Detección de Ataques mediante técnicas Side-channel y de Inteligencia Artificial en entornos IoT (DASIA-IoT).

Researchers:
Felipe Alejandro Lemus y Alejandro Domínguez.

Language Undefined

Description:
La eclosión de la tecnología Internet de las cosas ha derivado en el desarrollo de múltiples aplicaciones en muchos y diversos campos. Las posibilidades brindadas por esta tecnología, en combinación con las tecnologías de comunicación inalámbricas modernas, permiten obtener datos de diversos dispositivos en tiempo real y habilitan una toma de decisiones mejor informada. En el ámbito de la salud, estos dispositivos proporcionan una información valiosa que se traduce en un mejor tratamiento de pacientes y en una utilización más eficiente de los recursos sanitarios. A su vez, estos datos son especialmente sensibles y, si bien la tecnología IoT ha experimentado un gran avance, la securización de la misma no lo ha hecho en consonancia. El objetivo del presente proyecto es el fortalecimiento de los sistemas IoT especialmente sensibles mediante el análisis y estudio de técnicas de securización ya existentes y la aplicación de técnicas denominadas side-channel combinadas con técnicas de machine learning para implementar un sistema de detección de intrusiones específicas para dispositivos IoT.

Objectives: El objetivo general del presente proyecto es mejorar la seguridad de los dispositivos IoT mediante la implementación de un sistema de detección de intrusos (IDS), basado en la monitorización de su consumo eléctrico y la aplicación de técnicas de aprendizaje automático.
Del objetivo general del proyecto se desprenden los siguientes objetivos específicos:

• OE1 Desarrollar un entorno de pruebas para monitorizar el consumo de dispositivos IoT: mediante la combinación de dispositivos IoT reales y los elementos electrónicos necesarios para registrar el consumo de los dispositivos en tiempo real.

• OE2 Elaboración del dataset para la aplicación de técnicas de machine learning: mediante la realización de los perfiles de consumo de los dispositivos IoT actuando en condiciones normales y bajo ataque.
• OE3 Analizar y evaluar la eficacia del sistema de detección de intrusos resultante: mediante la preparación del dataset en cada caso, la aplicación de diferentes algoritmos sobre el mismo y la extracción de métricas de rendimiento del sistema final.
• OE4 Capacitar a la persona contratada en tecnologías consolidadas y en investigación: mediante la formación, por un lado, en tecnologías como IoT, machine learning y ciberseguridad; y, por otro, en campos relacionados con la investigación como son la metodología de trabajo, la búsqueda y análisis de artículos sobre el objeto de estudio, la gestión bibliográfica, o la propia preparación y escritura de artículos.

Funding sources:
Programa Investigo. Decreto 137/2021, de 15 de diciembre, por el que se establecen las bases reguladoras para la concesión de subvenciones destinadas a la financiación de los programas de empleo creados para la ejecución del Plan de Recuperación, Transformación y Resiliencia en la Comunidad Autónoma de Extremadura y se aprueban las primeras convocatorias de dichos programas. Financiado por la Unión Europea. NextGenerationEU.