IoT CHALLENGES & EVOLUTION

Mircea Constantin ŞCHEAU, PhD Candidate[*]

Abstract: *As a result of rapid social changes, the fundamental human right to information is increasingly linked more closely to the right of access to broadband services. The Internet is no longer just a technology, it becomes a way of life, one of the primary sources of all data categories, and perhaps the most common method of maintaining connectivity. In this context, the European Union Agency for Network and Information Security (ENISA) defines the Internet of Things (IoT) as "a cyber-physical ecosystem of sensors and interconnected action elements that allow intelligent decisions" [3]. However, IP protocols are no longer a sine qua non requirement of the IoT ecosystem, and therefore the word "Internet" in the meaning of IoT should be viewed as a generalization involving the notion of connectivity and should not be interpreted strictly technically. In another expression, the Internet of Things is presented as the entire amount of devices, vehicles, buildings and other electronics, software, and embedded sensors that communicate and exchange data [6]. In IoT environments, a "thing" is a physical or virtual object capable of being identified and integrated into communications networks, and it is imperative that all things be endowed with this connectivity capability alongside other optional features such as detection, recording, storage and processing of data, the execution of applications and / or functions required, Artificial Intelligence (AI), Machine Learning (ML), etc*

Keywords: *attacks, security, sectors, implications, protocols, communication, regularization*

JEL Classification: F50, K24, L51, O33

[*] PhD Candidate „Alexandru Ioan Cuza" Police Academy, Bucharest, Romania, E-mail: mirceascheau@hotmail.com

1. Regulatory, evaluation and certification IoT

IoTs may also be viewed as non-traditional computerized devices connected to the Internet, directly or indirectly, which may be classified according to the field of use in personal, service and control systems for public or private transport, smart homes, electric energy and building management systems, infrastructure systems, smart business, healthcare systems, industrial, space, etc. There is no complete list of possibilities created by Internet of Things technologies but practical value will be fully demonstrated when incorporated or separated applications and devices work together inside and outside the different sectors of a future "smart city", even if the reality of the years 2018 demonstrates that society is far enough from a harmonized system and that many segments are limited to Consumer Internet of Things (CIOT) only. The power energy system can be improved and the construction of a network or an intelligent infrastructure could reduce all costs in comparison to the traditional ones. Econometric modeling provides answers to many questions and the percentages relating to benefits can be calculated quite precisely. The field of passenger and freight transport would be more easily monitored and the decisions that need to be taken would be based on the observations and feedback provided in real real-time both by providers and by beneficiaries. In the health field, demographic trends suggest major challenges and clinical assistance related to prevention, early identification, treatment and in-hospital or remote monitoring could be greatly improved. Technical availability must be corroborated with the staff availability and other information that can lead to the saving of many lives. The desire to build completely autonomous agricultural farms is an indication that robotic farming is growing rapidly. In order to cope with environmental challenges, at this stage, field sensors provide information on ground humidity, temperature, wind speed, etc. In the new experiments, all sorts of devices capable of identifying and eliminating types / sets of weeds harmful to the crops / cultures concerned are used. It aims to maximize productivity and improve the food traceability. In the field of construction, intelligent buildings offer increased comfort, safety and optimum design at low cost. I listed only a few of the potential benefits of IoT under the conditions of responsible management.

In the first two decades of the second millennium, an entire ecosystem of institutions and organizations was created to focus on products testing, but reports have concentrated mainly on verifying the features declared by manufacturers in the presentation catalogs, performances have received more or less favorable reviews, depending on the outcome. However, in order to evaluate the software quality much experience is needed as well as access to both the documentation and the source code of the device firmware. Only the manufacturer has these information, the usual consumer having no significant accessible way regarding the security evaluation of any IoT device. This asymmetry of information between the consumer and the manufacturer relating to the safety of a product leads to a vicious cycle [3] and transparency can be seen as a notion on the edge which can be discussed only philosophically. In this situation, the role of the state institutions or of the international organisms is stated to be a regulatory, participatory or only a decorative one. It is considered that the effective involvement can determine the long-term evolution of this concept within a society and there are countries where the employed vision exceeds the simple proposals stage or the assistance:

- promoting a clear IoT policy;
- removing barriers and accepting a catalyst status;
- assuming the role of strategic expert and support for scalable demonstration projects to provide the environment and infrastructure needed for developers who are trying to implement new applications;
- building collaborative relationships with other experts from various fields and with regulatory authorities in order to draw up a roadmap for an IoT infrastructure;
- involving research communities and providing support for the development of standards to facilitate interoperability and security against cyber-crime and terrorism;
- including studying the concept in school curricula, educational sectors and prioritizing efforts to develop a skilled workforce;
- ensuring real-time access to innovative applications, paying attention first of all to the energy and transport sectors;

- developing a flexible and proportional model so as the areas affected by IoT might react quickly and effectively to technological changes and to balance taking into account the potential benefits and/or damage;
- developing collaboration with private entities and international partners to agree on best practices relating to security and confidentiality based on "default security";
- creating an advisory body bringing together the private and public sectors with the aim to coordinate the funding and support granted to relevant technologies, to promote public dialogue, and to oversee the potential risks and vulnerabilities associated with IoT implementation [15].

IoT communications systems are based on the ability to transmit and receive the information units in a structured manner even though the networks may have different sets of properties related to management, security, resilience, or Quality of Service Networking (QoS). Protocols ensure interoperability, whether distinct from each other or not, with different characteristics and they have defined their own standards: short-range radio, such as ZigBee, Bluetooth / Bluetooth Low Energy (BLE), Wi-Fi / Wi-Fi HaLow, RFID), long-range radio such as LoRaWAN, SigFox NarrowBand-IoT (NB-IoT) or LTE-M or on-IP, such as SMS, LiDar, Radar etc. [3] For scenarios in which data flows produced by the source devices owned by individual users can be made available to third-party data consumers (e.g., private data networks, including WI-FI, etc.), an "access token" can be used as proof of the authorized use of the system without requiring exposure or any other credentials. Resource owners may have subscribed to a Machine-to-Machine (M2M) service and third-party applications may be of the Web category used by the resource owner or another user who has permission to access the resource [11]. Analysis extended and to Sensor-to-Machine (S2M) and User-to-Machine (U2M).

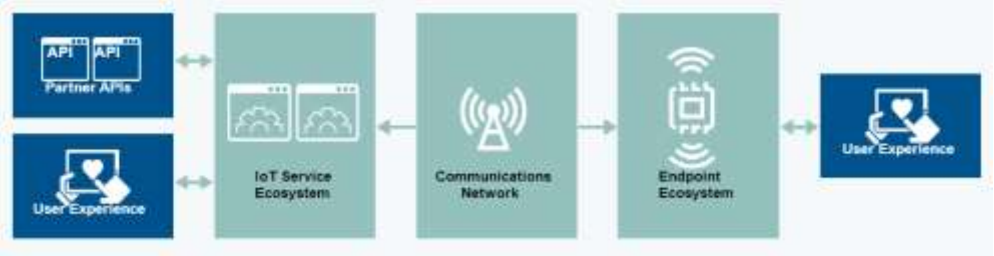

Figure no. 1: IoT Standard Model [5]

The idea of "evaluation and certification" is beginning to become more and more important. Based on the standard IoT model, a set of tests can be arranged to highlight some of the components' vulnerabilities in terms of reliability and service quality. The service ecosystem is the set of services, platforms, protocols and other technologies needed to provide capabilities and to collect data from the final points. The information is stored on servers, rendered to the user as values, parameters or commands, and may also be transmitted to authorized third parties. The endpoint ecosystem includes low-complexity devices that connect the digital world with the physical world through multiple types of networks and that includes sensors, digital locking systems for access areas, automotive telematics systems, industrial control systems and much more. The tools collect metrics (e.g. physical, chemical, biological metrics or information about network and applications) from the physical environment in which they were planted and provide data to different services, receiving orders or other specific instructions [4]. In order for IoT to evolve efficiently, the availability challenges need to be addressed - ensuring constant connectivity between services and endpoints, identity - authentication of services, endpoints and beneficiary customer, privacy - risk reduction for individual end users (e.g. automobiles, medical devices, etc.) and security-ensuring that the integrity of the system can be verified, monitored and corrected. Using the same operating language and common communication protocols between devices and / or components of different structures can lead to more rapid implementation of the same standards and to greater protection for the whole assembly. Managing processes and transmitting information in a controlled environment are essential conditions for ensuring a normal operating regime. If we talk about microprocessors, hard and soft producers will have a hard word to say in this case, and the competition related to the imposition on the market the most competitive products will be quite fierce. The scope of application is very broad and it is expected that the financial results of the companies will be proportional to the market share held, the effect sought at the population level being to increase confidence and a better understanding of the phenomenon. The establishment of a normal (or not) behavior is one of the biggest challenges in managing endpoints in a distributed IoT network, and this is not only important from a security perspective but also from the perspective of reliability. Often, the abnormal behavior may indicate a firmware or hardware problem and may be a signal of a possible exposure. Solving presupposes the ability to inspect and make decisions accordingly.

