Implementation of a Trusted Execution Environment (TEE) for RISC-V architecture in the IoT domain

1 Context and Scope of Study

In today's era of the Internet of Things, communicating embedded systems are massively spreading in our everyday lives. These systems contribute to improve our way to communicate in various fields of applications and also respond to recent societal challenges. Unfortunately, these types of system also participate to the increase of the global attack surface of information systems, which represents an unprecedented threat [1].

In order to counteract these security issues, it is therefore essential to guarantee the best level of protection for systems that manipulate sensitive or secret data. These systems generally face many software and hardware threats, due to their high connectivity. In this work, we focus on an application taken from the IoT domain, in which multiple objects can communicate within a network that is managed by a central gateway. A gateway is one of the key element of an IoT infrastructure and usually face constraints like time to market, sharing of cost due to hardware platforms (energy, hardware maintenance and exploitation) between customers. In such devices, adaptability and flexibility are additional interesting features to provide customers with the capability of deploying new services closed to constrained networks and to offer edge computing.

Gateways are also concerned by the management of devices' lifetime and guarantee run-time services with updates. In the future, they will undoubtedly host several customers, each requiring security and efficiency to implement their own services and protocols. In this context, a gateway will be expected to offer strong isolation between customers, reconfigurability for update, bug fixing, customers' waveforms implementation and computation power at the edge.

2 Objectives

The main objective of this thesis is to deal with gateways' security aspects by proposing flexible and secure mechanisms that provide protection and trust to customers in the context of edge computing. The work will be based on mechanisms that were currently proposed in the lab [2] to rely on an open source solution allowing audit. Moreover, another objective of the project is that the proposed software mechanisms (embedded libraries) will be easily implemented in various hypervisors, operating systems and applications.

Finally, we aim to develop a secure reconfigurable gateway allowing customers to have their exclusive environment in which they can run their own services, use/share wireless connectivity and use/share hardware security accelerators. The flexibility and security offered to customers will be implemented on a hardware platform featuring RISC-V processors that will support the Trusted Execution Environment (like in [3], for example). The target architecture is depicted in Figure 1. In this architecture, the software mechanisms will mainly be implemented in the TEE-monitor but also on hypervisors, eOS as well as in hardware in the eFPGA.

For the PhD working phase, we identified several issues to be treated jointly and identified three main scientific challenges.

1. Application isolation mechanisms under strigent power and performance constraints;
2. Secure reconfigurability for on-demand services and update requirements;

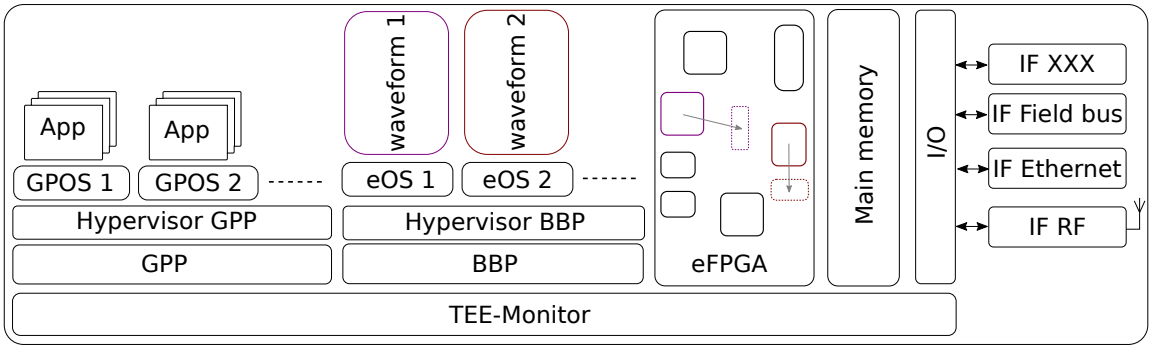

Figure 1: IoT Gateway as a Service for connectivity and edge computing

3. Secure I/Os sharing and hardware accelerators sharing for performance purposes.

The first scientific challenge is linked to the security mechanisms that should be implemented beside the TEE in order to enforce isolation mechanisms and trust since the attack surface is important. We propose here to build software and hardware mechanisms to be integrated in the TEE to guarantee security properties at low level. The second scientific challenge is related to run-time adaptability of the gateway. Secure reconfigurability for customers regarding on-demand services and update requirements will have to be designed. The third scientific challenge consists in providing solutions to guarantee secure I/Os and hardware accelerators sharing. A secure hardware IOMMU will have to be developed with dedicated architectural features to build a trusted hardware platform.

3 Pre-requisite

A good knowledge in C programming, hardware architecture is required. Furthermore, the candidate should ideally be familiar with Hardware Description Languages and reconfigurable devices such as FPGAs.

4 Contact and Organization

The thesis will take place at IETR (https://www.ietr.fr)
20 av. Des buttes de Coësmes, 35043 Rennes Cedex on the site of the "INSA de Rennes" (https://www.insa-rennes.fr)

Several theses have already been led at IETR in the domain of embedded computing and reconfigurable systems [4], [2], [5] for many years. Some of these theses were performed thanks to the CSC program. Researchers involved on this subject have already developed original and efficient algorithms to manage embedded platforms in real-time.

Jean-Christophe Prévotet (Full-Professor INSA-Rennes)

jean-christophe.prevotet@insa-rennes.fr

References

[1] H. Belhadj Amor and C. Bernier, "Software-hardware co-design of multi-standard digital baseband processor for iot," in *Design, Automation Test in Europe Conference Exhibition (DATE)*, 2019.

[2] T. Xia, Y. Tian, J. C. Prévotet, and F. NOUVEL, "Ker-ONE: A new hypervisor managing FPGA reconfigurable accelerators," *Journal of Systems Architecture*, vol. 98, no. May, pp. 453–467, 2019. [Online]. Available: https://doi.org/10.1016/j.sysarc.2019.05.003

[3] R. Bahmani, F. Brasser, G. Dessouky, P. Jauernig, M. Klimmek, A. R. Sadeghi, and E. Stapf, "CURE: A security architecture with customizable and resilient enclaves," in *Proceedings of the 30th USENIX Security Symposium*, 2021, pp. 1073–1090.

[4] Y. Tian, J. C. Prevotet, and F. Nouvel, "Efficient OS hardware accelerators preemption management in FPGA," in *Proceedings - 2019 International Conference on Field-Programmable Technology, ICFPT 2019*, vol. 2019-Decem, 2019, pp. 367–370.

[5] M. Al-Fadl Rihani, "Applying Partial Reconfiguration Technique on ARM-FPGA Systems in Context of Vertical Handover in Wireless Heterogeneous Networks," in *International Journal of Digital Information and Wireless Communications*, vol. 8, no. 1, 2018, pp. 70–74.