Análisis de vulnerabilidades en medidores eléctricos inteligentes (SMART METER)

Greivin Ramírez[1], Luis Mora[1], Katerine Castillo[1], Kennet Vega[1], Profesor: Antonio González[1], and Profesor Guía: Randall Barnett[2]

[1] Escuela de Ingeniería,
Universidad Latinoamericana de Ciencia y Tecnología,
ULACIT, Urbanización Tournón, 10235-1000
San José, Costa Rica
alumno1,alumno2@ulacit.ac.cr
http://www.ulacit.ac.cr
[2] Departamento,
Institución,
Siglas, Dirección, Apartado postal
San José, Costa Rica
alumno1@institucion.cr
http://www.institucion.cr

Abstract. Se pretende elaborar un análisis que permita identificar posibles vulnerabilidades en la red de medidores inteligentes que puedan provocar que esta tecnología no sea lo suficientemente segura, por consiguiente buscar respuestas a las incógnitas generadas en el problema, con el fin de diseñar una red segura, confiable, disponible y así lograr reducir el riesgo en seguridad, tomando en cuenta las medidas necesarias para garantizar a los clientes y al Instituto Costarricense de Electricidad (I.C.E) un eficiente y correcto funcionamiento de la red de medidores inteligentes (Smart Meter), lo que puede mejorar la gestión de la energía, la cual promete a los usuarios y a la empresa proveedora conocer cuánto se consume y genera respectivamente en tiempo real, permitiendo contar con un servicio eficiente y seguro. El uso de este tipo de dispositivos le permite al país avanzar un poco más en su meta de convertiste en una nación carbono neutral. La investigación se desarrollará haciendo pruebas de laboratorio en el (I.C.E), con apoyo de personal de la institución especializado, donde se recopilará la mayor cantidad de información posible, así como investigaciones bibliográficas basadas en artículos de la biblioteca EBSCO.

Keywords: Smart Meter(SM), Zigbee, Z-wave, Smart grid (SG), protocolo, estánda, seguridad,Instituto Costarricense de Electricidad (I.C.E), ciberdelicuencia, cifrado, medidor, hacker, Home Area Network (HAN), medidor inteligente (SM)

1 Introducción

Un SM se puede definir según la literatura como un dispositivo totalmente inteligente que puede medir y almacenar datos en intervalos específicos y actuar

como un nodo de comunicaciones automatizado de dos vías entre el proveedor y el consumidor. La utilización de estos dispositivos inteligentes muestra que la utilización en los hogares da a los usuarios información de re alimentación en tiempo real y el uso histórico para ayudarles a entender y gestionar su consumo de electricidad de una mejor manera logrando ahorros significativos entre 5 al 15 por ciento en su factura, ademas de que con este tipo de tecnología de los SM se pueden automatizar prácticamente todo tipo de dispositivos eléctricos diseñados para usarse con los SM en un hogar teniendo la posibilidad de ser hogares inteligentes con capacidad de ser controladas incluso por medio de dispositivos como celulares inteligentes lo cual es muy bueno pero también es una vulnerabilidad mas que se tiene ya que es una puerta abierta o posibilidad de más a ataques en la red.

2 Antecedentes

En nuestro país el Instituto Costarricense de Electricidad (I.C.E) ha implementado SM en hogares e industrias, como se podrá observar en la tabla siguiente, en muchas en partes del mundo, han optado por el uso de contadores inteligentes para controlar de mejor forma el consumo en los momentos "pico" del día en que hay mayor demanda de electricidad de sus clientes, así como mejorar la fijación de precios y evitar el fraude y robo a gran escala de los servicios públicos y con la medición inteligente se ofrece una manera de reducir este problema esto debido a la medición de consumos en tiempos reales. Un punto principal a destacar en este documento son los comentarios sobre medición inteligente en diferentes países, beneficios y problemas que ha tenido en la implementación de esta tecnología así como legislación que respalda el uso de estos medidores inteligentes.

La manera de trabajo convencional de los procesos para obtener la información de los gastos en consumo eléctrico de los clientes, es totalmente manual, se cuenta con una persona que realiza una revisión de cada uno de los medidores instalados en los hogares, siendo esta una tarea tediosa, con un gran porcentaje de error humano en las mediciones obtenidas y un gasto económico para la empresa. Con la entrada de los SM, todo eso queda en el pasado y ahora se debe trabajar en buscar mejorar la seguridad de los mismos, ya que al ser todo por medio de transmisión de datos tanto de forma inalámbrica como alámbrica, existen muchos tipos de vulnerabilidad y no hay un método que sea cien por ciento eficaz que asegure la protección ya que se ha demostrado a través de los años, los constantes ataques de hackers y delincuentes informáticos a distintas redes y empresas, que creían estaban seguras. Es por ello que con este artículo pretendemos dar un aporte sobre la mejor manera de poder contrarrestar la inseguridad que tienen los SM (Smart meter) dentro de las Redes Inteligentes (SG) en Costa Rica, representado por el I.C.E, entidad encargada como pionero y único proveedor estatal de estos servicios en el país.

Las SG son un complemento para nuestras redes convencionales del servicio eléctrico que le facilitan tanto a la empresa proveedora como a sus clientes el poder administrar mejor sus recursos y dinero en tiempo real. Permitiendo la

PAÍS O LUGAR	PRINCIPALES MOTIVOS	ESTADO DE MEDICIÓN INTELIGENTE	REGULACIÓN
California	Gestión de cargas / reducción de picos de consumo	En curso para medición de Electricidad y gas	Monopolios locales grandes, integración vertical
Italia	La reducción del fraude; poder contractual de control / limitación de carga	Casi completa (electricidad)	Competencia ligera
Holanda	Reducción de la demanda, Administración de la carga energética	Despliegue Obligatorio detenido; renegociado términos	Liberalizado; redes propias de medidores
Ontario, Canadá	Gestión de cargas	Implantación completa l	Muchos monopolios locales
Suecia	Facturación exacta	Despliegue completo	Liberalizado; redes propias de medidores

Fig. 1. Comparativa movimientos de SM en países

conexión y desconexión del servicio de manera remota, facilitando la detección de averías. Para la transición de tecnología, no solo se necesitara de personal especializado por parte de la empresa proveedora, sino que también se les debe de explicar a los usuarios todas estas nuevas opciones y los cuidados que deben de tener de los mismos.

Al implementar este nuevo avance tecnológico los clientes podrán identificar nuevos elementos en la red. Del SM al tendido eléctrico podrá ver dispositivos digitales así como la fusión con la infraestructura de telecomunicaciones y del medidor a la casa encontrara sensores inteligentes que permitirán la comunicación entre los dispositivos del hogar (refrigeradoras, televisor, entre otros), una infraestructura ya sea inalámbrica o cableada, que se comunicaran con el SM.

