CONSUMERS' REGULATIONS FOR INTERNET of THINGS

Robert-Alexandru CRĂCIUN[1], Radu Nicolae PIETRARU[1], Mihnea Alexandru MOISESCU[1]

Data services rise consumers' concerns which needs to be addressed. Consumers don't entirely understand how they must configure the Internet of Things (IoT) devices to be used in a secure way. There are regulations around the world that recommend the producers to implement secured IoT devices, but they come with some flaws. The present paper analyzes the attitude of consumers towards IoT devices, a brief analysis of some of the most important IoT regulations around the world and proposes a set of rules that can ensure the protection of both the manufacturer and the consumer.

Keywords: Internet of Things (IoT), IoT regulations, IoT security, IoT consumer devices

1. Introduction

All new data services, which are addressed for the consumers public (social networking services, search engines, digital economy services, price comparing services, IoT services) rise consumers concerns which needs to be addressed. The biggest worries for the consumers are the user's inability to control what data are used and for what purpose, maintaining data privacy and information security implicitly when the respective service is being used. This fact ensures consumers so that they can understand the vulnerabilities of devices and used services and how the consumers can notify those problems. Also, both the consumers and manufacturers, need to be responsible to keep the IoT services in a secure, predictable and trustworthy way [1].

The IoT concept represents the connection between every device, which can be turned on or off using a specific input, from an internet connection or from another device. IoT devices can be represented by any device which can establish a specific connection. Formally, the IoT concept can be defined as an infrastructure which interconnects objects, systems and information sources alongside services that allow processing of physical and virtual information from those elements. Commercial IoT devices can be of various types: intelligent vehicles, smart TVs, toys, security systems, washing machines, illumination systems. Also, IoT devices can be also used in other domains and provide solutions to uncommon applications for those domains like providing an IoT

[1] Faculty of Electronics, University POLITEHNICA of Bucharest, Romania, corresponding author's mail: robertcraciun28@gmail.com

monitoring system for beehives [2] or integrating IoT devices for renewable energy [3].

IoT brings some unique challenges when we talk about the security of the devices in this category. Most of the devices are deployed in environments that don't have a security model predefined. Also, the limited processing power of those devices is leading to security issues for the IoT devices. Those facts can lead to major exploits made by attackers, who can take advantage of the IoT devices and steal sensitive information, invade user's privacy and exposing them to security theft [4].

A simple representation of IoT architecture comprises of 3 layers: perception, network, and application layers [5]. A complex view of a reference model for IoT is proposed by Cisco [6] and addresses the following levels:

- Collaboration & Processes level related to People, Processes and Capabilities;
- Application level related to Reporting, Analytics, Control;
- Data Abstraction level related to Aggregation & Access;
- Data Accumulation level related to Storage;
- Edge Computing level related to Preprocessing and Data Analysis;
- Connectivity level related to heterogenous networks and Physical Devices & Controllers level comprising of all "Things" connected.

With the fast increase in number of IoT applications, numerous security issues appeared. Since IoT devices are becoming a part of the internet infrastructure, those devices inherit all the vulnerabilities found in classical computational systems. When everything will be connected to the internet, those vulnerabilities will be more obvious due to exposure of those devices to the global internet network. Thus, the security breaches can be exploited by hackers and they can obtain control of a digital environment which contains billions of IoT devices [7].

One of the most dangerous threats to computing devices is the malware. IoT devices also inherit this security issue which led to massive DDoS attacks back in 2016 [8]. Several organizations were targeted by the *Mirai* malware which consists in numerous exploited IoT devices, grouped in a botnet [9]. Basically, this malware is automatically discovering and infecting IoT devices, it uses brute force trying to gain access to the device and it also tries to exploit known vulnerabilities with the same final scope. These massive attacks highlighted the result of using IoT devices that are not ready to be securely used, having poor security mechanisms implemented by the manufacturers showcasing a devastating effect on the internet itself. The main cyberattacks that were presented to the public targeted the following [8]:

- A daily blog, started by Brian Krebs, covering computer security and cybercrime, which had a protection for DDoS attacks, but it was overwhelmed since the attack had approximately 620Gbps and it was too vast for the company that provided the protection to handle. The company withdrew the pro bono protection shield and the blog went offline until it used a solution offered by Google to mitigate the attack.

