PhD Position

Trusted Internet-of-Things integration into pervasive applications

Introduction

"Pervasive" means at the same time ubiquitous, ambient, seamless and transparent: it is the extension of software systems into the physical world. Pervasive systems offer sophisticated services to users by relying on smart, communicative, autonomous and diffused objects. Pervasive systems are so melted in the environment that features are accessible seamlessly naturally and unobtrusively. This invisibility makes usages so easy that users are consuming them even without noticing the system. Application domains are gathered to Smart-* (house, building, city, industry…) where sensors, actuators and connected devices interact transparently with the user. The integration between all these IoT devices and the application is done via a dedicated execution platform [Chollet, 2014] (Figure 1), which generally takes the function of gateway and the physical form of a digital-Box.

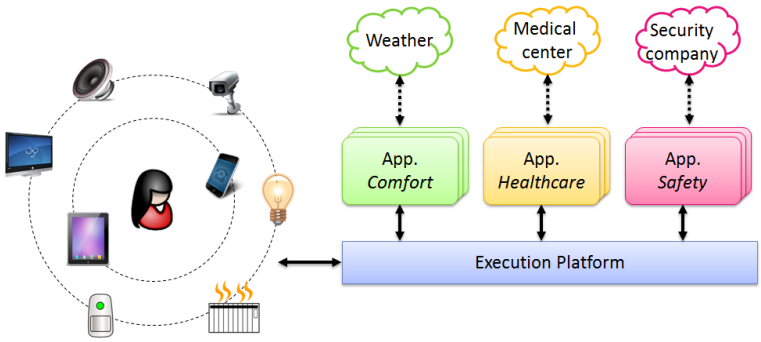

Figure 1 : Pervasive environment.

Research context

The objective of pervasive applications is to be efficient, invisible and to require a minimal amount of user attention. As a consequence device heterogeneity and volatility integration is a prerequisite. With this being said another very important topic is cyber security management (hardware and software). It is for the coming years a main concern of pervasive computing.

- Cyber security shall be managed in a consistent way on the system whole scale.
- It shall be as transparent as possible for devices and users.
- The scaling up of the system must be well managed.

We have already studied and demonstrated solutions based on Public Key Infrastructure (PKI), asymmetric cryptography, keys and certificates, micro vault and secure protocols. They answer to some of the above attributes, but have limitations: they are glutton (CPU, memory and power), they are not easy to use and are generally tagged as a “High-End” solution.

Proposal

We propose to integrate the concept of Physical Unclonable Function (PUF) technologies [Gassend, 2002; Holcomb, 2009] in order to directly have a unique digital identifier into the chip manufacturing process with a very low cost overhead. Another emerging PUF usage is to insure authentication in a communication protocol and even more to astutely replace cryptographic keys. This idea seems very useful and it exists some recent works and publications about it [Braecken, 2018; Barbareschi, 2018]. Nevertheless, most of the works are focusing on the device side and the whole scale integration is not so clear. We want to explore in this thesis the global integration of PUFs in the development of pervasive applications. We are convinced that security must be considered in its entirety: from hardware to software from the design to the runtime. The contribution of the thesis will be to propose, design and evaluate a software solution to secure pervasive applications based on devices integrating PUF.

Contributions

- A smart integration and coexistence of several security models and solutions at the application level.
- A new proposal for a protocol including PUF based mutual authentication for pervasive applications, sensors and actuators.
- The realization of a fully operational demonstrator platform.

Position and laboratory context

- The position is 3-year long, starting October 2019.
- The PhD candidate will be hosted at the LCIS laboratory in Valence (France) and integrated in the CTSYS team (security and safety for embedded, distributed and critical systems).
- The LCIS is a member of the well-known Grenoble-INP institute.
- The PhD will be supervised by Stéphanie CHOLLET, David HELY and Laurent PION (head of chair Trust).
- Chair Trust is a project founded by French companies: Crouzet Innovista sensors, Ingenico group and GRDF. The aim of the project is to develop new technologies and skills within the thematic of digital trust for embedded systems. This project is associated to the Grenoble-INP institute and located at the LCIS laboratory

Eligibility criteria

Candidates must hold a Master's degree (or be about to earn one) or have a university degree equivalent to a European Master's (5-year duration).

Candidates will have to send an application letter in English and attach:

- Their last diploma
- Their CV
- Letters of recommendation are welcome.
- The deadline for applications is May 31st, 2019. Late applications will be considered until the positions are filled.

Skills

- C/C++, Java languages and software engineering are mandatory.
- Hardware and/or software security knowledge and experience will be well appreciated.
- OSGi technology concept and basic knowledge should be a bonus.

We expect an excellent academic track record, including top grades. Good knowledge of cryptography is an advantage, but a lack of such knowledge may be compensated for by a demonstrated ability to learn advanced topics in related areas, such as mathematics, theoretical computer science, statistics or electrical and electronic engineering. Finally, we are looking for a curious and creative mind.

The candidates will have to demonstrate an excellent level of spoken and written English, possess good interpersonal and communication skills, and show the willingness to work as part of an international team.

Contact Person

Stéphanie CHOLLET

50, rue Barthélémy de Laffemas - BP54
26902 VALENCE Cedex 09 - FRANCE
Email: stephanie.chollet@lcis.grenoble-inp.fr

References

[Chollet, 2014] Escoffier, C., Chollet, S., and Lalanda, P. (2014). Lessons learned in building pervasive platforms. In 11th *IEEE Consumer Communications and Networking Conference*, (CCNC) 2014, Las Vegas, NV, USA, January 10-13, 2014, pages 7–12.

[Gassend, 2002] Gassend, B., Clarke, D. E., van Dijk, M., and Devadas, S (2002). Silicon physical random functions In *ACM Conference on Computer and Communications Security* 2002, pages 148—160.

[Holcomb, 2009] Holcomb, D. E., Burleson, W. P., and Fu, K. (2009). Power-Up SRAM State as an Identifying Fingerprint and Source of True Random Numbers. In *IEEE Trans. Computers* 58(9), pages 1198—1210.

[Braecken, 2018] Braeken, A. (2018).PUF Based Authentication Protocol for IoT. In *Symmetry* 10(8): page 352.

[Barbareschi, 2018] Barbareschi, M., De Benedictis, A., and Mazzocca, N. (2018). A PUF-based hardware mutual authentication protocol. In *J. Parallel Distrib. Comput.*, 2018, 119, pages 107—120.