A Systemic Approach for IoT Security

Conference Paper · May 2013

DOI: 10.1109/DCOSS.2013.78

CITATIONS
16

READS
83

5 authors, including:

Yacine Challal
Ecole Nationale Supérieure d'Informatique
132 PUBLICATIONS **1,190** CITATIONS
SEE PROFILE

Enrico Natalizio
Université de Technologie de Compiègne
70 PUBLICATIONS **401** CITATIONS
SEE PROFILE

Zied Chtourou
Military Academy, Tunisia
32 PUBLICATIONS **75** CITATIONS
SEE PROFILE

A Systemic Approach for IoT Security

Arbia Riahi, Yacine Challal, Enrico Natalizio, Zied Chtourou, Abdelmadjid Bouabdallah

A systemic approach for IoT security

Arbia Riahi*, Yacine Challal †, Enrico Natalizio†, Zied Chtourou*, Abdelmadjid Bouabdallah†
*VRIT Lab - Military Academy of Tunisia, Nabeul, Tunisia. e-mail: arbia.rahi@ati.tn, ziedchtourou@gmail.com
†Heudiasyc - Université de Technologie de Compiègne, Compiègne, France. e-mail: <firstname.lastname>@hds.utc.fr

***Abstract*—In this paper we want to explore a new approach for security mechanisms design and deployment in the context of Internet of Things (IoT). We claim that the usual approach to security issues, typical of more classical systems and networks, does not grab all the aspects related to this new paradigm of communication, sharing and actuation. In fact, the IoT paradigm involves new features, mechanisms and dangers that cannot be completely taken into consideration through the classical formulation of security problems. The IoT calls for a new paradigm of security, which will have to consider the security problem from a holistic perspective including the new actors and their interactions. In this paper, we propose a systemic approach to security in IoT and explore the role of each actor and its interactions with the other main actors of the proposed scheme.**

***Keywords*—Internet of Things, Security, Systemic Approach**

I. Introduction

The Internet of Things (IoT) paradigm is one of the most thrilling innovations of the recent years. The exploitation of the IPv6 addressing space, along with the miniaturization of electronic and transceiver devices opened the way to provide each object on Earth with an Internet address and the technological support to transform it in a communicating object. Once each object possesses communication capabilities, the number of possible applications becomes potentially infinite. This good news is counterbalanced by the consideration that also the number of possible attacks to persons' and objects' security will grow exponentially. Therefore, a new paradigm of trust, security and privacy is required to face these future issues in the IoT. In [1] authors describe a systemic and cognitive approach for IoT security. In their work, they consider three main axes: effective security for tiny embedded networks, context-aware and user-centric privacy, and the systemic and cognitive approach for IoT security. In this paper, we will focus on the third axis. Actually, authors affirm that the IoT is a complex system in which *people* interact with the *technological ecosystem* based on *smart objects* through complex *processes* [1] as shown in figure 1. In this approach, connections between different nodes have a specific character depending on complex environment of the IoT. By taking into consideration the dynamic and complex nature of this model, in this work, we will present our perspective in respect of the main elements illustrated in Figure 1 and that we will call "nodes" and "tensions".

In order to explain this model, we will describe each node and its functions in Section II. Then, we believe that the tensions between the different nodes need a special study and discussion, which will be our goal in Section III. In Section IV we will provide the reader with the logical connections between some classical domain of applications for the IoT and the presented scheme. Finally, we will provide our conclusions in Section V.

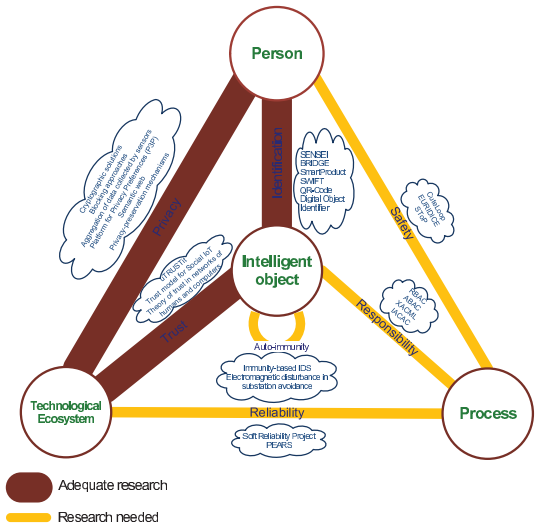

Figure 1. A systemic approach for IoT security

II. Nodes

In this Section we will present the main actors of the systemic approach to security in IoT, introduced in [1]. It is worth to note that the real novelty of the scheme in Figure 1 is the introduction of the "Intelligent Object" at the center of the interactions among Person, Process and Technological Ecosystem. In the following we will introduce each of the mentioned actors and their functions in the scheme.

