Seguridad Informática

Atacantes en redes OT: impacto funcional sobre PLC y procesos físicos

AUTORES

Gonzalo Heinen GonzaloHernan.Heinen@alumnos.uai.edu.ar
Valentina Heinen ValentinaLorelei.Heinen@alumnos.uai.edu.ar
Jorge Kamlofsky Jorge.kamlofsky@uai.edu.ar

FILIACION

Universidad Abierta Interamericana

LINEA DE INVESTIGACION

Seguridad Informática

Ingeniería en Sistemas Informáticos

PALABRAS CLAVE

Infraestructuras críticas, Ciberseguridad, Redes OT, Sistemas SCADA, Ransomware, Machine Learning, Convergencia IT/OT.

INTRODUCCIÓN Y CONTEXTO

La ciberseguridad en infraestructuras críticas constituye un aspecto central para la operación segura de los sistemas industriales, dado que las vulnerabilidades presentes en entornos de Tecnología Operacional (OT) pueden trasladarse directamente al plano físico y generar consecuencias operativas reales. Esta problemática quedó evidenciada a nivel internacional a partir de incidentes como el ataque a las instalaciones nucleares iraníes en 2010, que demostró la posibilidad de inducir fallas físicas deliberadas mediante la manipulación de sistemas de control industrial [1].

Diversos estudios posteriores documentaron incidentes adicionales en sistemas SCADA y PLC, asociados a accesos no autorizados, exposición de servicios de control y ausencia de mecanismos de autenticación en protocolos industriales ampliamente utilizados [4]. En paralelo, la convergencia entre redes IT y OT ha incrementado la superficie de ataque de los sistemas industriales, manteniéndose en muchos casos supuestos de confianza implícita en la red que facilitan la manipulación de variables de proceso [2].

En este contexto, se presenta un experimento práctico desarrollado sobre un banco de pruebas OT portátil, orientado a analizar el impacto funcional que puede generar un atacante con acceso a la red sobre un PLC físico en operación, utilizando exclusivamente protocolos industriales estándar y sin modificar la lógica de control del sistema.

LÍNEAS DE INVESTIGACIÓN Y EXPERIMENTO EN REDES IT/OT

Metodología: Se implementó un banco de pruebas OT portátil y reproducible, sobre el cual se ejecutaron acciones maliciosas controladas mediante comunicación Modbus TCP, evaluando sus efectos directos sobre un proceso físico representativo.

Objetivo: Analizar, mediante un experimento controlado, el impacto funcional que puede generar un atacante con acceso a la red OT sobre un PLC físico, utilizando protocolos industriales estándar y sin modificar la lógica de control del sistema.

CONTRIBUCIÓN ORIGINAL

La contribución original de este trabajo consiste en la ejecución y análisis de un experimento práctico y reproducible que demuestra el impacto funcional que puede generar un atacante con acceso a la red de Tecnología Operacional (OT) sobre un proceso físico controlado por un PLC. A diferencia de enfoques centrados en simulaciones o análisis teóricos, el experimento se realiza sobre un entorno OT físico y controlado, utilizando exclusivamente protocolos industriales estándar y sin modificar la lógica de control del sistema. De este modo, se evidencia cómo la ausencia de mecanismos de autenticación y control de acceso en protocolos ampliamente utilizados permite la manipulación directa de variables internas del PLC, derivando en fallas operativas visibles sobre una maquinaria representativa.

FORMACION DE RECURSOS HUMANOS

El presente proyecto está dirigido por el Mg. Lic. Jorge Kamlofsky, quien actualmente cursa un Doctorado y desarrollará este trabajo como parte de su tesis. Asimismo, contará con la participación de José Castro y Daniel Manrique, para quienes el proyecto también constituirá parte de sus respectivas tesis.
Para el desarrollo de las actividades está prevista la participación de Gonzalo Heinen, Valentina Heinen y Jonatan Schmidt estudiantes de grado de la Universidad Abierta Interamericana de la carrera de grado de Ingeniería en Sistemas de información.
Por otro lado, el presente proyecto se enmarca como una de las líneas de trabajo que viene desarrollando el Laboratorio CAETI de la Universidad, en donde alumnos de grado y posgrado realizan sus trabajos finales de carrera. Por lo tanto, está prevista la incorporación de dos alumnos de grado y posgrado, quienes profundizarán sus saberes y realizarán los aportes correspondientes.

REFERENCIAS

[1] Denning, D. E. (2012). Stuxnet: What has changed? Future Internet, 4(3), 672–687.
[2] Heinen, G., Milano, M. A., & Kamlofsky, J. (2025). Uso de técnicas de machine learning para la detección temprana de ransomware. ResearchGate
[4] Miller, B., & Rowe, D. (2012). A survey of SCADA and critical infrastructure incidents. Proceedings of the 1st Annual Conference on Research in Information Technology.