PhD offer:
Contribution to the design of hardware security mechanisms for a secured IoT gateway against wireless attacks

Published on March 24, 2022.

Keywords: Architecture, baseband processor, IoT, Cybersecurity

Context

Embedded system with network communication capabilities appears in critical infrastructures. With IoT networks it is expected a better control and optimization to increase their efficiency, costs and usage. Nevertheless, IoT devices/network increase the attack surface of information system which represents an unprecedented threat [1]. Use cases on top of those infrastructures need to consider cybersecurity threats: software, hardware and network. The figure 1 give an overview of the infrastructure with the threat model considered. End-devices send and receive data from the gateway. Each nodes are using one or several protocols (e.g. LoRaWAN, Bluetooth, etc.). Particularly, the gateway have to support several protocols because in this kind of use case it does not exist a wireless protocol which rule them all [2]. In the PhD thesis, we will consider wireless attacks. Indeed,

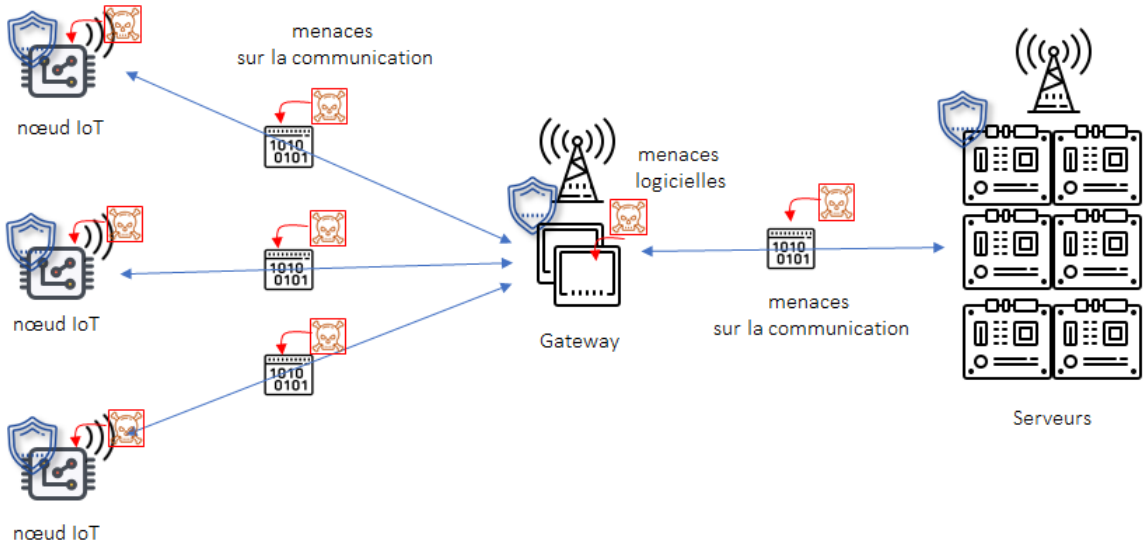

Figure 1: Infrastructure overview of the IoT newtork considered and the associated cybersecurity threats

attackers have now access to low-cost platform to consider the wireless medium as en entry point to compromise a system [**?**, 3] or disturb the network.

This work is supported by the ANR TrustGW project which addresses a growing challenge in the field of IoT infrastructures by proposing an architecture offering a heterogeneous, generic and secure gateway architecture that can host several isolated execution domains accessing shared resources.

Objectives

The PhD thesis deals with the communication part of the gateway and more specially the architecture of the processor which is commonly called baseband processor. The figure 2 shows an overview of the system on chip (SoC) we will consider. We will consider cybersecurity attacks exploiting the wireless network in our threat model. The main objective is to specialize the architecture of the wireless communication unit of the SoC to integrate new security mechanisms to address our threat model. To do that we will explore the RISC-V ISA with dedicated extension to support, increase performances (latence, consommation) and execute securely several waveforms.

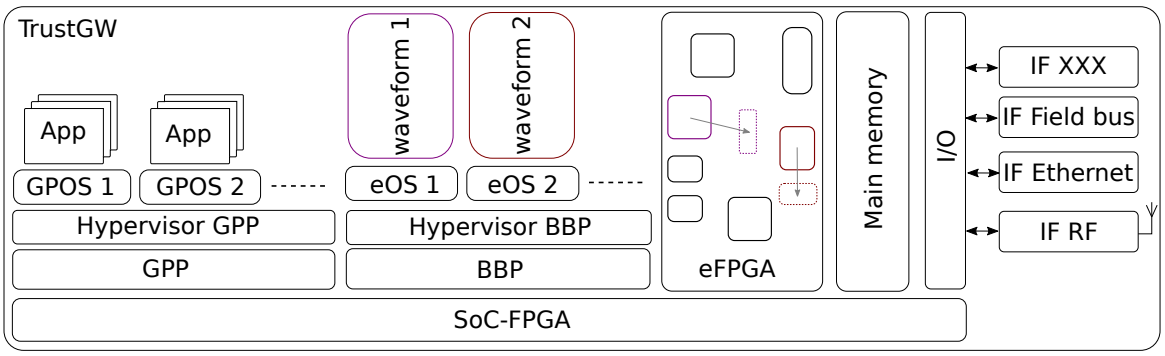

Figure 2: Architecture générale de la gateway. L'architecture est composée d'un processeur applicatif GPP hébergeant plusieurs machines virtuelles (GPOS) déployées par un hyperviseur dédié (hypervisor GPP), d'un processeur bande de base (BBP) hébergeant plusieurs machines virtuelles (eOS) déployées par un hyperviseur dédié (hypervisor BBP) et d'une matrice reconfigurable permettant de déployer des accélérateurs matériels (eFPGA). Comme illustré sur la figure une application est déployée en logiciel et matériel, créant ainsi un espace d'exécution.

Candidate profile

- Master (M2) or equivalent.
- Skills : architecture of processors, HDL (VHDL or other), FPGA
- Other skills (appreciate): digital communication, network protocol, security of embedded systems.

Other informations

- Supervisor: Guy Gogniat
- Co-supervisor: Philippe Tanguy
- Laboratory: Lab-STICC (`https://labsticc.fr/en`)
- Team: ARCAD (`https://labsticc.fr/en/teams/arcad`)
- Location: Lorient
- Start: October 1, 2022
- Duration: 3 years

How to apply

Email to contacts with

- Cover letter and full curriculum vitae
- Complete academic records, from Bachelor to MSc

Applications will be reviewed and processed on a rolling basis until a candidate is selected.

Contacts

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

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

References

[1] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar. A survey on iot security: Application areas, security threats, and solution architectures. *IEEE Access*, 2019.

[2] 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.

[3] Daniel dos Santos, Stanislav Dashevskyi, Jos Wetzels, and Amine Amri. How embedded tcp/ip stacks breed critical vulnerabilities. In *BlackHat Europe*, December 2020.