A systemic and cognitive vision for IoT security: a case study of military live simulation and security challenges

Arbia Riahi Sfar, Zied Chtourou, Yacine Challal

A systemic and cognitive vision for IoT security: a case study of military live simulation and security challenges

Arbia Riahi Sfar*, Zied Chtourou*, Enrico Natalizio†, Yacine Challal‡,
* VRIT Lab - Military Academy of Tunisia, Nabeul, Tunisia. e-mail: arbia.sfar@hds.utc.fr, ziedchtourou@gmail.com
† Sorbonne universites, Universite de Technologie de Compiegne, CNRS, Heudiasyc UMR 7253. e-mail: *name.lastname*@hds.utc.fr
‡ Centre de Recherche sur l'Information Scientifique et Technique, CERIST, Algeria. e-mail: y_challal@esi.dz

Abstract

Securing data, objects, networks, systems and people in the Internet of Things (IoT) will have a prominent role in the research and standardization activities of the next years. The high connectivity of intelligent objects and their severe constraints lead to many security challenges, which are not included into the classical formulation of security problems and solutions. To help interested researchers to contribute to this research area, an IoT security roadmap overview is presented in this work based on a novel cognitive and systemic vision. The role of each component of the approach will be explained and relations with the other elements and their impact on the overall system will be detailed. According to the novel taxonomy of IoT vision, a case study of military live simulation will be presented to highlight components and interactions of the systemic and cognitive approach. Then, a discussion of security questions about privacy, trust, identification and access control will be provided, and different research challenges will be highlighted.

Keywords

Internet of Things, security, systemic and cognitive approach, military live simulation.

I. Introduction

The paradigm of the Internet of Things (IoT) aims at connecting anything, anyone, at anytime in anyplace. It involves things or objects such as sensors, actuators, RFID tags and readers, to permit interaction between the physical and virtual worlds. In 2020 the number of interconnected systems is expected to reach 24 billion devices and the financial market size is around 1.3 trillion dollars for mobile network operators in various domains and applications like healthcare, transportation, public services and electronics [1]. The evolution from limited-access networks to open ones increased the need for security alarms to protect interconnected devices from intrusions as data modification, suppression, sniffing, Denial of Service (DoS) and DDoS, and many other threats. Consequently, many challenging security issues must be addressed before making the IoT vision a reality, such as trust, security, and privacy. The major contribution of this work is threefold: (a) we explain the systemic and cognitive vision of IoT, which was formerly introduced in [2], [3]; (b) we propose a case study in the live simulation of military application accordingly; and (c) we present a number of possible research issues related to IoT security.

II. A systemic and cognitive vision of IoT

In [3] [4], authors proposed a systemic and holistic view of IoT suggesting a systemic and cognitive vision for IoT security questions and issues. The proposed approach is originally inspired from [5], where L. Kiely et al. have proposed a systemic security management system for all types of organizations beginning with the micro level. As shown in figure 2, our illustration of the IoT context is described by a tetrahedron-shaped scheme made around four nodes: person, process, intelligent object and technological ecosystem. These nodes are connected to each other and their interaction is represented by the following adges: trust, privacy, identification and access control, safety, reliability, auto immunity and responsibility.

A. Nodes

1) People: security limitations and threats are more probable and influenced by a significant number of persons involved in the large-scaled structure. To explain the role of this node, we consider a scenario involving people with different security background levels. Their behavior depends on their personalities, skills, knowledge, motivations, expectations, visions, etc. To address security questions related to people in IoT context, it is meaningful to handle them within a systemic approach by providing a global

