PhD Offer:
Low-power Software-Defined Baseband Processor for Flexibility and Security

Laboratory : Lab-STICC [1], UMR CNRS 6285, Lorient, Brittany, France
Keywords : Hardware architecture, IoT, Low-power, Cybersecurity

Abstract

The concept of ubiquitous system will have a real application and an effective deployment through the paradigms of Internet of Things (IoT) or Cyber-Physical Systems (CPS) for the industry of the future. Nevertheless securing IoT devices is a challenging task which will be in the future one of the key elements allowing to make the difference in a competitive market and especially to build services acceptable to users for which data protection corresponds to a fundamental issue. The lifecycle of a device is also an important concern regarding updates & sustainability.

In this context, we propose to address the challenge of cybersecurity specifically at the level of the baseband processor which is part of the communication unit of an IoT device. Indeed, the threat model is changing due to the rise of Software-Defined Radio (SDR), the appearance of low-cost high-performance platforms and associated software that offer cybercriminals a much easier access to the lower layers of communication networks. In addition, the security flaws in algorithms or protocols at the level of communications have and will have a strong economic impact as for example recently with the update of Orange network security for the GSM part (flaw GSM protocol A5/1) [1]. It is a problem to be addressed from conception and which takes all the more important if forecasts of millions objects that should operate on battery for long time (more than 10 years) are realized.

The proposed project aims to integrate the cybersecurity threat from the design phase of architectures running software-defined waveforms used in IoT devices with low resources. For this, the objectives are flexibility and the integration of software updates mechanisms while considering low-power consumption and security (e.g. authentication and confidentiality) constraints. It is about developing a flexible, reconfigurable, durable and secured architecture under very low-power consumption constraints (lower than mW) in order to meet the challenges of future connected devices. The proposed work will use the architecture of the RISC-V processor to rely on a very active community, contributing to the development of an open solution and above all to allow an audit.

Context

IoT devices are growing and they have an important attack surface. One of the potential entry point concerns their communication capabilities. Indeed the threat model regarding digital communication is changing [2] due to the rise of Software-Defined Radio, the development of low-cost high-performance platforms and associated software that allow cybercriminals a much easier access to the lower layers of communication networks. Thus, security breaches on communication-level algorithms or protocols have and will have an impact. Similarly, updating the LoRaWAN standard to improve the security (upgrade in v1.1) shows that the ability to upgrade protocols is mandatory. This is a problem that must be addressed from the design point of view. And the problem becomes more important with the forecasts of massive IoT where devices should work on battery for long periods of time (greater than 10 years).

Software-Defined Radio is a concept that could offer flexibility. These last years SDR has been studied and applied where ultimately hardware architectures and resources were not necessarily a strong constraint. In the context of constrained IoT, the execution of a software-defined waveform becomes more challenging. This is why currently the communication part of a communicating device is generally separated and linked by an I2C or SPI bus to the SoC executing the application part. However, recently an industrial solution integrating the radio part within a SoC with the Texas Instrument CC1352R goes in the direction of the execution of several waveforms on the same architecture (Cortex M0). Moreover, recently [3] proposed extending the RISC-V instruction set for the LoRaWAN protocol. Chen *et al.* [4] propose a specific architecture allowing software-defined waveform execution for IoT.

1. `https://www.labsticc.fr/en/index/`

Other solutions as the work done by Roux *et al.* [5, 6] where authors share the observation of the need for protection for the IoT base their solution on spectrum-level logs to extract behaviors or see attempts of connections exploiting potential vulnerabilities on radio protocols. Their approach is based on adding an Intrusion Detection System (IDS) at the network core level which uses machine learning techniques to classify flows using PHY layer metrics from probes positioned in the network. Their IDS is original because it processes information at the physical layer which makes it independent of layers encountered in the IoT. However, in their work they apply this concept by adding probes and a dedicated Intrusion Detection System node which adds complexity to the deployment. Indeed, their working hypothesis is that due to the strong constraints in connected devices it is not possible to add security/protection mechanisms into a device.

Our approach aims to remove this constraint and add these features of security/protection at each node to make surveillance and protection more robust. To address this lock we think the flexibility of an IoT SDR will allow the addition of software code for supervision and protection inside a node.

Challenges

As part of this work, two issues will be addressed. The first issue deals with the definition of a hardware architecture based on RISC-V processor for applying a software-defined waveform in a context of very low-power consumption in order to meet the challenges of IoT in terms of energy efficiency. The second issue deals with integration into the design of protection mechanisms in the baseband processor on the one hand to protect the system and the data handled and on the other hand to guarantee a secure update of a software waveform. These include guaranteeing versioning, authentication, confidentiality and integrity of data. For this second challenge we can in particular rely on some previous work carried out in Michael Grand's PhD thesis [7, 8].

