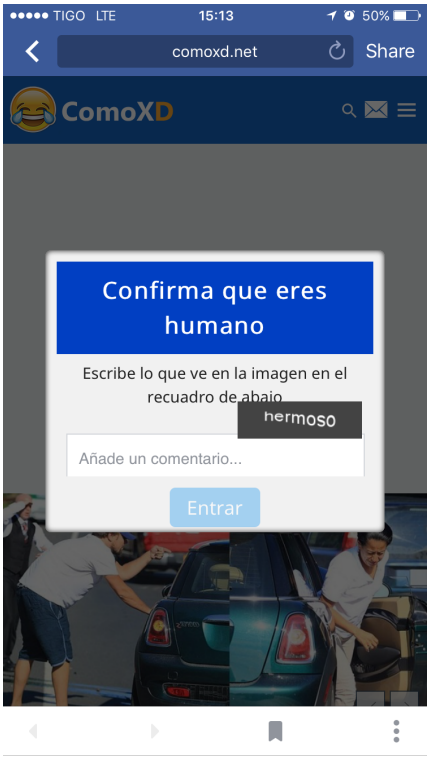
Dentro del articulo de www.es.gizmodo.com se ve que la mayoría de los dispositivos utilizados en el ataque mantenían contraseñas y parámetros de fabrica, niveles muy bajos de seguridad.

Es vulnerable el IoT?

En las descripciones de funcionalidad de los IoT Smart TV, Refrigerador, Aire Acondicionado podemos notar una falta de seguridad en las conexiones que estos realizan, como saber si la programación de dichos componentes no está comprometida al momento de conectarse a internet?

Imagina un virus o malware que se capaz de controlar tu refrigerador? Sabrías con seguridad si tus alimentos se mantendrán frescos? Si manejará la temperatura adecuada?... Lo mismo puede suceder con un Smart TV, imagina una versión de ramsonware que pueda bloquear todas las funciones, y que puedas usarla solamente pagando dicho secuestro.

Tras el ataque muchos sitios de internet tratan de controlar las conexiones o solicitudes. El captcha es el más utilizado.



Smart TV, smartphones, sistemas de entretenimiento, refrigeradores, NDVR, cámaras web, cámaras de vigilancia, tostadores, etc. Todo esto conforma el IoT. La seguridad es el punto más importante a tomar al momento de utilizarlos, que tanto queremos comprometer nuestra privacidad, que tanto queremos depender de ellos, son preguntas importantes que debemos hacernos.

Necesitamos cifrado para las comunicaciones, asegurar que nada puede ser interceptado al momento de utilizar el IoT, que actualizar nuestra tarjeta de crédito en un SmartTV para utilizar los servicios de Netflix sea realmente seguro, que la cámara web de mi SmartTV o computadora no tenga que estar tapada o desconectada, por el temor de que un malware tome el control de la misma sin que yo esté enterado.

Conclusión.

El IoT transformará nuestra manera de estar conectados, pero también se puede convertir en la piedra en el zapato mientras no se le brinden los ajustes de seguridad que necesita. Cifrado de conexiones, sistemas operativos que puedan trabajar bajo diversos análisis de seguridad en tiempo real.

Los proveedores de servicios de internet brindan routers como parte del servicio contratado, muchos de estos funcionan con contraseñas de fabrica y con niveles bajos de seguridad, los usuarios finales no tienen idea de que hay detrás de su router casero, incluso muchos no sabrán si ellos fueron parte de la caída de los servicios de internet.

Recomendación.

Dejar de usar el IoT porque es vulnerable? Respuesta difícil de dar pues el usuario se interesa cada vez menos en la seguridad, siempre y cuando funcione y brinde los servicios que necesita... Entonces está bien.

Los fabricantes de IoT deben prestar mucha atención a cerrar esas brechas de seguridad en sus dispositivos. Los grandes de la seguridad deberán diseñar soluciones de seguridad que puedan combinar las funciones del IoT y la seguridad, con esto me refiero a que yo como usuario de un sistema inteligente de aire acondicionado estaré tranquilo de saber que mi equipo cuenta con actualizaciones constantes, con una solución de seguridad que se mantiene analizando las líneas de programación y que la conexión a internet está asegurada.

La seguridad es el eslabón faltante en el IoT, hasta cuando este se logre integrar tendremos un IoT robusto y listo para emerger, de momento puedo asegurara que el IoT es un prototipo en producción.

Y por ultimo me atrevo a decir lo siguiente: *"El único sistema seguro, es aquel que se almacena en un búnker de concreto y acero, bajo 100 metros de tierra, en una isla desierta y apagado."*

Referencias.

Imagen de portada tomada de http://www.stockvault.net *como imagen gratuita.*
Links de referencia utilizados se encuentran dentro del texto, como link de acceso para ampliar la información recopilada.
www.es.gizmodo.com, www.wikipedia.com, www.cnet.com www.globbsecurity.com