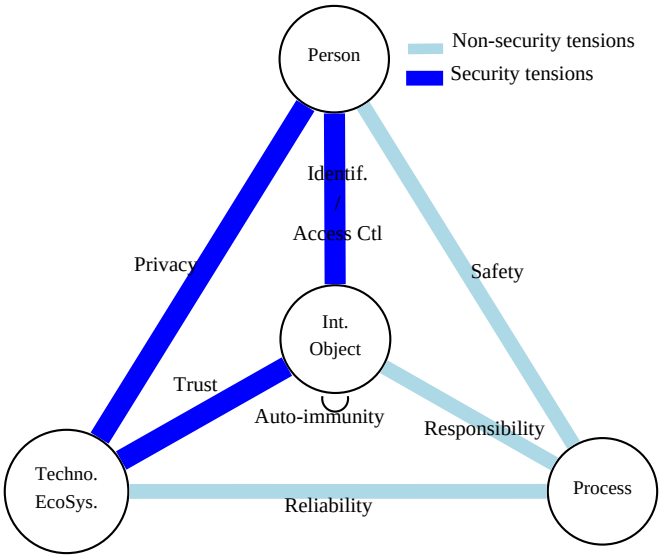

Figure 1: Graphical illustration of the IoT context according to its main elements (nodes) and their relationships (edges)

revision of rules and practices. For example, we consider different types of human profiles such as consumers, end users, service or technology providers, etc. All of them are necessary in controlling and improving security issues. Constrained by their privacy and safety, identification mechanisms and access control rules, persons have to perform many tasks associated with security principles and controls, according to Plan-Do-Check-Act approach described in ISO/IEC 27000-series [6].

2) Process: handles procedures, ways to accomplish tasks with respect to a specific security policy(ies). To guarantee a satisfying level of the overall system security, various architectural components need to be adequately protected. Therefore, process has to thoroughly fulfill constraints related to regulation, standardization, plans, practices and so on. During system operation, people node has to interact with process node without any safety risk. Then, safety requirements need to be considered during each step of the system lifetime (specification, conception, realization, etc.).

3) Intelligent object: covers various entities such as tags, sensors, actuators, equipment, etc. These devices have different communication capabilities regardless of their processing power, memory or energy. Intelligent objects can be deployed to work autonomously, as is the case of body sensors for an aging family member, or as part of a more complex system such as a smart lighting system providing the suitable city lighting needed by time of day, season, and weather conditions. Design of these objects have to deal with such pervasive character to comply with specific security levels.

4) Technological ecosystem: stands for technological solutions chosen to set up efficient functioning and acceptable security level of the overall system. Due to the considerable number of novel applications and entities, a comprehensive ecosystem is required to allow applications integration, data collection and processing, security measures, and interoperability. In a real implementation in IoT context, many questions need to be discussed about communications technologies, structural design, software and algorithms, privacy and trust methods, etc. For example, relation between people and technological ecosystem nodes has to fulfill user privacy requirements once technological ecosystem is used.

B. Edges

1) Privacy: stands for the relation between person and technological ecosystem nodes. It is about attention required to protect sensitive data of persons from disclosure in IoT environment. Due to the omnipresence of IoT endpoints and their ability to communicate over heterogeneous networks, data transmitted may be collected, assembled, and analyzed, which may lead to serious menaces of privacy. To provide an adequate privacy protection comparable to real world scenarios, privacy preferences of IoT users need to be considered during the conception phase of IoT technical solutions (privacy by design), and/or later, through privacy enhancing technologies.

2) Trust: relates the intelligent object node to the technological ecosystem node. In [7], trust is defined as "the subjective probability by which an individual, A, expects that another individual, B, performs a given action on which its welfare depends". In IoT context, it is very useful to set up a method of verifying collected data content, owner and usage. This allows users to decide how and when trust intelligent objects, and act accordingly. Based on an appropriate model of trust (rule-based, reputation-based, recommendation-based, social trust), persons become able to surmount ambiguity and accept novel IoT applications much easier. In addition, with the growth of contributors number, setting up mutual trust between entities become essential to improve the system functioning.

3) Identification / Access control: used to identify and localize objects, systems and persons. Due to its specific features (size, ubiquity, heterogeneity, etc.), IoT architecture has to consider access and identification of any intelligent object by any remote system through a global identification and addressing system would be mandatory. Researchers and constructors are looking for alternative solutions, and considering three important fields, namely: (i) multiple vs. unique identifiers, (ii) identifiers vs. network addresses; and (iii) resolution and discovery mechanisms.

