Operating Systems for IoT Devices: Characteristics, Challenges, Attack Surfaces, and OS Landscape

Paul Christian Pienkny
Freie Universität Berlin
IoT & Security Seminar Report - Skeleton Structure Reworked

***Abstract*—The report aims to provide a comprehensive overview of the current landscape of IoT operating systems, highlighting their differences and unique features, as well as security challenges they face in the landscape of rapidly evolving IoT ecosystems.**

(This document is only a tentative skeleton structure for the upcoming report)

***Index Terms*—Operating Systems (OS), Internet of Things (IoT), Characteristics, Security Challenges, Attack Surfaces, MCUs, Embedded Devices**

I. Introduction
(1 page)

A. Security Relevance of IoT Devices & MCU-based Systems

Brief context: Why especially MCU-based systems are a security concern...

B. Objectives & Research Questions

C. Report Structure

II. Fundamentals & Characteristics
(2 pages)

How do MCU-based IoT Systems work technically, what are their characteristics,
and what are the general security fundamentals in this context?

A. IoT Hardware Models & Architectures

MCUs vs. MPUs - focus on MCUs,
typical hardware architectures, ...

B. Characteristics of MCU IoT Operating Systems

Resource constraints, real-time capabilities,
(energy) efficiency...

C. Security Fundamentals

Threats, vulnerabilities, attack vectors
in IoT environments...
(general theoretical background)

III. Security Requirements & Principles for IoT Operating Systems
(3 pages)

What security requirements do these systems have to fulfill, and which principles guide their design?

A. Security Principles for MCU-based Systems

Avoidance Principle, Minimality Principle,
Defense-in-Depth, Fail Secure,
Secure-by-Design...
(concrete guidelines and methods)

B. Integrity & Authenticity

e.g. Secure Boot, Firmware-Signatures,
Update-Authenticity, Rollback Protection...

C. Isolation & Access Control

e.g. Memory Protection, Task-Isolation,
Scheduling-Isolation, Kernel Architecture...

D. Lifecycle Security Requirements

e.g. Provisioning, Update-Mechanisms, ...
(requirements and not specific implementations)

IV. Overview of IoT Operating Systems
(3.5-4 pages)

How do selected IoT OSes implement these principles and requirements?
What are their differences, strengths, and weaknesses?

A. Brief Introduction of Selected MCU-based IoT Operating Systems

RIOT, FreeRTOS, (Zephyr, TinyOS)...
Maybe Mbed OS?

B. Comparison of Selected Operating Systems

Use cases, (kernel) architecture, resource consumption,
security features, real-time capabilities...

C. Known Vulnerabilities and Historical Attacks

e.g., related to Privilege Escalation, Memory Protection,
Buffer overflow...

D. OS-specific Security Mechanisms

1) RIOT Security Features: e.g. Secure-Boot, Cryptographic Libraries,
Modularity,...

2) FreeRTOS Security Features: e.g. Memory Protection, Task Isolation, Secure Sockets,...

3) Zephyr Security Features: e.g. Kernel Mode Separation, MPU Abstractions, MCUboot,...

4) TinyOS Security Features: e.g. Component-based Architecture, Access Control,...

V. Challenges & Research Directions (2.5-3 pages)

Why will it stay challenging to secure IoT OSes, and what are current research trends?

A. Resource Constraints vs. Security Mechanisms

e.g. Isolation, Cryptography, Scheduling...

B. Lifecycle Management & Update Strategies

e.g. Secure OTA, Rollback Protection, Maintenance... (and why these will remain challenging)

C. Formal Verification, Microkernels & Trusted Execution Environments

D. Recent Trends in Research

e.g., Edge Security, rBPF on MCU, Trusted Execution Environments,
Microkernel Isolation, Lightweight Cryptography...

VI. Conclusion & Outlook (1 page)

A. Summary of Insights

B. Future Developments in IoT OS Security

C. Open Questions & Ongoing Challenges

References

[1] A survey of security and privacy issues in the Internet of Things from the layered context (2020, published)

[2] OAT: Attesting Operation Integrity of Embedded Devices (2020, published)

[3] RIOT: an Open Source Operating System for Low-end Embedded Devices in the IoT (2018, published)

[4] Trusted secure embedded Linux (2007, published)

[5] A Survey of the Security Challenges and Requirements for IoT Operating Systems (2023, unpublished)

[6] Real Time Operating Systems for the Internet of Things, Vision, Architecture and Research Directions (2016, published)

[7] A survey on IoT & embedded device firmware security: architecture, extraction techniques, and vulnerability analysis frameworks (2023, published)