VULNERABILIDAD EN LOS SISTEMAS DE MEDICIÓN INTELIGENTE

F. A. Elizalde Canales[a], I.J. Rivas Cambero[b], A.M. Godinez Jarillo[c], E. Cortes Palma[d]

Universidad Politécnica de Tulancingo
francisca.elizalde@upt.edu.mx[a], ivan.rivas@upt.edu.mx[b]
alicia.godinez@upt.edu.mx[c], elizabeth.cortes@upt.edu.mx[d]

RESUMEN

La red inteligente (Smart Grid) es una modernización de la red eléctrica, para supervisar, inspeccionar, proteger y optimizar automáticamente el control y la fiabilidad de las operaciones de la red eléctrica a través de sistemas de monitoreo y control distribuido. A la red inteligente se integran las de Tecnologías de Información y Comunicación (TIC) que permiten el monitoreo y control remoto, sin embargo, la integración expone a los sistemas de energía inteligentes a las amenazas de seguridad y vulnerabilidad, que podrían verse comprometidos por usuarios maliciosos y atacantes, debido al aumento de la conectividad y la apertura de Internet.

En este trabajo se realiza un análisis de los requisitos de seguridad, amenazas y vulnerabilidades en los sistemas de medición inteligente para que facilite la comprensión y visualización de los principales riesgos cibernéticos a fin de que fortalezca la seguridad y establezca contramedidas. El caso específico que se aborda en este artículo es el de los medidores inteligentes (Smart Meter), los que se encargan de registrar la información de cada consumidor para que sea recolectada y procesada para el cálculo de la factura de consumo, sin embargo esta información puede ser usada con fines diferentes.

La finalidad de este artículo es que se comprenda cómo los atacantes maliciosos pueden comprometer la seguridad de los sistemas de medición inteligente refiriendo ataques sofisticados y vulnerabilidades así como su impacto.

1. INTRODUCCIÓN

Uno de los principales objetivos de la red inteligente es que los usuarios finales tengan información sobre sus consumos y dispongan de herramientas que favorezcan el control eficiente de sus cargas, generando así eficiencia energética [1].

Las comunicaciones para las aplicaciones de redes inteligentes manejan datos sensibles, la seguridad física como la seguridad cibernética y la privacidad constituyen factores clave para su amplio despliegue y adopción. Para determinar las vulnerabilidades dentro de estas aplicaciones se examina la metodología de ataque, debido a que los métodos exactos pueden variar. La

comprensión de los motivos del atacante y las vulnerabilidades inherentes de los sistemas ayudan a determinar cómo podría acercarse un atacante, evaluar y romper la seguridad de un sistema.

Por su parte la función principal de los medidores inteligentes comprende: la lectura remota de la energía consumida mejorando la gestión operativa de los proveedores y facilitando la comprensión del consumidor de energía y costo, permitiendo la inhabilitación del suministro de energía en casos de emergencia, la detección de fugas de energía o fraude y finalmente el apoyo a los métodos de pago (prepago).

En este documento se presenta el ámbito de utilización de los medidores de energía actuales en el entorno de la red eléctrica inteligente, a través de una revisión de la literatura sobre vulnerabilidades detectadas en los sistemas de medición, y se muestran los principales riesgos cibernéticos, revisando una serie de propuestas que permitan fortalecer la integridad, disponibilidad y confidencialidad de los datos involucrados estableciendo contramedidas.

2. ANTECEDENTES

Los consumidores buscan la mejor prestación del servicio de energía eléctrica, que se representa en la calidad de la energía, en mediciones exactas y en precios razonables, por ello las empresas proveedoras de este servicio se ven obligadas a modernizar el sistema de medición, adaptándose a las nuevas condiciones del mercado y brindando una información más detallada sobre el consumo de cada cliente [2]. Una de estas alternativas que ha tomado auge en los últimos años es la denominada “medición inteligente”. Concepto que nace a partir de la búsqueda de la optimización de los procesos de medición, lectura del medidor y facturación, principalmente con el fin de contribuir a los objetivos mundiales de eficiencia energética de reducir el impacto climático generado por emisiones de gases de efecto invernadero y de satisfacer en general las necesidades de una “red inteligente” o Smart Grid.

