Towards a Personal Data Protection Framework in an IoT environment: Smart Hotel use case

Mohamed-Ayoub Messous, Sabrine Aroua, Laurent Goncalves, Jean-Paul Truong, Remy Abdelwahab

Towards a Personal Data Protection Framework in an IoT environment: Smart Hotel use case

***Ayoub MESSOUS*[1], *Sabrine AROUA*[2], *Laurent Goncalves*[3], *Jean Paul TRUONG*[4], *Remy Abdelwahab*[5]**

[1]*DRIVE EA1859, Univ. Bourgogne Franche Comté, F58000, Nevers France.*

[2] *L3i lab, Univ. of la Rochelle, France.*

[3] *Softeam group, Toulouse, France.*

[4] *Thales Group, Paris, France.*

[5] *NXP Semiconductors, Colombelles, France.*

ayoub.messous@u-bourgogne.fr; sabrine.aroua@univ-lr.fr; laurent.goncalves@softeam.fr;
jean-paul.truong@thalesgroup.com; remy.abdelwahab@nxp.com

Abstract

The tremendous growth of Internet of Things (IoT) related services made the overlapping ecosystem a privileged target for cyber-attacks. The constrained nature for most of IoT devices and their limited resources, in terms of computation, storage, communication and energy, have led to serious vulnerabilities. Thus, addressing the underlying technical and research challenges has become a central focus for many research groups in industry and academia. In this context, the ITEA PARFAIT European R&D project was concocted in order to develop a new framework for cyber-security preserving and personal data protection in IoT environments. The project, mainly, aims to build cross-platform software enablers to support the deployment of seamless security measures and protocols. Therefore, a consortium of eleven leading actors from three different countries, covering industry and academia, are joint together to innovate and generate new state-of-the-art solutions addressing security challenges in the IoT ecosystem. This newsletter explains the main goals for the PARFAIT project, outlines its overall architecture and highlights relevant proposals and contributions.

1. Introduction

Throughout the last decade, the Internet of Things (IoT) paradigm has known a great deal of interest from research groups in academia and industry. It is preserved by many as one of the most prominent and exciting emerging technologies with a great potential to shift our daily life and improve the way we interact with our environment. Specifically, the IoT paradigm enables a wide range of connected smart devices (also known as objects), equipped with sensing, storage, processing and actuation capabilities, to seamlessly communicate and possibly interact with any device through the Internet. Indeed, IoT related technologies hold high the promise of revolutionizing the way we do business and our interactions with our surroundings by offering new opportunities and dimensions for unheard-of services that will greatly develop economies and enhance the quality of life. Some of the underpinned solutions range from home appliances control to personal health monitoring, from automobile engines to transportation systems, from manufacturing systems to smart industry, from electrical generators to smart grids [1]. These promising potentials have risen serious challenges related mainly to scalability and efficiency, handling large data, and security and privacy related issues. Definitely, security aspects in IoT is a crucial concern that requires special focus. It is indeed a major priority for every organization because dealing with compromised IoT systems might expand security costs to 20% of annual security budgets [2].

In one of their worldwide threat assessment statements, the US intelligence community identified IoT as a major source of cyber threats with the potential of jeopardizing data integrity, privacy and services availability [3]. They expressly stated that the deployment of IoT has introduced vulnerabilities into both the infrastructure that they support and on which they rely, as well as the processes they guide. Many research groups are highlighting the ever-evolving nature of cyber threats and complexity of cyber-attacks affecting IoT systems and targeting different layers of its architecture [4]. Compromised IoT systems might have disruptive consequences on personal safety, security and privacy, and even some times life-threatening conditions [5].

Indeed, the open nature of wireless communications, the rise of smart devices, as well as the heterogeneous and dynamic structure of IoT, heighten existing cyber-security issues and introduce a whole new degree of potential threats. Sloppy or not adapted authentication and access control mechanisms for IoT networks represent a serious vulnerability. Many famous cyber-attacks targeting IoT networks have been already documented in the last few years. For instance, a malicious program called Mirai [6] has been developed in 2016 to take control of vulnerable connected objects such as surveillance cameras and routers. This attack fully controlled and turned the compromised devices into a botnet, which has been eventually used to generate massive distributed denial of service attacks (DDoS). Furthermore, in 2017, a malware named BrickerBot has compromised many IoT devices through a brute force attack on the telnet password [7] to destroy their memory and delete their data.

