Analysis of the security solutions implemented in current Internet of Things Platforms

Stefan-Ciprian Arseni, Simona Halunga, Octavian Fratu, Alexandru Vulpe
Faculty of Electronics, Telecommunications and Information Technology
University POLITEHNICA of Bucharest
Bucharest, Romania
stefan.arseni@radio.pub.ro

George Suciu
R&D Department
Beia Consult International
Bucharest, Romania

***Abstract*—Our society finds itself in a point where it becomes more and more bounded by the use of technology in each activity, no matter how simple it could be. Following this social trend, the IT paradigm called Internet of Things (IoT) aims to group each technological end-point that has the ability to communicate, under the same "umbrella". In recent years many private or public organizations have discussed on this topic and tried to provide IoT Platforms that will allow the grouping of devices scattered worldwide. Yet, while information flows and a certain level of scalability and connectivity have been assured, one key component, security, remains a vulnerable point of IoT Platforms. In this paper we describe the main features of some of these "umbrellas", either open source or with payment, while analyzing and comparing the security solutions integrated in each one of these IoT Platforms. Moreover, through this paper we try to raise users and organizations awareness of the possible vulnerabilities that could appear in any moment, when using one of the presented IoT Platforms.**

Keywords—Internet of Things platforms, platforms security, Internet of Things architectures

I. INTRODUCTION

Society finds itself in what it seems a continuous loop of development, in which new findings modify the environment and services provided, while hoping to ease the interaction with the user. Yet, as multiple embedded devices and sensors are becoming more scattered and integrated in a range of domains, with different applications, the idea of tying them in a smart network for a better control, seemed more appealing.

Internet of Things (IoT) can be considered as the point where multiple technological advances from various domains intersect.

IoT is a concept that can be implemented both in public and private organizations, in order to provide powerful functionalities that will ensure a better administration of assets and an optimization of performance and quality of provided services, by creating means of interaction between users and the lowest level of sensors and devices available in the network.

Through the mechanisms used when implementing an IoT system and the results it offers, this technology trend is described in [1] as the next major economic and social revolution, facilitated by the Internet, that will allow objects to connect to the Internet and other objects or people. Therefore, a new network of interlinked systems and people is created, which, in return, induces new security risks that could allow attackers to steal even more personal information about the users or the organizations that are connected to such an IoT system.

In this paper, we want to present some of the current used Internet of Things platforms, either open-source or with payment. Also, by analyzing and comparing the security solutions implemented in these systems, we want to address the means of how data is being protected.

The paper is structured as follows: Section II presents an architectural view of an IoT system, while Section III present the IoT platforms that are going to be compared in Section IV. Finally, the Conclusions section tries to summarize the results and raise the awareness of users when selecting one of the presented platforms or another one.

II. INTERNET OF THINGS SYSTEM ARCHITECTURE

Even though IoT is a concept that became a well-known and used term, in different areas of the society, when talking about a definition that is generally agreed both by the industry and standardization organisms, it has not been stated until now. Although many definitions exist, they try to formulate similar ideas but in different forms and taking into consideration different components or aspect of an IoT system.

One the most suitable definitions for an IoT system is envisioned by ITU-T as a network with anyplace and anytime connectivity for anyone or anything. Still, as presented in [2], this definition can be extended to a 6A connectivity: connecting people and objects, Anytime, from Anyplace with Anyone or Anything, while, ideally using Any network or Any service.

Having in mind this extended definition, we can state that a correct and easy implementation of an IoT system mainly depends on identifying the right principles regarding the proper discovery, identification, configuration and

manipulation of interconnected devices and sensors. In order to succeed in implementing such an IoT architecture, [3] mentions that suitable technologies, with a certain degree of autonomy and self-management, must be implemented.

From the network point of view, an IoT architecture resembles a classical TCP/IP protocol stack, while substituting protocols that cannot be implemented due to certain design constraints of sensors or other embedded devices, with similar communication protocols that can assure a certain level of network integration for these constrained devices. Based on this statement, we can then differentiate between the stack layers and separate the informational flows that can occur between them.

