Security Risk Evaluation Methods in IoT

Pučko, Marjeta; Kos, Andrej; and Pustišek, Matevž

Abstract: ***The paper addresses the field of cybersecurity threats and risk evaluation with focus on the Internet of Things (IoT) where, for the business and private users, it is extremely difficult to get a balanced picture about risk severity. The reasons are the amount of different data sources, lack of common methodology, and market orientation of the security reports. An important part of risk evaluation methodology is a risk classification. In the paper we overview a set of existing IoT risk classification methods regarding restrictions that they are either architecture or product oriented. We present an original risk classification method, combining the architectural and product views with the view of business risks on top of risk classification. Practical examples of use in the IoT domains of energy production and distribution and in eHealth are also given.***

Index Terms: ***cybersecurity* threats, *Internet of Things (IoT), information security risk classification, information security risk evaluation***

1. INTRODUCTION

It is evident that with the continued increase of the Internet use, particularly via mobile devices, the gap between the level of global cybersecurity threats and the ability to early detect the risks and prevent from cyberattacks increases continuously, too. According to Eurobarometer cybercrime research [1] just under a half (47%) of EU citizens feel well informed about the risks of cybercrime. At the same time, European internet users express a high level of concern about cyber security. For example, 89% agree that they avoid disclosing personal information online and 85% agree that the risk of becoming a victim of cybercrime is increasing. 73% agree they are concerned that their online personal information is not kept secure by websites. Around two in three Internet users in the EU are concerned about experiencing identity theft (68%) and about discovering malicious software on their devices (66%). The same source also reports that these levels of concern about specific types of cybercrimes are considerably higher than in previous years, with the largest increase in relation to the identity theft (up to 16 percentage points).

KPMG [2] shows that many organizations lack the insight, both in terms of the outside threats and in terms of what is at stake for their organizations: 48% say that employees are not sufficiently aware of cyber risk, 44% of executive boards are not sufficiently aware of the risks of cybercrime, 51% cannot detect ongoing attacks, and 59% are not convinced that their service providers know how to defend against cyberattacks. 75% of respondent organizations agree that the main driver for intensifying controls is the occurrence of an incident and 51% believe that cyberattacks cannot be prevented.

According to Cisco 2016 Annual Security Report [3] particularly small and medium businesses pay less attention to security risks and security threat defenses. Only about 40% of the organizations use mobile security, secured wireless, and vulnerability scanning. For all of mentioned defenses their use was reduced about 10% in comparison to the year 2014.

However, a high level of awareness and concern about information security can be hardly achieved for business and private users without providing a clear picture on risk severity based on common risk evaluation methodology. In this paper we address the field of cybersecurity threats and risk evaluation in the Internet of Things (IoT), with focus on the methodological level to provide more balanced risk classification in the process of risk evaluation and planning of defenses.

2. MOTIVATION AND OBJECTIVES

2.1 Background and Motivation

Despite the enormous number of available public and private information sources on the state of cybersecurity threats, it is extremely difficult to get a realistic insight into actual security threats and risks. The reasons are the amount of different data sources, lack of common methodology and market orientation of security reports, provided by leading security equipment vendors from the viewpoint of their product portfolio. For an average Internet user and even for an ICT security professional, the actual state

Manuscript received June 10, 2016; revised June 27, 2017; accepted June 28, 2017. The work was supported in part by the Ministry of Education, Science and Sport of Slovenia. T. C. Author is Marjeta Pučko is a private consultant and lecturer, Slovenia (e-mail: marjeta.pucko@guest.arnes.si). A. Kos and M. Pustišek are with the Faculty of Electrical Engineering, University of Ljubljana, Ljubljana SI-1000, Slovenia, e-mails: andrej.kos@fe.uni-lj.si; matevz.pustisek@fe.uni-lj.si.

of cyber security and severity degree of security risks in her/his sphere of use is in practice difficult to estimate. There are so many data sources available and various alerts dispatched that the current situation leads more to confusion of business and private users rather than to supportive feeling. What they would require is a realistic cyber risk understanding as the base for the effective security management. IoT specifics brings, in addition to the security threats related to information technology, additional threats related to building blocks of operational technology and smart objects, where each device can be at the same time a target, as well as a possible entry point of attack.