These considerations lead us to focus on the design of new methodologies and mechanisms to mitigate risks and respond to the application requirements in terms of security, privacy, and reliability [8] [9]. To this extent, the ITEA PARFAIT project (2018-2020) [10] has been focusing on the development of end-to-end solutions for personal data protection in different IoT environments. The rest of this newsletter is organised as follow: Details about the ITEA PARFAIT project, its main goals along with a global overview for the project main architecture are presented in Section 2. Whereas, Section 3 provides relevant details regarding one of the two main use cases developed during the project lifetime, namely the Smart Hotel use case, along with the different possible interactions between its underlying components. Section 4 concludes this letter and outlines the main technological directions and milestones.

2. The PARFAIT Project: General description

Interoperability, along with security and privacy of personal data, are the two most important limitations for the growth of the Internet of Things (IoT) market. Interoperability increases the complexity of service production processes and the cost of production. Lack of security and trust for the protection of privacy puts a barrier between service providers and consumers. To address these challenges, the PARFAIT project, which stands for "**P**ersonal d**A**ta p**R**otection **F**r**A**mwork for **I**o**T**" was proposed. It aims to develop a platform for protecting personal data and to reduce the complexity of integrating and deploying services in today's IoT ecosystem by providing interoperable software libraries, tools and SDK elements. The main goals achieved during the project lifespan along with a synoptic representation of the proposed architecture are presented in the following subsections.

2.1. Project's main goals

Our main goal during the PARFAIT project is to develop a platform for protecting personal data in IoT applications which will be tested with 2 main use-cases. Another goal is to decrease complexity of integrating and deploying services in today's IoT technology by providing interoperable software libraries, tools and SDK elements. Indeed, the research and technological barriers, described previously in this letter, directly affect the wide adoption of IoT services in the consumer lifestyle and business applications. Therefore, through finding solutions to the underlying problems and challenges, PARFAIT project aims at offering services with high socio-economic and business potential. The business impact of the project will be generated through an integrated, scalable and extendable privacy and security framework which will be demonstrated through 2 use cases leaded by industrial partners of the project consortium. These use cases are selected as personal information management services in a smart hotel and smart home environment. Instead of restricting the business potential to selected vertical domains, PARFAIT consortium aims at presenting a global privacy and security framework, where various vertical thematic frameworks can be built on. This approach will increase business potential and adoption of project outcomes in a wider market. While presenting a global framework targeting privacy and security in IoT applications, PARFAIT also aims at presenting two ready-to-market vertical domain applications to demonstrate the usage of security and privacy preserving framework and to exploit the results by the end of the project. Through this methodology, the different partners involved are focusing on the establishment of a modular ecosystem around the proposed platform for both application developers and service providers.

Furthermore, in order to achieve this highly picturesque vision, one of the milestones for PARFAIT is to define interoperability and security/privacy methodologies, rules and guidelines to make recommendations for the policy makers. Defined methodologies and policies will be used as the keystones to develop libraries, tools and SDKs which will construct the foundation layer for domain specific IoT service frameworks and connected application ecosystems. With strong ambitions to develop a European originated platform, the PARFAIT project consortium consists of global leaders and pioneers of IoT technology as service providers, application developers, infrastructure providers and academia.

