PhD subject:

"Extraction of Fingerprint for Smart Home Authentication"

Supervisor : Jean-Luc Danger †
Co-supervisor : Tarik Graba †
EdF supervisor : Nathalie Rodionoff ‡

† SSH team of the COMELEC department and LTCI laboratory
Institut TELECOM / TELECOM ParisTech
37, rue Dareau – 75014 Paris
({firstname}.{lastname}@telecom-paristech.fr)

‡ EdF R&D
7 Boulevard Gaspard Monge – 91120 Palaiseau
(nathalie.rodionoff@edf.fr)

1 Context

A key aspect of a secure application based on IoT, like Smart Home or Smart Building, is to use robust authentication protocols. This allows the connected objects to identify each other and to make sure a trusted exchange of information can take place afterwards. There are numerous cryptographic protocols, as the digital signatures, to ensure a high level of security an authentication. They require an enrollment stage which allows an element to present his credentials to a trusted server. The credentials generally relies on an identifier specific to the element to authenticate. This identifier depends on an authentication factor which is of 3 types according to NIST [2]:

1. What the element knows: password, serial number, configuration date, pin code...
2. What the element owns: smartphone, memory, CPU, HW blocks, SW code, Cryptographic key,
3. What the element is: some biometric data, its behaviour or some intrinsic feature.

This typology applies to a person able to differentiate a known data from a owned data. For instance a cryptographic key is owned but unknown to the user. The difference is not so clear for an object: a cryptographic key can be considered known by the object. Hence, we can consider that there are only two types of identifiers: the **Data** type and the **Inherent** Type. Generally an object identifier is of type **Data**: a cryptographic key or a random number programmed in a non-volatile memory. But this type of identifier introduces weaknesses:

- the read/write operation in a memory can be tampered,
- the data can be hacked by reverse engineering of the storage element.

On the contrary, an identifier of type **Inherent**, auto-generated by the element itself, needs no configuration phase and no storage. This corresponds to the Physically Unclonable Function (PUF) [1] which can be seen as the fingerprint of the device. When addressing the Smart Home or Smart Building application, we can think about ways to enhance the security level based by taking advantage of the numerous elements composing the system and by mixing up the two types of identifiers. The main identification sources in a Smart Home are:

- Phyical: the connected objects and the communication channels.
- Human: the inhabitants or users.

The combination of different identification sources may be achieved by a multi-modal authentication [3]. Beside the main two type of identifiers **Data** and **Inherent**, these sources can be either static, as the power lines, or dynamic, as they can change over time, like the inhabitant of an apartment, the type of radio network and IoT. The dynamic property involves specific action, as a new enrollment mechanism to register a new object or a new configuration or user.

2 Objectives

Many questions arise about the level of trust of the Smart-Home fingerprint, the main ones are :

1. **What are the reliable identity sources that can be used to build the Smart-Home fingerprint ?** The biometric data from the inhabitants and the installed system offer a first set of identifiers. The ISP router (*internet Box*) PUFs and some information specific to the IoT configuration could be use. Indeed, the system in a house or an apartment is unique as the walls, furnitures, location of IoT objects are hardly reproducible. For instance the communication channel between objects directly depends on the space, nature and topology of the walls and their respective positions. Another identification source comes from a statistical approach based on the system usage, unveiling a specific behaviour of the users. Of course there could be some privacy concern but it will not be taken into account for the study.
2. **How to combine these sources in a trusted manner to create/use a protocol based on the Smart-Home fingerprint ?** The combination of identification data needs specific cryptographic protocols. Many studies have been done on this topic. This work will require to make an overview of the most useful ones to fit the Smart Home fingerprint application. An important property of the Smart-Home is its potential evolution in time, as new owners, new objects or new places for these objects, new routers, involve a different behaviour. All these changes imply an update of the identifiers. If certificates are generated, steps of revocation or certificate updates should be considered, still by keeping a high level of security.

3 Organization

This work is undertaken in collaboration with EdF. Some realistic configurations given by this partner will be used to build a Smart-Home fingerprint.

The PhD candidate main research tasks are the following:

- To **identify the physical sources** of identification. There are two types : the communication channel and the connected devices to the network. The characteristics of the communication channel greatly depends on the topology of the local power grid for poweline communication and the shape of the room for the radio channel. The PUF can be used as source of identification for the device. A state of the art of PUF and communication channel identification is a result of this task.
- To **evaluate the physical sources** of identification. The identifier needs to meet at least the properties of steadiness and uniqueness. Test platforms will be developed to assess these characteristics and conclude about the quality of discrimination and the reliability off the identifiers.
- To **study the human sources** of identification which relies on the activity generated by the users. The frequency and intensity of consumption/communication defines a specific behaviour which can be extracted by machine learning techniques. The EdF database will be used to generate classes of activity. Then they will be evaluated as the static sources in terms of reliability and uniqueness.
- To **study a multi-modal method** to combine the different sources of identification. The objective is to produce a secure, reliable and unique identifier of the Smart Home which is not merely the concatenation of the different sources. The results is a comparison of different algorithmes according to reliabaility, security , unicity and laso agility in order to take into account the dynamic property of some identification sources.
- To **publish the results** by writing scientific papers and the final PhD thesis manuscript.

References

[1] J-L Danger, Sylvain Guilley, Philippe Nguyen, and Olivier Rioul. Pufs: Standardization and evaluation. In *Mobile System Technologies Workshop (MST), 2016*, pages 12–18. IEEE, 2016.

[2] Paul A Grassi, Michael E Garcia, and James L Fenton. Digital identity guidelines. *NIST Special Publication*, 800:63–3, 2017.

[3] Arun Ross and Anil K Jain. Multimodal biometrics: An overview. In *Signal Processing Conference, 2004 12th European*, pages 1221–1224. IEEE, 2004.