A. Person

The first node plays a fundamental role in the IoT security framework. The human resources are responsible for security rules management, which includes:

- Defining security practices and rules.
- Auditing practices and rules efficiency.
- Applying practices and rules when into operational mode.

Due to the complex environment of the IoT, this node is a vital component in security management and enhancement. To this purpose, the human component should be able to analyse the context of IoT, individuate its advantages and limitations, and exploit the technology evolution to bring adequate solutions.

B. Process

The second node refers to a means to accomplishing tasks in the IoT environment according to some security requirements. The process is required to be compliant with

the security policies in order to keep the environment secure at different levels. Furthermore, due to the complexity of the model and the presence of different interactions originating from this node, security processes are difficult to implement.

The Federal Financial Institutions Examination Council's (FFIEC) presented a first classification of standard areas to deal with when considering security processes:

- Information Security Risk Assessment.
- Information Security Strategy.
- Security Controls Implementation.
- Security Monitoring.
- Security Process Monitoring and Updating [3].

In practices, security process need to meet requirements of standards, strategies, policies, procedures and other afferent documents. Thus, an adequate compromise must be found between complexity of security process practices and the needed security level.

C. Intelligent Object

This node is the heart of the new approach. It refers to an "object" augmented by the electronic features needed to let it communicate with other objects in the surrounding environment. These objects will become active participants in business, information and social processes [2]. In fact, objects in the IoT framework will be able to cooperate, share and exchange information about the environment, and respond to events happened in the environment by accomplishing adequate operations. Due to their expected pervasivity, the correct design and development of security practices within the conception of intelligent objects is fundamental to ensure the right level of security to the whole environment surrounding them.

D. Technological ecosystem

This node refers to technological choices made to ensure IoT security. According to [26], information security technology falls into several broad categories:

- Security Design and Configuration
- I&A: Identification and Authorization
- Enclave internal
- Enclave boundary
- Physical and environmental

The choices related to each of these elements may include system architecture, communications protocols, implemented algorithms, access control methods, performance, etc. It is evident that a trade-off among security requirements, feasibility and technology evolution should be found in order to ensure the appropriate level of security without degrading the performance of the system.

III. Tensions

In the systemic and cognitive approach for IoT security of Figure 1, the nodes are the originating and destination actors of a tension that represents their interaction, and takes into consideration the complexity of the environment. Specifically, the tensions that we are going to consider are: identification/authentication, trust, reliability, auto-immunity, privacy, responsibility and safety. To better explain our systemic approach, these tensions need to be deeply analyzed, measured and discussed.

A. Identification and authentication

"Identification and authentication" is the tension that ties the *intelligent object* with the *person*. In the IoT context, objects are spread globally. An efficient resolution scheme needs to be set to identify different entities. Privacy and other security issues must be taken into consideration as well as the specific function of the object, which can change over the time. Furthermore, an object can have one core identity and several temporary identities; an hospital can become a meeting place for a health conference or a shelter after a fire [4].

A lot of research has already been proposed on this axis. We will limit our analysis to the presentation of some important projects of this domain. First, we cite SENSEI (Integrating the Physical with the Digital World of the Network of the Future) which proposes an architecture that integrates Wireless Sensors and Actuators networks to ensure their cooperation [5]. The second project is BRIDGE (Building Radio Frequency IDentification for the Global Environment) which aims to find and invent tools permitting the deployment of RFID and EPCglobal Network applications [6]. Other projects can be listed here, such as SmartProduct [7], SWIFT (Secure Widespread Identities for Federated Telecommunications) [8], QR-Code [9] and Digital Object Identifier [10].