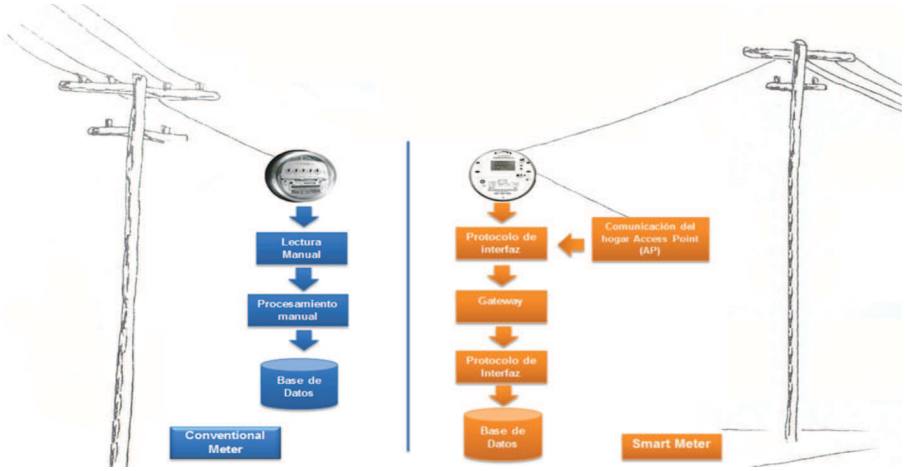

Fig. 2. Gráfico comparativo de medidores convencional - SM

Al ser un sistema tan amplio vamos a realizar un análisis del medidor a la casa, cual es el tipo de infraestructura mínima que se debe de tener, los requerimientos en seguridad necesarios para poder gozar de un sistema que nos facilite nuestras funciones en el día a día y no se convierta en una pesadilla que pueda no solo hacer perder credibilidad en la tecnología y en la empresa proveedora sino que pueda atentar contra nuestra seguridad en caso de algún ataque cibernético.

Seguridad

Iniciaremos comentando que la red que se necesita para este tipo de implementación es una red de área doméstica (HAN), en ella se encontraran solamente conectados los dispositivos a los que se desea administrar su consumo eléctrico, y como la gran mayoría de las redes, para funcionar se requiere de protocolos de comunicación. Estos protocolos permiten que sin importar la marca de los electrodomésticos que tengamos en casa, se pueda realizar una transmisión de información trasparente con el SM.

A nivel mundial hay dos protocolos muy fuertes, que son Z-Wave y Zigbee ambos pertenecen a organizaciones sin fines de lucro que buscan ir perfeccionando las características de esta tecnología.

Al ser en su mayoría implementaciones inalámbricas, pueden implementarse diferentes protocolos ya sea abiertos o propietarios, pero las vulnerabilidades que puede sufrir son las mismas que cualquier otra red inalámbrica.

La opción de una implementa de criptografía de clave simétrica, tiene una desventaja y es que tanto el emisor como el receptor deben de conocer la clave para cifrar y descifrar el mensaje. A continuación se mencionaran los tipos de criptografía simétrica que existen pero a lo largo del texto se profundizara en AES

que es el protocolo por excelencia de ZigBee, donde se analizaran sus ventajas y desventajas Existen varios tipos de tipos de criptografía simétrica como los son:
• Cifrado en flujo:
o Cifrado de César.
o Cifrado con máquina enigma.
o Cifrado de Vernam. También llamado one use pad, cuaderno de uso único.
• Cifrado en bloque:
o Cifrado de Hill.
o DES.
o AES. ((Hui Shi1, 2014)).

Seguridades mas usadas en Redes Inteligentes ZigBee / Z-Wave

Como a se ha mencionado anteriormente, la seguridad es un tema primordial en las redes de comunicaciones, más cuando de una SG se habla, donde todos los componentes que la conforman son fundamentales y cumplen una función esencial, es importante la validación de todos los dispositivos que deseen tener acceso a la red, con el fin de evitar accesos no deseados y la manipulación de los paquetes que viajan a través de la red, Con el objetivo de que un intruso no pueda conectarse a un SM, y transmita información falsa, alterando los informes de consumo de energía en el hogar del cliente ((Zhongmin LI1, 2014)) la tecnología ZigBee, es un conjunto de protocolos de red de área personal inalámbrica (WPAN), fiable, eficiente, de alta disponibilidad, de bajo precio, de bajos requisitos de recursos, seguro y basado en el estándar IEEE802.15.4. Debido a las ventajas que presenta la tecnología Zigbee, esta puede ser grandemente utilizada en el campo de red de los hogares. La seguridad que ofrece dicho protocolo, utiliza el algoritmo criptográfico simétrico o de secreto compartido específicamente AES-128 (Advanced Encryption Standard) con claves de 128 bits, ((Bertol?n., 2011)) ,((Kangude, 2011)), este estándar ha sido emitido por el Instituto Nacional de Estándares y Tecnología (NIST) y especifica que es un estándar de cifrado de clave simétrica, adoptado por el gobierno de Estados Unidos y utilizado para la protección de datos electrónicos. Debido a sus características anteriormente mencionadas AES se considera confiable y eficiente ya que es un estándar adoptado por esta gran potencia mundial, la cual se ha caracterizado por ser uno de los pioneros en cuanto a seguridad se trata. Por un lado lo convierte en un algoritmo robusto y de prestigio a nivel mundial, por otro lado puede convertirse en un peligro a la red si es implementado con errores, como todo proceso de aseguramiento de información en las comunicaciones tecnológicas, ya que como se menciona anteriormente en este mismo artículo, AES es un cifrado simétrico que utiliza la misma clave para los procesos de cifrado y descifrado la cual puede ser más fácil de interceptar por un intruso en la red. ((Kangude, 2011)) se está de acuerdo y se considera importante complementar Zigbee con otro tipo de cifrado para asegurar y minimizar las vulnerabilidades que este estándar pueda presentar, entre unas de nuestras recomendaciones es el de implementar cifrado asimétrico

ya que ((Barukab, 2012)) este tipo de criptografía es más confiable y mucho más complejo, al utilizar dos claves diferentes para el proceso de encriptación, una clave pública o compartida para cifrar y una clave privada o secreta para descifrar. Ejemplos utilizados en Zigbee son la autenticación basada en firma digital como RSA (Rivest, Shamir y Adleman) y el intercambio de claves D-H (Diffie-Hellman) basado en ECC (Elliptic Curve Cryptography). Se analizaron los dos tipos de criptografía que pueden ser utilizadas en Zigbee, tanto la asimétrica y simétrica, según características especificadas ((Barukab, 2012)) y se determinó que ambos mecanismos tienen características diferentes y se enfocan en diferentes puntos, por un lado la encriptación simétrica sacrifica el aseguramiento de la información para ser más eficiente en términos de velocidad en el procedimiento de encriptación (cifrado y descifrado) al ser con una sola clave conocida tanto por el emisor como por el receptor, y por otro lado el mecanismo de criptografía asimétrica sacrifica la velocidad, volviéndolo más lento al utilizar dos claves, con tal de ofrecer mayor confiabilidad, mayor integridad y una autenticación e identificación más eficientes en la red. Además del protocolo anteriormente analizado en este artículo llamado Zigbee, existe otro protocolo comúnmente utilizado en las SG, este es el protocolo Z-wave, el cual se analizan las características y mecanismos de encriptación que son utilizados en dicho protocolo, con el fin de hacer una comparación entre los dos protocolos vistos, para general una propuesta ideal para las SG. ((Alliance, 2014)), Z-Wave es un protocolo desarrollado con el fin de controlar aplicaciones de control remoto y diseñado para automatizar el hogar es una tecnología de potencia baja. No cuenta con el respaldo y reconocimiento de un estándar internacional, pero si cuenta con el apoyo de Z-Wave Alliance ((Alliance, 2015)), opera en frecuencias diseñadas para comunicaciones de bajo ancho de banda en los dispositivos integrados, como los sensores de seguridad, alarmas y paneles de control domótico, posee una transmisión de datos con velocidades de hasta de 100 kbps, el cual necesita tener la seguridad necesaria para el aseguramiento de la información en la red ((Knight, 2006)), Z-wave cuenta con diferentes opciones de encriptación, como por ejemplo mecanismos de cifrado por bloques, entre ellos, CTR – Counter Mode, OFB – Output Feedback Mode, CFB – Cipher Feedback Mode, (CBC-MAC), este último es con un código para autenticar los mensajes como, el valor MAC, asegura que el protocolo Z-Wave no sea manipulado durante la transmisión de los datos y así mismo asegura que haya sido enviado por el nodo que dice ser la fuente del mensaje (se crea una validación)((Hui Shi1, 2014)). Se determina que el protocolo ZigBee y Z-wave tiene una serie de características similares y de igual forma cuenta con una serie de atributos que los diferencian el uno del otro, ambas son tecnologías de comunicación en redes inalámbricas, basadas en chip, son utilizadas para la creación de sistemas que controlen funciones específicas en las SG como por ejemplo sistemas de seguridad, acceso a puertas, sistemas de iluminación, entre otros sistemas que puedan implementarse en un hogar inteligente, se determina que ambas son de muy bajo consumo de energía, fiables, eficientes, de alta disponibilidad, la gran diferencia entre ambos según el análisis de las características de cada protocolo es que Zigbee, es respaldado por el estándar IEEE802.15.4 y en el caso de Z-