2. IoT Security

Until the beginning of the year 2016, IT security related to IoT was a concept that was mainly approached theoretically. The frequency of major incidents till that moment had been reduced, and maybe that was why it had not been given proper attention: in the year 2009 in Puerto Rico, repeated acts of energy theft occurred with the implementation of smart meters, and only in 2015 did the automotive industry receive a troubling wake-up call when it was demonstrated that it could be controlled on several vehicles simultaneously. However, everything changed between 2016 and 2017 when a large number of IoT devices became victims of massive Distributed Denial of Service (DDoS) attacks and many individuals, small private companies, multinational companies, or even national / international institutions suffered. Perimeter cameras, webcams, and affected routers made the security of IoT become a priority [13] and debates were launched in public space on issues related to restricting access to a device, the management transfer of ownership on a system, data auditing, Security Development Lifecycles versus Security Maturity Models, Secure Hardware versus Open Hardware, etc. One of the events attracted public attention in particular because it involved part of the country’s representative sports team [17] and all these cumulative incidents determined a clear repositioning of the phenomenon in question [18]. Must data be private? Do the data have to be secure? Is it important to receive timely data and in a secure manner? Is it necessary to restrict the access to devices and / or their control? Is it necessary to update the devices’ software? Should the property on the device to be managed or transferred in a safe manner? Do the data need to be audited? The answers to the set of questions led to the same conclusions in the specialized publications. It is estimated that to the global level IoT security spending will reach US $ 1.5 billion in 2018 and will exceed US $ 3 billion by 2021 [20], even if a study conducted under controlled conditions by a team within a university has revealed the fact that in about 30 minutes control over almost any wide-ranging IoT device can be taken with tools accessible to a simple internet search [10].

If we were to enumerate and try to classify some types of attacks according to their importance and the possible negative influence they can exert on the IoT medias I think that those on the first places are those acting against the network connections between the controllers and the actuators, against the sensors, modifying the values read by them or the threshold values / settings, against the separate actuators, modifying their normal settings or against the IoT management systems. Methods may include routine injection into command and control consoles, manipulation of power / voltage sources, alteration of acquired / captured metrics, exploitation of communication protocols vulnerabilities, implantation of a ransomware, or launch of a DDoS using the IoT botnet**.**

It can no longer be ignored that in the year 2018 criminals use botnets of tens or hundreds of thousands of compromised IoT devices to attack and temporarily take control of websites, corporate servers, and even critical internet infrastructures. This means that billions of extremely unreliable devices continue to proliferate public or private information transmission systems, facilitating access for criminals / hackers, even if the declared trend is to do everything "smart". The Internet is thus becoming a "polluted" ecosystem of exposed devices. And if a company with dedicated IT staff needs an average of 100 days to find that their systems have been compromised, how long may it take a domestic user to realize that their own router is part of a botnet? [8]. The desire to achieve a consistent profit is one of the triggering causes and therefore the financial and / or communications sector, like any other sector, can easily become the victim of well-prepared attacks [19], the recorded damages being up to the measure.

IoT can lead to an increase in the level of comfort but also creates new opportunities for exploiting cyber-attacks, which can cause material damage, harm to individuals and in the worst scenario, death. Devices and processes that have never been vulnerable to such aggression in the past can be handled with disastrous consequences [6]. In a system of equations with multiple unknown figures, the prioritization of security measures becomes a function dependent on the potential impact. Risk models differ substantially across the IoT ecosystem and those for industrial consumers (e.g. energy suppliers, nuclear operators, etc.) are wholly others than those for retailers.

IoT users should deliberately analise whether continuous connectivity is needed in view of the devices operation and the risks associated with their interruption. In the network environment, there is the probability that any IOT component might be disrupted over the life cycle, and therefore developers, manufacturers and IoT consumers should consider how an interruption can affect the main function of the device and the impact on the activity.

