AUTORES
Brian Llamocca, llamoccas.brian@gmail.com
Aldana Tedesco, aldanatedesco28@alu.ing.unlp.edu.ar
Facultad de Informática
UNIVERSIDAD NACIONAL DE LA PLATA
Paula Venosa, pvenosa@info.unlp.edu.ar
Sofía Martin, smartin@linti.unlp.edu.ar
Patricia Bazán, pbaz@info.unlp.edu.ar
Agustín Candia, acandia@linti.unlp.edu.ar
LINTI | Laboratorio de Investigación y Formación en Informática Avanzada
Facultad de Informática
UNIVERSIDAD NACIONAL DE LA PLATA
Calle 50 esq. 120, 2do Piso. Tel: +54 221 4223528

Evaluación de vulnerabilidades y desempeño en redes IoT en un entorno experimental controlado

RESUMEN

El trabajo presenta una línea de investigación orientada al estudio de la seguridad en entornos IoT mediante la construcción de un entorno experimental controlado y de bajo costo. El estudio se justifica por el crecimiento sostenido de ataques a estos dispositivos, la baja visibilidad de los mismos en redes organizacionales y la heterogeneidad de tecnologías y fabricantes, que incrementan la superficie de ataque.
Se implementa un ecosistema basado en dispositivos Bluetooth Low Energy (BLE) en modo beacon y tecnologías LoRa/LoRaWAN, con el fin de analizar tráfico, identificar vulnerabilidades y ensayar mecanismos de mitigación.
Los resultados alcanzados confirman la viabilidad del entorno propuesto para realizar evaluaciones de seguridad en redes IoT y promover la definición de estrategias de ciberseguridad y su implementación.

CONTEXTO

La línea de investigación que se presenta, propone profundizar la investigación de tácticas, técnicas y procedimientos de los atacantes a nivel regional mediante el uso de honeypots. En este contexto, se abrió una línea de trabajo para construir un marco teórico y analizar el estado del arte del uso de honeypots y honeynets como herramienta para estudiar comportamiento malicioso poniendo énfasis, en las amenazas que afectan a los dispositivos de IoT (Internet de las Cosas) y a sus protocolos. Este trabajo presenta las primeras etapas de investigación en torno a IoT, con el objetivo final de contar con un ecosistema prototipo de una red de sensores con comunicación inalámbrica sin internet. Este ecosistema se utilizó para analizar tráfico, evaluar vulnerabilidades existentes y establecer estrategias de ciberseguridad.

LÍNEAS DE INVESTIGACIÓN, DESARROLLO E INNOVACIÓN

ESTRATEGIAS DE CIBERSEGURIDAD DISTRIBUIDA.

ANÁLISIS DE TÉCNICAS DE ATAQUE Y COMPORTAMIENTOS MALICIOSOS.

ANÁLISIS DE DISPOSITIVOS DE IOT PARA EVALUAR LA SEGURIDAD Y RENDIMIENTO DE REDES DE IOT DE BAJO COSTO EN UN ENTORNO CONTROLADO, SIMULANDO CASOS DE USO REALES Y REALIZANDO PRUEBAS DE SEGURIDAD ÉTICAS.

FORMACIÓN DE RECURSOS HUMANOS

Las líneas de investigación del proyecto permitieron producir dos propuestas de grado en el marco de las Prácticas Profesionales Supervisadas, para la carrera de Ingeniería en Computación de la Facultad de Informática de la UNLP, de Brian Llamocca y Aldana Tedesco, bajo la tutoría de Paula Venosa y Sofía Martin, cuyos objetivos son desarrollar y evaluar un entorno experimental de red IoT utilizando dispositivos de bajo costo para conformar un ecosistema funcional a pequeña escala.

Además, se concluyó el Trabajo Final Integrador para la Especialización en Redes y Seguridad, de Pablo Germán Maddalena Kreff cuyo objetivo es relacionar a los honeypots como fuente de información con una herramienta de Cyber Threat Intelligence (CTI) [1].

El trabajo de investigación presentado se enmarca en el proyecto de I+D+i “Redes de Honeypots: alcances, implementaciones y utilidad en la ciberseguridad de las organizaciones” de la Facultad de Informática de la UNLP llevado a cabo durante el año 2024-2025.

REFERENCIAS

· Venosa, P., Bazán, P. A., Martin, S., Del Rio, N., Magdalena Kreff, P. G., Gagliardi, P., & Díaz, F. J. (2025). Honeypots como fuente de inteligencia de ciberamenazas. In XXVII Workshop de Investigadores en Ciencias de la Computación (Mendoza, 10 y 11 de abril de 2025).

· Venosa, P. (2021). Detección de ataques de seguridad en redes usando técnicas de ensembling (Doctoral dissertation, Universidad Nacional de La Plata). http://sedici.unlp.edu.ar/handle/10915/120856. https://doi.org/10.35537/10915/120856

· Gallardo Urbini I. Estrategia de Ciberseguridad distribuida, aplicando el concepto de Operación de Inteligencia. Tesis Doctoral. La Plata 2023. http://sedici.unlp.edu.ar/handle/10915/152594

· Diaz J, Venosa P, Macia N. Investigación en Ciberseguridad en un año de pandemia. WICC 2021.
https://sedici.unlp.edu.ar/handle/10915/119490

· Washofsky, A. D. (2021). Deploying and analyzing containerized honeypots in the cloud with t-pot (Doctoral dissertation, Monterey, CA; Naval Postgraduate School).

· Roa Parra, E. F. (2019). Análisis de seguridad de tecnologías inalámbricas de comunicación basado en radio definida mediante software (Bachelor's thesis).

· Arregui Caballero de Tineo, A. (2016). Beacons BLE (Bluetooth Low Energy) en el sector turístico, control de afluencia y servicios de valor añadido.

· Saltzstein, W. (2020). Bluetooth Wireless Technology Cybersecurity and Diabetes Technology Devices. Journal of Diabetes Science and Technology, 14(6), 1111-1115. https://doi.org/10.1177/1932296819864416