wave, no cuenta con el respaldo de ningún estándar internacional, en cuanto a seguridad se trata. ZigBee también toma ventaja de acuerdo a su comparación en este artículo, al implementar AES-128 (Advanced Encryption Standard) un mecanismo de encriptación reconocido y adoptado por una potencia mundial como lo es los Estado Unidos, también toma ventajas en cuanto a la frecuencia que utilizan, la velocidad de datos, y la capacidad de dispositivos conectados en la red. Según datos recopilados de ((Barukab, 2012)), ((Alliance, 2014)), incluyendo una serie de características tanto en ventajas, encriptación y capacidad de cada protocolo estudiado en este artículo Se han mencionado algunas vulnerabilidades en las redes y en este caso específico hablando de redes HAN, que son las comúnmente utilizadas para SG y en SM, además de ser las utilizadas por el I.C.E, en conexiones a casas inteligentes, el problema surge que todavía no hay una solución cien por ciento segura, ya que si por ejemplo se maneja la seguridad por medio de anonimato quien es el responsable de asignar claves robustas y fuertes y de estar cambiándolas cada cantidad de tiempo, además de qué manera se asegura no vayan a surgir confusiones y malestares en los clientes que cuentan con poco conocimiento sobre la seguridad en redes como por ejemplo adultos mayores en un hogar con este tipo de tecnologías, cabe destacar que todavía hay muchas incógnitas en cuanto al modus operandi de este tipo de tecnologías tan nuevas de estar en marcha y no solo en este país sino alrededor del mundo ya que estamos hablando de máximo una década de la puesta en marcha mundial de estas tecnologías y hasta hoy en día el acceso a ella, es la mínima población que las tiene ya que sus costos de implementación son muy altos, y por último que garantiza que dichas claves no puedan ser interceptadas por un hacker, deberían de ser creados acuerdos nacionales e internacionales de seguros acerca de garantías que se deberían brindar para la tranquilidad de los clientes con este tipo de SM.

ZigBee	**Z-Wave**
Protocolo Abierto	Protocolo Propietario
IEEE 802.15.4	UIT-T G.9959 rPHY / MAC con pila de protocolos de Sigma Designs
Redes inalámbricas	Radio Frecuencia
Frecuencia 868 MHz, 915 MHz y 2,4 GHz	Variable dependiendo de región o país
Transferencia 250 Kbps	
Topología estrella, malla	Topología malla
Encriptación simétrica	
Distancia de 10 a 100 metros línea vista	30 metros línea vista

Fig. 3. Tabla comparativa ZigBee / Z-Wave

Vulnerabilidades en las Smart Grid y los Smart Meter

Como es mencionado a lo largo de este articulo las tecnologías de la información son de gran importancia al implementar una red eléctrica avanzada como lo son las SG, que cuenta con una comunicación bidireccional entre el proveedor de servicio eléctrico y el cliente final. Convirtiendo la distribución de la energía en un proceso automático más eficiente ya que desaparece la lectura manual a cada medidor. Por un lado las SG ofrecen ventajas importantes tanto a los proveedores del servicio eléctrico como al consumidor, entre ellas está el poder administrar en tiempo real el consumo de energía eléctrica en nuestros hogares, también facilitar a la empresa proveedora de energía llevar un control con mayor eficiencia del abastecimiento de todos los hogares que utilizan SM, así como también generar avances al país en los sectores; productivo (electricidad), el económico (ahorro en el hogar y en la empresa proveedora de energía eléctrica) y el ambiental (menos contaminaciones en las plantas hidroeléctricas) . Por el otro lado, la necesidad de tener conexión a Internet y el uso fundamental de las TICs, hace que nuestra red inteligente sea más vulnerable a las amenazas, ya que serán expuestas a los ciberataques por tener una conexión 24/7 y podría generar resultados con pérdidas importantes tanto para el consumidor como para el proveedor de la energía que en este caso al I.C.E. La seguridad debe ser considerada en todas y cada una de las fases de la red, desde la fase de diseño, en la del desarrollo, el mantenimiento, entre otras. La seguridad debe responder a todo tipo de ataques tanto del lado del proveedor como del lado del consumidor; desde ataques de empleados de la empresa proveedora, terroristas cibernéticos, consumidores astutos para alterar el informe de consumo hasta fallas o daños a los dispositivos de la red. Para lograr una seguridad eficiente se necesita identificar y analizar una serie de vulnerabilidades y amenazas que las SG, están expuestas tanto en la arquitectura, los protocolos, la encriptación y los dispositivos que son utilizados en una red de SM e incluso en el factor humano de las organizaciones. En el ámbito de las TICs se conoce que ningún método o proceso es totalmente seguro, todo sistema cuenta con diferentes tipos de vulnerabilidades las cuales se tienen que identificar y tratar de evitar que se convierta en un peligro latente para los sistemas o tratar de mitigar su impacto de llegar a suceder, como por ejemplo una vulnerabilidad que se presenta en el protocolo ZigBee utilizado en las redes inteligentes ((Alliance, 2015)) es que este utiliza la encriptación simétrica AES-128, a pesar de ser un método de cifrado muy conocido y respaldado, al ser simétrico este trabaja mediante una clave tanto para el proceso de encriptación como para el proceso de des encriptación, el cual ((Alliance, 2015)), propone implementar cifrado asimétrico, ya que este método utiliza dos claves para los procesos de cifrar y descifrar, y se considera una medida válida para adoptar en las redes inteligentes con el fin de asegurar al máximo la red porque entre mayor seguridad tenga una red y se puedan reducir la amenazas que la envuelven, más eficientes van a ser y generará mayor confianza entre proveedor y el consumidor. Hoy en día alrededor del mundo se está dando una situación de suma importancia en cuanto al avance de las tecnologías, por el hecho que van avanzando muy rápidamente pero no así la seguridad ((nCircle, 2014)) y los controles que