2.2. Project's overall architecture

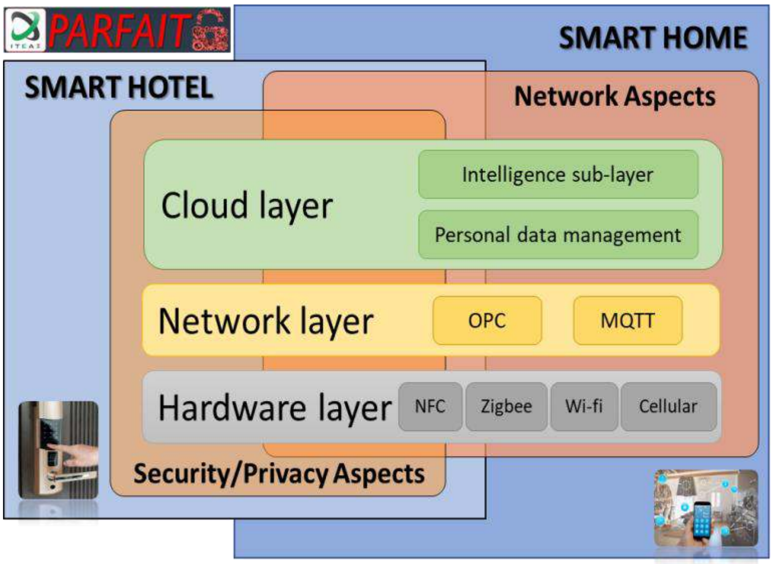

Figure 1: PARFAIT architecture

During the PARFAIT project, the two main use cases considered are the Smart Home and the Smart Hotel use case. Figure 1 provides a general view of the overall architecture along with its main components and possible overlapping between its building blocks. The contributions for each of the partners covers at least one of the components shown in figure 1. Two main features are covered namely: (i) Security& privacy preserving aspects; and (ii) Network management & communications aspects. Furthermore, the overall framework covers three main layers: (i) hardware, (ii) network, and (iii) cloud. First, the hardware layer ensures connectivity to field equipment including IoT sensors and/or controllers through dedicated interfaces. Second, the network layer involves the protocols used in data communication, namely OPC and MQTT communication protocols are both considered respectively for automation process and for IoT message exchanges. A wide range of compatibility communication protocols is also supported and can be easily adopted thanks to the modularity of the proposed architecture. Finally, the cloud layer covers two sub-layers: (i) the intelligence sub-layer is specific for each application, implementing tailor-made analytic functions. Whereas, (ii) the sub-layer dedicated to personal data management handles registration, authentication, encryption and specific access control to the proposed services.

To increase the market access of the proposed solutions, two main use cases have been identified. First, the Smart Home use case focuses on end users/system integrators looking for a plug-and-play, easy to manage solution to increase security in existing or new applications, and solution developers, having the capacity to integrate security and privacy drivers or APIs directly in their products. Second, the Smart Hotel use case aims at providing adaptable cyber security services in order to offer an improve reservation, seamless and secure access to the purchased accommodation. Also, preserving clients' privacy has the outmost importance.

3. Secure deployment of IoT services in Smart Hotels as a use case

This section describes the contributions related to the Smart Hotel demonstrator during the PARFAIT project. An overview for the different components developed in this use case are shown in Figure 2. The main contributions by the different partners cover: secure registration, authentication along with secure data exchanges and privacy preserving for end-users. Nowadays, regular hotels are equipped with electronic locks. Electronic cards used to grand access need to be personalized and initialized for each client, which depends on a human operator. The next generation for these locks is Smart/Connected locks, which are able to interact with the local IT systems and communicate with their environment. The main required building blocks in order to achieve this vision are given throughout the following sections.

