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

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

***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 an ALPHA version of the upcoming report)

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

I. Introduction

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

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

Good Overview for Questions and Numbers. [1]
Reasons of Security Relevance for Embedded Systems. [2]
Reasons regarding intellectual property. [3]
Challenges with IoT Devices. [4]
Security Requirements of IoT Systems (on MCUs). [5]
Use Cases of RTOS in IoT. [6]
Severity of IoT System vulnerabilities. [7]

B. Objectives & Research Questions

Goal is to highlight differences, current problems and possible solutions regarding the security of (especially MCU-based) IoT operating systems on IoT devices.

Separating between problems that are bound to Hardware/Architecture and problems that are bound to the Operating System.

C. Report Structure

II. Fundamentals & Characteristics

"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, ...

Differences in Architecture on ARM. [8]
Architecture Types and Features of OS for IoT. [9]

B. Characteristics of MCU IoT Operating Systems

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

List of possible Hardware Limitations. [1]
Resource Exhaustion as a Security Issue. [4]
What is an RTOS? Includes Architectural Layers of RTOS for IoT. [6]
Data for different specifications of IoT OSes. [10]

C. Security Fundamentals

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

Good example for Vulerabilities, Architectural Issues. [1]
Specifically Side-Channel-Attacks on MCUs. [2]
Common Weaknesses/Vulnerabilities: [11]
Attacks on TEEs. Also Side-Channel-Attacks. Architectural Attacks. [12]
Common Threats to IoT Devices. Also Side-Channel-Attacks, Network Attacks. Security Issue Layers. [4]
Kinds of Securities (Not Layers). [5]
Constraints on employing conventional security solutions. Attack Surfaces & Device, Communication, Service Vulnerabilities. [7]

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

RIOT, FreeRTOS, Zephyr, Mbed OS, Contiki, TinyOS

Windows, Linux, Android are not in the list, because they not MCU-based. Also good Overview of Operating Systems. [13]
Another good Overview of Operating Systems. [11]
General informations about various OSes. [9]

E. Comparison of Selected Operating Systems

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

Use cases and characteristics of multiple OSes. [9]

Scheduling on different OSes. Also Networking, Memory Management. [9]

Overview of OSes and from into RTOS. Figure 3 gives a good overview over the different OSes/Groups. Also includes complete comparison chart for (probably all) different OSes. [10]

III. Security Requirements & Principles for IoT Operating Systems

"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

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

OS Comparison Table could also help here. [10]

A. Known Vulnerabilities and Historical Attacks

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

B. 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

"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...

Hardware & Cost may not be a bottleneck of IoT Security. [5]

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

Trusted Execution Environment: TrustZone. [8]

List of Trusted Execution Environments. How to still get around TEE. [3]

Capabilities, Applications of TEEs (also TrustZone). Exploits in TrustZone [12]

D. Recent Trends in Research

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

Features for code protection of isolation. [3]

Countermeasures for software-based, architecture-based, memory protection. [12]

Solutions to various security layers like hardware, system/firmware, network, data. [5]

Research Directions of RTOSs for IoT. [6]

VI. Conclusion & Outlook

A. Summary of Insights

B. Future Developments in IoT OS Security

Possible Solutions for Architectural and ISA Issues, Privilege Separation, Memory Corruption, Code Disclosure, Memory-Safe Programming, Firmware Updates & Future Directions [1]

More Examples for future Work. [11]

Available Solutions to mitigate IoT threats. (Table 6) [7]

C. Open Questions & Ongoing Challenges

Open Challenges for TEEs. [12]

Open Challenges for IoT Devices. [4]

Open Challenges in general IoT Security. [7]

REFERENCES

[1] X. Tan and Z. Ma, "SoK: Where's the "up"?! A Comprehensive (bottom-up) Study on the Security of Arm Cortex-M Systems."

[2] A. Fournaris, L. Pocero Fraile, and O. Koufopavlou, "Exploiting Hardware Vulnerabilities to Attack Embedded System Devices: A Survey of Potent Microarchitectural Attacks," *Electronics*, vol. 6, no. 3, p. 52, Jul. 2017.

[3] M. Bognar, C. Magnus, F. Piessens, and J. V. Bulck, "Intellectual Property Exposure: Subverting and Securing Intellectual Property Encapsulation in Texas Instruments Microcontrollers."