se deben tener para las mismas, el hecho es que eso trae muchos riesgos, ya que al adquirir tecnologías nuevas e instalarlas sin los debidos estándares mínimos de seguridad puede traer muchas complicaciones a corto, mediano o largo plazo como lo son la suplantación de identidad, el quedar abiertos o expuestos a la manipulación y el espionaje de datos por ciberdelicuentes y otras cosas a las que se podría quedar vulnerable al usar tecnologías poco maduras en cuanto a seguridad se refiera, es tan serio este asunto que se están financiando proyectos en busca de seguridad alrededor del mundo como "El proyecto Avud", financiado por la Oficina de Suministro de Electricidad y Fiabilidad Energética del Departamento de Energía de los Estados Unidos, quienes están facilitando económicamente la posibilidad de desarrollo de un sistema para la detección de vulnerabilidad de la seguridad cibernética en los componentes de SG ((Sensus, 2010)). Se analiza una posibilidad, que en un país de escasos recursos como Costa Rica, se debería implementar este tipo de tecnologías, pero cuando existan ya los debidos avances probados y garantizados en los países de mayor recurso como lo es Estados Unidos, quienes dan la debida importancia al este asunto que incluso el mismo gobierno está financiando proyectos como el anteriormente mencionado, por ello es un gran riesgo implementar este tipo de tecnologías sin los debidos estándares de seguridad ya que en lugar de hacer un bien podrían estar abriendo puertas a catástrofes lamentables en cuanto a la ciberdelincuencia se refiere, según pruebas hechas en el reino unido y partes de Europa un ciberdelicuente que hackee un SM puede inclusive dar un apagado remoto a todo un hogar lo cual podría traer serias lamentaciones a una familia, ya que luego de un apagón podrían venirse los asaltos a dichas viviendas , es por ello que salen comentarios en investigaciones académicas como la de este investigador Kris Sangani el cual proyecta esta incógnita: "¿Ahorraremos en el costo de la energía excelente, pero vamos a pagar con nuestra pérdida de privacidad?,y se le podría inclusive agregar aun más con nuestra propia seguridad ((Sangani, 2010))." El asunto con las SM es que por sus ventajas como la de tener un mejor control de los gastos en electricidad, hasta el de poder controlar toda una vivienda por medio de estas tecnologías, esta tan de moda que inclusive el gigante google creo una app para el uso de SM mediante SG llamada PowerMeter la cual brinda información de consumo de energía a los usuarios con casas inteligentes y sugerencias de ahorro pero para tener este tipo de software los interesados deben como en casi todo programa descargable, facilitar algunos datos de usuario a la compañía lo cual a nuestro criterio es una gran vulnerabilidad ya que se sabe que hay muchos hackers que suben este tipo de programas en páginas web de descargas no oficiales modificados con virus, keyloggers, otros para poder robar la información de los que lo descarguen, lo cual pone sin duda alguna en entredicho la privacidad y seguridad reales de un usuario con tecnologías SM en redes SG((Sangani, 2010)). Las cuestiones de seguridad en general provienen de los ataques, los cuales pueden ser clasificados como ataques externos y ataques internos. Los ataques externos generalmente ocurren en el proceso de transmisión de datos entre el SM y el sistema central y los ataques externos se pueden dividir en dos categorías ((VV, 2009)): los ataques pasivos y ataques activos. Los ataques pasivos implican el

monitoreo del tráfico en la red con el fin de capturar claves, contraseñas u otros datos con información importante que se envía por medio del SM lo cual viene siendo espionaje el cual es generado por un hacker o un individuo curioso que trata de obtener información privada por distintos motivos o el solo hecho de hacerlo por diversión o retos de intelectualidad, los ataques activos vienen siendo un tipo de tergiversación de los datos, el robo o la pérdida de los mismos. Es decir un atacante puede manipular la información que un SM envía con objetivo de beneficiarse u manipular la información para engañar, los ataques internos implican: robar la información de datos realizada en el SM desde su casa o las afueras de la misma por el atacante a través de la captura de datos salientes o entrantes del SM, de esta manera, el atacante podría obtener la privacidad del usuario legal, suplantarla y aprovecharse violar el derecho del usuario legal, como pretendiendo ser el dueño para fines ilegítimos como manipular la información de datos a su conveniencia tales como la cantidad eléctrica generada, recargarla a su favor, u obtener informacion valiosa para un futuro ataque a las SG.

Existen una gran diversidad de sistemas de anonimato, encriptación, cifrados, antivirus, firewall, otros, ((Kangude, 2011)), ((Barukab, 2012)), ((Hui Shi1, 2014)), ((B Fouladi, 2014)), ((Saputro, 2014)), ((Chim, 2015)), pero al ser las tecnologías de los SM tan nuevas en el mercado todavía existen muchas brechas al respecto y de cuál es la mejor solución contra la cantidad de vulnerabilidades que existen como las maneras de llegar a la mejor forma de vivir en un mundo totalmente informatizado que se ha generado con el internet de las cosas y su gran auge e incremento visto en estos últimos años ((DYNA, 2014)) en las SG y SM, ya hemos nombrado en este documento y nos parece que la mejor forma para contrarrestar las vulnerabilidades no depende solo de que sistema de protección se pueda acceder o utilizar, sino también es de suma importancia de la manera en que se manejen los procesos con los SM desde su propio inicio (creación e instalación), la puesta en marcha hasta la verificación constante del tipo de manipulación de los datos que viajen a través de las SG, se deben dar capacitaciones sobre seguridad y riesgos a los clientes que adquieran estas tecnologías ya que de nada valdría tener las mejores herramientas de seguridad en los SM si los clientes caen ignorantes ante cualquier tipo de estafa u ataque informático, proporcionando datos o claves como se logra ver a menudo hoy en día que personas sin conocimientos son estafados por su ignorancia y desconocimiento obviamente con esto no se pretende asustar a las personas, ni marginarlas pero si de hacer conciencia tanto a los clientes como al I.C.E en este caso de que las personas con este tipo de tecnologías puedan obtener una visión clara de que es lo que están adquiriendo y de los riesgos que conlleva no estar capacitados para manejarla adecuadamente((L?pez Jim?nez, 2011)), ese es uno de los puntos más importantes para darle una solución al problema central de este análisis además de que el I.C.E firme una clausula con los clientes de contrato de responsabilidades, les pueda brindar una adecuada capacitación a las personas que contraten los servicios de SM y también brindarles seguimiento y la posibilidad de evacuar dudas ya sea por medio de call center, en línea e inclusive en caso de pérdida u olvido de alguna contraseña, que el cliente este en