- A web hosting provider, OVH, which was targeted by a combined DDoS attack of 990Gbps which was considered to be the vastest attack of the time and consisted of approximately 145.000 IoT devices.
- DNS provider Dyn which claimed that the attack originated from 100.000 of endpoints. The attack caused issues for a large variety of popular websites like Amazon, Twitter, Reddit, Netflix and Spotify. The attack was mitigated after several hours and several waves of attacks.

A study led by a multinational company which is involved in the IT field, with a wide experience in producing computing devices revealed the fact that approximately 70% of the most used IoT devices from the market have some serious security issues. IoT devices contain serious security problems due to the way those devices were designed. Some issues can be insecurity of the communication environment, insufficient authorization and authentication configuration. Another vulnerability is reflected by the interconnection of IoT devices. This fact leads to a variety of new security and data exploiting methods which needs to be taken into consideration.

Connected devices for consumers do not include basic security features, hence they are vulnerable to the basic types of attacks. The lack of security for those devices is highlighted by the fact that manufacturers have no legal obligation to respect minimum security for the devices they design and to the fact that the awareness of the consumers is still low. Since there is no regulatory incentive that oblige manufacturers to implement at least minimum-security features for their devices, the market fails to provide appropriate measures. A general legal obligation for the cybersecurity and consumer protection for IoT products doesn't exist either in the Europe Union nor in Romania. Although, there are some general regulations present in different regions around the globe, they are not mandatory, and they are proposed as a recommendation.

The current paper is proposing to highlight the attitude of the consumers on the IoT devices, a brief analysis of some of the most important and recognized regulation recommendation articles and I will try to provide a set of rules that will protect the consumer by applying them by the companies in the manufacturing process. Those rules should be seen as a minimum-security effort that should be followed to ensure that the consumer can safely use all the benefits of the IoT devices they purchase.

2. Consumers’ Attitude on IoT

An attitude can be interpreted as a relatively enduring evaluation of people and things [10]. Attitudes can be related to cognition, affection, and behavior. The relation and order of components can be linked with the dominant component [11]:

- thinking / analyzing suggests the Cognition – Affect - Behavior model;
- action suggests Behavior - Affect - Cognition model;
- feeling may suggest Affect- Behavior – Cognition model.

Norms can influence attitude towards IoT. Norms influence behavior and can be expressed as formal – written and approved by a community, organization or legal body and informal – based on observation and imitation [10].

In general, IoT consumers must acquire separately the applications in order for them to use the IoT devices they purchased, and they need to configure on their own those applications. It is possible that the consumers may not fully understand the way that they need to configure the application and this fact leads to security issues regarding the used data. This characteristic increases the potential for vulnerabilities of IoT applications. That’s why, most of the time, the user needs to be informed about the capabilities of the application in order to get rid of those vulnerabilities as much as possible [12].

In most of the cases, IoT devices require numerous third-party applications in order for consumers to use all the capabilities of the devices. For example, a certain device needs two software applications in order for the device to be used with all its built-in features. In the moment when either one of those applications is not working anymore, the IoT device will no longer have access to all its features that were accessible through the respective application. Thus, there is a large variety of IoT devices and services on the market which can make a device perfectly functional, but whose features can’t be used on their entire exploitation capacity due to third party applications that don’t promise to provide support throughout the entire lifespan of the device [13].

The consumer needs to understand what services he acquires when he buys the IoT commercial product. IoT devices don’t come with integrated long-time support for the services that make the device to be usable with all its features. If the IoT application which is used to operate the device is disabled or it is deleted from the application store, then the device can no longer be used and it becomes a *bricked* device. The manufacturers need to offer application support for a predefined period of time when the application and device can be used without any issues [13].

A lot of devices and IoT services that are put into the market have a relatively low price. This price comes with a lot of limitations regarding robustness and overall system capabilities which offer poor privacy and security for a lower price. There needs to be a balance between two regulations: one that needs to force the IoT services to be designed with priority to security and another one that the IoT devices and services need to be sold with a minimum acceptable security to prevent the most common exploits [13].