Open research issues: In [2], many research issued have been illustrated. For example, global ID schemes need to be considered when intelligent objects and humans interact. Also, an efficient identity management approach should be defined. Mobility, privacy, pseudonimity, anonymity aspects need deeper analysis and research. For example, when we limit our scope to to the RFID framework, we can easily individuate partially studied research topics related to the definition of distributed logical readers or the study of a RFID networks where both tags and readers are mobile.

B. Trust

"Trust" is the tension that ties the *intelligent object* with the *technological ecosystem*. Basically, it represents the level of confidence that the environment can grant to the intelligent object. The IoT environment can be permeated with very heterogeneous objects, which might differ for both their functions and their capabilities. In such a heterogeneous environment, when defining trust management, we must take into account also the severe resource constraints to which the objects are subjected, and which will constraint the choices of the technological ecosystem. Thus, trust management operations such as establishing, updating, and revoking keys and certificates are very important research topics in the IoT framework.

An important project that deals with the mentioned issues is uTRUSTit [11]. Its objective is to model and implement a tool for building and testing trust. In another context, Gligor and Wing present "a theory of trust in networks of humans and computers that consists of elements of computational trust and behavioral trust" [12]. In [14], authors propose a subjective behavioral trust model for Social IoT, which exploits the "social" bound existing among objects (ownership, parental, co-location, etc.). This model has been further detailed in [13].

Open research issues: The main objectives of trust research in IoT framework are the following. First, the conception of new models for decentralized trust. Second, the implementation of trust mechanisms for the cloud computing. Third, the development of applications based on node trust (ex. routing, data aggregation, etc.).

According to [12], an interesting issue is to develop a theory for computational trust. In turn, this means to deal with relationships between computational trust and behavioral trust, in order to create new protocol areas, and to maintain stability trust properties. In practice, authors propose a network infrastructure to manage trust concepts [12].

On the another hand, when managing trust, aspects such as topology of the objects, coverage deployment, target tracking, localization and IoT applications should be considered [27].

C. Privacy

"Privacy" is the tension that ties the *person* with the *technological ecosystem*. Privacy is an important tension in the systemic model for IoT security because of the ubiquitous character of the environment. Despite the existence of adequate research activities in privacy management mechanisms in general, there is still a list of objectives to be fulfilled. To make things clearer, in [16], authors divide privacy into three main axes: 1) Privacy in data collection, 2) Privacy in Data Sharing and Management and 3) Data security issues. In the following we will cite the most important research activities for each of these directions.

With reference to the first research axis, "privacy in data collection", we can mention the cryptographic solutions and the blocking approaches detailed in [15] and [19]. For the second axis, we can enumerate aggregation of data collected by sensors [16], the Platform for Privacy Preferences (P3P) [17], semantic web [18] and other privacy-preservation mechanisms, such as: k-anonymity, l-diversity, and t-closeness. Finally, in the data security issues, we can name password protection [19] and [20], cryptographic solutions and web entities with a semantic policy language [21].

Open research issues: Even though a lot of research has already been proposed for this tension, still many topics need to be further investigated. Here we can propose a list of interesting topics. First of all, the automated key management scheme. This operation is very sensitive in the case of IoT. It may include key provisioning, updating, revocation, transporting and key agreement. Also non-cryptographic operations like enrollment, backup and recovery should be addressed to guarantee a high level of security. Another issue is to develop a new scheme for asymmetric key management including generation, validation and distribution.

D. Responsibility

"Responsibility" is the tension that ties the *intelligent object* with the *process*. In order to share resources and other added values, which are useful for different processes, privileges and access rights must be clearly defined according to privacy constraints. In addition, responsibilities and liabilities rules of each entity must be considered in order to avoid dangers when the object regulates a process.

In literature, two main access control models have been developed: Role-based access control (RBAC) and Attribute-based access control (ABAC). In practice, main implementations include XACML (Policy decision language based on XML) and its extension known as Distributed Access Control [22]. Recently a new model was proposed in [32]. The IACAC (Identity Authentication and Capability based Access Control) presents a new scheme for authentication and access control in IoT and aims at replacing the existing approaches.

Open research issues: The main objective of responsibility for IoT is to make access control rules easy to create, understand and manipulate. In this sense, a possible research issue is the integration of the IACAC model in an identity management component of a RFID middleware [32]. Another direction can focus on access control rules propagation and revocation [32].