la capacidad de poder reportarlo y se le solucione de inmediato, como se hace en la actualidad al perder un celular inteligente que lo bloquean apenas se reporta perdido u robado. Según un artículo publicado el periódico el Economista, en su sección de tecnología exponen un estudio realizado por dos especialistas en seguridad en España donde se pudo identificar una seria vulnerabilidad en la seguridad de los medidores inteligentes, los especialistas Javier Vázquez y Alberto García Illera identificaron un código defectuoso en los chips de memoria reprogramable que permite que piratas informáticos puedan cambiar datos de los SM, desconectar la energía de un hogar a distancia o hasta insertar gusanos en la red que podría desencadenar un apagón generalizado en toda la infraestructura de SG por medio de los SM. "Puedes simplemente quitar el hardware e inyectar lo que quieras" ((Illera, 2014)), dijo Vázquez, refiriéndose al riesgo de que los piratas informáticos pueden infiltrar software malicioso en uno de los sistemas y como consecuencia lo usen para controlar los medidores más cercanos, y de ese modo atacar a través de toda la red. Esta falla identificada es de suma importancia debido a que si un pirata logra identificar la vulnerabilidad en el código defectuoso de los chips que poseen los SM, podrían manipular los consumos de los hogares a su gusto provocando pérdidas millonarias a la empresa proveedora de energía lo que lleva a la pregunta ¿Qué tan segura es la medición inteligente? Su repuesta no la sabemos ya que son muchas las interrogantes que tenemos acerca de la medición inteligente pero durante el desarrollo de este articulo iremos aclarando. En la investigación desarrollada por los especialistas en seguridad aclararon que la falla en la seguridad solo se da en los dispositivos de un fabricante determinado. Vázquez Vidal cree que la empresa podrá solucionar el problema a distancia, sin tener que reparar individualmente cada terminal. Según la conferencia de hacking Black Hat Europe que se celebró en el 2014 en Ámsterdam a la cual asistieron los dos investigadores Illera dijo, "No vamos a difundir detalles concretos, no vamos a decir cómo lo hicimos", "Hay que arreglar este problema". Los investigadores se abstuvieron en brindar detalles en como lograron vulnerar la seguridad de los SM y mucho menos brindar detalles del dispositivo que presenta la falla para evitar que piratas intentaran vulnerar la seguridad de los dispositivos que presentan la falla. El hackeo a los dispositivos de medición inteligente se realizó superando la encriptación que utiliza el dispositivo para asegurar la comunicación debido a que los medidores utilizan claves simétricas relativamente fáciles de piratear, con códigos AES-128, según comentaban Vázquez e Illera " una vez superada esta barrera pudimos tomar el control total de la caja, cambiar su ID única para hacerse pasar por otros dispositivos o convertir el medidor en un arma con la que lanzar ataques contra la red eléctrica." Esta situación deja mucho que hablar sobre qué tan segura es la medición inteligente, porque múltiples investigaciones y pruebas en laboratorio han revelado que estos dispositivos presentan fallas en su seguridad que podrían desencadenar serios problemas tanto a sus usuarios como a las empresas energéticas y aún más grave se podría desencadenar un ataque mundial en la infraestructura de estos dispositivos que causaría un corte de energía por parte de un pirata informático que tiene el control de estos aparatos inteligentes . El

artículo “Introduction to NISTIR 7628 Guidelines for Smart Grid Cyber Security ((N. varios, 2015))”, mencionan grandes vulnerabilidades que se presentan en las SG: Privacidad personal: este tipo de tecnología deje vulnerable la información de los usuarios, ya que información como los tipos de dispositivos, cuando está o no en la casa o no, cuando hace uso de algún electrodoméstico, entre otros. Todo este tipo de información es considerado como personal según el HIPAA (Health Information Privacy) según ((H. varios, 2015)). Toda la información de los suscriptores debe de ser aprobada por ellos mismos. Vulnerabilidades que se presentan en la operación de la red eléctrica: por medio de manipulación de los dispositivos, alterando los dispositivos afectando las lecturas. Administración de string: la transferencia de datos en la red. Ataques DoS : solución autenticación de accesos para el control de acceso en las redes de acceso AMI garantizando que el acceso a la HAN es es solo de entidades autenticados y autorizados. Pero este tipo de Control es un desafío en una topología de Malla debido a su gran dimensión y variedad de configuraciones que se pueden presentar. Menciona los modelos de confianza hob by hob y end to end otra vulnerabilidad es la de regular que sistema puede acceder o hablar con otro sistema, se deben de considerar actualizaciones de firmware, como puede afectar este simple proceso el rendimiento de la red. Procedimientos de análisis de tráfico. Para analizar la frecuencia, el tamaño del mensaje, menciona herramientas de análisis como lo son: Herramienta de análisis GoodFET : es un hardware que permite la depuración de numerosas plataformas / chipsets, se centró principalmente en la previsibilidad del poder-glitching a los mecanismos de seguridad de hardware de derivación. Herramienta KillerBee-ZigBee®analysis: permite la captura y análisis de ZigBee® en la red y la interacción respectiva con los dispositivos. ((G. varios, 2014)).

3 Resultados

Se está de acuerdo con lo beneficioso de sustituir las lecturas manuales de consumo de los medidores convencionales para automatizarlos por medio de los SM, sus protocolos y redes pero de acá surge la incógnita de la cual nace la necesidad de la investigación, la infraestructura de redes de nuestro país, está capacitada para soportar el traslado de los datos en tiempo real y con la seguridad adecuada, ya que para dar un ejemplo de seguridad, encriptar datos con el tipo de encriptación homomórfica a menudo la misma para proporcionar estadística, valores como la suma, promedio y varianza tiende a aumentar el tamaño de los datos de texto cifrado y es computacionalmente caro en comparación con el cifrado tradicional eso sin contar que para mayor seguridad en caso de ataques no solo con una encriptación seria eficiente ya que la ciberdelincuencia también avanza cada día((varios autores, 2014)). entonces se podría dar una combinación de la encriptación homomórfica junto con encriptación por nodos hop by hop haciendo una mezcla de ambas para mayor seguridad de los datos, lo que conlleva a la necesidad de redes de alta velocidad exclusivamente para las SG por ello se pone en duda la estabilidad de la infraestructura de redes en el

país donde constantemente se leen noticias de fallos lo que podría perjudicar la estabilidad de la información generada por los SM, un ejemplo de la diferencia de velocidades necesarias de internet para el traslado de los datos sin cifrado y con cifrados se aprecia en la gráfica g-1. Según datos recopilados de((Saputro, 2014)), ((Madrigal, 2013)).

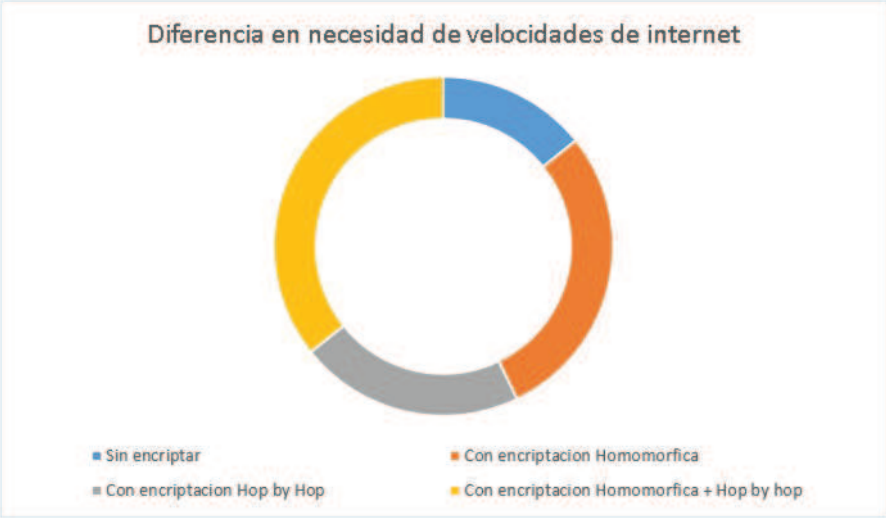

Fig. 4. Gráfico de aumento en necesidades de velocidad en internet para trasladar datos