From a general point of view, a high-level architecture of an IoT system is required to implement at least three components. In our opinion, one of the best representations of a high-level architecture of IoT is the one introduced by the IoT-A project [4], as presented in fig. 1. This reference model acts as a foundation and a common language for the targeted IoT system implementation, allowing a natural derivation of functionalities, according to the requirement of the new implementation.

As presented in fig. 1, the IoT model consists of three sub-models. This division offers a more accurate and rapid access to the required data, as the arrows from fig. 1 point out the different informational flows that could arise in a IoT system that implements this project. Next, we will briefly present each of these three sub-models:

- The first component is the IoT Domain Model is responsible for integrating all the sensors or devices that needed to be connected to the system. It has an abstraction level that it permits to be independent of specific technologies of the devices or specific scenarios of usage.
- The second component is the IoT Information Model that, based on the Domain Model, defines the structure, such as relations and attributes, of data flowing between these components.
- The third component is the Functional Model, which has the role of identifying and grouping functionalities depending on how they encompass key elements from the IoT Domain Model. By dividing and grouping the services offered to connected users and devices, there is certain degree of independence between functionalities that is being offered, but also there is the possibility of connecting and transmitting information between one and another Functional Group.

Within the Functional Model there are identified two main Groups: Communication and Security. The first one handles the communication constraints imposed by the heterogeneous environments where the infrastructure is implemented. The second one, Security, is one the most important aspects. It offers the means of integrating Trust, Security and Privacy for objects or users connected or with the intention of connect.

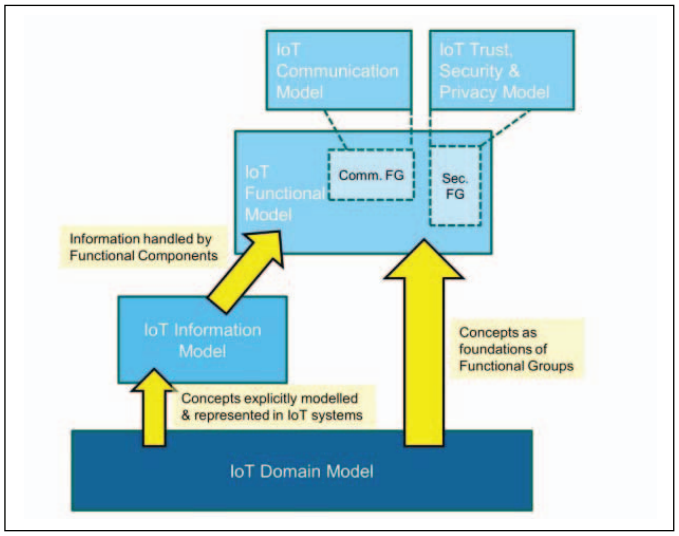

Fig. 1. IoT system reference mode [4]

III. Internet of Things Platforms

Given the recent advances and developments of Cloud computing and storage systems and their increase in usage by regular users, platforms that have the ability to interconnect various types of devices have also been ported into the Cloud or make use of its benefits.

Therefore, there are two categories of platforms available for users:

- Ones that act as a local point of connection for several types of devices, depending on their features, or have the requirement of using a specialized software core on the device;
- Others that are implemented as PaaS (Platform-as-a-Service) and, usually, have the capability of connecting more devices, by accepting data transmissions over the Internet through HTTP or similar protocols.

Except this split into categories, IoT platforms can also be provided as open-source projects or access can be restricted, with only a few members being allowed to work with that platform. Another case is regarding the platforms that impose a regular or one-time fee payment in order to get access to their provided services.

Because there are many domains in which IoT could provide a better understanding and control over that it, there is also a trend in platforms to become specialized either to a certain domain, by implementing functionalities and building the entire structure of the framework on the characteristic requirements of it, either to a certain class of objects.

In this regard, project HomeKit introduced by Apple in 2014, is, basically, a new common network protocol that allows users to take control of their home appliances or to access certain services or devices that were previously connected. By being integrated into an iPhone, the platform allows users to even search for different applications in the

Application Store they have on their mobile devices and use it to control de smart things around them.

