Integrating Cybersecurity Measures into Smart Grid Design: Enhancing Resilience and Protecting Critical Infrastructure

Pablo Petrashin, PhD, Walter Lancioni, PhD, Agustin Laprovitta, PhD and Juan Castagnola, PhD
Laboratorio de microelectrónica, Universidad Católica de Córdoba, Cordoba, Argentina
ppetrashin@gmail.com, walter.lancioni@gmail.com, juanluiscastagnola@gmail.com, agustin.laprovitta@gmail.com

Summary – This article analyzes the implementation of a protocol for cybersecurity applied to the design of smart electrical networks (smart grids) and its impact on the resilience and protection of critical infrastructure. The topic is part of a home automation project, based at the Catholic University of Córdoba. For the first tests, a mini server called Micro_UCC has been implemented whose main task is to return web pages in response to HTTP GET requests directed to TCP port 80 in a conventional way. At the lowest level, the server responds to ARP requests, identifying itself as an active device on the network with a previously assigned fixed IP address. It also responds to ICMP echo requests, commonly called ping requests. The server could send and receive UDP packets, however, this project does not make use of this capability, leaving it for a future expansion.

Keywords-- Resilience; TCPIP; Integration; Intelligent networks

Integración de medidas de Ciberseguridad en el Diseño de Redes Inteligentes: Mejora de la Resiliencia y Protección de la Infraestructura Crítica

Pablo Petrashin, PhD, Walter Lancioni, PhD, Agustin Laprovitta, PhD and Juan Castagnola, PhD
Laboratorio de microelectrónica, Universidad Católica de Córdoba, Cordoba, Argentina
ppetrashin@gmail.com, walter.lancioni@gmail.com, juanluiscastagnola@gmail.com, agustin.laprovitta@gmail.com

Resumen– ***En este artículo se analiza la implementación de un protocolo para ciberseguridad aplicada al diseño de las redes eléctricas inteligentes (smart grids) y su impacto en la resiliencia y protección de la infraestructura crítica. El tema se enmarca en un proyecto de domótica, con sede en la Universidad Católica de Córdoba. Para las primeras pruebas, se ha realizado la implementación de un mini servidor denominado Micro_UCC cuya principal tarea es devolver páginas web ante requerimientos HTTP GET dirigidos al puerto 80 de TCP en una forma convencional. En el nivel mas bajo, el servidor responde a requerimientos ARP, identificándose como un dispositivo activo en la red con una dirección IP fija asignada previamente. También responde a requerimientos de eco ICMP, comúnmente llamado requerimiento ping. El servidor podría enviar y recibir paquetes UDP, sin embargo, este proyecto no hace uso de esta capacidad dejándola para una futura ampliación.***

Palabras clave-- Resiliencia; TCPIP; Integración; Redes Inteligentes.

I. Introducción

La integración de sistemas de energía eléctrica con tecnologías de información y comunicación ha dado lugar a las smart grids, que se caracterizan por su capacidad para recopilar, analizar y utilizar datos en tiempo real para optimizar la generación, transmisión y distribución de energía [1]. Sin embargo, esta convergencia también ha abierto nuevas puertas a posibles amenazas cibernéticas, como ataques maliciosos, intrusiones y robos de datos sensibles [2]. Estas amenazas pueden tener consecuencias devastadoras, incluyendo interrupciones en el suministro de energía, daños a la infraestructura crítica y riesgos para la seguridad pública [3, 4].

El estado del arte en el diseño de Smart Grids destaca la importancia de la comunicación, la seguridad cibernética y la integración de fuentes de energía renovable [5, 6]. Se han realizado avances significativos en estos campos para garantizar el rendimiento óptimo, la eficiencia y la confiabilidad de las redes eléctricas inteligentes [7].

En cuanto a la comunicación, se han identificado tecnologías y estándares clave para habilitar la transmisión eficiente de datos en tiempo real dentro de las Smart Grids. Esto incluye la adopción de protocolos de comunicación confiables y escalables, así como el desarrollo de infraestructuras de red robustas y seguras [8].