Gráfica g-1 En la gráfica g1 se pueden apreciar las diferencias en las necesidades o requerimientos de velocidades de internet, ya que los datos con encriptación hop by hop requerirían un 7 por ciento más de velocidad de internet que si no tuviera ninguna, con encriptación homomórfica se requeriría un 15por ciento más de velocidad de internet que sin ninguna encriptación y con ambos tipos de encriptación hop by hop y homomórfica se requeriría un 22 por ciento más de velocidades para funcionar adecuadamente. Se dice que uno de los beneficios de Z-Wave darle el poder al cliente para que pueda desde su propio teléfono celular, computadora o Tablet controlar su casa. Eso está muy bien pero y la seguridad, que pasa si te roban las claves de los dispositivos si te las hackean para tener acceso a tu casa terceras personas y peor aún que pasaría si te roban los dispositivos, son incógnitas que no quedan claras o no están contempladas dentro de la información que brindan en la casa matriz de Z-wave y de suma importancia ya que la perdida de algún dispositivo podría causar catástrofes para un cliente con dicha tecnología, porque delincuencia ya no necesitaría ni siquiera forzar puertas ni nada como se ha hecho hasta hoy sino con solo hackear las claves podrían enterarse de las horas en que no hay nadie en casa y hacer

sus fechorías sin necesidad de la fuerza sino por medio del control de un SM, además que se podrían duplicar las probabilidades de robo ya que se crea una puerta de acceso más de ser una víctima, de forma convencional físicamente, de forma cibernética o de ambas, se puede apreciar las diferencias en riesgo en la grafica g-2. ((alliance, 2015)).

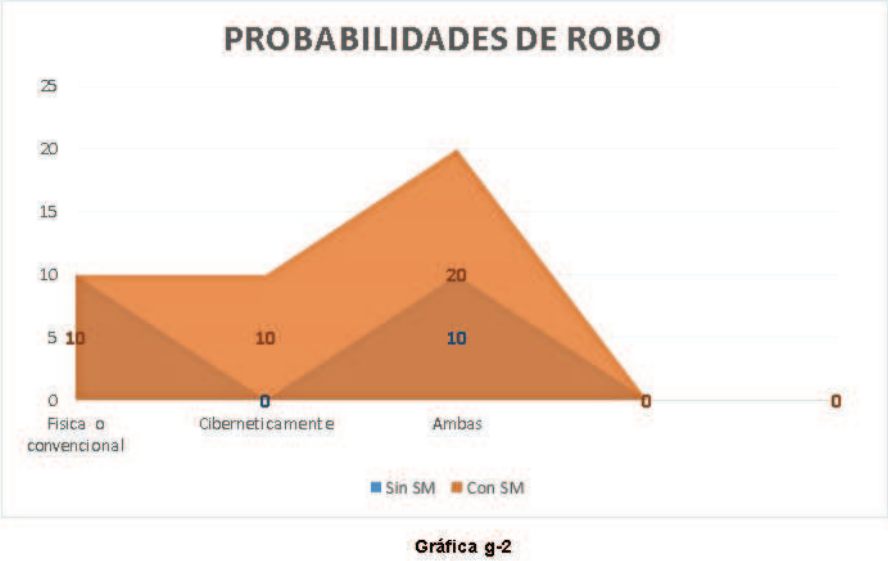

Fig. 5. Gráfico incremento en probabilidades de robo al tener SM

Gráfica g-2 En la gráfica g-2, se puede apreciar que en una casa tanto con SM como sin él, puede haber un 10 por ciento de probabilidades de robo físicamente ya que el medidor no tiene parte si un ladrón decide entrar a una casa de manera convencional , cibernéticamente es totalmente diferente ya que se puede dar un 10 por ciento de probabilidades de un delito informático en una casa con SM ya que viene figurando como una puerta o posibilidad más de ser atacada, pero disminuye totalmente a cero el riesgo de este tipo de robo en una casa sin SM; y como se puede apreciar en una casa con SM se tiene el doble de riesgo ya que podría ser robada de las dos maneras ósea se duplica el riesgo de un robo. Ya se sabe de las muchas vulnerabilidades en las redes y en este caso específico hablando de redes HAN que son las más comunes utilizadas para SG y en SM además de ser las utilizadas por el I.C.E con conexiones a casas inteligentes, el problema surge que todavía no hay una solución totalmente segura, ya que si por ejemplo se maneja la seguridad por medio de anonimato quien es el responsable de asignar claves robustas y fuertes y de estar cambiándolas cada cantidad de tiempo, además de qué manera se asegura no vayan a surgir confusiones y malestares en los clientes con poco conocimiento sobre la seguridad de internet

como adultos mayores en un hogar con este tipo de tecnologías, cabe pensar que todavía hay muchas incógnitas en cuanto a modus operandi de este tipo de tecnologías tan nuevas de estar en marcha y no solo en este país sino alrededor del mundo ya que estamos hablando de máximo una década de la puesta en marcha mundial de estas tecnologías y hasta hoy en día el acceso a ellas es la mínima población que las tiene ya que sus costos de implementación son muy altos, y por último que garantiza que dichas claves no puedan ser interceptadas por un hacker existen acuerdos de seguro de garantías que se pueden dar o crear para la tranquilidad de los clientes. Según datos recopilados de ((Chim, 2015)).

Resultado análisis Zigbee y Z-Wave: Estos protocolos han sido énfasis ya que son utilizados en los SM que implementa el I.C.E. por un lado ambos protocolos brindan una serie de ventajas en común y por otro lado también tienen algunas características que los diferencian uno del otro, como los tipos de cifrado, las frecuencias, latencia, cantidad de dispositivos soportados en la red y estándares, se determina según la información investigada de artículos sobre los SM y sus protocolos que dependiendo de las necesidades del cliente-proveedor y el tipo de red, así se escogerá que protocolo o tipo de red se implementara ya que a pesar que los dos protocolos cuentan con una serie de ventajas semejantes también estos como se menciona anteriormente cuentan con diferentes características que podrán ser explotadas dependiendo de las necesidades y el uso que se les quiera dar, por ejemplo Zigbee soporta una mayor cantidad de dispositivos en la red, aproximadamente (65.536), mientras que Z-wave es limitada en comparación de Zigbee al soportar una cantidad aproximada de (232) por lo tanto se podría decir que en caso de querer implementar un SM con una cantidad de dispositivos que sobre pase el límite los XX dispositivos el protocolo necesario para este tipo de red seria Zigbee. Un punto importante a considerar en las TICs son los estándares internacionales, y es importante porque ofrecen y recomiendan una serie de normas o guías asegurando un correcto y seguro funcionamiento en las tecnologías de la información ya que estos rigen el mejor camino o la mejor forma de avanzar en la tecnología, además se mantiene en constante actualización y revisión por lo que la aplicación de estos garantiza eficiencia y calidad en las TICs, por esto es que Zigbee tiene una gran ventaja en comparación de Z-wave ya que es respaldado por IEEE802.15.4, mientras que Z-wave no cuenta con el respaldo de un estándar internacional solo con el apoyo de Z-wave Alliance. Este estándar de IEEE es el estándar de base de Zigbee y cuenta con características; soporte para dispositivos de latencia críticos, como palancas de mando, CSMA-CA de acceso al canal, la administración de energía para asegurar un bajo consumo energético según ((Group4, 2015)).