E. Autoimmunity

"Autoimmunity" ties the *intelligent object* in self-loop. The objective of this tension is to propose an artificial immune system solution for IoT. In this trend, two main research activities can be evoked here. First, authors in [24] describe a simulation and immunity test of a wireless sensor in order to avoid electromagnetic disturbance in substation. Second, immunity-based schemes can be used to detect intrusions in the IoT. For example, the authors of [23] simulate self and non-self antigen in IoT, as well as immature, mature and memory detector, to detect attacks in the IoT.

Open research issues: As a relevant open research issue related to the autoimmunity, we propose the conception of a new autoimmunity technique, where intelligent objects can distinguish if special access or privileges are permitted to the all or a part of the system content data, and react according to the context constraints.

F. Safety

"Safety" is the tension that ties the *person* with the *process*. An environment permeated with intelligent objects is supposed to cope with many security challenges. One of these is ensuring safety when a sudden failure occurs for one or many system components. Then, safety must be considered as a mean to reduce the possibility of damage.

When considered as a research axis for the IoT, safety purposes have been widely investigated. We can list as examples: the CuteLoop project [28], EURIDICE (European Inter-Disciplinary Research on Intelligent Cargo for Efficient, safe and environment-friendly logistics)[29] and SToP (Stop Tampering of Products) [30].

Table I. IoT Application Domains-Tension examples

Tension / **Application**	*Identification*	*Privacy*	*Trust*	*Safety*	*Responsibility*	*Reliability*	*Auto-immunity*
Transportation and logistics domain	RFID-based identification management of consumers, providers and products	At the subscription moment, a customer can provide private data in order to benefit from some advantages	Objects that perfectly accomplished their previous tasks in a supply chain	Vehicles and consumers safety services	Traffic monitoring and control devices	Detection, analysis and avoidance of anomalies	Stop techniques in case of intrusion detection
Health-care domain	Identification of staff and patients	Data, including clinical diagnosis and treatment, must be kept private	Patients should trust medical institutions in terms of reliability and privacy	Medical institutions must ensure the patient safety during health-care activities	Parameters setting of health-care objects	Reliability of the link in case of remote diagnosis	An object that provides alert in case of accident
Smart environment domain	Identification of the employees in the same enterprise	Financial details of a given project (domestic or professional) should be confidential	Newly bought objects belonging to the same owner	A trainer that assign the adequate exercise according to the health parameters of the trainee	Control devices for personal environment	For the continuity of services assurance, an electric power supply reliability should be guaranteed	Disaster prediction and alerting

Open research issues: Several applications can be considered as drivers of technological and scientifical innovations along this research axis. For example, we can focus on the environment observation: pollution effects, forest fires studies, etc.; the physical security of building: VMC, leaks, intruders, etc.; and also the commercial field: protection of products against counterfeit.

G. Reliability

"Realibility" is the tension that ties the *process* with the *technological ecosystem*. The reliability deals with data and communications management. The reliability aims at guaranteeing availability of information over time through efficient ways of managing data repositories. Reliability of communication links can be ensured through the redundancy provided by multiple paths.

In this direction, we can list two main projects: the Soft Reliability Project [25] and PEARS (Feasibility Privacy-Ensuring Affordable RFID System / Feasibility) [31].

Open research issues: An open research issue is related with the development of clustering communication strategies to ensure links reliability. Another issue will focus on creating an automated solution for IoT service management to enhance their reliability.

IV. The systemic approach for new applications of the IoT

The integration of an intelligent object within the IoT implies the creation of new applications as well as the extension of existing ones. In this Section, we want to detail the link between some of the classical application domains and the tension of our systemic approach, in order to highlight constraints and requirements imposed by the security. Concretely, in Table I we choose transportation and logistics, health-care and smart environment as domains of application, and we characterize each tension of the proposed scheme by the means of an example in the context of that domain.

V. Conclusion

In this paper we proposed a systemic approach for IoT security base on [1]. The model is made up of four nodes: person, technological ecosystem, process and intelligent object. The last node is the newest and reflects the IoT dimension. These nodes interact through tensions, namely identification, trust, privacy, safety, auto-immunity, reliability and responsibility. As a first task, we aimed to define each node and its roles. Then, we focused on the analysis of literature and open issue related to the tensions. To this purpose, we described each tension's meaning, effect, related work and possible research issues. Finally, we proposed real examples taken from classical application domains to substantiate the use of our systemic approach.