En términos de seguridad cibernética, se ha reconocido la importancia de proteger las Smart Grids contra amenazas y ataques maliciosos. Se han propuesto soluciones para garantizar la integridad, confidencialidad y disponibilidad de los datos y sistemas en entornos ciberfísicos complejos [9]. Esto involucra la autenticación de usuarios, el cifrado de datos, la detección y respuesta a intrusiones, y el diseño seguro desde el inicio.

La integración de fuentes de energía renovable es otro aspecto crucial en el diseño de Smart Grids. Se han realizado investigaciones para optimizar la generación, transmisión y distribución de energía a partir de fuentes como la solar y eólica. Además, se han explorado técnicas de gestión de demanda y respuesta para mejorar la eficiencia energética y la estabilidad del sistema [10]. También se ha prestado atención a la seguridad en aplicaciones específicas, como la salud electrónica, donde la confidencialidad y la privacidad son fundamentales para la protección de datos personales sensibles.

II. Protocolo de Ciberseguridad para Smart Grids Resilientes (CSGR)

En el contexto de la ciberseguridad, un Protocolo de Ciberseguridad para Smart Grids es un conjunto de medidas y prácticas diseñadas para salvaguardar las redes eléctricas inteligentes (smart grids) contra amenazas cibernéticas. Estas redes son componentes vitales de la infraestructura crítica, y su operación segura es fundamental para el bienestar de las comunidades y la economía.

El protocolo tiene como objetivo principal proteger la confidencialidad, integridad y disponibilidad de los datos y sistemas críticos en las smart grids. Esto se logra mediante la implementación de medidas como la autenticación de usuarios, el control de acceso, la detección y prevención de intrusiones, el cifrado de datos y la monitorización constante.

Además, el protocolo promueve una cultura de ciberseguridad sólida, la colaboración entre partes interesadas y la adaptabilidad continua para hacer frente a las amenazas en evolución. Su implementación contribuye a la resiliencia de las redes eléctricas inteligentes, asegurando que puedan resistir y recuperarse de ataques cibernéticos, manteniendo así la

integridad y la disponibilidad de la infraestructura crítica que respaldan.

Objetivo: Proteger y mejorar la resiliencia de las redes eléctricas inteligentes al garantizar la confidencialidad, integridad y disponibilidad de los datos y sistemas críticos.

Componentes del Protocolo CSGR:

Segmentación de Redes: Divide la red en segmentos aislados, con controles de acceso estrictos entre ellos. Esto limita la propagación de amenazas y facilita la detección de intrusiones.

Detección y Prevención de Intrusiones (IDS/IPS): Implementa sistemas avanzados de detección y prevención de intrusiones en tiempo real para identificar actividades maliciosas y detenerlas de manera proactiva.

Autenticación Fuerte: Exige autenticación multifactor para acceder a sistemas críticos, con políticas de contraseñas robustas y certificados digitales.

Cifrado de Datos: Utiliza cifrado de extremo a extremo para proteger la confidencialidad de los datos en tránsito y en reposo.

Actualizaciones y Parches Automatizados: Implementa un proceso de actualización y parcheo automático para mantener el software y los dispositivos actualizados y protegidos contra vulnerabilidades conocidas.

Monitorización Continua: Realiza una monitorización continua de la red y los sistemas mediante análisis de comportamiento, inteligencia artificial y aprendizaje automático para detectar anomalías.

Respuesta a Incidentes: Establece un plan de respuesta a incidentes sólido que incluya la identificación rápida, mitigación y recuperación de amenazas, junto con la colaboración con agencias gubernamentales y otros sectores críticos.

Formación y Concienciación: Educa a todo el personal sobre las mejores prácticas de ciberseguridad y fomenta la concienciación sobre amenazas.

Colaboración Sectorial: Promueve la colaboración entre empresas eléctricas, reguladores, agencias gubernamentales y la comunidad de ciberseguridad para compartir información y buenas prácticas.

Blockchain para Auditoría y Registro: Utiliza tecnología blockchain para crear un registro inmutable de eventos y actividades de red, lo que facilita la auditoría y la trazabilidad.

Redundancia y Recuperación ante Desastres: Implementa sistemas redundantes y planes de recuperación ante desastres para garantizar la continuidad del servicio en caso de un ataque exitoso.