From these two issues to be treated jointly, we identified two main scientific challenges. The first challenge is linked to the definition of a low-power architecture allowing to run several waveforms in the Sub-Ghz bands for the IoT. The second scientific challenge is linked to the security mechanisms that should be implemented in the baseband processor. It is about imagining the software mechanisms and hardware to be integrated with processor and memory in order to guarantee security properties.

According to the answers given by this research, the development prospects for a supervision within a baseband processor could be considered in order to expand the threats model to the detection and protection of radio attacks aiming at exploiting protocols vulnerabilities or with strategies targeting the battery lifetime. The idea would be to propose inside a communication node a solution inspired from an Intrusion Detection System. Finally, it would also target to implement security techniques exploiting the physical layer (PHY secrecy, fingerprinting, etc.)

Scientific program

Firstly, we propose to study baseband processors for the use of protocols in the Sub-bands GHz available in the scientific literature. This analysis will allow us to consider improvements and to propose techniques whose main objective will be the trade-off between more flexibility and low-power consumption. An architectural solution around the extension of the instruction set of a RISC-V processor for a software-defined waveform dedicated to protocols in bands of Sub-GHz frequency is targeted. Regarding sustainability, which is part of a problem of sobriety (energy and resource consumption which are also essential in the deployment of IoT), the flexibility that a SDR radio can bring by allowing scalability of applications and extending the hardware life cycle is an essential point that will be addressed.

Secondly, we will study how adding protection mechanisms to the design in order to obtain the secure realization of these waveforms, intrusion detection and secure update mechanisms. There exists a fairly rich literature in this area, one should study how to integrate these protection mechanisms into each IoT node with resource constraints and very low-power consumption.

Although these two steps are presented sequentially here, the definition of an SDR architecture will integrate the security dimension from the design phase in order to especially take into account potential security vulnerabilities at the architectural level.

Candidat skills

- Master degree or equivalent.
- Key skills :
  - architecture of processors
  - VHDL, FPGA
  - C, assembler

— Other skills (appreciated) :
  — security for embedded systems
  — network protocols, digital communication

Informations

— Supervisor : Guy GOGNIAT
— Co-supervisor : Philippe TANGUY
— Co-supervisor : Jean-Philippe DELAHAYE
— Laboratory : Lab-STICC (`https://www.labsticc.fr/en/index/`)
— Research team : MOCS (`https://www.labsticc.fr/en/teams/m-10-mocs.htm`)
— Location : Lorient
— Starting date : October 2020 (3 ans)
— Doctoral school : MathSTIC (`https://ed-mathstic.u-bretagneloire.fr/`)

Candidature

Email to Philippe TANGUY with :
— Motivation letter and full CV (student projects, ...)
— Complete academic records (MSc)
Deadline : as soon as possible

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
Associate professor (Maître de conférences)

Références

[1] Orange : une mise à jour de sécurité sur le réseau 2g bloquera certains téléphones. `https://www.nextinpact.com/news/105316-orange-mise-a-jour-securite-sur-reseau-2g-bloquera-certains-telephones.htm`. Accessed : 2020-29-01.

[2] Chaouki Kasmi. De la radio matérielle à la radio logicielle : impact sur l'étude de la sécurité des réseaux sans l. page 17.

[3] Hela Belhadj Amor and Carolynn Bernier. Software-Hardware Co-Design of Multi-Standard Digital Baseband Processor for IoT. In *Design, Automation and Test in Europe (DATE)*, Florence, Italy, March 2019.

[4] Y. Chen, S. Lu, H. Kim, D. Blaauw, R. G. Dreslinski, and T. Mudge. A low power software-defined-radio baseband processor for the internet of things. In *2016 IEEE International Symposium on High Performance Computer Architecture (HPCA)*, pages 40–51, March 2016.

[5] J. Roux, É. Alata, G. Auriol, V. Nicomette, and M. Kâaniche. Toward an intrusion detection approach for iot based on radio communications profiling. In *2017 13th European Dependable Computing Conference (EDCC)*, pages 147–150, Sep. 2017.

[6] J. Roux, É. Alata, G. Auriol, M. Kaâniche, V. Nicomette, and R. Cayre. Radiot : Radio communications intrusion detection for iot - a protocol independent approach. In *2018 IEEE 17th International Symposium on Network Computing and Applications (NCA)*, pages 1–8, Nov 2018.

[7] Michael Grand, Lilian Bossuet, Bertrand Le Gal, Guy Gogniat, and Dominique Dallet. Design and implementation of a multi-core crypto-processor for software defined radios. In *Proceedings of the 7th International Conference on Reconfigurable Computing : Architectures, Tools and Applications*, ARC'11, page 29–40, Berlin, Heidelberg, 2011. Springer-Verlag.

[8] M. Grand, L. Bossuet, G. Gogniat, B. L. Gal, J. Delahaye, and D. Dallet. A reconfigurable multi-core cryptoprocessor for multi-channel communication systems. In *2011 IEEE International Symposium on Parallel and Distributed Processing Workshops and Phd Forum*, pages 204–211, May 2011.