Los ataques que han sufrido los SM por los hackers han sido por medio del virus Stuxnet, creado por los estados unidos e Israel con el fin de poder detener el proyecto nuclear de los iranis. Es un ataque fácil de implementar ya que por medio de algún dispositivo de almacenamiento (CD-ROM, Disco Externo). Este tipo de código lo que hace en el equipo es el de almacenar los procesos q se ejecutan y cuando se considere necesario atacar se activa para interrumpir los procesos. Ataques similares pueden afectar los SM, según la empresa Symantec

Fig. 6. Ilustracion Zigbee / Z-wave

ellos tienen detectado este tipo de virus pero un simple cambio en el código que no se tenga identificado puede crear un caos en la red ((Symantec, 2013)).

Problemas en la lectura de dispositivos debido a problemas en tarjeta Sim, un caso de eso lo reporta le empresa British Gas que reporta que el problema se presenta en 1 por ciento del total de los dispositivos instalados ((Gas, 2015)).

Como se puede observar en el siguiente gráfico existen múltiples factores que pueden afectar la correcta implementación de los SM en nuestro país, uno de los factores más importantes con un 40 por ciento es la infraestructura obsoleta del tendido eléctrico con la que cuenta el país , Costa Rica cuenta con una infraestructura eléctrica y de telecomunicaciones que ya cumplió su vida útil lo que provocaría que afecte el correcto funcionamiento de los SM debido a la sobre carga en muchos puntos del territorio nacional, como lo son el gran área metropolitana (GAM) , Heredia y ciertos sectores de Alajuela , a esta situación debemos de sumarle las interferencias electromagnéticas (EMPs) por el funcionamiento de múltiples sistemas de transmisión de datos que operan en estos sectores, otro de los factores de suma importancia con un 30 por ciento es la falta de políticas para la implementación de los SM, nuestro país aún se encuentra en un proceso de prueba en lo referido a medición inteligente por lo que no se cuenta con mucha legislación acerca del tema, no existen políticas sobre el uso de los SM en los hogares, su correcta instalación y medidas de seguridad física que se deben considerar para la instalación de estos dispositivos. Con un 20 por ciento se encuentran las condiciones ambientales, nuestro país por su ubicación geográfica presenta altos índices de humedad que podrían afectar el funcionamiento de los SM, otra condición a considerar es la cercanía que se tiene con el mar lo que provoca corrosión en los circuitos eléctricos y carcasas de los dispositivos de medición , en lugares como Limón, Puntarenas y Guanacaste es de suma importancia porque los niveles de corrosión son elevados provocando

serios problemas en el funcionamiento y daños constantes en estos dispositivos. Con un 10 por ciento se encuentra la geografía de nuestro país, Costa Rica es un territorio que cuenta con relieves como montañas, cordilleras y un amplio territorio boscoso que impediría la implementación de medidores inteligentes utilizando la tecnología Wireless para la transmisión de datos ya que la señal se vería reducida por tanta interferencia, aunque existen dispositivos con conexión cableada seria recargar aún más la infraestructura eléctrica y de telecomunicaciones de nuestro país provocando problemas más serios a la situación actual del país. Estos factores nos dejan ver que en nuestro país una implementación completa y adecuada de los SM es un tema un poco complicado, debido al abandono en que se encuentra la infraestructura eléctrica y de telecomunicaciones esto sumado a la ausencia de políticas de regulación y correcta implementación de los SM, lo que está provocando que la implementación completa de esta tecnología se verá retrasada hasta que se mejore las condiciones del país.

Fig. 7. factores de afectación

4 Conclusiones

Como parte de nuestro trabajo de investigación logramos determinar que la implementación de medición inteligente en nuestro país, será una herramienta muy importante, para que los ciudadanos puedan administrar de mejor manera el consumo de electricidad en sus hogares; así como para la empresa proveedora

la cual lograra tener mayor control de sus operaciones en este caso el ICE empresa pionera, pero la puerta está abierta para que se pueda implementar por otras instituciones o cooperativas enfocadas en la venta energética, además es un gran beneficio para disminuir el impacto de CO2 en el medio ambiente debido a que permite que usuarios puedan generar electricidad de sus hogares mediante paneles solares, pequeñas represas hidroeléctricas lo que disminuye la necesidad de generar electricidad con combustibles fósiles por parte del proveedor, al utilizar esta tecnología de medición inteligente ofrece la capacidad de inyectar los kilovatios que no utiliza el cliente a la red nacional de electricidad obteniendo una retribución económica por parte del proveedor de electricidad. Se debe de tener en cuenta que es de suma importancia el poder capacitar a cada uno de los usuarios para evitar escenarios donde se presenten vulnerabilidades que puedan afectar el desempeño de esta tecnología así como para minimizar el número de víctimas que pueden ser afectadas por un ataque indeseado así como el poner en riesgo la integridad y seguridad de la empresa proveedora.

El país debería además crear políticas y estándares de uso e instalación de estos dispositivos de medición inteligentes que permita reducir el impacto a sufrir ataques volviéndolos más seguros, ya que según lo investigado muchas de las vulnerabilidades que sufren estos aparatos son por su mala instalación y exposición a factores climáticos. Nuestro país actualmente no cuenta con una regulación seria en materia de medición inteligente lo que ha frenado un poco la implementación adecuada de estos dispositivos, actualmente el ICE ha instalado SM en ciertos hogares e industrias pero solo con la función de medición de consumo periódico de electricidad del cliente dejando rezagadas muchas de las funcionalidades que permiten implementar estos dispositivos. Se concuerda que por más que se programen nuevos sistemas o medios de seguridad, siempre van a existir hackers que podrán quebrar estas seguridades y se ha demostrado a través de los años, ya sea por diversión para hacer daño o simplemente para subir el ego propio, ya que como dijimos en este documento no hay redes cien por ciento seguras, obviamente con las herramientas existentes mencionadas en este artículo se puede hacer muy complicado para un ciberdelicuente que quiera pasar por alto la seguridad en los SM, pero de igual forma si uno o varios hackers se empeñan en quebrar una seguridad con el tiempo lo harán, ya que sus herramientas se perfeccionan al mismo ritmo que las herramientas de seguridad, uno de los métodos más eficientes para controlar los accesos ilegales es el monitoreo constantemente de las HAN y las SG, chequear el estado de las conexiones, tener certeza del conocimiento en seguridad de los propietarios de estos tipos de SM y brindarles herramientas y capacitaciones de que deben hacer en caso de hallazgo de hackers o intentos de acceso de terceros a su SM y estar al día de los nuevos métodos que usan los hackers para romper estas vulnerabilidades en los SM y en todas las SG para lograr crear una red segura e integra tanto para la empresa proveedora como para el consumidor final y que se pueda brindar un servicio de alta calidad.

