Towards a IoT secure Smart Environment System

Pedro Oliveira, Tiago Pedrosa, Paulo Matos
poliveira@ipb.pt, pedrosa@ipb.pt, pmatos@ipb.pt

INSTITUTO POLITÉCNICO DE BRAGANÇA

Introduction

Systems that deal with personal data always bring privacy and security issues. And also the balance of these issues, with the need that persons have in interact with spaces in a transparent way and that those spaces smartly adapt to their preferences.
That said, in this project, is proposed a solution to overcome these issues, and don't compromise the balance between security and personal comfort.
Currently this challenge has as main difficulty, the mobility of people, the disparity of habits, schedules and every individual comfort preferences. The same is aggravated when depending on physiological conditions, derived from a large number of factors (tiredness, mood, etc.), user preferences often suffer significant changes, that current systems can not measure.
Figure 1, shows the scenario of an environment where it intends to develop this work. Explaining this figure, it can be seen the user who through its different devices (smartphone, wearable, and other compatible) communicates with the system, and for that can be used different technologies, like Near Field Communication (NFC) [1], Bluetooth Low Energy (BLE) [2] and Wi-Fi Direct [3]. Next, the system performs communication with the Cloud, to validate the information. And the system will perform the management of the different components in the environment (climatization systems, security systems, other smart systems).

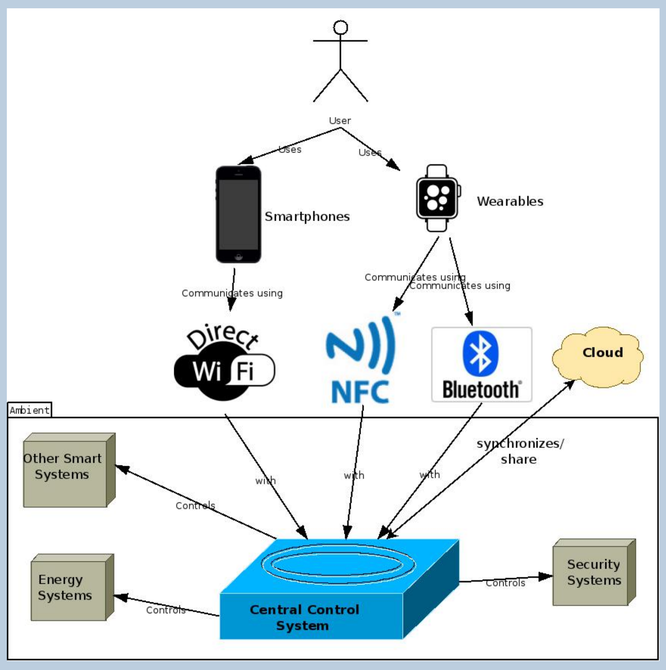

Figure 1: Problem Statement

Conclusion

Currently IoT systems are in a big security risk. Especially because the developers, are not worried enough about the safety of such systems. However, with the growing trend of such systems and is integration in our everyday lives, this concern will have to increase as they start to appear isolated cases which have harmed the users, both financially and in their safety and welfare.
The proposed security architecture, to one of these IoT systems, wants to avoid any of the presented risks, to the users of this system.

For future work, we have identified the need to develop solutions that enable communication between the application and the local system, using different communication technologies without user interaction. Some extra work must be done to overcome this constraint, and get a transparent use solution for every user.

References

[1] Roy Want. Near field communication. *IEEE Pervasive Computing*, (3):4–7, 2011.

[2] SIG Bluetooth. Bluetooth core specification version 4.0. *Specification of the Bluetooth System*, 2010.

[3] Daniel Camps-Mur, Andres Garcia-Saavedra, and Pablo Serrano. Device-to-device communications with wi-fi direct: overview and experimentation. *Wireless Communications, IEEE*, 20(3):96–104, 2013.

[4] Paul J Leach, Michael Mealling, and Rich Salz. A universally unique identifier (uuid) urn namespace. 2005.

[5] Tim Dierks. The transport layer security (tls) protocol version 1.2. 2008.

[6] Doug White and Alan Rea. Server hardening tactics for increased security. Technical report, Working Paper, 2003.

Materials and Methods

The aim of this project is to create a solution that takes advantage of emerging technologies on the market that support wearable devices (e.g. smartwatches, smartphones, fitness trackers) and the non-invasive characteristic of these, for collecting data in an autonomous and transparent way and without any need of intervention by the user. And with that information assist the decision-making process of comfort systems to adapt the environment to suit the comfort preferences of each user (e.g. thermal, acoustic, air quality, lighting, sun exposure).
In figure 2 (right), an example of an environment is illustrated to demonstrate the use cases described above. Note that the communication processes represented in this figure on arrow format is expected to be transparent to the user and completely independent of its intervention.
After the validation in the Cloud of the user ID, the respective preferences card is downloaded into the system, and the control is made automatically by the local system, adjusting all the preferences existing in the environment. In this example, will be adjusted lighting, radiator and air conditioning.
In this project, the user identification, is one of the essential tasks. In a first approach, it is planned that there are two situations, explained below:

- **User ID sharing:** in this situation, when the user enters in the environment, the devices that are with him (smatphone, wearables, etc) pass the user ID to the system that controls the environment. The system, validates the ID in the Cloud, and from this gets the user's preference card. The system will then use the card information received, to adapt the environmental comfort conditions, using the automation available in the environment.

  In this case the system is permanently connected to the Internet, so that is allowed access to the Cloud.