[4] M. Aziz Al Kabir, W. Elmedany, and M. S. Sharif, "Securing IoT Devices Against Emerging Security Threats: Challenges and Mitigation Techniques," *Journal of Cyber Security Technology*, vol. 7, no. 4, pp. 199–223, Oct. 2023.

[5] B. Pearson, L. Luo, Y. Zhang, R. Dey, Z. Ling, M. Bassiouni, and X. Fu, "On Misconception of Hardware and Cost in IoT Security and Privacy," in *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*. Shanghai, China: IEEE, May 2019, pp. 1–7.

[6] M. H. A. Abdelsamea, M. Zorkany, and N. Abdelkader, "Real time operating systems for the internet of things, vision, architecture and research directions," in *2016 World Symposium on Computer Applications & Research (WSCAR)*. Cairo, Egypt: IEEE, Mar. 2016, pp. 72–77.

[7] M. Hossain, G. Kayas, R. Hasan, A. Skjellum, S. Noor, and S. M. R. Islam, "A Holistic Analysis of Internet of Things (IoT) Security: Principles, Practices, and New Perspectives," *Future Internet*, vol. 16, no. 2, p. 40, Jan. 2024.

[8] B. Ngabonziza, D. Martin, A. Bailey, H. Cho, and S. Martin, "TrustZone Explained: Architectural Features and Use Cases," in *2016 IEEE 2nd International Conference on Collaboration and Internet Computing (CIC)*. Pittsburgh, PA, USA: IEEE, Nov. 2016, pp. 445–451.

[9] F. Javed, M. K. Afzal, M. Sharif, and B.-S. Kim, "Internet of Things (IoT) Operating Systems Support, Networking Technologies, Applications, and Challenges: A Comparative Review," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 2062–2100, 2018.

[10] T. B. Chandra, P. Verma, and A. K. Dwivedi, "Operating Systems for Internet of Things: A Comparative Study," in *Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies*. Udaipur India: ACM, Mar. 2016, pp. 1–6.

[11] A. Al-Boghdady, K. Wassif, and M. El-Ramly, "The Presence, Trends, and Causes of Security Vulnerabilities in Operating Systems of IoT's Low-End Devices," *Sensors*, vol. 21, no. 7, p. 2329, Mar. 2021.

[12] A. Muñoz, R. Ríos, R. Román, and J. López, "A survey on the (in)security of trusted execution environments," *Computers & Security*, vol. 129, p. 103180, Jun. 2023.

[13] A. Antony and S. S., "A Review on IoT Operating Systems," *International Journal of Computer Applications*, vol. 176, no. 24, pp. 33–40, May 2020.

[14] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," in *2015 IEEE Symposium on Computers and Communication (ISCC)*. Larnaca: IEEE, Jul. 2015, pp. 180–187.

[15] E. Baccelli, C. Gundogan, O. Hahm, P. Kietzmann, M. S. Lenders, H. Petersen, K. Schleiser, T. C. Schmidt, and M. Wahlisch, "RIOT: An open source operating system for low-end embedded devices in the IoT," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 4428–4440, Dec. 2018.

[16] S. Deep, X. Zheng, A. Jolfaei, D. Yu, P. Ostovari, and A. Kashif Bashir, "A survey of security and privacy issues in the internet of things from the layered context," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 6, p. e3935, Jun. 2022.

[17] C. Gao, L. Luo, Y. Zhang, B. Pearson, and X. Fu, "Microcontroller Based IoT System Firmware Security: Case Studies," in *2019 IEEE International Conference on Industrial Internet (ICII)*. Orlando, FL, USA: IEEE, Nov. 2019, pp. 200–209.

[18] A. Jawad, "A survey of the security challenges and requirements for IoT operating systems," Oct. 2023.

[19] D. Strobel, D. Oswald, B. Richter, F. Schellenberg, and C. Paar, "Microcontrollers as (In)Security Devices for Pervasive Computing Applications," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1157–1173, Aug. 2014.

[20] Z. Sun, B. Feng, L. Lu, and S. Jha, "OAT: Attesting operation integrity of embedded devices," in *2020 IEEE Symposium on Security and Privacy (SP)*. San Francisco, CA, USA: IEEE, May 2020, pp. 1433–1449.

[21] S. Ul Haq, Y. Singh, A. Sharma, R. Gupta, and D. Gupta, "A survey on IoT & embedded device firmware security: Architecture, extraction techniques, and vulnerability analysis frameworks," *Discover Internet of Things*, vol. 3, no. 1, p. 17, Oct. 2023.