Good practice guides, including those related to about IT security, contain general guidelines as well as proposals for measures that are recommended to be implemented with a special character in this area. They are elaborated by experienced practitioners and trying to cover an area as large as possible of many gaps / breaks that can generate chain reactions:

- different and inconsistent / superficial approaches in matter of security;
- lack of public awareness abuot the security of IoT devices;
- initial design without an analysis about long-term evolution;
- poor administration of security management in the production process (e.g. IoT with malware installed from the fabrication);
- lack of interoperability between different architectures, platforms or simple IoT devices;
- communication solutions with matching deficiencies;
- lack of solid economic support to sustain adaptability;
- lack of good product life cycle management, etc.

Four key segments are identified [12]:

- General safety principles applicable to any devices, sensors and applications referring to a rigorous security including penetration tests and vulnerability reporting programs;
- User access and credentials referring to passwords encryption requirements, authentication devices, and integration processes of mechanisms with the purpose of preventing the connection attempts by "brute force";
- Privacy and transparency referring to the option / capability made available to users to reset devices to factory default settings, to the applicable regulatory requirements, including the General Data Protection Regulation (EU) 2016/680 (GDPR) and the principles of confidentiality, as

well as to the presentation of the possible impact on product features or functionality if connectivity is disabled;

- Notifications and best practices referring to promptly informing users about the threats and actions required, the need for authentication enabling the messages communicated to be received by the real recipient, etc.

Although there is no universal solution to mitigate the IoT security risks, assessed as an integrated part of any device connected to the network, it is recommended to include the concept as early as the design stage (e.g. ensuring through design security, confidentiality, communications protection, asset management, risk / threat identification and evaluation, etc.), but even so, some vulnerabilities are only to be discovered after the products have been installed. The identified errors can be mitigated through patches, security updates, and vulnerability management strategies. When drawing up these strategies the implications of a possible failure associated with sustainability should be taken into account, as well as the anticipated cost of fixing issues, and the fact that several phases should be followed in the process of implementing the projects, which is recommended to be in chronological order. The first phase refers to concept, design, market analysis, competitive analysis and research, the second phase to requirements and history, phase three to design, architecture and technological selection, followed by phase four on implementing/deploying, phase five regarding the verification and testing, and last but not least, phase six, which must address ensuring and maintaining the security of products. In addition, we can say that it is just as important for developers and manufacturers to know their own supply chain and implicitly if there are vulnerabilities associated with software and hardware packages provided outside of the organization [9].

The widespread adoption of strategic principles and associated practices could lead to an improvement. Several steps can be taken that begin with the elaboration and development of a security methodology and continue with the identification of particular features of the agreed security platform, the setting of objectives and levels of protection, design hardware-based security (e.g. the use of cryptographic modules, physical protection, fault protection, etc.), data protection through adequate selection of IoT communication protocols, applications and secured services analysis associated, implementation of the certification system in order to preserve the logical interfaces/API (Application programming interface), securing the update process, implementation of authentication, authorization and access control functions, elaboration of secure key management procedures, providing of registration and sample management mechanisms, internal and external security review / audit, resilience analysis, etc. [2] Additional steps may refer to simulate the worst-case scenarios, to the classification of information from the point of view of their value, determining the devices and databases that can be isolated and implementation of rollback functions ("reset" functions) to the factory defaults [1]. The solutions offered by research in engineering are essential for managing the growing complexity of systems interconnection dynamics and are based on a set of international standards published by the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC) and the Institute of Electrical Engineering and Electronics (IEEE). It is important for decision-makers to understand and address confidentiality risks in specific contexts such as: the responsibility of companies with regard to data protection and privacy, identifying the balance between "information anonymization / encryption" and government's legal access to information, the establishment of appropriate enforcement measures and penalties, etc. All the elements mentioned above are particularly useful in the risk assessment process and the objective is to address security issues from the perspective of needs, concerns and requirements for the protection of interested parties and to use the established processes with professionalism and appropriate rigor, early and in a sustainable manner, consistent with the life cycle of the systems [14].

