Práctica 1

Nombres de los autores

September 2025

1 Resumen

El Trabajo de Fin de Máster propone el diseño, implementación y evaluación de una plataforma de actualización remota (OTA) segura y escalable para dispositivos IoT. La motivación principal radica en la elevada cantidad de dispositivos que sufren por vulnerabilidades y la falta de actualizaciones para solucionarlas, lo que crea vectores de ataque a gran escala. Esta plataforma permite la distribución de actualizaciones firmadas y cifradas a flotas de dispositivos para garantizar la autenticidad, integridad y confidencialidad del software desplegado.

El sistema está pensado para todo tipo de escenarios: desde dispositivos sencillos con pocos recursos hasta situaciones críticas que necesitan protegerse de futuros ordenadores cuánticos. Por eso, soporta dos tipos de criptografía: algoritmos post-cuánticos y algoritmos ligeros (lightweight cryptography), ideales para equipos con poca memoria y batería.

El trabajo incluye un análisis del estado de la práctica sobre actualizaciones OTA en IoT y de las necesidades de seguridad actuales, mostrando la importancia de incorporar criptografía ligera para dispositivos con recursos limitados y la opción de soluciones resistentes a la computación cuántica cuando el contexto lo requiera. Además, se desarrolla un prototipo de plataforma, desplegable en la nube y diseñado para escalar horizontalmente.

Palabras clave: OTA, IoT, actualizaciones seguras, post-cuántico, criptografía ligera, firma digital, cifrado.

Impacto en los Objetivos de Desarrollo Sostenible (ODS): xxx,

Abstract

This Master's thesis proposes the design, implementation, and evaluation of a secure and scalable over-the-air (OTA) update platform for IoT devices. The main motivation is the large number of devices that suffer from vulnerabilities and are not updated, creating large-scale attack vectors. The platform enables distributing signed and encrypted updates to device fleets to ensure the authenticity, integrity, and confidentiality of deployed software.

To accommodate both resource-constrained devices and scenarios requiring resilience against future quantum attacks, the system supports two families of cryptographic algorithms: post-quantum resistant encryption and signing algorithms, and lightweight cryptography algorithms optimized for devices with limited memory, CPU, and energy.

The work includes an analysis of current OTA practices and security needs, highlighting the importance of incorporating lightweight cryptography for constrained devices and offering post-quantum options when the context requires it. Additionally, a cloud-deployable prototype platform is developed, designed for horizontal scalability.

Keywords: OTA; IoT; secure updates; post-quantum; lightweight cryptography; digital signatures; encryption.

Laburpena

Master Amaierako Lan honek IoT gailuetarako OTA (over-the-air) eguneratze-plataforma segurua eta eskalagarri baten diseinua, inplementazioa eta ebaluazioa proposatzen du. Motibazio nagusia da ahultasunak dituzten eta eguneratzerik jasotzen ez duten gailu ugariena, eta horrek erasotze-bideak sortzen ditu eskala handian. Plataforma honek eguneratze sinatuak eta zifratutakoak banatzeko aukera ematen du, sistema batean instalatutako softwarearen jatorria, osotasuna eta konfidentzialtasuna bermatzeko.

Baliabide mugatuak dituzten gailuetarako eta etorkizuneko eraso kuantikoen aurrean erresistentzia behar duten egoeretarako egokituz, sistemak bi kriptografia-familiari laguntza eskaintzen die: kuantumaren aurkako erresistentzia duten zifratze eta sinadura algoritmoak, eta memoria, CPU eta energia murrizketak dituzten gailuentzako optimizatutako 'lightweight' kriptografia algoritmoak.

Lanak OTA eguneratzeei buruzko egungo praktiken analisia eta segurtasun-beharren azterketa barne hartzen ditu, baliabide mugatutako gailuentzako kriptografia arina sartzeko garrantzia nabarmentzen du eta beharrezkoa denean kuantumaren aurkako soluzioak aukeratzearen garrantziaz mintzo da. Gainera, hodeian martxan jar daitekeen eta horizontalki eskalatzeko diseinatutako plataforma prototipo bat garatu.

Gako-hitzak: OTA; IoT; eguneratze seguruak; post-kuantikoa; kriptografia arina; sinadura digitala; zifratzea.

2 Lista de acrónimos

AEAD Authenticated Encryption with Associated Data (Cifrado Autenticado con Datos Asociados)

AES Advanced Encryption Standard (Estándar de Cifrado Avanzado)

API Application Programming Interface (Interfaz de Programación de Aplicaciones)

ASCON Algoritmo de criptografía ligera estandarizado por NIST

CPU Central Processing Unit (Unidad Central de Procesamiento)

CRA Cyber Resilience Act (Ley de Resiliencia Cibernética de la UE)

DDoS Distributed Denial of Service (Denegación de Servicio Distribuida)

DFU Device Firmware Update (Actualización de Firmware del Dispositivo)

ECDSA Elliptic Curve Digital Signature Algorithm (Algoritmo de Firma Digital de Curva Elíptica)

ICS Industrial Control Systems (Sistemas de Control Industrial)

IoT Internet of Things (Internet de las Cosas)

LWC Lightweight Cryptography (Criptografía Ligera)

ML-DSA Module-Lattice-Based Digital Signature Algorithm (Algoritmo de Firma Digital basado en Redes de Módulos, antes Dilithium)

NIST National Institute of Standards and Technology (Instituto Nacional de Estándares y Tecnología de EE.UU.)

ODS Objetivos de Desarrollo Sostenible

OTA Over-The-Air (Actualización remota por aire)

PC Personal Computer (Ordenador Personal)

PQC Post-Quantum Cryptography (Criptografía Post-Cuántica)

RAM Random Access Memory (Memoria de Acceso Aleatorio)

RSA RivestShamirAdleman (Algoritmo criptográfico de clave pública)

SDK Software Development Kit (Kit de Desarrollo de Software)

SPHINCS+ Esquema de firma digital post-cuántico basado en funciones hash

TFM Trabajo de Fin de Máster

TUTK ThroughTek Kalay (Plataforma IoT)

UE Unión Europea