Newcastle University

Securing the Internet of Things: A Zero-Trust Architecture Framework for Resilient, Adaptive, and Scalable IoT Ecosystems

Supervision team

Main Supervisor: Dr. Yinhao Li (yinhao.li@newcastle.ac.uk)

Research project

The rapid proliferation of Internet of Things (IoT) devices in critical sectors—such as smart cities, healthcare, and industrial automation—has introduced unprecedented security risks. Traditional perimeter-based security models fail to address the dynamic, distributed, and heterogeneous nature of IoT ecosystems, leaving them vulnerable to ransomware, botnet attacks, and data breaches. This project proposes a novel **Zero-Trust Architecture (ZTA)** framework specifically tailored for IoT systems, integrating continuous authentication, context-aware access controls, and lightweight cryptographic protocols to enforce security *by design* across resource-constrained devices.

Research Objectives:

1. **IoT-Specific Zero-Trust Policies**: Develop adaptive access control mechanisms that account for device capabilities (e.g., low-power sensors, edge gateways) and dynamic network conditions (e.g., intermittent connectivity).
2. **Lightweight Device Attestation**: Create energy-efficient protocols for continuous verification of device integrity and firmware authenticity, even in low-compute environments.
3. **Micro-Segmentation for IoT Networks**: Design scalable network partitioning strategies to isolate compromised devices and prevent lateral movement of threats (e.g., Mirai-style botnets).
4. **AI-Driven Anomaly Detection**: Implement federated learning models to detect behavioral anomalies across distributed IoT nodes while preserving data privacy.