Evaluación de Riesgos Continua: Realiza evaluaciones periódicas de riesgos y pruebas de penetración para identificar y mitigar nuevas amenazas

III. VULNERABILIDADES DE LOS SISTEMAS

Las vulnerabilidades en los sistemas de control y monitorización representan un desafío crítico en la ciberseguridad de las infraestructuras tecnológicas. Estos sistemas, que se utilizan en diversos sectores, como la industria, la energía y las infraestructuras críticas, están expuestos a una serie de amenazas que pueden comprometer su integridad, disponibilidad y confidencialidad [11-13].

Estas vulnerabilidades pueden manifestarse en diferentes formas, como:

Fallos en el diseño y la implementación: Estos pueden incluir problemas de diseño de software, deficiencias en la configuración de los sistemas, falta de autenticación adecuada o controles de acceso débiles.

Fallos en la seguridad física: La falta de medidas de seguridad física, como acceso no autorizado a los dispositivos de control o monitorización, pueden permitir a los atacantes comprometer la integridad del sistema [14-16].

Fallos en las redes de comunicación: Las vulnerabilidades en las redes utilizadas para transmitir datos entre los dispositivos de control y monitorización pueden permitir ataques de intercepción, manipulación o denegación de servicio.

Fallos en las actualizaciones y parches de seguridad: La falta de aplicación de actualizaciones de seguridad y parches en los sistemas de control y monitorización puede dejarlos vulnerables a las últimas amenazas y exploits.

Un ejemplo de aplicación de estas vulnerabilidades puede ser un ataque dirigido a un sistema de control industrial, como un sistema de control de una planta de energía o una fábrica automatizada. Un atacante podría explotar una vulnerabilidad en el software de control para tomar el control de los dispositivos y alterar su funcionamiento. Esto podría resultar en daños a la infraestructura, interrupción de los servicios, pérdida de producción o incluso riesgos para la seguridad de las personas.

Para abordar estas vulnerabilidades, es fundamental implementar medidas de seguridad sólidas, como el uso de autenticación robusta, cifrado de datos, segmentación de redes, supervisión continua, implementación de parches y actualizaciones de seguridad, así como la concienciación y formación de los usuarios para promover prácticas seguras en los sistemas de control y monitorización [17, 18].

En resumen, la interconexión de sensores y actuadores dentro y fuera de una vivienda inteligente permite maximizar el rendimiento al ofrecer automatización personalizada y eficiente para electrodomésticos comunes. Esto se logra mediante la recopilación de datos a través de sensores y su procesamiento inteligente para activar los actuadores adecuados, lo que brinda mayor comodidad, eficiencia energética y control al usuario.

Una mejora concreta que se puede mencionar en este protocolo en comparación con los protocolos existentes es la implementación de la tecnología blockchain para garantizar la

integridad y la trazabilidad de los datos críticos en las redes eléctricas inteligentes (smart grids). Esto ofrece ventajas significativas en términos de seguridad y confiabilidad.

En contraste con muchos protocolos convencionales, que pueden depender en gran medida de sistemas centralizados y registros de auditoría que pueden ser vulnerables a manipulaciones, la utilización de blockchain ofrece:

Inmutabilidad de Datos: Los datos registrados en un blockchain son prácticamente inalterables una vez confirmados, lo que significa que no se pueden eliminar ni modificar sin dejar rastro. Esto asegura que los datos críticos, como la generación y distribución de energía, permanezcan intactos y confiables.

Transparencia y Trazabilidad: Cualquier cambio en los datos se registra en un libro de registro distribuido y transparente. Esto facilita la identificación de cualquier actividad sospechosa y proporciona una trazabilidad completa de los cambios realizados, lo que es esencial para la auditoría y la respuesta a incidentes.

Seguridad de la Información Mejorada: La tecnología blockchain utiliza fuertes mecanismos criptográficos para proteger los datos, lo que reduce significativamente el riesgo de compromiso de la información sensible.

Resistencia a Ataques Centrales: Dado que los datos se almacenan en una red descentralizada de nodos, no hay un solo punto de fallo que los atacantes puedan aprovechar. Esto mejora la resistencia de la infraestructura a los ataques dirigidos.

Facilita la Colaboración y la Confianza: Al utilizar un sistema de registro compartido y confiable, la colaboración entre diferentes partes interesadas, como empresas eléctricas y reguladores, se facilita y se fortalece la confianza en la integridad de los datos.