2.2 Objectives

Objectives of this research are particularly to:

- overview the relevant existing classifications of IoT risks and ability to cover different views,
- develop an integrated classification, wide and open enough for use in different IoT domains (energetics, industry production, automotive, health, etc.), business oriented, and based on international information security management standards,
- provide practical examples of use in different domains of IoT.

2.3 Terminology

Terms related to information security and the IoT are used in the paper with reference to the ISO/IEC 27001:2013 considering general terms of information security systems [4]. Terms considering information security risk management are used with reference to the ISO/IEC 27005:2011 [5] and in reference to the security risk assessment methodology with reference to IntelliGrid environments [6].

3. RELATED WORK

We analyzed a set of existing classifications to cover different views of technology and products relevant for inclusion in an integrated view.

Cvitić, Vunjić and Husnjak [7] presented an IoT technological layer-oriented classification made bottom up from the perception layer to the application layer. Threats and vulnerabilities and protections are systematically analyzed for each layer considering, also, particular technologies (as Bluetooth, 6LoWPAN, etc.). The work is focused on the technology aspect and provides a solid methodology base to cover the IoT architecture and technology view of risk classification.

Cisco classification [8] is based on types of the connected devices defined as an origin of potential vulnerabilities/security risks. The Internet of Things is defined as the convergence of IT networks, operational technology (OT), and smart objects where each device can be a target of a possible attack. The model considers both cyber security and physical security to protect the operational technology and information technology networks working together. However, different security policies and priorities can be applied when needed. The classification covers the technological and the product view of different IoT building blocks and provides a security model regarding visibility of security events, control over security policy, analytics of real-data data from network and end-devices, and decision support.

Another product oriented view to risk threat/risk classification is used in the Security intelligence and event management (SIEM). SIEM solutions include products designed to aggregate data from multiple sources to identify patterns of events that might signify attacks, intrusions, misuse, or failure. The SIEM products are currently in a transitional period, which stands at a crossroads between legacy SIEM solutions, and newer solutions focused on the integration of big data, network forensics, and User and Entity Behavior Analytics (UEBA) focused tools [9]. The products are being improved by threat intelligence [10], with the addition of behavior profiling and better analytics. A similar classification concept is used in the unified threat management (UTM) and the next generation firewall product view [11]. It is based on product capability and feature strengths. Devices combine multiple security functions under one roof, incorporating next-generation firewall, intrusion prevention system (IPS) functionality, antimalware, virtual private networks (VPN), application control and other threat detection mechanisms. For now the UTM products lack more granular features with strong analytical support.

3.1 Security Affecting Features of the IoT

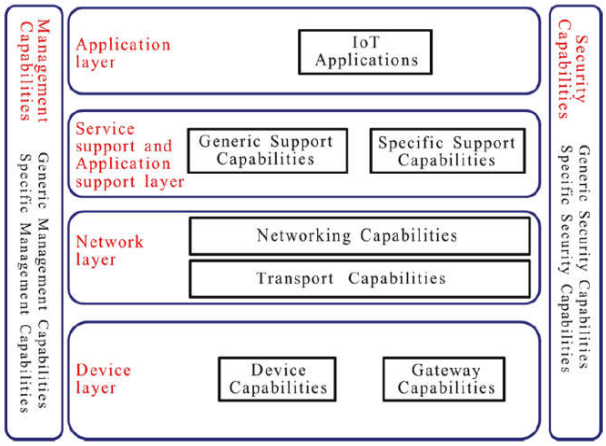

Figure 1: ITU-T Y. 4000 IoT reference model [12]

The IoT reference model [12] refers to security through the overall architecture (Figure 1).

There are several aspects of the use and operation of the IoT systems, which have a significant impact on their security evaluations.

In terms of IoT system architecture—as shown in Figure 1 - an IoT can be decomposed to smart (physical) devices, communication gateways and networks, and set of backend systems, usually provided as cloud-based services. Cloud backend systems collect, process, analyze, and act on data generated by connected devices, enable long term storage and (big data) analytics, and facilitate easy development of the IoT applications. Security capabilities stretch along all these layers.