A study conducted by Parks Associates [14], a company which is specialized in research and documenting in the IoT industry, the usage of the IoT devices that transform the houses into smart ones changes the attitude of the consumers regarding energy usage. Using energy efficiently in smart homes saves money, enhances sustainability and reduces carbon footprint [15]. From this point of view, IoT has a big potential to make a transition from centralized energy system to a decentralized system. Buildings can be both producers or consumers of energy and they can decide whether to act as one of those two cases. The standard case of a building it is that it consumes power from the electrical power grid, even though it has another renewable source that is helping producing energy. If a building has enough energy to sustain itself with renewable energy and it can produce more, then the building can be a producer and it can provide the excess energy to the electrical power grid of the area. This case is possible today using consumer IoT devices that can calculate the amount of energy that is needed for the smart home to run autonomous.

The role of labelling of IoT device packages is important for the purchasing behavior of the consumers. According to a study [16], security labels have a high potential from the standpoint of consumer choice and their desire to buy a specific IoT device. By using labels, the manufacturers need to ensure the consumers that the device they are paying for has a certain level of security. The labelling issue is also relevant for the packaging design. Since that on the device package there are already certification and conformity labels, there also can be a label which indicates the security level of the device. There is room for different variants of labeling styles, like presented in the study. It is imperative that this labeling should be used on every IoT device packaging for the consumers to be influenced to buy a product that fits the best his needs. The labelling system for IoT devices is still a sensible policy option despite of the high necessity of it.

There are a serious number of electronic devices users that don't know that they are using an IoT device. They can be unaware of the security issues of those type of devices or about the rights and obligations which the IoT device consumers should have. In an article published by Internet Society in 2018 [17], they highlight the most important rights that the IoT consumers should have, as well as the most important obligations that the same category should have. As a consumer, you should have the following rights: you should be able to buy a device that is designed to be secure, you should have a device that it is easy to make maintenance on, easy to make software updates and for how long the support is going to be available, you should know what personal data is collected, how it is collected and used, how it is protected and stored and who has access to it. Although, as a consumer you must be also aware of the obligations you have when using the IoT devices: you should only buy devices that you know that are secure, you should update your devices as soon as an update was issued for it, you should only buy devices which you know how the data is used and you should educate yourself about practices that you need to know for an acceptable level of data protection. This is just some basic information that every IoT device consumer needs to know when buying and using this kind of devices, with the recommendation that the user always needs to make research about security measures that he can apply for a better security.

3. Regulations Relevant for IoT

a. **U.K.** [18] – Even though there is a Code of Practice published in 2018 by the U.K. government, it is presented with a recommendation title and it is not mandatory for manufacturers to strictly follow it. Indeed, the Code of Practice is intended to be implemented as a legally measure by the U.K. Government to force the manufacturers to amend their product design and security policies for consumer IoT devices. Even though the recommended regulation it’s not coming to solve all the security challenges of the IoT devices, it assesses the most important security features that a device should have. The Code of Practice consists in thirteen guidelines which raises awareness to the industry for the most common security issues and helps it to implement them. The regulatory proposal starts with three of the most important security requirements that should be mandatory for every IoT device. The first one says that every IoT device must have a unique password and, if a reset is performed to the device, there must not be a universal password setting. The change for the default pair of authentication username and password combination was expected to be done by the user and this led to major security issues in the past. The second guideline states that every company, that provide a device which can be connected to the internet, must have a point of contact that can be reached by security researchers and other interested individuals to address vulnerabilities, which needs to be addressed in a timely manner. Companies should also continuously monitor, identify and fix security vulnerabilities for their own products. The third most important guideline addresses the fact that the software needs to be kept up to date. Updates must be offered for a minimum period of time stated when the manufacturer puts the device on the market. The updates must be made in a safely manner and if a device cannot be physically updated, then the product must be isolated or replaced. Alongside with the rest of the guidelines, this regulation is meant to increase the basic level of security for the products and U.K. can be the one of the first countries in the world which can have a mandatory regulation for IoT devices.