En resumen, la incorporación de blockchain en este protocolo representa una mejora concreta en términos de garantizar la integridad y la trazabilidad de los datos críticos en las redes eléctricas inteligentes. Esta característica puede hacer que el protocolo sea más resistente a manipulaciones y más adecuado para entornos de infraestructura crítica donde la confiabilidad de los datos es esencial.

IV. Enfoques y mejores prácticas para garantizar la ciberseguridad en smart grids

Esto se refiere a las estrategias y medidas que se deben implementar para proteger de manera efectiva las redes eléctricas inteligentes contra amenazas y ataques cibernéticos. Estos enfoques y mejores prácticas abarcan desde la implementación de medidas técnicas y de seguridad, hasta la adopción de políticas y procedimientos adecuados [19].

Por ejemplo:

Segmentación de redes: Dividir la red de smart grid en segmentos o zonas de seguridad para limitar la propagación de un ataque y reducir la superficie de exposición. Por ejemplo, separar la red de control de la red de gestión y la red corporativa [20].

Autenticación y acceso seguro: Utilizar autenticación multifactor y controles de acceso adecuados para garantizar que solo los usuarios autorizados tengan acceso a los sistemas críticos de la smart grid. Esto puede incluir el uso de certificados digitales y sistemas de gestión de identidad.

Encriptación de datos: Aplicar técnicas de encriptación para proteger la confidencialidad e integridad de los datos transmitidos en la red de smart grid. Por ejemplo, utilizar protocolos de encriptación como SSL/TLS para proteger las comunicaciones entre dispositivos.

Monitorización continua: Implementar sistemas de monitorización y detección de intrusiones para identificar y responder rápidamente a cualquier actividad sospechosa o anómala en la red. Esto puede incluir el uso de herramientas de análisis de tráfico y sistemas de gestión de eventos de seguridad (SIEM).

Educación y concienciación: Capacitar al personal y los usuarios de la smart grid sobre las buenas prácticas de ciberseguridad, como la gestión de contraseñas seguras, la identificación de correos electrónicos de phishing y la actualización regular de software y firmware.

V. Monitoreo y detección de intrusiones.

El monitoreo y detección de intrusiones en una vivienda inteligente conectada a la red implica supervisar constantemente los dispositivos y las comunicaciones en busca de actividades sospechosas o intentos de acceso no autorizados [21, 22].

Caso de test

Supongamos que un atacante intenta ingresar a la red de la vivienda inteligente a través de un dispositivo IoT comprometido, como una cámara de seguridad. El atacante intenta utilizar el dispositivo comprometido para acceder a otros dispositivos de la red y robar información confidencial.

Se muestra a continuación un ejemplo básico de código en Python para ilustrar cómo evitar la intrusión descrita anteriormente utilizando una regla de firewall para bloquear un tráfico sospechoso:

Listado 2. Código en Python

```
import iptc
# Obtener la cadena de reglas de entrada
chain = iptc.Chain(iptc.Table(iptc.Table.FILTER), "INPUT")
# Crear una nueva regla para bloquear el tráfico de un puerto específico
rule = iptc.Rule()
rule.protocol = "tcp"
```

```
rule.src = "IP_DEL_ATACANTE"
match = rule.create_match("tcp")
match.dport = "PUERTO_SOSPECHOSO"
target = rule.create_target("DROP")
rule.add_match(match)
rule.target = target
# Agregar la regla a la cadena de reglas de entrada
chain.insert_rule(rule)
```

Este código crea una nueva regla en la cadena de reglas de entrada del firewall para bloquear el tráfico proveniente de la dirección IP del atacante en un puerto sospechoso.

Es importante destacar que la seguridad en una vivienda inteligente debe ser abordada de manera integral, combinando medidas técnicas, como el monitoreo y la detección de intrusiones, con buenas prácticas de seguridad, como la gestión adecuada de contraseñas.