- **User preferences card sharing:** In this case the user when enter the environment, share directly with the system, its preferences card, with the card available in the compatible device (smartphone, wearable, etc.).

  The system collects data from these preferences and adapts, as in the previous case, the environment comfort conditions, using for that purpose the automated systems available in the environment.

  In this case, the system does not require an Internet connection, all the process may be performed offline.

Both situations assume that the user has no part in the process, which is completely transparent to him.
The use case diagram present in figure 2 (left), illustrate the operating modes provided for the implementation of the user detection process, and sharing of his preferences card with the system on the environment.

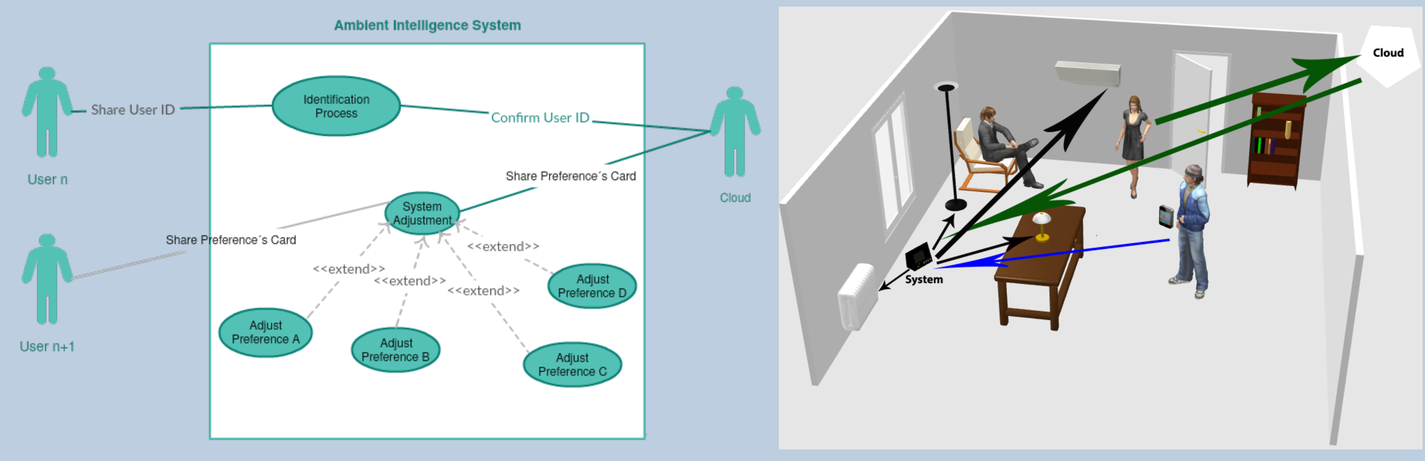

Figure 2: AmI System - Use Case diagram (left); AmI System - Communication process (right)

Results

All attack vectors identified, are minimized using the techniques identified. Consequently increasing significantly the degree of complexity so that an attacker can gain access to useful information, or can link this information to take advantage, or even affect the system users.
To achieve this goal, several mechanisms are designed in order to minimize the possible attack vectors. Figure 3 shows the overall context of the proposed architecture for the system.

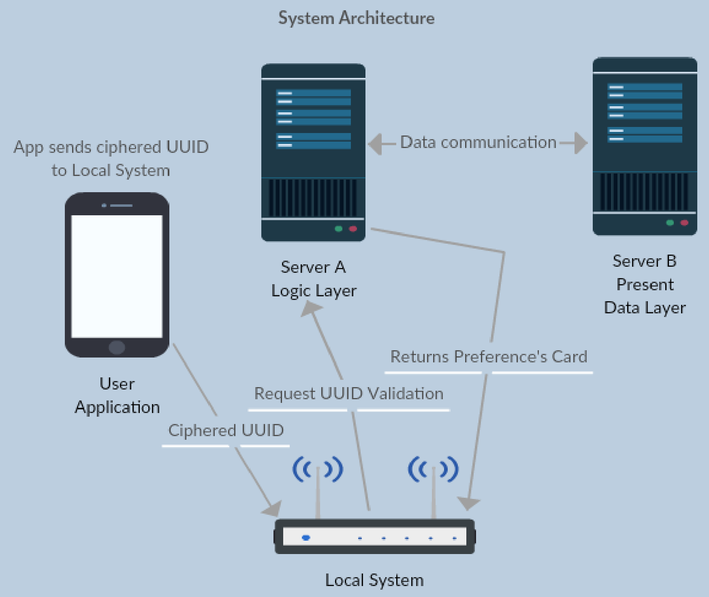

Figure 3: System Architecture System

Use of universally unique identifier (UUID), to identify the user. The user identification process is performed by generating a UUID in the first use of the system application [4].
Servers and component isolation, two physical servers will be used. In order to separate the logic and data layer (database). Therefore possible individual attacks, which enable access to the servers do not compromise the entire system.
Data encryption, all data transmitted between the servers are encrypted using SHA-256 hash mechanisms, which introduces an extra security layer in protection of the data stored in the system [5].
Server hardening, both servers only allow access through key mechanisms. Communication processes will be based on HTTPS and TLS [5][6].
Communication with the local system, the communication between the user's smartphone and local system, can be performed using BLE, NFC or Wi-Fi Direct with their own security mechanisms implemented at the stack level.
Mask of GPS coordinates, for greater safety it is planned to convert the GPS coordinates of the systems.

The implementation of these mechanisms significantly reduce the attack vectors identified. At the data privacy level, we don't store any user information, so even if the data is compromised, will not be possible identify the user.