La red inteligente requiere de información en tiempo real, por lo que necesita una nueva forma de medir denominada Smart Metering o “medición inteligente”, refiriendo a un multiproceso simultáneo que incluye: medición, registro, almacenamiento y transferencia bidireccional de información en tiempo real (o cercano), de las cantidades de energía consumida junto con otras variables útiles para la gestión de la red. Mediante la “medición inteligente” se mantiene informado al consumidor para que pueda proponer sus propias políticas de consumo, según lo considere [3].

Existen diferentes funciones de los medidores inteligentes, dentro de las cuales destacan:

- *Control de robo de energía eléctrica*: Algunos medidores pueden detectar la manipulación del medidor, detectando situaciones anormales como el no registro del consumo de energía por un período de 24 horas.
- *Registro y almacenamiento de datos*: En general, los medidores tienen la capacidad de registrar y almacenar datos de perfiles de carga, eventos como perturbaciones, caídas y elevaciones de tensión, cortes y suministros del servicio, etc.
- *Control de electrodomésticos inteligentes*: Algunos medidores inteligentes pueden reducir el tiempo de utilización de electrodomésticos inteligentes.

El sistema de medición es una infraestructura que integra una serie de tecnologías para lograr sus objetivos. Incluye medidores inteligentes, redes de comunicación en los diferentes niveles de la jerarquía de la infraestructura, sistemas de gestión de datos de medición, y los medios para la integración de los datos recogidos en las plataformas e interfaces de aplicaciones de software [4].

Los medidores inteligentes tienen dos tareas específicas: medición y comunicación, y por lo tanto cada medidor tiene dos subsistemas: metrología y comunicación. La parte de metrología varía dependiendo de un número de factores que incluyen región, fenómeno medido, precisión requerida, el nivel de seguridad de los datos, la aplicación. El método de comunicación también hay factores como la seguridad y encriptación [5].

Como el número de medidores inteligentes aumentan exponencialmente, los problemas de seguridad asociados con la red inteligente y el sistema de medición crecen sustancialmente desde dentro y fuera del sistema. La información detallada del consumo de los clientes es fundamental, ya que puede revelar su estilo de vida. La transmisión de datos a larga distancia, así como el almacenamiento de los datos en varios lugares para la retransmisión o análisis también puede crear vulnerabilidades en términos de robo de datos o la manipulación de estos. La señal de precio y comandos recibidos por los consumidores también son áreas potenciales para ciberataque con el objeto de espionaje, dañando la infraestructura o el robo de energía.

Al analizar los datos de los medidores inteligentes, es posible llevar a cabo un "perfil del consumidor" con una precisión alarmante. Los ejemplos van desde cuántas personas viven en la casa, tipo de dispositivos utilizados, la seguridad y los sistemas de alarmas, el comportamiento de los residentes, incluso sin la utilización de sofisticados algoritmos y herramientas asistidas por computadora[6] ya que es posible identificar el uso de los electrodomésticos en una casa, mediante el análisis de sólo unos 15 minutos de datos de consumo energético acumulado, y una vez que se tenga acceso a los datos de la red en el sistema de medición, también se tendrá acceso a la información de nombre y dirección del cliente, recogida y almacenada para fines de facturación.

Aunque la obtención de información detallada es uno de los objetivos de las redes inteligentes, el proceso puede ser contraproducente cuando se recoge y utiliza sin el consentimiento de los clientes. La importancia de la privacidad será más clara si se tiene en cuenta el número de hogares cubiertos por la infraestructura de medición, actual y futura. Debido a que cada dispositivo tiene diferentes comportamientos medibles desde el punto de vista del consumo, hay un atributo único o "firma" en cada comportamiento de consumo de dispositivo eléctrico que podría medirse.

Los ataques contra sistemas de medición deben ser estudiados desde la perspectiva de los atacantes y sus motivaciones que puede ser por intereses propios, fines de sabotaje o terrorismo. Categorizar a los atacantes y su motivación es especialmente importante cuando se trata de diseñar contramedidas; considerando que los atacantes con suficientes recursos y nivel de experiencia tienen poca motivación para cometer robo de energía, sin embargo pueden utilizar las vulnerabilidades de los medidores inteligentes para la denegación de servicio o invasión de la privacidad.