VI. Implementación Física

La implementación de un sistema de autenticación y control de acceso depende en gran medida de la plataforma y el lenguaje de programación que se está utilizando. A continuación, se ilustra un ejemplo en Python para implementar la autenticación y el control de acceso en la placa utilizada. Este ejemplo utiliza un diccionario para almacenar usuarios y contraseñas.

```
# Base de datos de usuarios (solo para fines de demostración, no es segura)
users_db = {
    "usuario1": "contraseña1",
    "usuario2": "contraseña2",
    "usuario3": "contraseña3",
}

# Función para autenticar a un usuario
def autenticar_usuario(username, password):
    if username in users_db and users_db[username] == password:
        return True
    else:
        return False

# Función para verificar los permisos del usuario
def verificar_permisos(username, recurso):
    # Si el usuario tiene acceso al recurso, devuelve True; de lo contrario, devuelve False.
    return True

# Ejemplo de uso
username = input("Nombre de usuario: ")
password = input("Contraseña: ")
if autenticar_usuario(username, password):
    recurso = input("Ingrese el nombre del recurso al que desea acceder: ")
    if verificar_permisos(username, recurso):
        printf("Acceso concedido a {recurso}")
    else:
        printf("No tiene acceso a {recurso}")
else:
    printf("Autenticación fallida. Verifique su nombre de usuario y contraseña.")
```

La plataforma básica consiste de un adaptador de Ethernet y un microcontrolador PIC 16F877. La placa de red debe configurarse para que tenga deshabilitado (en caso de que lo posea) el modo "plug&play" y establecer al adaptador a una dirección de entrada/salida fija.

Figura 1. Vista del sistema general compuesto por la placa de red, la plataforma básica

En esta implementación se eligió la dirección base 0x260. Debido a que no se usan interrupciones, no interesa como la IRQ de la placa queda configurada. El bus puede usar hasta 54 señales sin contar las conexiones de fuente y de masa. El microcontrolador tiene solamente 33 líneas de entrada/salida, de manera que es necesario encontrar una forma para poder conectarlo al adaptador de red.

El sistema empleado se muestra en la figura 1.

VII. Conclusiones

La ciberseguridad aplicada al diseño de smart grids es esencial para garantizar la resiliencia y protección de la infraestructura crítica de energía. Los desafíos en este campo son complejos y evolucionan constantemente, pero adoptar

enfoques proactivos y soluciones de vanguardia puede ayudar a mitigar los riesgos asociados con las amenazas cibernéticas. Los esfuerzos de investigación y desarrollo deben centrarse en la creación de sistemas seguros desde su concepción, la implementación de medidas de protección robustas y la promoción de la conciencia sobre la importancia de la ciberseguridad en el diseño y operación de las redes eléctricas inteligentes.

En resumen, los casos y ejemplos abordados en este artículo proporcionan las siguientes conclusiones:

Las vulnerabilidades en los sistemas de control y monitorización de smart grids pueden ser explotadas por amenazas internas y externas. Es crucial realizar un análisis de riesgos y aplicar controles adecuados para prevenir y mitigar posibles ataques.

La evolución de las tácticas de ataque y hacking requiere estar al tanto de las nuevas técnicas y algoritmos utilizados por los atacantes. Es importante mantenerse actualizado, fortalecer las defensas y utilizar técnicas de codificación segura en el desarrollo de software.

Los enfoques y mejores prácticas para garantizar la ciberseguridad en smart grids incluyen la implementación de sistemas de detección de intrusiones, la gestión de vulnerabilidades, la protección de datos y la colaboración entre los actores involucrados en la red.

La implementación de un diseño seguro y resistente desde el inicio implica considerar la seguridad en todas las etapas del proceso de desarrollo y adoptar estándares y marcos de seguridad reconocidos. Esto ayuda a reducir las vulnerabilidades y aumentar la resiliencia de los sistemas.

La segmentación de red y el control de accesos son medidas clave para limitar el alcance de un incidente y proteger los dispositivos y sistemas de la vivienda inteligente. La implementación de firewalls, reglas de acceso y autenticación sólida son ejemplos de cómo aplicar estas medidas.

El monitoreo y detección de intrusiones permiten identificar y responder rápidamente a actividades sospechosas. Mediante la supervisión constante de la red y el establecimiento de alertas personalizadas, es posible detectar y mitigar las amenazas de manera oportuna.

En este trabajo se han realizado con éxito los primeros pasos para la implementación de un sistema autónomo de seguridad en smart grids, implementando una placa original de conexión a internet, demostrando que es viable su implementación.