The Internet is part of a global ecosystem and it is important that regulatory activities do not fragment and dissipate in inconsistent sets of international standards. Self-regulation in a field must take into account the already existing regulations in the areas with which it interacts and incorporate a flexible approach that allows adaptation to change at the same time. One of the keys to rapid progress in this area must be used to unlock all avenues of collaboration between the public and private sectors. Cyber-security is a common/shared responsibility, impacting all those involved in the process, and the failure to implement appropriate measures could become detrimental to both the final beneficiary and the producer who may be experiencing financial or reputational losses or the cost of imposing the withdrawal sanction of the product on the market. Even the groups of IT specialists who participated in the elaboration / implementation of the concepts would be affected because, although there is no body of jurisprudence yet that addresses the IoT context separately, the traditional principles regarding product liability infringement could be expected to be applied at the first instance [16].

3. Conclusions

GCI 2017 Edition [7] measured the commitment of the ITU member states related to cyber-security and highlighted a number of illustrative practices from different parts of the globe. This approach has motivated countries to improve their IT security connected work, has led to an increase in awareness of the need to commence and develop bilateral / multilateral international cooperation and has increased the visibility of what Member States are continually striving to improve - IT security. However, research has shown that although Internet access has increased and more mature technological development is correlated with improving IT security worldwide, this is not necessarily true for countries with developing economies and with lower levels of technological development. Data collection shows that developing countries do not have well-trained IT security experts as well as an in-depth assessment and necessary education on cyber security issues for law enforcement and continued challenges in the area of justice and legislation. Cyber-security has become an important part of everyday life, and the degree of interconnectivity of networks implies that everything and anything can be exposed. From national critical infrastructure to fundamental human rights, everything can be compromised. Therefore, decision-makers must seriously take in consideration policies that support the continual growth of complexity and refinement of the technology, accessibility and security, being very important for each country to adopt a national IT in the context of one common European / worldwide security strategy.

BIBLIOGRAPHY

Books, Articles:

AT&T - The CEO's Guide to Securing the Internet of Things, Exploring IoT Security, AT&T Cybersecurity Insights, Volume 2, 2016.

Cloud Security Alliance, IoT Working Group - Future-proofing the Connected World: 13 Steps to Developing Secure IoT Products, 2016.

ENISA - Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, November 2017.

GSMA (GSM Association) - IoT Security Assessment, 2017.

GSMA (GSM Association) - IoT Security Guidelines Overview Document, 2017.

HM Government - National Cyber Security Strategy 2016 to 2021.

International Telecommunication Union (ITU) - Global Cybersecurity Index 2017.

Jan-Peter Kleinhans - Internet of Insecure Things, 2017.

Ollie Whitehouse - Security of Things: An Implementers' Guide to Cyber-Security for Internet of Things, Devices and Beyond, An NCC Group Publication, 2014.

Omer Shwartz, Yael Mathov, Michael Bohadana, Yuval Elovici, Yossi Oren - Opening Pandora's Box: Effective Techniques for Reverse Engineering IoT Devices, Ben-Gurion University of the Negev, 2018.

OneM2M - Technical Report, 2016.

Online Trust Alliance and The Internet Society (ISOC) - IoT Security & Privacy Trust Framework v2.5, 2017.

PwC - Uncovering the potential of the Internet of Things, How the right cybersecurity and privacy safeguards can help businesses realize the promises of the IoT, 2017.

Ron Ross, Michael McEvilley, Janet Carrier Oren - Systems Security Engineering, Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, NIST Special Publication 800-160, 2016.

The Government Office for Science - The Internet of Things: making the most of the Second Digital Revolution, A report by the UK Government Chief Scientific Adviser, 2014.

U.S. Department of Homeland Security - Strategic Principles for Securing the Internet of Things (IoT), Version 1.0 November 15, 2016.

Internet resources:

Carolina – Sauna security camera hacked; nude videos of Dutch Women's Handball Team leaked, HackRead, (2018, March), [Online]. Available: https://www.hackread.com/sauna-security-camera-hacked-nude-video-dutch-handball-team-leak/.

Sead Fadilpašić - UK goverment looks to up security of IoT devices, ItProPortal, (2018, March), [Online]. Available: https://www.itproportal.com/news/uk-goverment-looks-to-up-security-of-iot-devices/.

Tom Spring - Mirai variant targets financial sector with iot ddos attacks, threat post, (2018, April), [Online]. Available: https://threatpost.com/mirai-variant-targets-financial-sector-with-iot-ddos-attacks/131056/.

Wunmi Bamiduro - Gartner Says Worldwide IoT Security Spending Will Reach $1.5 Billion in 2018, Gartner, (2018, March), [Online]. Available: https://www.gartner.com/newsroom/id/3869181.