En otro escenario, los datos podrían ser alterados mientras se transfiere a través de la red. Esto comprende de inyectar datos falsos en el sistema, o interceptación de las comunicaciones dentro de la infraestructura.

Algunos ejemplos de estos ataques se listan a continuación:

- EE.UU. (2010) Tom Donah de la CIA, intrusiones en compañías de suministro de energía eléctrica ocasionan cortes de suministro en varias ciudades.
- Reino Unido (2011) se obtienen de manera fraudulenta millones de libras, mediante claves de recarga pirateadas en medidores de prepago.
- Termineter (2012), programa que permite modificar el software o cambiar la tarifa de factura de consumo.
- Investigadores españoles (2014), logran hackear un medidor inteligente de electricidad a través de la reingeniería, provocando cortes en el suministro y suplantar la identidad de del usuario.

Con el fin de disminuir estos ataques se establecen medidas de seguridad al analizar las iniciativas existentes y estándares de seguridad en las redes inteligentes, las arquitecturas de seguridad en el ámbito de la red inteligente, los protocolos de red y elementos de red inteligentes y las herramientas de seguridad para el análisis de protocolos de red desde los medidores inteligentes hacia el primer nodo conocido como Acces Poin (WAP).

3. CIFRADO DE FLUJO DE DATOS

El Sistema de Medición es una infraestructura que integra una serie de tecnologías para lograr sus objetivos de medición que incluye medidores inteligentes, redes de comunicación en los diferentes niveles de la jerarquía de la infraestructura, sistemas de gestión de datos de medición, y los medios para la integración de los datos recogidos en las plataformas e interfaces de aplicaciones de software [7]. El cliente está equipado con un dispositivo medidor que recoge los datos basados en el tiempo y puede transmitir los datos recogidos a través de redes fijas comúnmente, así como las redes públicas tales como teléfono fijo o celular. Los datos de consumo medidos son recibidos por el sistema host. Posteriormente, se envía a un sistema que gestiona el almacenamiento y análisis de datos y proporciona la información en una forma útil para el proveedor.

La investigación de vulnerabilidades y módulo de verificación tiene como objetivo identificar las vulnerabilidades en los servicios de trasmisión de los datos basado en la metodología SQUARE *(Security Quality Requirements Engineering)* para la obtención, análisis, clasificación y priorización de los requisitos de seguridad [8].

La metodología esta compuesta de 9 pasos, cada uno describe su finalidad:

Paso 1: Definiciones. Entre los más importantes, vulnerabilidad se define como un punto débil en un sistema que puede ser explotada por amenaza de código y los resultados en incumplimiento o violación de la política de seguridad del sistema. Una amenaza se define como el potencial o la capacidad de la amenaza de código para explotar o ejercicio / desencadenar una vulnerabilidad.

Paso 2: Identificar los Objetivos de Seguridad. Confidencialidad, integridad, autenticación, autorización, control de acceso, la disponibilidad y el no repudio.

Paso 3: Diseños de la arquitectura.

Paso 4: Realizar la evaluación de riesgos. El riesgo se define como "una función de la probabilidad de que una amenaza de determinada fuente ejerza vulnerabilidad potencial en particular y el impacto resultante de ese acontecimiento adverso en la organización."

Paso 5: Técnicas de selección de requisitos.

Paso 6: Elección de requerimientos de seguridad.

Paso 7: Clasificar Requisitos bajo las siguientes categorías. Integridad, confidencialidad, autenticación, autorización, control de acceso, de rendición de cuentas (no repudio), y la disponibilidad.

Paso 8: Priorizar Requisitos. Se Priorizan los requisitos de seguridad: alta, mediana y baja.

Paso 9: Requisitos de Inspección. Se examinan los requisitos para garantizar la exactitud, la organización y la corrección.