b. **Australia** [19] – The Australian Government proposes a good practices guide named *Code of Practice: Securing the Internet of Things for Consumers*. Like in the case of the regulation proposed by the U.K Government, this guide proposes a set of rules which can be applied in the design and implementation process of IoT consumer devices. This code was developed in collaboration with various Australian institutions, which are involved in the cyber protection of the nation and with the help of the consumer IoT public. Australia co-signed a statement regarding security of IoT [20] alongside the Public Safety Ministers of the United States of America, Canada, New Zeeland and the United Kingdom. According to the governments, the proposed code of practice is built and aligned with the guideline provided by the U.K. which was described earlier. A similar code has also been developed by the European Union [21] which follow and propose the same ideas as described in the code presented by the U.K.

c. **NIST - Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline** [22] – The document proposed by the National Institute of Standards and Technology gives recommendations for manufacturers on how to improve the security and privacy in the design process of the IoT devices. Manufacturers need to perform actions or provide services for their consumers to keep the cybersecurity of the device up do date for the entire lifespan of the device. This document offers a set of six cybersecurity activities that manufacturers need to keep in mind in the design process. Those activities are meant to improve the security of a new IoT device. The first four activities are addressed by the manufacturer before a device is sent into the market. Those activities focus on identifying the use cases of the device, as well as the users, in order to determine which security features the device should have, determining what kind of security is needed by the customers, in order for manufacturers to fully understand the consumers' risks, determining how to address customers' needs and making a plan to support the customer, in order for the IoT devices manufacturers to quickly address the issues that a user will have. The other two activities focus on actions performed by the manufacturers after the device sale and they involve defining approaches for communicating with the consumer and what information to communicate to consumers. Those six activities should provide a better support for the security efforts of the consumer and they should reduce the number of compromised IoT devices.

d. **ENISA - Baseline Security Recommendations for IoT** [23] – This document is proposed by the European Union Agency for Network and

Information Security and it defines a set of rules which offer a detailed overview of the security requirements of IoT devices, making a connection between the critical points of the system and relevant threats, addressing different security attacks and identifying good practice security measures to apply in the manufacturing process of the IoT devices. This guide proposes 7 recommendations for the design and implementation of an IoT device: promote consistency between security initiatives and regulations for IoT, raise awareness for IoT security, define guidelines for hardware and software lifecycle development, achieve interoperability for the IoT ecosystem, use economic and administrative incentives for IoT security, establish a secure IoT product and service lifecycle management and clarify liability among stakeholders.

4. Directions for Improving of Regulation for IoT Devices Consumer Protection

After the analysis made in the previous chapter, as well as others that have not been described in the current paper, it must be noted that those regulations are recommended with an optional title and they are not mandatory to be followed in the design and implementation phases of the IoT devices. There needs to be found common grounds in all of the existing regulations, propose other rules and try to make a unification. A new regulation must be proposed with a mandatory title and it must be followed by all manufacturers that produce consumer IoT devices.

Following the summary, a set of ten rules is proposed and defined that must be followed by manufacturers in order for them to provide an experience without security problems and without legal problems for consumers of IoT devices. Some of the following rules are taken from the current existing regulations, but others are new, which were not defined in the past in any of the studied regulations. The first half of the guide consists in new rules that come to complete the most important rules picked from all the studied regulations. To define those rules, there were analyzed several characteristics of consumer IoT devices that are available on the market and there were found common characteristics that those devices are lacking.

1. **Implementing a non-disclosure for user data** – There needs to be implemented a standing order in which to be exactly defined what kind of data are processed, what data are saved, in what way data are used, the time period for which data are collected, followed by an agreement made by the user for accepting or declining the rules in order for him to use the IoT device.
2. **Offer information about purchased services** – The manufacturer needs to offer specific information about all the hardware and software components purchased in the acquisition moment. The consumer needs

to know when he purchases the IoT device what software applications can be used to ensure that he can use all the features built-in the device. He needs to know how long the application can be used and the application developer need to offer support for the connection with the device. If the application stopes working and the connection with the device will be broken the user needs to know if he can still use the IoT device, if it can be changed with a new one or if it can be used with a third party application and with what benefits and risks can be used.