Recomendaciones para usuarios finales

Como se ha mencionado, el sistema de SM, se va a estudiar del medidor a la casa, por lo cual es de suma importancia que la empresa proveedora del servicio enseñe a los sus suscriptores a ser usuarios inteligentes capaces de poder identificar una amenaza y proteger su información por medio de las siguientes prácticas: 1- El dispositivo móvil sea celular, portátil, Tablet debe de contar con una contraseña segura: debe de contar con 12 dígitos, letras en mayúscula, minúscula, signos, números. 2- Cambiar la contraseña de manera periódica y nunca repetir contraseñas. 3- El dispositivo debe de bloquearse cada "5 segundos" con el fin de evitar que en algún descuido sea víctima de robo y de fácil acceso al a información. 4- Debe capturar la MAC de cada dispositivo y el IMEIC (Ambos son números únicos de los dispositivos) registrarlos con el proveedor de servicio, en caso de robo del mismo el suscriptor debe llamar y reportarlos para que el dispositivo móvil sea inhabilitado. 5- Se le debe de explicar al suscriptor que cada una de las descargas que realice en el dispositivo móvil debe de realizarlo de páginas seguras y de desarrolladores confiables. 6- Se le debe de indicar al usuario que en caso de recibir correos o mensajes de un destinatario desconocido debe de abstenerse de responder o abrir el archivo y debe de reportarlo al proveedor de servicio para que analice el origen del mismo. 7- Al momento de conectarse a una red pública debe de tomar medidas de seguridad para que no sea blanco fácil de un posible ataque al dispositivo móvil. Como por ejemplo: Man in the middle, malware. 8- En caso de necesitar realizar un chequeo podría hacer uso de una VPN para conectarse y realizar la conexión. 9- El suscriptor cada vez que realice la descarga de alguna aplicación debe de leer los permisos que necesita acceder la aplicación ya que pueden capturar información sensible para un futuro ataque.

10- La casa debe de contar con sistema de tierras para evitar picos que corriente que afecten el funcionamiento de los dispositivos, así como daños en el cableado de red o dispositivos inalámbricos.

References

Alliance, Z.-W. (2014). Estudio y desarrollo de un sistema basado en una librer?a abierta para el uso del protocolo inal?mbrico de dom?tica z-wave. *Web*. Retrieved from `http://hdl.handle.net/2099.1/22360` pages 6, 7

Alliance, Z.-W. (2015). Z-wave alliainfo general information. *Web*. Retrieved from `http://www.z-wavealliance.org/` pages 6

alliance, Z.-W. (2015). Z-wave beneficios. *Web*. Retrieved from `http://www.z-wave.com/z-wave_benefits` pages 14

Alliance, Z.-W. (2015). Z-wave technology comparation. *Web*. Retrieved from `http://z-wave.sigmadesigns.com/about_z-wave#technology_comparison` pages 8

Barukab, K. A. a. S. M. s. M. M. m. . K. S. s., O. o. (2012). Secure communication using symmetric and asymmetric cryptographic techniques.international journal of information engineering & electronic business. *4(1), 36-42*. pages 6, 7, 10

Bertol?n., J. A. (2011). Identificaci?n, an?lisis y evaluaci?n de la seguridad en las comunicaciones con tecnolog?a zigbee. *no definido*. pages 5

B Fouladi, S. G. (2014). Security evaluation of the z-wave wireless protocol. *research.sensepost.com*. pages 10

Chim, Y. S. L. V. O. H. L. C. . Z. J., T. W. (2015). Prga: Privacy-preserving recording & gateway-assisted authentication of power usage information for smart grid. *IEEE Transactions On Dependable & Secure Computing, 12(1), 85-97.*. pages 10, 15

DYNA. (2014). Internet de las cosas. - *Ingenier?a e Industria, 89(5), 478.*. pages 10

Gas, B. (2015). Why does it take so long to fix a smart meter that isn't transmitting readings? *British Gas*. Retrieved from `http://www.britishgas.co.uk/business/help-and-advice-business/meters-and-readings/technical-questions/Why-does-it-take-so-long-to-fix-a-smart-meter.html` pages 16

Group4, T. (2015). Ieee 802.15 wpan. *Web*. Retrieved from `http://www.ieee802.org/15/pub/TG4.html,2015` pages 15

Hui Shi1, J. L. h. Y. J. h. C. W. h. J. G. h. . Y. D. h., h. (2014). The new key-stream generator based on the ofb mode of aes. applied mechanics & materials,. *(644-650), 2768-2771.*. pages 5, 6, 10

Illera, J. V. . A. G. (2014). Los contadores inteligentes fallan en la seguridad: pueden ser hackeados. *elEconomista.es Leer m?s: Los contadores inteligentes fallan en la seguridad: pueden ser hackeados - /Los-contadores-inteligentes-carecen-de-seguridad-pueden-ser-hackeados.. elEconomista.es, p.1.*. Retrieved from `http://www.eleconomista.es/tecnologia/noticias/6140290/10/14` pages 11

Kangude, W. P. . R. S., N. (2011). Advanced encryption standard. international journal of computer science engineering & technology. *1(3), 118-126.*. pages 5, 10

Knight, M. (2006). How safe is z-wave? [wireless standards]. *Computing & Control Engineering 17(6), 18-23.*. pages 6

L?pez Jim?nez, d. (2011). Los c?digos de conducta como soluci?n id?nea frente a la elevada desprotecci?n de la privacidad en internet. (spanish). *Revista De Derecho Comunicaciones Y Nuevas Tecnolog?as, (5), 1-21*. pages 10

Madrigal, r. (2013). fallo del ice dej? sin internet a clientes de todo el pa?s. *Web*. Retrieved from `http://www.crhoy.com/fallo-en-el-ice-dejo-sin-internet-a-clientes-de-todo-el-pais/` pages 13

nCircle. (2014). Survey: Energy security pros believe smart meters vulnerable to false data injection. business wire (english). *Survey*. pages 8

Sangani, K. (2010). You're being monitored. *Engineering & Technology (17509637), 5(10), 28-29. doi:10.1049/et.2010.1003*. pages 9

Saputro, . A. K., N. (2014). On preserving user privacy in smart grid advanced metering infrastructure applications. *Security & Communication Networks, 7(1), 206-220*. pages 10, 13

Sensus. (2010). Sensus joins enernex and oak ridge national laboratory to heighten cyber security in smart meters with new function extraction (fx). *Technology for Vulnerability Detection. Business Wire (English)*.. pages 9

Symantec. (2013). Stuxnet 0.5: The missing link. *Web*. Retrieved from `http://www.symantec.com/connect/blogs/stuxnet-05-missing-link` pages 16

varios, G. (2014). Herramienta de an?lisis goodfet. *GoodFET Sitio web*. Retrieved from `http://goodfet.sourceforge.net/` pages 12

varios, H. (2015). Health information privacy. *HIPPA*. Retrieved from `http://www.hhs.gov/ocr/privacy/` pages 12

varios, N. (2015). Smart grid cybersecurity strategy, architecture, and high-level requirements. *NIST*. Retrieved from `http://csrc.nist.gov/publications/drafts/nistir-7628-r1/draft_nistir_7628_r1_vol2.pdf` pages 12

varios autores. (2014). El desafio de la privacidad en internet. *Web*. Retrieved from `http://www.eset-la.com/pdf/tendencias_2014_el_desafio_de_la_privacidad_en_internet.pdf` pages 12

VV, D. (2009). Wireless communication system for energy meter reading. *In: Proc. International Conference on Advances in Recent Technologies in Communication and Computing, pp. 896?898, 2009*. pages 9

Zhongmin LI1, M. S. s. . L. G. g., h. (2014). Design of smart home system based on zigbee. applied mechanics & materials. *(630-642), 1086-1089*. pages 5