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

IoT & Security Seminar

by Paul Christian Pienkny

Introduction & Overview

- Embedded Operating System Diversity

- Hardware Limitations

- Security Relevance & Requirements

- Security Implementations & Practices

- Testing

- Future Perspectives

Motivation

- increasing security risks

- diverse hardware

- constrained resources

- critical environments

- lacking security mechanisms

⟹ High need for systematic survey of challenges and solutions

Report Structure

- Introduction
    - Security Relevance of IoT Devices & OS
    - Objectives & Research Questions
- Fundamentals
    - IoT Devices & Architectures
    - General Requirements for IoT-OS
    - Security Requirements (basics)
- Overview of IOT-OS
    - Brief Introduction into Selected IoT-OS
    - Comparison of Selected OS
    - Known Vulnerabilities in IoT-OS
- Security Features & Requirements of IoT-OS
    - Security Principles (in detail)
    - Integrity & Authenticity
    - Isolation & Access Control
    - OS-Specific Security Mechanisms

Report Structure

- Challenges & Research Directions
  - Resource Constraints vs. Security Mechanisms
  - Lifecycle Management & Update Strategies
  - Formal Verification, Microkernels & Trusted Execution Environments (possible solutions)
  - Recent Trends in Research (possible solutions)
- Conclusion & Outlook
  - Summary of Findings
  - Future(!) Developments & Research Perspectives
  - Remaining Open Questions & Challenges

→ Possible duplications leave room for reduction and reorganization!

References for Broad Coverage

- A survey of security and privacy issues in the Internet of Things from the layered context (2020)
  - general security challenges & privacy concerns
- A survey on IoT & embedded device firmware security: architecture, extraction techniques, and vulnerability analysis frameworks (2023)
  - firmware-level vulnerabilities, extraction techniques, and OS implications
- A Survey of the Security Challenges and Requirements for IoT Operating Systems (2023, unpublished)
  - updated overview of threats, requirements and research directions
- RIOT: an Open Source Operating System for Low-end Embedded Devices in the IoT (2018)
  - OS characteristics, architecture and security mechanisms with highly constrained ressources
- Trusted secure embedded Linux (2007)
  - embedded Linux security, secure boot, kernel protection, characteristics
- Real Time Operating Systems for the Internet of Things, Vision, Architecture and Research Directions (2016)
  - RTOS characteristics, real-time requirements, challenges and research directions
- OAT: Attesting Operation Integrity of Embedded Devices (2020)
  - integrity and authenticity approaches for embedded devices
- IoT Security: Ongoing Challenges and Research Opportunities (2014)
  - further security challenges and research directions

Solution for In-Depth-Coverage

Should be :

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

Might be :

Efficient Isolation of Trusted Subsystems in Embedded Systems (2010)

More to come…

Schedule Breakdown

1. Literature Review & Source Collection (still on it)

2. Outline & Report Skeleton (done, reworking)

3. Draft Sections: Introduction, Fundamentals, IoT-OS Overview (+ additional sources)

4. Draft Sections: Security Features, Challenges, Research Directions (+ additional sources)

5. Review & Refinement, integrate "In-Depth-Coverage"

6. Error-Checking, Formatting, integrate References

7. Finalize Report & Submit

Open Questions

- What are actual(!) recent research directions and opportunities?

- Which IoT-OS should I focus on?

- What are redundant topics in my report?

- Are Security Implementations my In-Depth source/topic?

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

IoT & Security Seminar

by Paul Christian Pienkny