Con ello permite deducir que la amenaza crea un ataque que explota una vulnerabilidad detectada en un dispositivo, generando un impacto (ver Figura 1), que puede ser desde un pequeño apagón hasta la interrupción total del suministro de energía eléctrica y provocar graves daños económicos o comprometer los datos que están siendo procesados, almacenados o trasmitidos por un medidor inteligente. Siempre existe un riesgo probable de que una amenaza se materialice utilizando las vulnerabilidades existentes en un dispositivo.

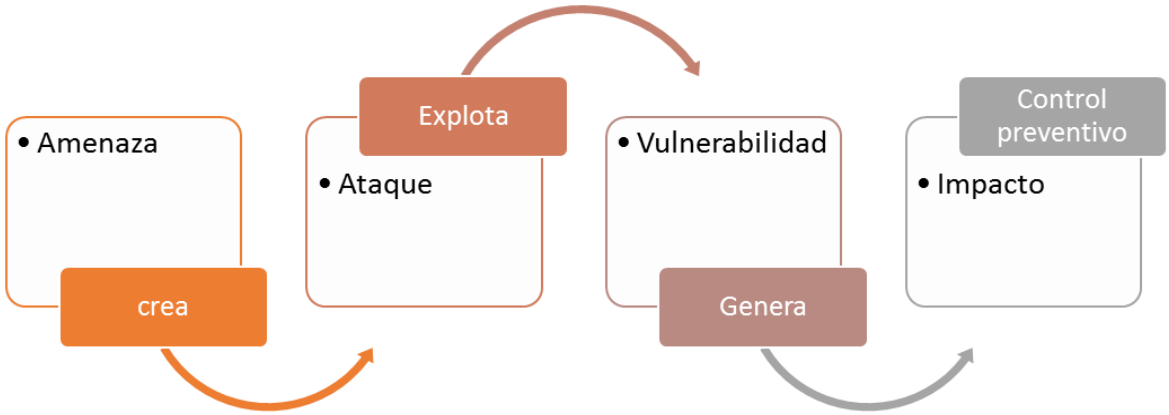

Figura 1. Esquema de análisis de riesgo.

Un propósito es atacar una de las vulnerabilidades propiciadas en el nodo inicial protegiendo tanto el acceso al sistema del dispositivo de medición como el fortalecimiento de la seguridad en la trasferencia de datos del dispositivo al primer nodo de conexión. Esto a través de medidas de seguridad eficaces que permitan mejorar la resistencia a ciberataques en los sistemas de medición y contribuir a mitigar este tipo de acciones.

Apoyado en la criptografía que desarrolla métodos de cifrado para proteger la información se propone crear un algoritmo de cifrado para el flujo de datos desde el dispositivo de medición o nodo inicial como puede apreciarse en la figura 2.