The IoT devices can be numerous and very diverse. Often they have limited communication and computation resources, which can inhibit the use of the most advanced security algorithms. Moreover, cost reduction of the devices is often of key importance and life-cycles in IoT ecosystem can be longer than in e.g. use of mobile phones or computers. Along with increased users' expectation for ubiquitous and easy to use service, security in the IoT can be neglected for sake of utility, too.

4. CLASSIFICATION

4.1 Integrated Classification

The classifications described in Section 3 provide a detailed insight in different aspects of security risk evaluation and serve as the base of a multilevel integrated classification, taking into account also the business part of security risks.

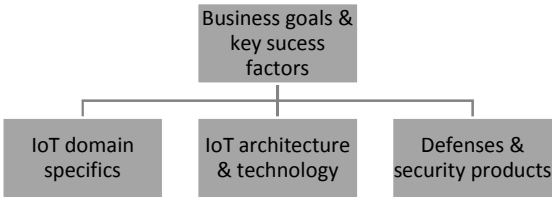

Figure 2: Levels of an integrated view to risk classification

Each risk of the view on higher level is decomposed into risks of the view on the lower level. The end result of this classification method is a tree of security risks, starting with the business view at the top and detailed technological view at the bottom. The classification level structure is presented in Figure 2. Risk classification starts with consideration of key business goals, success factors and identification of related security risks. At the technology level, security specifics of the IoT domain (data privacy requirements, regulation etc.) is analyzed in the next step, followed by the architecture and technological view to analyze and identify the IoT architecture layers with potential risks. In the final step of classification, actual defenses and security products are analyzed to secure the selected

Table 1: Security risks classification – an example of the smart grid IoT domain

View of risk evaluation	Outline	Risk description	Severity level
Business goals and key success factors	Increasing number of end customers	Low level of confidence in maturity and security of smart grid solutions	Medium
	Total operational cost reduction	Initially no cost reduction through investment, data breaches and opportunity costs	High
	Distributed sources of energy		
IoT domain specifics	Devices installed at every household	Dependent on existing energy grid infrastructure	High
	High manageability of network and end devices		
	Responsibilities for implementation depend on national regulation/policy	Service coverage dependent on geographical area	Medium
IoT architecture & technology	Use of smart meters	Architecture not designed for high level of security	High
	Use of smart gateways	Vulnerabilities in energy grid implementation, data breaches	High
	Use of SCADA systems		
Defenses and security products	Network protection devices – threat management	Insufficiently protected network, in particular wireless	Medium
	Analytic tools (SIEM)	Analytics not implemented or insufficient to detect security incidents	High
	IoT device management, hardware security		

architecture. The end result is a tree with the business view at the top (at the root node) and subsequently derived technological view of risks at the bottom (at the leaves).

4.2 Use in the Smart Energy IoT Domain

Electric power grid is facing rapid changes that reflect gradual introduction of distributed power sources (e.g. photovoltaic, wind), increase in number of electric vehicles, automatic meter reading, demand side management and the overall ambition for a highly reliable and manageable electricity production and grid operation.

The key IoT devices in smart grid are smart meters. These are numerous, unattended devices, installed typically in every household. Their communication capabilities are limited, since they usually rely on power-line communications or long-range low-power wireless technologies. The smart meters can be upgraded to smart gateways, to support the control of demand (e.g. by switching off/on specific loads). There is a clear financial motivation for potential fraudulent actions in smart meters, with known examples of successful breaches.

In terms of IoT backend systems, smart grid and energy productions strongly relies on established Industrial control systems (ICS), including Supervisory control and data acquisition (SCADA). SCADA systems were not originally designed to be connected to the Internet, so their role in smart grid presents enormous security risk, with unfortunately many successful breaches.

A simplified example classification is presented in Table 1. Business goals of smart grid deployment are focused on the increasing area coverage/number of end-users and reduction of total operational cost. The top risks related to the mentioned goals considering information security are a low level of confidence in maturity and security of smart grid solutions, and no initial cost reduction through investment, data breaches and opportunity costs. These risks are then decomposed through the underlying structure into a subset of most relevant risks related for each particular view. As a risk case, insufficiently protected network is not designed for a high level security, can be dependent on existing grid infrastructure and leads to data breaches.