3. **Offering a predefined support period** – The IoT device manufacturer needs to mandatory offer a standard period of support of the sold device to ensure the consumer that for the entire predefined period the product can be used without any restrictions and no changes will occur when using all the components of the system.
4. **Offer support for connecting with other IoT devices –** The IoT devices are developed to be used as a standalone system and interconnected with other IoT devices. The manufacturers need to offer information for the consumers in order for them to know what other devices are compatible and how they can make the connection.
5. **Possibility to remain anonymous –** The producers need to ensure the consumer that, if he wants, he can offer information about the IoT system utilization anonymously and he should have the option to select this mode. In this case, previous used data should be deleted or anonymized.
6. **Using unique passwords** – There needs to be set a unique factory password, which shouldn't be easy to crack, it should be complex and unpredictable. Associated services need to have a form of multi-factor authentication for a more powerful protection against attackers.
7. **Protecting personal data** – When the devices or services process personal data, it needs to follow the protection laws in effect for all the geographic regions where the product will be sold. Consumers' personal data should be collected only if necessary and this process should be done with full transparency with the user. Also, privacy settings on an IoT device should be enabled by default and force full protection of the device.
8. **Offer an option to delete collected data from the device –** There needs to be an option where consumers can choose to delete data that was collected from the moment when the IoT device was initialized. There needs to be specific information on how the users can achieve this action and how consumers can verify if the data was really deleted from the manufacturer.

9. **Offer security updates for the software and hardware** – The manufacturers need to offer periodical updates for a predetermined period of time since the launch of the product on the market. The updates need to address all the vulnerabilities and security breaches which were discovered both by the community and the producer. It is also important that the updates must be made in a secure way that will not allow exploiting the devices since the moment of the new security patch update.
10. **Installation and maintenance should be easily done** – The manufacturers need to offer a guide for the consumer to easily install and setup the IoT device. The consumer should use the device without any issues described in this guide and most of those that weren't treated.

The guide described earlier should be mandatory used by any manufacturer of IoT devices to ensure at least minimal security requirements in order for them to be used in a fast expanding IoT market.

5. Conclusions

IoT devices are used in a large variety of environments, like houses, offices, buildings, cities, industry and military domain. Based on the application type and the device type, the data produced by the IoT devices can vary from environmental data, like temperature or humidity, to health care data, like hearth rate or blood pressure. Not all the data provided by the IoT devices are secured and confidential. Therefore, the need for the data that are coming from those devices that need to be secured has increased drastically recently, both for the data transmitted on the internet and for the stored data.

In general, IoT devices have a relatively lower price and they offer a limited computing power, leading to the incapacity of those systems to offer efficient security mechanisms. This fact leads to the incapacity of the IoT device manufacturers to consider, in the production process, the security component with high priority, leading to a faster implementation, a lower production cost and a faster delivery time. IoT devices security needs to be done from the design and implementation phases because the producers are those who need to offer a secured utilization experience for those devices.

There are numerous regulations available around the world, but they are recommended with an optional title and they are not mandatory to be followed by the manufacturers. Every regulation that was discussed in the current paper offers robust rules that can help manufacturers to build secure IoT devices, that can be used for an extended period of time and which it can ensure the consumers that all the data stored or transmitted in the utilization of the system it's being used without any concerns.

Most of the regulations offer efficient guides to follow to achieve security for the IoT device, but they don't cover all the cases in which the consumer can use the device with all its benefits. The regulations treated in the current paper don't cover an important fact for the consumers that is the support offered for the applications associated with the purchased device. None of those regulations cover what happens if the application stopes working and it can't be used anymore to access the IoT device's features.

The current paper seeks to provide a guide that combines some of the most important practices selected from existing regulations but also proposes new ones to improve the consumer experience. The guide is proposed in such way that both the manufacturers and consumers are protected from the most common problems that IoT devices have in present.