IoTivity is another platform for the implementation of future IoT systems. It was developed by Intel and currently is being proposed as a good architectural model by the Open Internet Consortium (OIC). By not implement HTTP and using only CoAP [5] as application level protocol, this platform offers a limited support for both devices and applications. Yet, because it is an open-source project and it is focused on assuring security and simplicity, while having a small number of modules, as presented in fig. 2, it will lead to a rapid development.

Another platform example is AllJoyn. It was lauched in 2010 under the format of a framework that tries to initiate and sustain peer-to-peer communication between devices. The framework is constructed from a Fundamental Layer, that will assure the interconnection of different types of sensors and devices, on top of which various modular Services will be enabled to provide functionalities such as discovery of adjacent devices, pairing, message routing or security.

Another example of platform that can be used for the integration of home or personal areas sensors into an IoT system is the Sen.se platform. The services related with this platform are provided using the Internet, by making data transfers and initiating communications through the HTTP protocol.

Xively is one of the few IoT platforms that are focused primarily on companies and assurance of business processes. From a functional point of view, the platform is similar to the others, but some differences exist when referring to the processes available to users for managing and defining connected devices or controlling the deployment lifecycle or products.

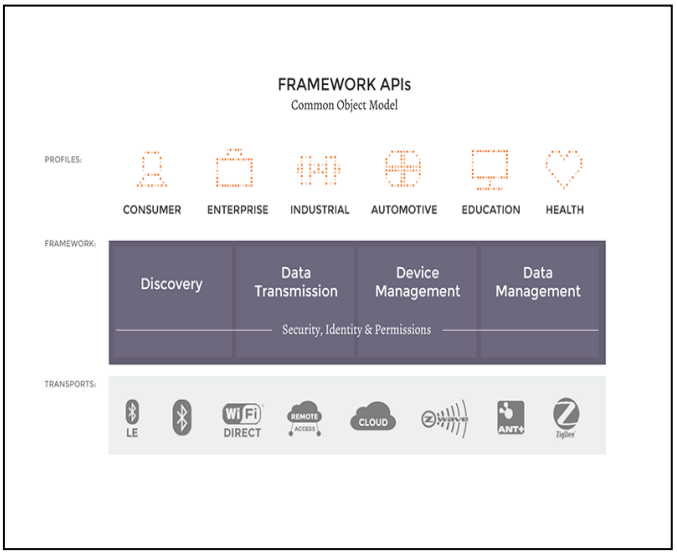

Fig. 2. IoTivity architecture[1]

[1]Image source: https://www.iotivity.org/documentation/architecture-overview, accessed on 22nd of September 2015.

IV. Analysis and Comparison

When talking about the HomeKit platform from Apple, there are several features and security measures that prevent loss of data, or even more dangerous situations in which the user loses control to anyone else that is in the range. One of these methods is the secure pairing of devices that insures users of the fact that they are the only persons capable of controlling the pared device. Also, for a better grouping of elements, HomeKit supports the definition of "scenes" in which users can add devices found in the same area. This will result in a good control over the targeted areas in the smart environment. Yet, because the main controller of the objects is only a smart device, and not another solution that can have a better protection, the main vulnerability is represented by that central point: the iDevice. Any possible breach in the security of that device will lead to possible breaches in the entire IoT system being put in place.

Under its current form, IoTivity is a platform meant primarily for usage in secure environments or in organizations that do not transmit any classified data. The platform does not provide any kind of protection, neither for authenticating devices, nor for securing communication links when querying sensors and making some data transfers. Still, the platform is capable of implementing security methods through the use of a variation of "tinydtls" protocol that has not been enabled yet.

Similar to other presented frameworks, AllJoyn implements security mechanism at application level, therefore there is no trusted connection being realized at lower levels. In the moment when a new device tries to connect, an authentication demand is triggered between the applications. This action supports multiple algorithms like PIN codes, PSK or ECDSA (Elliptical Curve Digital Signature Algorithm). After the authentication process is completed, the security mechanisms also ensure the confidentiality and integrity of transmitted data, using AES-128 CCM.