4) Reliability: links the technological ecosystem to the process node and stands for the probability of failure of the system elements. Obviously, the speedy increase of communications number in dynamic contexts necessitates important reliability regarding environmental configuration, application strength in front of uncertainty and many other security threats. Possible solutions to guarantee system reliability may include redundancy tools (information, space, time, etc.).

5) Safety: focuses on protecting people and devices in the process running. In some cases, intelligent objects may behave randomly and lead to catastrophic results on the overall system. The main objective of this interaction is to facilitate our lives in a safe manner through many automated tasks (eg. notification of firefighters in the case of fire). IoT practical solutions may be build using sensors and actuators to supply databases with useful information and act efficiently to ensure people safety.

6) Responsibility: handles access rules granted to intelligent objects during process execution. An illustrative example is about an intelligent device which has the capacity of establishing and managing simultaneous connections with other devices, and differentiate their relevant authorizations.

7) Auto-immunity: concerns exclusively intelligent objects because they may be exposed to physical attacks in hostile areas (absence of communication channel, limitations of memory and calculation capacity, limited physical defense, etc.). In some risky situations, the intelligent object operation may be suspended or stopped. Then, it is useful to enhance system immunity against electromagnetic intrusion [8].

III. Case study: military live simulation

To highlight the usefulness of the systemic and cognitive approach, we consider the case of military live simulation. In the real world, operational units are facing a physical enemy in a real environment [9]. Live simulation is used to contribute in their operational preparation. That means, real people operate real instrumented systems, and only weapon's effects are simulated. These exercises will affect every sub-group, combine shots and maneuvers action and reveal the leaders skills. The replay and the after action review of actors choices and individual performances are also an important lesson for optimizing actions of actors [10]. In this scenario, nodes of the tetrahedron correspond to the following actors of live simulation:

Process: combat exercises such as injure control training, target recognition, penalizing effects, etc. Data provided by sensors, armored vehicles, tank, and other devices are assembled and analyzed to create instantaneous models, and scheduling algorithms of equipment control. This may be helpful to improve effectiveness and overall system operation.

Person: soldiers, troop commandant, personnel of the operations control center, tele-operators (conferencing, vehicles maintenance, medical service provider, etc.).

Intelligent object: sensors, actuators, equipment and vehicles, able to produce an exact image of real operations, to permit real-time control. Examples of intelligent objects may include tactile suit, integrated head based systems, etc.

Technological ecosystem: visualization tools (large screen projection, 3D-glasses, base flight simulator, human models, locomotion, gestures, etc.), tele-operating environment, communications infrastructures, etc.

In our IoT vision, interactions between military live simulation system nodes may be understood as follows:

Privacy: aims to reduce the risk of privacy disclosure of personal data (troop) when exchanged with technological ecosystem (radio link). Data control techniques such as anonymization, encryption, aggregation, integration and synchronization may be used to hide sensitive details while providing essential information usable for the relevant applications.

Trust: concentrates on soft security (technological ecosystem) to establish mutual trust between intelligent objects and persons, to create security guarantees and transparency during the military exercise. This leads the global system to make timely and trusted information available where it is needed, when it is needed, and to those who need it. Trust establishment will depend on two factors: the ability of the intelligent object to protect itself against a hostile environment, and person's ability to interrogate the node to see if it is still trustworthy.

Identification / Access control: consist of controlling illegitimate intrusions of persons/objects in restricted areas. They may concern identification and localization of artillery and arms, measurement of explosives and toxic chemicals, tracking of soldiers, detection of snipers, and surveillance parameters management in sensitive areas.

Reliability: focuses on reliability of information collected and results reported by technological ecosystem during the military process. For example, if simulators do not induce the same stress of a real combat, the consequence on a virtual simulation's reliability is imprecise, since humans act in different ways when stressed. In addition, occasionally equipment or vehicle may crash because unreliability was not simulated properly. To overcome this weakness, the simulated equipment behavior may model work failure, oil consumption or ammunition utilization at values deduced from real exercises.