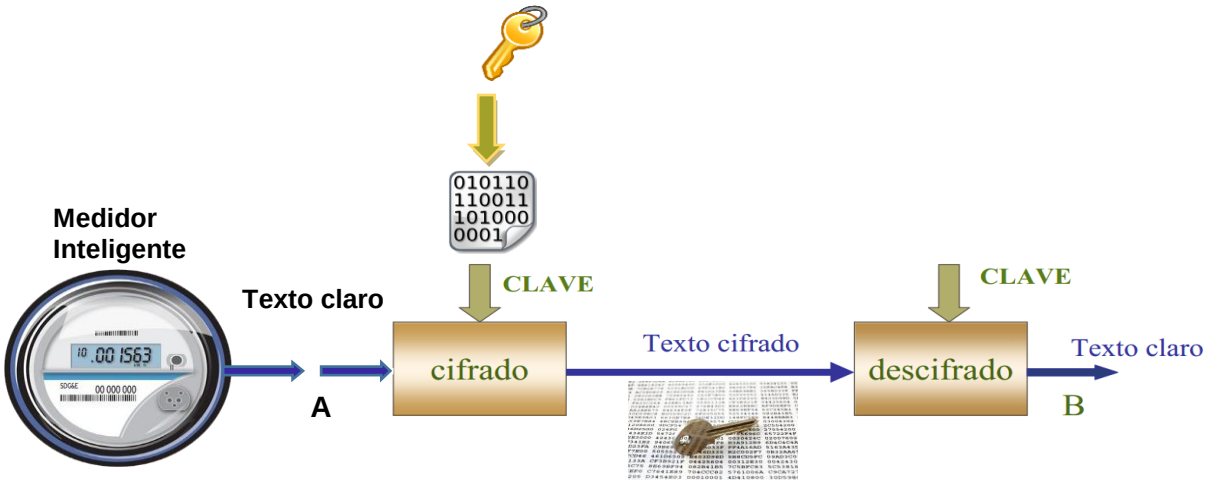

Figura 2. Cifrado de flujo de datos.

4. CONCLUSIONES

El mundo está experimentando una evolución derivada de las innovaciones en la tecnología de la información que, si bien se crean nuevas oportunidades económicas y sociales, plantean desafíos a nuestra seguridad y expectativas de privacidad. Medidores de energía inteligentes, dispositivos de seguridad y aparatos inteligentes están siendo utilizados en muchas ciudades, todo ello conducirá a mejoras sin precedentes en la calidad de vida y para beneficiarse de ellas, las infraestructuras y los servicios están cambiando con nuevos sistemas interconectados de seguimiento, control y automatización.

Los cambios traen consigo dos importantes desafíos: la seguridad y la privacidad. La seguridad incluye el acceso ilegal a la información y los ataques físicos causando interrupciones en la disponibilidad del servicio teniendo en cuenta que como ciudadanos digitales se está cada vez más equipados con datos disponibles acerca de ubicación y de las actividades que se realizan donde la privacidad tiende a desaparecer, proteger la privacidad de sistemas que recopilan datos es uno de los desafíos tecnológicos que van mano a mano con los retos de seguridad continua.

La medición inteligente es una herramienta que implementa una infraestructura que se ha materializado para llevar a cabo la adquisición de datos en tiempo real de los consumidores y transmitirlos. Los datos adquiridos pueden ser utilizados para la regulación del consumo, tanto de los consumidores, y como proveedores. La vulnerabilidad en los dispositivos de medición de energía eléctrica se debe a las características de seguridad débiles, a los protocolos de comunicación y sistemas operativos utilizados en los dispositivos que han sido diseñados para garantizar la calidad de conectividad, control y rendimiento, pero adolecen de seguridad. Garantizar la seguridad y privacidad de la información de los usuarios, requiere un análisis de riesgos potenciales de problemas de ciberseguridad en los sistemas de medición.

BIBLIOGRAFÍA

[1] H. Suleiman, I. Alqassem, A. Diabat, E. Arnautovic, D. Svetinovic (2014). Integrated smart grid systems security threat model. doi:10.1016/j.is.2014.12.002

[2] M. Lehtonen, A. Ortiz, et al. "Evaluation of Energy Meters' Accuracy Based on a Power Quality Test Platform," En: Electric Power Components and Systems, vol. 35, no. 2, pp. 221–237, Feb. 2007.

[3] C. Díaz, J. Hernandez, "Smart Grid : Las TICs y la modernización de las redes de energía eléctrica - Estado del Arte." En: Revista S&T, vol. 9, pp. 53–81, 2011.

[4] National Energy Technology Laboratory for the U.S. Department of Energy. Advanced metering infrastructure, NETL modern grid strategy; 2008.

[5] Silicon Laboratories, Inc. smart metering brings intelligence and connectivity to utilities, green energy and natural resource management. Rev.1.0. http://www.silabs.com/Support%20Documents/TechnicalDocs/Designing-Low-Power-Metering-Applications.pdf> [accessed August, 2013.

[6] Murrill BJ, Liu EC, Thompson II, RM. Smart Meter Data: Privacy and Cyber security. Congressional Research Service; 2012.

[7] National Energy Technology Laboratory for the U.S. Department of Energy. Advanced metering infrastructure, NETL modern grid strategy; 2008.

[8] H. Suleiman D. Svetinovic. Security Requirements Analysis of Smart Grid Advanced Metering Infrastructure: A Case Study Using the SQUARE Method," IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC 2012), Shanghai, China, March 2012.