3.1. Secure reservation system

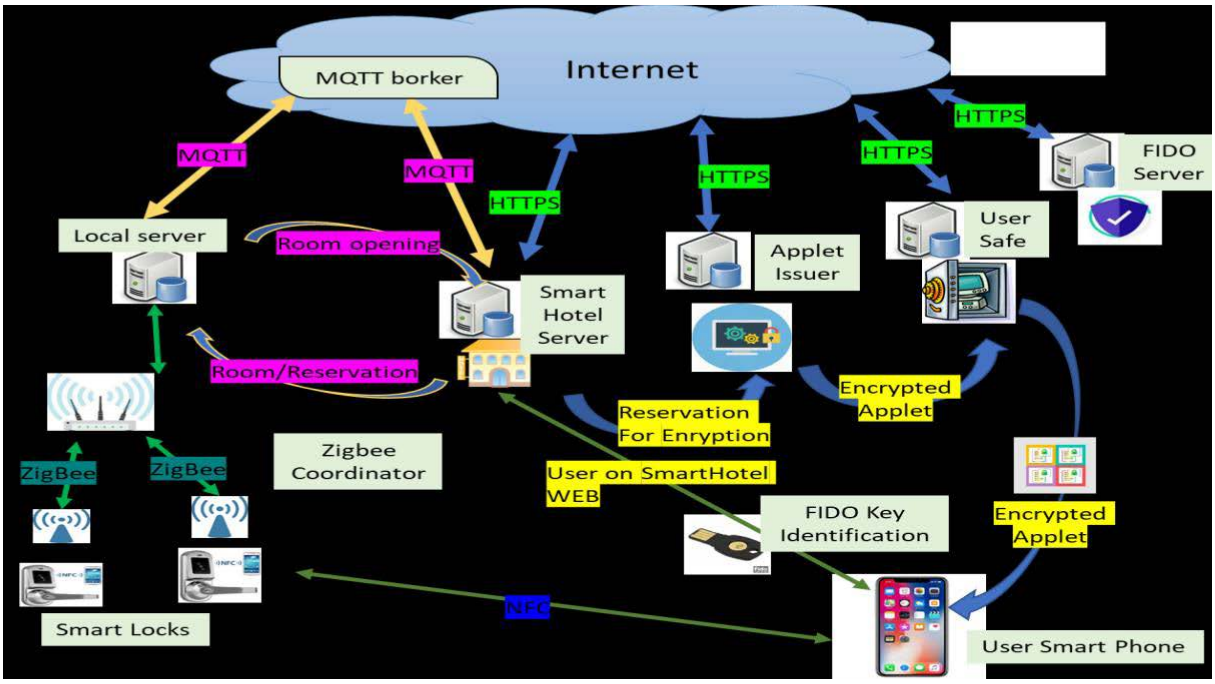

Figure 2: Smart Hotel use case Overview

One of the key challenges for IoT integration today is interoperability. A lot of solutions are proprietary-based and hard to connect with other systems. On the other hand, privacy, furthermore in hotel, is one of the most important features that need to be preserved. These two main challenges were the focal points during the definition and development of the Smart-Hotel use case. To allow a smooth connection with the IoT ecosystem, we have built a Smart-Hotel application able to exchange with the MQTT protocol. This application is composed of an authentication service available for 3 types of users: (i) System administrator, (ii) Hotel manager and (iii) Client. The application allows a full configuration for the hotel manager of all the hotel rooms and door lock details. Thanks to this configuration, the customers are able to book and pay for the available accommodations. Moreover, given a Personal Information Management Service (PIMS), the credentials are securely stored in a "Safe" allowing the customer to fine-use these credentials just as any other personal information. The PIMS is secured with FIDO passwordless connection (see next sub-section).

3.2. Fido based authentication

As part of the security and privacy enforcement objective of this project, FIDO authentication standards based on public key cryptography for authentication is introduced at 2 levels: (i) At user authentication level: FIDO Authentication replaces password-only logins with secure and fast login experiences across websites and apps. (ii) At device authentication level: FIDO provides a comprehensive authentication framework for IoT devices. On the Smart Hotel use case, a passwordless secure authentication is demonstrated using a smart token as Fido authenticator. This token is connected to the Smart-Hotel application hosted on the user smart phone using a USB connection and handling the CTAP (Client To Authenticator Protocol). The smart hotel web application is using the WebAuthn APIs supported by standard web browsers to handle the FIDO authentication procedure. A FIDO Server hosted in the PIMS server is managing the user's account identifier provided by the service to select the correct key and trigger the authentication challenge.

3.3. Secure access through combined Software & Hardwar components

The software component is based on a specific Java applet adapted for Java Card applications in order to respect the limited memory size available in smart cards. Besides, a secure and inviolable hardware component, called Secure Element (SE), that can be seamlessly integrated into small chip for smart cards, cell-phones, etc, is considered. The SE contains different sensors detecting any physical or logical attack. It stores confidential data and hosts Java Card applets allowing protected access control, transit, payment, etc. It is possible within the SE to have different authentication keys depending on the required level of security and the algorithm used to generate these keys.

The first applet loaded in the SE is called the ISD (Issuer Security Domain). It is similar to a virtual domain containing all the basic and mandatory applets managing the life cycle of the SE, such as the card manager. The ISD owns all the privileges to manage the SE and the applets. By authenticating to the ISD, the user can create new security domains (SD) and also attribute specific privileges and rights to handle the loaded applets. Each SD has its own keys for authentication. Without authenticating, the user cannot execute different operations such as loading and instantiating an applet. If the number of failed authentication attempts to the ISD reaches a specific threshold, the SE considers these attempts as a possible attack and moves thus to a locked state in order to safeguard the contained data.