Safety: aims to meet the need for intelligent objects, ensure their whole life cycle safety, and improve persons safety by reducing injuries and fatalities during exercises. In defense operations, an adversary may exploit the vulnerability of a medical device as cardiac pacemakers or diabetic pumps and cause death of victims. Another scenario may occur, when a soldier is

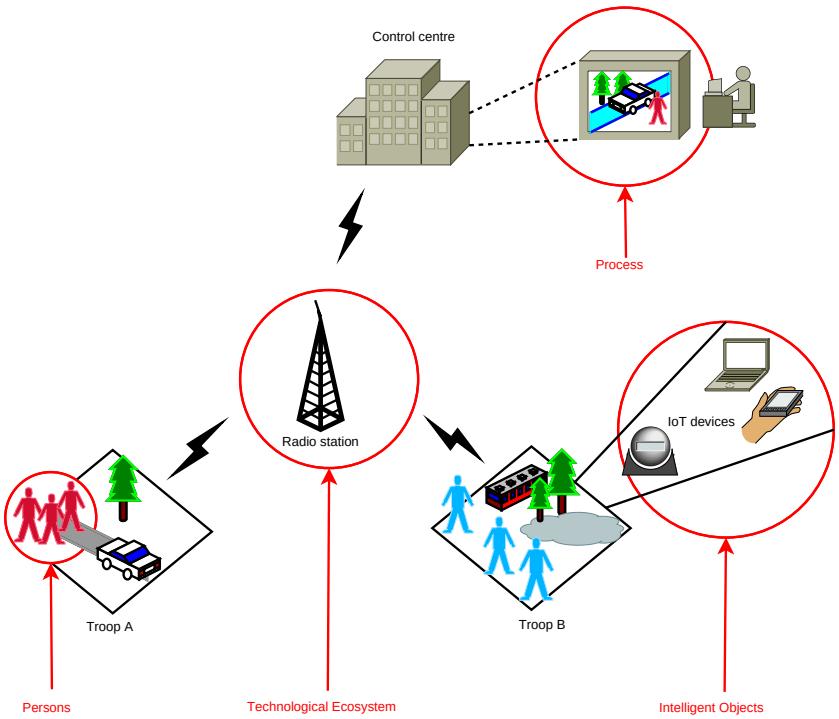

Figure 2: IoT systemic approach in military live simulation

warned dehydration, elevated heart rate, low blood sugar, etc. Monitoring systems may enable an efficient health system and/or supplying health services if necessary.

Responsibility: handles liability of intelligent object to perform a process. In live simulation scenario, IoT devices must answer only authorized reader's request. If a tactical change occurs, the responsibilities for monitoring would change automatically, and responsibilities are distributed across multiple intelligent objects to perform new processes. Consequently, it is the responsibility of the whole system to maintain a consistent task agenda by inserting missing actions, guaranteeing general domain knowledge and causality, and so on.

Auto-immunity: deals with the way to protect intelligent objects from physical attack in extremely harsh environments of military operations and providing resistance to shock and vibration; with the ability to self-monitor and reporting. It also focuses on better immunity of intelligent objects and communication channels towards interference and jamming.

IV. Open research issues

According to the concerns presented previously, many possible directions may be defined in the IoT security field. Issues related to safety, auto-immunity, reliability and responsibility will not be explored because they are regarded as prevention measures and considered at the system design phase.

Regarding *privacy* concerns, it is meaningful to implement applications for data minimization principle to reduce the amount of personal data collected and saved among IoT systems. In addition, new solutions can be developed to help people managing their own privacy settings and mechanisms instead of expecting the IoT system to implement their requirements. One possible solution is the use of game theory to model privacy management by data owners.

Identification in IoT context can be improved at different levels. A global identification scheme may be developed to help people when handling a large number of identification schemes, especially when hierarchical naming scheme used in Internet seems inadequate for heterogeneous and highly mobile environment. Also, interoperability problem caused by industries employing proprietary standards for entities identification needs to be discussed and solved. Another issue concerns the development of a new infrastructure using non-colliding unique addresses in dynamic and heterogeneous networks.