REFERENCES

[1] T. Alladi, V. Chamola, B. Sikdar and K. Choo: Consumer IoT: Security Vulnerability Case Studies and Solutions, IEEE Consumer Electronics Magazine 9 (2019) pp. 15-25

[2] M. VIDRASCU, P. SVASTA: IoT BEE HIVE MONITORING SYSTEM, U.P.B. Sci. Bull., Series C, Vol. 82, Iss. 2, 2020 pp. 189-199

[3] M. NAOUI, B. LEJDEL, M. AYAD: INTEGRATING IOT DEVICES AND DEEP LEARNING FOR RENEWABLE ENERGY IN BIG DATA SYSTEM, U.P.B. Sci. Bull., Series C, Vol. 82, Iss. 3, 2020 pp. 252-265

[4] Lee M; Lee K; Shim J; Cho SJ; Choi J. Security threat on wearable services: Empirical study using a commercial smartband. In: IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia). IEEE; 2016. p. 1–5.

[5] Santos, M. G. D., Ameyed, D., Petrillo, F., Jaafar, F., & Cheriet, M. (2020). Internet of Things Architectures: A Comparative Study. arXiv preprint arXiv:2004.12936.

[6] The Internet of Things Reference Model, http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf - Last accessed on February 23, 2021

[7] Internet of Things (IoT) | The rise of the connected world, https://www2.deloitte.com/content/dam/Deloitte/in/Documents/technology-media-telecommunications/in-tmt-IoT_Theriseoftheconnectedworld-28aug-noexp.pdf - Last accessed on February 23, 2021

[8] Major DDoS Attacks Involving IoT Devices, https://www.enisa.europa.eu/publications/info-notes/major-ddos-attacks-involving-iot-devices - Last accessed on February 23, 2021

[9] M. Baammi: Malware static analysis and DDoS capabilities detection. (2018) arXiv: 1812.00784.

[10] Niosi A. Introduction to Consumer Behaviour, https://kpu.pressbooks.pub/introconsumerbehaviour/chapter/understanding-attitudes/ - Last accessed on February 23, 2021

[11] Glasman, L. R., & Albarracín, D. (2006). Forming attitudes that predict future behaviour: A meta-analysis of the attitude-behaviour relation. Psychological Bulletin, 132(5), 778–822.

[12] Dupuis, Marc & Ebenezer, Mercy: Help Wanted: Consumer Privacy Behavior and Smart Home Internet of Things (IoT) Devices. (2018) 117-122

[13] Leonard, Peter G: Business-to-Consumer IoT Services, Consumer Protection and Regulation (December 1, 2017). Available at SSRN: https://ssrn.com/abstract=3154235

[14] Parks Associates https://www.parksassociates.com/ - Last accessed on February 23, 2021

[15] A. R. Al-Ali, I. A. Zualkernan, M. Rashid, R. Gupta and M. Alikarar, "A smart home energy management system using IoT and big data analytics approach," in IEEE Transactions on Consumer Electronics, vol. 63, no. 4, pp. 426-434, November 2017, doi: 10.1109/TCE.2017.015014.

[16] Johnson SD, Blythe JM, Manning M, Wong GTW (2020) The impact of IoT security labelling on consumer product choice and willingness to pay. PLOS ONE 15(1): e0227800. https://doi.org/10.1371/journal.pone.0227800

[17] IoT and the Role of Consumers IoT Campaign 2018 Article 2, https://www.isoc.vc/wpcontent/uploads/2018/12/IOT-Campaign-2.pdf - Last accessed on February 23, 2021

[18] Code of Practice for consumer IoT security, https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/code-of-practice-for-consumer-iot-security - Last accessed on February 23, 2021

[19] Code of Practice | Securing the Internet of Things for Consumers, https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf - Last accessed on February 23, 2021

[20] Statement of Intent regarding the security of the Internet of Things, https://www.gov.uk/government/publications/five-country-ministerial-communique/statement-of-intent-regarding-the-security-of-the-internet-of-things - Last accessed on February 23, 2021

[21] Cyber Security for Consumer Internet of Things, https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf - Last accessed on February 23, 2021

[22] Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline, https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf - Last accessed on February 23, 2021

[23] Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot - Last accessed on February 23, 2021