3.4. Privacy preserving data sharing

Here, we focus on making the housekeeping in a smart hotel more efficient, considered as challenging, particularly for big hotels with hundreds of rooms and accommodations. In this context, multiple sensors are deployed in each room to collect different measurements, such as ambient temperature, humidity, light and CO2 measurements. The smart hotel server collects these data to improve the housekeeping efficiency and productivity. However, sharing such kind of data through a central server can compromise private information. For example, it can reveal if the client is currently sleeping, making a shower, etc. This raises serious privacy concerns. To cope with this problem, our platform offers a privacy preserving data sharing to the clients [11]. Every client shares an anonymized/noisy version of the original collected data with the smart hotel server. In return, based on the quality of the transmitted data, the server provides the client with a discount on his reserved room. The proposed discounts will encourage the clients to continue sharing good quality of data. The proposed approach executes in three steps: First, clients select their level of privacy allowed. Then, the server determines the set of clients that will be selected to share their distorted data and sends back to them their associated discounts. Finally, every selected client applies locally an obfuscation technique to protect his privacy and transmits the distorted data to the server. By doing so, this scheme protects the clients' privacy, motivates them to provide high data quality and more importantly allows collecting valuable data for service management.

4. Conclusion

As the number of services offered by emerging IoT-based systems keeps increasing, the amount of data exchanges has known a tremendous growth. Victim of its success, on the one hand, the underlying IoT ecosystems have become a privileged target for cyber-attacks. On the other hand, the constrained nature of most of IoT devices and their limited resources, in terms of computation, storage, communication and energy, are the main sources for their vulnerabilities. The overlapping of these constraints brought serious security and privacy risks. In this context, the PARFAIT project has been proposed to address the challenges with the aim of developing a new framework for personal data protection in the IoT environment. Two main use cases have been covered to validate and test the proposed schemes and tools. This newsletter provided a brief introduction to the PARFAIT project and its main objectives. An overview of the main architecture along with the different interactions and possible overlapping between its components are presented. Finally, relevant technological details related to the development of the different building blocks considered for a Smart Hotel demonstrator have been provided.

References

[1] P. Bellavista, G. Cardone, A. Corradi and L. Foschini, "Convergence of MANET and WSN in IoT Urban Scenarios," in *IEEE Sensors Journal*, vol. 13, no. 10, pp. 3558-3567, Oct. 2013.

[2] Woods, V. "Gartner Press Release", Dec 2016, [http://www.gartner.com/newsroom/id/3185623], [June 2020].

[3] Daniel R. Coats, Statement on Worldwide Threat Assessment of the US Intelligence Community, May 11, 2017, [https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf] [June 2020.]

[4] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," in *IEEE Internet of Things Journal*, vol. 4, no. 5, pp. 1125- 1142, Oct. 2017.

[5] Makhdoom, M. Abolhasan, J. Lipman, R. P. Liu and W. Ni, "Anatomy of Threats to the Internet of Things," in *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1636-1675, 2019.

[6] Manos Antonakakis & al., "Understanding the Mirai Botnet", 26th USENIX Security Symposium, 2017.

[7] Catalin Cimpanu, "BrickerBot Dev Claims Cyber-Attack That Affected Over 60,000 Indian Modems", July 2017, [www.bleepingcomputer.com/news/security/brickerbot-dev-claims-cyber-attack-thataffected-over-60-000-indian-modems/], [Accessed June, 2020].

[8] D. Bandyopadhyay, and J. Sen, “Internet of things: applications and challenges in technology and standardization,” *Wireless Pers. Commun*., vol.58, no.1, pp.49-69, 2011.

[9] R. Roman, J. Zhou, and J. Lopez, “On the features and challenges of security and privacy in distributed internet of things,” *Computer Networks*., vol. 57, no. 10, pp. 2266-2279, 2013.

[10] PARFAIT project webstie [http://www.itea3-parfait.com/] [June, 2020]

[11] S. Aroua, R. Ben Messaoud, Y. Ghamri-Doudane. “Bid-Aware Privacy-Preserving Participant Recruitment in Mobile Crowd-Sensing”, to appear in IEEE 92nd Vehicular Technology Conference: VTC2020-Fall, October 2020.