References

[1] Yacine Challal, *Internet of Things Security: towards a cognitive and systemic approach*, HDR Thesis, Université de Technologie de Compiègne, 2012.

[2] O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, H. Sundmaeker, A. Bassi, I. S. Jubert, M. Mazura, M. Harrison, M. Eisenhauer, P. Doody, *Internet of Things Strategic Research Roadmap*, 2011.

[3] http://www.ffiec.gov.

[4] R. Roman, P. Najera, J. Lopez, *Securing the Internet of Things*, IEEE Computer, vol. 44, no. 9, pp. 51–58, September 2011.

[5] http://www.ict-sensei.org.

[6] www.bridge-project.eu.

[7] http://www.smartproducts-project.eu.

[8] http://www.ist-swift.org/.

[9] http://www.qrcode.com.

[10] http://www.doi.org/.

[11] http://www.utrustit.eu.

[12] V. Gligor and J. M. Wing, *Towards a Theory of Trust in Networks of Humans and Computers*, 19th International Workshop on Security Protocols, Cambridge, UK, March 28-30, 2011.

[13] M. Nitti, R. Girau, L. Atzori, A. Iera, and G. Morabito, *A Subjective Model for Trustworthiness Evaluation in the Social Internet of Things*, 23rd Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, 2012.

[14] L. Atzori, A. Iera, and G. Morabito, *SIoT: Giving a Social Structure to the Internet of Things*, IEEE communications letters, 2011.

[15] D. Molnar, D. Wagner, *Privacy and Security in Library RFID: Issues, Practices and Architectures*, CCS, 2004.

[16] C. C. Aggarwal, P. S. Yu, *Privacy-preserving data mining : models and algorithms*, Springer, 2008.

[17] http://www.w3.org/TR/P3P11/.

[18] F. Gandon, N. Sadeh, *Semantic Web Technologies to Reconcile Privacy and Context Awareness*, Web Semantics: Science, Services and Agents on the World Wide Web, vol. 1, no. 3, pp. 241–260, 2004.

[19] R. Kumar, E. Kohler, M. Srivastava, *Harbor: software-based memory protection for sensor nodes,* IPSN Conference, 2007.

[20] R. Acharya, K. Asha, *Data integrity and intrusion detection in wireless sensor networks*, Proceedings of the IEEE ICON, 2008.

[21] L. Kagal, T. Finin, A. Joshi, *A Policy-based Approach to Security for the Semantic Web,* ISWC, 2003.

[22] http://xacmllight.sourceforge.net/.

[23] C. Liu, J. Yang, Y. Zhang, *Research on Immunity-based Intrusion Detection Technology for the Internet of Things*, Seventh International Conference on Natural Computation, 2011.

[24] A. Bo, Z. Weidong, C. Xiang, L. Jikun, S. Yingbin, L. Shaoyu, *A Study on Immunity of Wireless Sensor Unit in Substation,* Electromagnetic Compatibility (EMC EUROPE), 2012 International Symposium on , vol., no., pp.1,5, 17-21 Sept. 2012.

[25] http://www.softreliability.org.

[26] L. Kiely, T. Benzel, *Systemic Security Management: A new conceptual framework for understanding the issues, inviting dialogue and debate, and identifying future research needs*, Institute for Critical Information Infrastructure Protection (ICIIP), 2008.

[27] H. C. Hsu, K. D. Chang, J. L. Chen, H. C. Chao, *A Survey on Trust Management Mechanisms for Wireless Sensor Networks & Future Internet of Things*, Journal of Electronic Science and Technology, vol. 9, no. 4, pp. 364–367, 2011.

[28] www.cuteloop.eu

[29] www.euridice-project.eu

[30] www.stop-project.eu

[31] www.friendlytechnologies.com

[32] N. Mahalle, B. Anggorojati, N. R. Prasad and R. Prasad, *Identity, Authentication and Capability Based Access Control (IACAC) for the Internet of Things,* Journal of Cyber Security and Mobility, Vol. 1, No. 4, p. 309-348., mar. 2013.