REFERENCIAS

[1] Farhangi, H. (2010). The path of the smart grid. IEEE Power and Energy Magazine, 8(1), 18-28.

[2] Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., & Hancke, G. P. (2011). Smart grid technologies: Communication technologies and standards. IEEE Transactions on Industrial Informatics, 7(4), 529-539.

[3] Jazebi, S., Grijalva, S., & Baldick, R. (2013). A survey of cyber-physical energy systems security research. IEEE Transactions on Smart Grid, 4(4), 1965-1974.

[4] Li, Q., Xu, Z., Jiao, L., & Li, Y. (2014). Cybersecurity for smart grid systems: Recent advances and future research directions. IEEE Transactions on Industrial Informatics, 10(2), 1078-1087.

[5] Zhang, Y., Chen, Y., Zhang, P., Li, Q., & Wang, Y. (2015). Cyber-physical system security in smart grid: Survey and challenges. IEEE Communications Surveys & Tutorials, 17(4), 2291-2312.

[6] Hu, X., Liang, T., Zhou, K., & Hu, Y. (2016). State-of-the-art cyber security technologies of smart grid. In 2016 IEEE PES Asia-Pacific Power and Energy Engineering Conference (APPEEC) (pp. 1-6). IEEE.

[7] Alcaraz, C., Najera, P., Lopez, J., Roman, R., & Sklavos, N. (2017). Security in wireless sensor networks for e-Health applications. Sensors, 17(7), 1557.

[8] Bhattacharya, S., Raza, S., Azab, A., & Stankovic, J. A. (2018). A comprehensive review on demand response in smart grids: Perspectives, frameworks, and technical challenges. IEEE Communications Surveys & Tutorials, 20(1), 869-900.

[9] Mahmood, A. N., & Mahmood, A. (2019). Cyber-physical system security in smart grids: A survey. Journal of Network and Computer Applications, 131, 46-63.

[10] Ashokumar, V., Selvamani, S. K., & Narayanasamy, P. (2020). Integration of renewable energy sources and smart grid technologies—A review. International Journal of Electrical Power & Energy Systems, 118, 105785.

[11] Schneier, B. (2006). Applied Cryptography: Protocols, Algorithms, and Source Code in C++. John Wiley & Sons.

[12] Viega, J., Messier, M., & Chandra, P. (2003). Network Security with OpenSSL: Cryptography for Secure Communications. O'Reilly Media.

[13] Wu, Q., Zhang, W., & Wang, J. (2018). Efficient Implementation of AES Encryption Algorithm Based on ARM Cortex-A9 Processor. IEEE Access, 6, 35868-35879.

[14] Stallings, W. (2013). Cryptography and Network Security: Principles and Practice. Pearson Education.

[15] Kocher, P., Jaffe, J., & Jun, B. (1999). Differential power analysis. In Advances in Cryptology - CRYPTO'99 (pp. 388-397). Springer.

[16] Farhangi, H. (2010). The path of the smart grid. IEEE Power and Energy Magazine, 8(1), 18-28.

[17] Marín, J. M., Caballero-Gil, P., & Fuentes-Cabrera, A. (2017). A review on cybersecurity of the smart grid: Threats, vulnerabilities and countermeasures. Renewable and Sustainable Energy Reviews, 72, 1384-1396.

[18] Liu, C., Wang, Q., & Gao, W. (2019). A comprehensive review on cyber security of smart grid: Threats, vulnerabilities and security solutions. Sustainable Cities and Society, 44, 101011.

[19] Kamhoua, C. A., Kwiat, K. A., & Njilla, L. (2017). Cybersecurity for smart grid systems: Challenges and solutions. IEEE Communications Surveys & Tutorials, 19(4), 2578-2595.

[20] Alzahrani, A. S., & Varol, C. (2019). Cybersecurity threats, vulnerabilities, and attacks on smart homes: A systematic review. IEEE Access, 7, 22436-22452.

[21] Vlachos, I., & Hatziargyriou, N. (2018). Cyber-physical security of future smart grids: Challenges and research directions. Electric Power Systems Research, 162, 234-245.

[22] Radhakrishnan, S., Zhou, R., & He, X. (2019). Cybersecurity of smart grids: Threats, vulnerabilities, and mitigation strategies. IEEE Transactions on Smart Grid, 10(1), 715-725.