Postdoc Offer: Edge security through enhanced IoT reconfigurable gateway for customers isolation

Laboratory :

— Lab-STICC [1], UMR CNRS 6285, Lorient, Brittany, France

— IETR [2], UMR CNRS 6164, Rennes, Brittany, France

Keywords : Hypervisor, Cybersecurity, Hardware architecture, IoT, Update, Reconfiguration, Isolation
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 a networked architecture which is generally composed by endpoint devices, one or several gateways (GWs) and a server which gather and process data. In this context, we propose to address the challenge of edge security with IoT gateway.

A GW is one of the key element of an IoT infrastructure in charge of managing constrained network, to forward data to cloud server, to process data at the edge. GWs are also concerned by usual needs like time to market, sharing of cost due to hardware platforms (energy, hardware maintenance and exploitation) between customers. Similar requirements are taking into account by the ETSI with the Multi-access Edge Computing (MEC) initiative Industry Specification Group of ETSI [1] and researchers in the area of mobile communication [2]. The adaptability and flexibility of a system is another interesting requirement to offer customers the capability to deploy new services closed to constrained networks and to offer edge computing. GWs are also concerned by the management of the device lifetime and runtime services with updates. A GW will host several customers, each requiring security and efficiency to implement their own services and protocols. The GW will be expected to offer strong isolation between customers, reconfigurablity for update, bug fixing and customers' waveforms and computation power to perform edge computing. Building such a GW is challenging and will rely on virtualization.

Virtualization of embedded systems is a promising solution to bring all these needs for a provider of a Gateway as a Service (GaaS). Virtualization makes it possible to host different guest operating systems on the same machine. 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) also called hypervisor constitutes the interface to the guest OS and fully controls available resources [3].

In conventional para-virtualization approaches, a guest OS is normally equipped with a virtualization patch to interact with the VMM, which requires the OS source code to be available [4]. 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 [5],[6]. 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 [7]).

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 target 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, MQTT, ... 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://www.labsticc.fr/en/index/
2. https://https://www.ietr.fr/

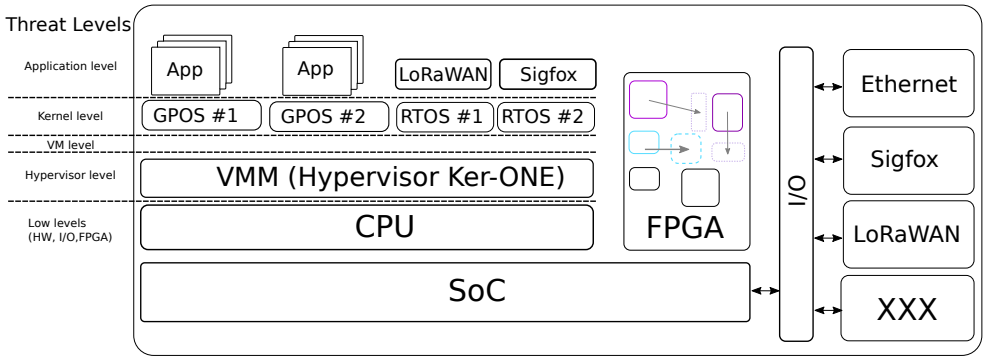

FIGURE 1 – IoT gateway as a service for connectivity and edge computing

Fig. 1 describes our use-case with threat levels as described in [8]. In this example two constrained networks (LoRAWAN and Sigfox) bringing connectivity to end-devices are seeing as a service. And two customers are deployed exploiting data from constrained network and doing edge computing.

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

(C1) Guest OS isolation mechanisms under 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 [8] 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 is designing software and hardware mechanisms to guarantee Secure I/Os and hardware accelerators sharing. A secure hardware MMU will have to be developed with dedicated architectural features to build a trusted hardware platform.

Ker-ONE hypervisor will be extended as a demonstrator to address these challenges but all concepts are expected to be generic to be implemented in other light-weight hypervisors targeting security for reconfigurable gateways.

Références

[1] Multi-access edge computing (MEC). `https://www.etsi.org/technologies/multi-access-edge-computing`. Accessed : 2020-05-27.

[2] Y. Mao, C. You, J. Zhang, K. Huang, and K. B. Letaief. A survey on mobile edge computing : The communication perspective. *IEEE Communications Surveys Tutorials*, 19(4) :2322–2358, 2017.

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

[4] 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.

[5] 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.

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

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

[8] 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 :
  - Hypervision/Virtualization
  - architecture of processors
  - C, assembler
- Other skills (appreciated) :
  - security for embedded systems

Informations

- Supervisor : Jean-Christophe Prevotet
- Co-supervisor : Guy Gogniat
- Co-supervisor : Philippe Tanguy
- Contract : the scholarship is on demand. Obtaining funds is dependent on the outcome of a commission which decides according to the quality of the subject and the proposed candidate.

Apply

Email to Philippe TANGUY with :

- 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 1 May 2017 and the start date of the project in order to be eligible. Other comment : a PhD student who will soon finish in the coming months can also apply.

Contacts

GOGNIAT Guy
✉ guy.gogniat@univ-ubs.fr
☎ +33 (0)2 97 87 46 41
Professor (Professeur des universités)

PREVOTET Jean-Christophe
✉ jean-christophe.prevotet@insa-rennes.fr
☎ +33 (0)2 23 23 84 52
Associate professor (Maître de conférences)

TANGUY Philippe
✉ philippe.tanguy@univ-ubs.fr
☎ +33 (0)2 97 87 45 67
Associate professor (Maître de conférences)