Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Vicepresidencia Primera del Gobierno · Ministerio de Asuntos Económicos y Transformación Digital · Secretaría de Estado de Digitalización e Inteligencia Artificial
Plan de Recuperación, Transformación y Resiliencia
España | digital 2026
incibe_ Instituto Nacional de Ciberseguridad

Gonzalo de Francisco Rodríguez
presenta el resumen del trabajo

TBQ Técnicas Básicas Iberseguridad Quantum

A Testbed for a Nearby-Context Aware: Threat Detection and Mitigation System for Connected Vehicles

Miguel Martín-Pérez, Jordi Marias Parella, Javier Fernández, Pablo de Juan Fidalgo, Jordi Casademont, Antonio Álvarez Romero, Rodrigo Díaz-Rodríguez

Actas VIII JNIC, atlanTTic, 163-170, (2023).

22 de julio de 2024

SERIE DE RESÚMENES EN ESPAÑOL

Palabras clave: MQTT, SIEM, V2X, Vehículo Conectado, XL-SIEM

Introducción

En la era de la digitalización del transporte y la conectividad, los vehículos conectados representan un avance significativo en la industria del transporte ofreciendo beneficios como la mejora de la seguridad, la eficiencia en el tráfico y la experiencia del usuario. Sin embargo, esta interconexión también introduce nuevos desafíos, especialmente en términos de ciberseguridad. Los vehículos modernos, equipados con sistemas de información y entretenimiento avanzados, así como capacidades de comunicación V2X (Vehicle-to-Everything), son susceptibles a ciberataques que pueden comprometer la seguridad del vehículo, la privacidad del usuario y la integridad de los datos. Es por ello que la ciberseguridad de los vehículos conectados se ha convertido en una prioridad crucial, siendo cada vez más necesaria la implementación de sistemas de ciberdefensa robustos para proteger la integridad y seguridad de las operaciones de transporte conectado.

El artículo original presenta un sistema innovador basado en una arquitectura jerárquica de Sistemas de Gestión de Información y Eventos de Seguridad (SIEM) diseñado específicamente para detectar, mitigar y responder eficazmente a ciberamenazas en flotas de vehículos. La importancia de este estudio radica en su capacidad para abordar las vulnerabilidades emergentes (como en los sistemas de comunicación inalámbrica, las unidades de control electrónico u otros componentes críticos del vehículo) en un entorno donde la conectividad y la interoperabilidad son esenciales pero también aumenta el riesgo de ataques maliciosos.

Además, el artículo expone un marco integral que combina tecnologías emergentes como SDN (Software-Defined Networking), MQTT (Message Queuing Telemetry Transport) y SIEM para proporcionar una defensa robusta y adaptable contra ataques en entornos dinámicos y heterogéneos. La arquitectura jerárquica del SIEM permite la colaboración efectiva entre diferentes capas de infraestructura de red, desde la nube hasta los dispositivos en vehículos individuales, facilitando una detección temprana de amenazas y una respuesta coordinada en tiempo real.

1. Metodología

La metodología del estudio se centra en un enfoque experimental robusto utilizando un banco de pruebas que simula entornos reales de operación de vehículos conectados. La arquitectura SIEM jerárquica comprende cuatro capas principales: Cloud, Borde (Edge), Pasarela (Gateway) y CPS (Sistemas Ciber-Físicos). Cada capa desempeña un papel crítico en la detección y respuesta ante eventos de seguridad:

1. **Capa Cloud**: incluye un controlador SDN para gestionar flujos de tráfico y un SIEM XL-SIEM (Cross-Layer SIEM) global que recopila eventos y alarmas de toda la red. Utiliza un broker MQTT para la comunicación entre capas.
2. **Capa de Borde (Edge)**: aquí se encuentra un nodo Edge con Openstack esencial para entornos compartidos. Incluye un broker MQTT para la comunicación con los nodos de la Capa CPS y un XL-SIEM de área que detecta y responde a eventos dentro de una zona geográfica específica.
3. **Capa de Pasarela (Gateway)**: facilita la comunicación entre la Capa de Borde y la Capa CPS mediante IEEE 802.11p.
4. **Capa CPS**: la capa más baja donde residen los CPS, como las unidades a bordo (OBU), que conectan dispositivos a la infraestructura y

otros vehículos. Aquí opera el XL-SIEM local, que recolecta eventos de dispositivos y sensores, correlacionándolos y generando alarmas locales que se escalan a niveles superiores cuando se detectan amenazas.

2. Resultados

Los resultados del estudio demuestran la efectividad del sistema SIEM jerárquico en diferentes escenarios de ataque:

- **Escenario local**: enfocado en la defensa dentro de un vehículo individual, donde el SIEM detecta y responde a ataques dirigidos a dispositivos vulnerables como unidades de comunicación Bluetooth. Se implementan acciones correctivas como la validación de firmware mediante tokens de seguridad hardware (HST), garantizando la integridad y seguridad de las actualizaciones.
- **Escenario de área**: aborda ataques que afectan a múltiples vehículos dentro de una zona geográfica limitada, como una ciudad o carretera. El XL-SIEM de área coordina la respuesta bloqueando comunicaciones con repositorios de malware después de detectar múltiples eventos de actualización ilegítima en vehículos cercanos, mitigando así la propagación de amenazas.
- **Escenario global**: trata con ataques a gran escala que afectan a toda la red de vehículos conectados. El SIEM global recibe y analiza alarmas de múltiples nodos de área, ejecutando acciones preventivas como el bloqueo sistémico de comunicaciones con repositorios de malware y la generación de informes detallados para la mejora continua de la seguridad.

3. Discusión/Conclusiones

Como hemos visto, la flexibilidad del sistema SIEM jerárquico le permite adaptarse a entornos dinámicos y heterogéneos como las flotas de vehículos conectados. La capacidad de compartir información entre diferentes capas y nodos heterogéneos destinados a contextos distintos permite una detección temprana y una respuesta coordinada ante amenazas emergentes. La integración de las tecnologías avanzadas V2X y XL-SIEM (en su versión *Lightweight*) asegura un rendimiento óptimo en condiciones de red variables y recursos limitados, respectivamente.

4. Valoración del documento original

El trabajo original proporciona una solución innovadora y viable para la ciberdefensa en vehículos conectados, destacándose por su enfoque jerárquico y el uso eficiente de tecnologías emergentes. La validación a través de un banco de pruebas experimental demuestra un avance significativo en la protección contra ciberataques en el sector automotriz.

Referencias

· Miguel Martín Pérez, Jordi Marias Parella, Javier Fernández, Pablo de Juan Fidalgo, Jordi Casademont, Antonio Álvarez Romero, Rodrigo Díaz Rodríguez, *"A Testbed for a Nearby-Context Aware: Threat Detection and Mitigation System for Connected Vehicles"* , Actas de las VIII Jornadas Nacionales de Investigación en Ciberseguridad, Vigo (21 a 23 de junio de 2023).