Access control mechanisms including *authentication* and credentials management are very important to IoT, whose sheer size makes implementing them a challenge. In addition to scalability issues, the complex relationships between persons and objects make credential management more difficult. The diversity of people and object identification techniques is another technological obstacle that requires detailed examination. Moreover, ubiquity of communicating objects facilitates the sharing of contents, entertainment, resources, etc. and leads to the emergence of a new sharing vector through people nomadism. We believe that

this sharing, will be a prime target for security attacks. Hence, it is necessary to develop effective solutions for peaceful secure sharing through adequate access control mechanisms supporting mobility. We can design peer-to-peer sharing systems, which are secure, efficient and equitable, while supporting users mobility.

Finally, we noticed a need for a general and generic theory for *trust* in heterogeneous networks where people and objects need to interact. Conceiving and implementing trust mechanisms to protect services/people/objects in changing infrastructures seems to be a challenging research direction. For example, understanding the exact relationship between computational trust and behavioral trust in IoT environment may be an important issue. Also, trust updating in changing network environments where entities (humans and objects) may be exposed to external attacks or may face severe energy conditions may be debated. Moreover, we remarked the lack of design and implementation of trust mechanisms in real network infrastructures such as cloud computing and IoT. Although various mathematical models of trust were proposed, their applications in real networks (such as WSN or RFID) are still limited.

V. Conclusion

The ubiquitous nature of IoT raises legitimate questions about security issues, and how to cope with the heterogeneity of user and application requirements accordingly. This requires the development of adaptive, context-aware security solutions. The ubiquity of objects encourages content sharing which, in turn, means paying special attention to security and privacy in a dynamic and heterogeneous environment. In this work, we provided a holistic systemic and cognitive vision of IoT involving four components. We have demonstrated that, by following our approach, it is possible to track and understand security challenges in a given context. To highlight this point, we presented a case study of IoT application in the military live simulation. Most of these challenges result from the vulnerabilities of IoT objects and the tight coupling of the real work of human beings to the virtual world through objects. Finally, we provided a concise discussion recapitulating the possible research issues in IoT security.

References

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future Gener. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.

[2] Y. Challal, "Securite de l'internet des objets : vers une approche cognitive et systemique," HDR, Universite de Technologie de Compiegne, 2012.

[3] A. Riahi, Y. Challal, E. Natalizio, Z. Chtourou, and A. Bouabdallah, "A systemic approach for iot security," in *DCOSS*. IEEE, 2013, pp. 351–355.

[4] A. Riahi, E. Natalizio, Y. Challal, N. Mitton, and A. Iera, "A systemic and cognitive approach for IoT security," in *International Conference on Computing, Networking and Communications (ICNC 2014)*, Honolulu, United States, 2014, invited Paper.

[5] L. Kiely and T. V. Benzel, "Systemic security management," *IEEE Security and Privacy*, vol. 4, no. 6, pp. 74–77, 2006.

[6] [Online]. Available: http://www.27000.org/

[7] D. K. Klair, K.-W. Chin, and R. Raad, "A survey and tutorial of rfid anti-collision protocols," *IEEE Communications Surveys and Tutorials*, vol. 12, no. 3, pp. 400–421, 2010.

[8] R. Acharya and K. Asha., "Data integrity and intrusion detection in wireless sensor networks," in *2008 16th IEEE International Conference on Networks*, Dec 2008, pp. 1–5.

[9] D. J. Medeiros, E. F. Watson, J. S. C. II, and M. S. Manivannan, Eds., *Proceedings of the 30th conference on Winter simulation, WSC 1998, Washington DC, USA, December 13-16, 1998*. WSC, 1998. [Online]. Available: http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=5993

[10] J. E. Hannay, O. M. Mevassvik, A. Skjeltorp, and K. Brathen, "Live, virtual, constructive (lvc) simulation for land operations training: Concept development & experimentation (cd&e)." NATO Science and Technology Organization, 2014.