Towards to secure an IoT Adaptive Environment System

Pedro Oliveira[1],[2], Tiago Pedrosa[2], Paulo Novais[1], and Paulo Matos[2]

[1] Algoritmi Centre/University of Minho, Department of Informatics, Braga, Portugal,
[2] Institute Polytechnic of Bragança, Dep. of Informatics and Communications,
Bragança, Portugal

Abstract. This paper, deals with the actual problem of secure an IoT adaptive system, namely using secure techniques to secure a Smart Environment System, and the privacy of their users. On a new era of interaction between persons and physical spaces, users want that those spaces smartly adapt to their preferences in a transparent way. This work wants to promote a balanced solution between the need of personal information and the user's privacy expectations. We propose a solution based on requiring the minimal information possible, together with techniques to anonymize and disassociate the preferences from the users.

Keywords: adaptive-system, AmI, security, privacy, iot

1 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.

In addition to the physiological conditions mentioned above, there are two critical/essential dimensions, these are the space (user location) and time. In the case of the space can be as an example, the differences between the preferences of a personal, professional, recreational or other environment. Contextualize the user location is essential to optimize the conditions of comfort and contribute to the performance and effectiveness of the solution.

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 then the system will perform the management of the different components in the environment (climatization systems, security systems, other smart systems).

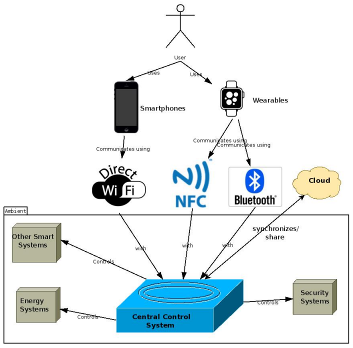

Fig. 1: Problem Statement

2 Materials and Methods

2.1 Security and Privacy

The technological revolution that is felt, particularly in behavioral analysis fields, IoT or big data, brings significant new challenges, including those related to the type of user information that can be collected, and the knowledge that can be obtained derived from the compilation of this information. Although not necessarily existing the user's authority to make this kind of information collection.

This IoT revolution has yet clearly identified problems. In particular, the privacy and security of user data. Foreseeing the dissemination of intelligent spaces, of which the user can, and want to take advantage of the interaction between systems, and the consequent sharing of personal data, this is a theme that needs resolution in a short-term [4].

Obviously at this point there will be the requirements for concessions and commitments on the part of the user.

Because it is understood that the solution will include the user's authority in relation to the autonomous information sharing with the system and what is the information that it believes that it should be shared, block, and in concrete with which systems.

The IoT increases the risk of personal privacy, and the confidentiality and integrity of data in organizations. Some IoT applications for consumers, particularly those related to health and wellness, which store sensitive personal information, and that consumers may not want to share.

Normally, it is known that on latter case, there must be commitments by the user, so it has access to all system capabilities. But it is up to each one, set his own commitment threshold, between privacy and comfort that it intends to have by using the system, in the environments that it uses.

3 Results

All attack vectors identified, are minimized using the techniques identified in this section. 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.

As mentioned in section 2.1, one of the priorities of this project will be ensure privacy and data confidentiality. To achieve this goal, several mechanisms are designed in order to minimize the possible attack vectors.

- **Use of universally unique identifier (UUID)**, to identify the user. The user identification process, it is necessary in this context to relate him to his preferences card, and is performed by generating a UUID in the first use of the system application. This unique UUID is randomly created by the application and is then validated their nonexistence on the server, if the validation is positive, the UUID is associated with the user's preference card. If the validation is not positive is generated a new random UUID and the validation process will be held again.
  The application will allow the user to export the UUID created for his personal email or store it locally in another way, so that if it wants to use more than one device in the system or switch the device, this can be done. Note that only the randomly generated UUID and the preferences card are transmitted to the server, so there was no possibility of identifying the user [5].
- **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 [6].
- **Server hardening**, both servers only allow access through key mechanisms. Communication processes will be based on HTTPS and TLS [6]. Other most common mechanisms for server hardening will be applied [7].
- **Communication with the local system**, as explained above, the communication between the user's smartphone and the local system, can be performed using BLE, NFC or Wi-Fi Direct. These technologies have their own security mechanisms implemented at the stack level, which will be properly configured in the local systems to maximize security. However, the UUID is also ciphered with the server A public key before is sent to the Local System. With that we can guarantee that the UUID can't be captured in clear, and is only known by the smartphone application and the Server A.
- **Mask of GPS coordinates**, even though the user anonymization process is covered, for greater safety and because issues related to the user's location storage are critical. It is planned to convert the GPS coordinates of the local systems. This process is achieved by associating the coordinates to a

randomly and periodically change of the Local System ID. Therefore the user's location information from a system, will be stored using the UUID of the user and the system ID, which due to its periodic change will not relate any information that can allow to achieve the user tracking.

The implementation of these mechanisms allows to significantly reduce the attack vectors identified. At the user data privacy level, this work allowed to don't store any user information. So even if the data is compromised, will not be possible identify the user, or make any relationship with that information.

4 Discussion and Conclusions

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.

Acknowledgements

This work has been supported by COMPETE: POCI-01-0145-FEDER-007043 and FCT Fundação para a Ciência e Tecnologia within the Project Scope: UID/CEC/00319/2013.

References

1. R. Want, "Near field communication," *IEEE Pervasive Computing*, no. 3, pp. 4–7, 2011.
2. S. Bluetooth, "Bluetooth core specification version 4.0," *Specification of the Bluetooth System*, 2010.
3. D. Camps-Mur, A. Garcia-Saavedra, and P. Serrano, "Device-to-device communications with wi-fi direct: overview and experimentation," *Wireless Communications, IEEE*, vol. 20, no. 3, pp. 96–104, 2013.
4. R. Khan, S. U. Khan, R. Zaheer, and S. Khan, "Future internet: the internet of things architecture, possible applications and key challenges," in *Frontiers of Information Technology (FIT), 2012 10th International Conference on.* IEEE, 2012, pp. 257–260.
5. P. J. Leach, M. Mealling, and R. Salz, "A universally unique identifier (uuid) urn namespace," 2005.
6. T. Dierks, "The transport layer security (tls) protocol version 1.2," 2008.
7. D. White and A. Rea, "Server hardening tactics for increased security," Working Paper, Tech. Rep., 2003.