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

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

***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,**

I. Introduction
(1 page)

A. Security Relevance of IoT Devices & Operating Systems

B. Objectives & Research Questions

C. Report Structure

II. Fundamentals
(2 pages)

A. IoT Devices & Architectures

B. Requirements for IoT Operating Systems

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

C. Security Fundamentals

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

III. Overview of IoT Operating Systems
(2.5-3 pages)

A. Brief Introduction of Selected IoT Operating Systems

RIOT, FreeRTOS, OAT, (Zephyr, TinyOS,)...
Buildroot(Linux), Yocto(Linux)...

B. Comparison of Selected Operating Systems

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

C. Known Vulnerabilities or Attacks on IoT Operating Systems

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

IV. Security Features & Requirements of IoT Operating Systems
(3-4 pages)

A. Security Principles

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

B. Integrity & Authenticity

e.g., Secure Boot, Code Signing, (Firmware-)Updates...

C. Isolation & Access Control

e.g., Memory Protection, Sandboxing, (Micro-)Kernel Architecture...

D. OS-Specific Security Mechanisms

e.g. RIOT Secure Boot, FreeRTOS/Zephyr Memory Protection...

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

A. Resource Constraints vs. Security Mechanisms

B. Lifecycle Management & Update Strategies

C. Formal Verification, Microkernels & Trusted Execution Environments

D. Recent Trends in Research

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

VI. Conclusion & Outlook
(1 page)

A. Summary of Findings

B. Future Developments & Research Perspectives

C. Remaining Open Questions & 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)