Moving on to Sen.se platform, it provides less protection than the other platforms, because it only ensures the authentication of devices linked in an exchange of information and it does not ensure also the security of the communication. Regarding the authentication process, every communication link established between one of the personal devices with Sen.se platform, a Sen.se key that is specific and unique for each user. Still, only assuring the correct authentication of devices is not sufficient when a higher level of security is needed, for example when this kind of IoT system is being used in environments where sensitive data could be available. Also, the fact that the unique user key is being kept online, on their personal account, it is possible for someone to hack that account an steal not only that private key but also have access to some personal data.

In the case of Xively platform, security is being assured right from the location where the platform is hosted that is a proprietary cloud infrastructure that can ensure the data is protected and available. When initiating communications from personal devices to a service on the platform, the transfer of data will be secured using the HTTPS protocol, which limits the attacking possibility of an attack like man-in-the-middle or eavesdropping.

TABLE I. COMPARISON OF PRESENTED IOT PLATFORMS

IoT Platform / Security method	HomeKit (Apple)	IoTivity (Intel)	AllJoyn	Sen.se	Xively
Device authentication	X	Not yet enabled	X	X	X
Resource access control	X	Not yet enabled		X	X
Secure communication link	X	Noe yet enabled	X		X
Auto-authentication of registered devices					X
Designed for Industry use				X	X
Designed for Home use	X	X			

Also, for access control on resources, the platform implements the use of API Keys, similar to the other platforms. Through these keys, requests for resources are authenticated, while the user is able to deny access to some of the resources manages by that key, with instant feedback after the alteration of rights. Moreover, device activation can be guaranteed, so that it is done automatically, without requiring any implication from the user.

As an overall view of the differences between security methods of each one of the five platforms that were mentioned in this paper, table I summarizes the comparison. From this we can observe that the Xively platform, a platform that was first designed to control devices in an industrial environment, has the best security assurance. Yet, viewing the image at a greater scale, this can be the effect of the importance each asset from an organization has for the entire operational cycle, as compared to a device that we use at home that will not interfere in such a way that will affect the organization.

V. CONCLUSIONS

Internet of Things is a vast domain, still spreading over different areas of the society, with a fast pace. Even though there are currently many choices of IoT platforms to choose from, one must take into consideration multiple factors, like security, support for different devices, ease of use and integration.

The paper tries to emphasize the need of a good security implementation in a platform so that users would be fully satisfied with their experience and assured that all data exchanged when communicating between devices. Still, as seen in section IV, the constraints that embedded devices or sensors have, limit the ability to implement stronger security mechanisms over these platforms.

Therefore, any user needs to pay attention first to what type of sensors he wishes to connect with the IoT platform and if he wants that platform to be local or provided as a service on the Internet. Depending on these factors, a user could then easily find out, as this paper indicated, which solutions best apply to his case and what the security assurance will be.

As mentioned in an article posted in September on Forbes website, now we call this network the Internet of Things, but tomorrow it will be the Internet of Analytics-Enabled Secure Automated Wearable Things (IoA-EASWT).

Acknowledgment

The work has been funded by the Sectoral Operational Programme Human Resources Development 2007-2013 of the Ministry of European Funds through the Financial Agreement POSDRU/187/1.5/S/155536.

References

[1] O. Vermesan, P. Friess, „Building the Hyperconnected Society: IoT Research and Innovation Value Chains, Ecosystems and Markets”, vol. 43, ed. River Publishers, 2015.

[2] European Research Cluster on Internet of Things, „Internet of Things Strategic Research Roadmap”, SRA Cluster, 2011.

[3] European Research Cluster on Internet of Things, „IoT Semantic Interoperability: Research Challenges, Best Practices, Recommendations and Next Steps”, 2015.

[4] Deliverable D1.5 - “Final architectural reference model for the IoT 3.0” of project “Internet of Things Architecture”, coordinator Gunter Kulzhammer, 2013.

[5] C. Bormann, A. Castellani, Z. Shelby, „CoAP: An application protocol for billions of tiny Internet nodes”, IEEE Internet Computing, vol. 16, nr. 2, 2012, pp. 62-67.