Postdoc offer: Edge Security through Reconfigurable Gateways for Customers Isolation

Laboratory: IETR[1]; Lab-STICC[2]
Project leader: Jean-Christophe Prévotet (IETR ASIC Team)
Participants: Jean-Christophe Prevotet (IETR), Philippe Tanguy (Lab-STICC).
Keywords: Hypervisors, Virtualization, Hardware architecture, IoT, Reconfiguration, FPGA
Duration: 24 months

Context

The concept of ubiquitous system will have a strong and sustained deployment through the paradigms of Internet of Things (IoT) or Cyber-Physical Systems (CPS) for the industry of the future. The IoT paradigm is based on an architecture which is generally composed by endpoint devices, one or several gateways (GWs) and a server which gathers and processes data. In this context, we propose to address the challenge of edge security in IoT gateways.

GWs are one of the key elements of an IoT infrastructure and are usually facing constraints like time-to-market, sharing of cost due to hardware platforms (energy, hardware maintenance and exploitation) between customers. In such systems, 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. GWs 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 GW will be expected to offer strong isolation between customers, reconfigurability for update, bug fixing, customers'waveforms implementation and computation power at the edge. Building such new GWs is very challenging and we propose to apply virtualization concepts to meet these requirements.

Virtualization is a promising solution for a Gateway as a Service (GaaS) provider since it allows different isolated applications or OSes to be hosted on the same device. Generally, a guest OS runs in a secure isolated virtual machine (VM), which is a virtual model of a real computer system. A Virtual Machine Monitor (VMM) or hypervisor constitutes the interface to the guest OS and fully controls available resources [1]. In conventional para-virtualization approaches that are often implemented in small embedded devices, a guest OS is normally equipped with a virtualization patch to interact with the VMM, which requires the OS source code to be available [2]. As a consequence, the majority of currently-supported embedded OSs are limited to several widely-distributed open-source OSs, such as embedded Linux and μC/OS-II [3],[4]. Further variants of these OSs are developed to deal with various para-virtualization techniques. One possible para-virtualization solution is to use a micro-kernel, which is a small trust-computing-base set of features defined as address space, threads and inter-process communication (see [5]). In this context, the Ker-ONE hypervisor has been designed to target very small embedded devices with a low memory footprint and low resources while featuring a small amount of lines of code. Ker-ONE has been developed at IETR and constitutes the foundation for this project. The work will use Ker-ONE to rely on an open source solution allowing audit but the main objective is to contribute to the development of security aspects in order to propose a flexible secure gateway to bring protection and trust to customers in the context of edge computing.

Challenges

In order to readch our goal, several challenges need to be addressed. We propose a use-case with applications related to edge computing and applications managing I/O with IoT protocols such as LoRaWAN, bluetooth, etc. We aim to develop a secure reconfigurable GW allowing customers to have their exclusive environment, where they can run their own services and waveforms.

[1] https://https://www.ietr.fr/, UMR CNRS 6164, Rennes, Brittany, France
[2] https://www.labsticc.fr/en/index/, UMR CNRS 6285, Lorient, Brittany, France

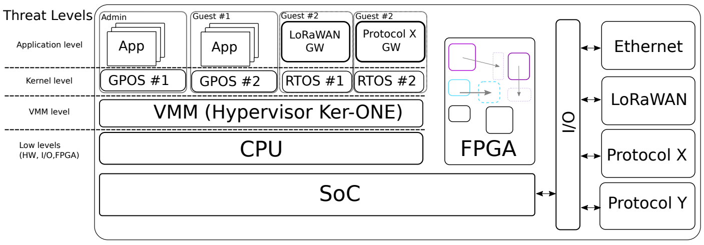

Figure 1: IoT Gateway as a Service for connectivity and edge computing

Figure 1 describes our use-case with threat levels. For the Post doc working phase, we identified several issues to be treated jointly and identified three main scientific challenges.

(C1) Guest OS isolation mechanisms under stringent power and performance constraints;

(C2) Secure reconfigurability for on-demand services and update requirements;

(C3) Secure I/Os sharing and hardware accelerators sharing for performance purposes.

The first 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 second scientific challenge is linked to the security mechanisms that should be implemented beside the hypervisor in order to enforce isolation mechanisms and trust. As seen in [6] the attack surface is important. Here, it is about designing the software mechanisms and hardware to be integrated within the hypervisor in order to guarantee security properties at low levels. The third scientific challenge consists in designing software and hardware mechanisms 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. Our hypervisor will be extended as a demonstrator to address these challenges but all concepts are expected to be generic and implemented in other light-weight hypervisors.

References

[1] Gerald J Popek and Robert P Goldberg. Formal requirements for virtualizable third generation architectures. *Communications of the ACM*, 17(7):412–421, 1974.

[2] Niels Penneman, Danielius Kudinskas, Alasdair Rawsthorne, Bjorn De Sutter, and Koen De Bosschere. Formal virtualization requirements for the arm architecture. *Journal of Systems Architecture*, 59(3):144–154, 2013.

[3] Lei Xu, Zonghui Wang, and Wenzhi Chen. The study and evaluation of arm-based mobile virtualization. *International Journal of Distributed Sensor Networks*, 2015:1–10, 2014.

[4] Seehwan Yoo and Chuck Yoo. Real-time scheduling for xen-arm virtual machines. *Mobile Computing, IEEE Transactions on*, 13(8):1857–1867, 2014.

[5] Jochen Liedtke. *On micro-kernel construction*, volume 29. ACM, 1995.

[6] Daniele Sgandurra and Emil Lupu. Evolution of Attacks, Threat Models, and Solutions for Virtualized Systems. *ACM Computing Surveys*, 48(3):1–38, February 2016.

Candidate Skills

- PhD
- Key skills
  - Hypervisors/Virtualization
  - Architecture of processors
  - C Language, Assembly
  - HDLs
- Other skills (appreciated)
  - Security in Embedded Systems

Contact

Ass. Prof. Philippe Tanguy, Labsticc, UBS
philippe.tanguy@univ-ubs.fr;

Prof. Jean-Christophe Prévotet, IETR, INSA de Rennes
jean-christophe.prevotet@insa-rennes.fr

Apply

Email to P. Tanguy/J.-C. Prévotet with

- a motivation letter and full academic CV (publication list, ...)

Deadline : as soon as possible (hard deadline mid-June)

Eligibility : applicants must have spent at least 18 months abroad between 1st May 2020 and the start date of the project in order to be eligible. Other comment : PhD students who will soon finish in the coming months can also apply.