4.3 Use in the eHealth IoT Domain

Use of eHealth worldwide strongly influences medical services market in the last years. Rapidly growing market of telemedicine services—such as teleconsultations, telemonitoring, different forms of teleinterventions—sets up high level of security requirements for service implementation.

As stated in [13] networked medical devices are vulnerable to more than just criminal intent. Like any other technology, they are prone to failure. Should any high-profile failures take place, societies could easily turn their backs on networked medical devices, delaying their deployment for years or decades. A second immediate concern is protecting patient privacy and the sensitive health data inside these

Table 2: Security risks classification – an example of the eHealth IoT domain

View of risk evaluation	Outline	Risk description	Severity level
Business goals and key success factors	To reach the target population of patients and health personnel	Slowly increasing number of end-users	High
	Total cost reduction of health services	Initially no cost reduction through investment, data breaches and opportunity costs	Medium
IoT domain specifics	Medical safety and information security of services	Improper implementation, loss of confidentiality	Medium
	Depending on population size/age for particular diseases	Too low awareness of end-users about importance of information security	High
	Importance of best customer experience	Inability to manage the devices properly (especially by elderly)	High
IoT architecture & technology	Use of telemedicine platforms and personal sensor devices	Unsafe and unsecure technology selected, unsecure services implementation	Medium
	Use of smart phone applications		
Defenses and security products	Network protection equipment – threat management	Insufficiently protected network, in particular wireless	Low
	Cryptography on different levels (data, communications)	Too poor level of cryptography	High
	Analytic tools (SIEM)	Analytics not implemented or insufficient to detect security incidents	High

devices.

A typical example eHealth service architecture is composed of telemedicine platform, smart phone (or other mobile device with data hub) application and set of end-user medical sensor devices, such as ECG, glucometers, blood pressure meters etc. Mobile and home-based devices connect via the Internet to clinicians to reduce hospitalization through early detection of critical medical conditions.

In the example presented in Table 2, top business goals of reaching the target population of patients and health personnel, and total cost reduction of health services can be affected by similar top risks from the business view, but quite different underlying subsets of risks, depicting the specifics of eHealth services deployment. Too low awareness of end-users about importance of information security for personal medical data and inability to manage the devices properly, especially by elderly, are typical risks origination from the IoT use and application. Unsafe and unsecure technology selected, with poor defenses on the lowest level, lead to improper implementation and loss of confidentiality.

5. CONCLUSION

The presented risk classification method, where we enhanced the architectural and product views with the view of business risks at the top of risk classification, has been developed. It provides an improved methodological tool starting the risk evaluation process with focus on business goals and key success factors and thus leading to the highest risks and consequentially information security costs. Its use was demonstrated by the practical examples in the IoT domains of energy production and distribution and eHealth.

For the future, we plan to continue our research by development of a full risk evaluation methodology and supporting tools based on big data analytics.

REFERENCES

[1] European Commission, Special Eurobarometer 423, "Cyber Security Report 2014", February, 2015, http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_en.pdf

[2] KPMG, "Clarity on Cyber Security", *KPMGKPMG International Cooperative*, Switzerland, 2015, http://www.kpmg.com/CH/en/Library/Articles-Publications/Documents/Advisory/pub-20150526-clarity-on-cyber-security-en.pdf

[3] Cisco, "Cisco 2016 Annual Security Report", *Cisco*, USA, January, 2016.

[4] ISO, International standard ISO/IEC 27001:2013, "Information technology -- Security techniques -- Information security management systems – Requirements", *International Organization for Standardization,* Switzerland, 2013.

[5] ISO, ISO/IEC 27005:2011, "Information technology -- Security techniques -- Information security risk management", *International Organization for Standardization*, Switzerland, 2011.

[6] IEEE, "Security Risk Assessment Methodology Using IntelliGrid Environments", IEEE, USA, IEEE P1649 Draft ver 1, October, 2005.

[7] Cvitić, Ivan, Vujić, Miroslav, and Husnjak, Siniša, "Classification of Security Risks in the IoT Environment", Proceedings of the 26th DAAAM Symposium on Intelligent Manufacturing and Automation, B. Katalinic (Ed.), *DAAAM International*, ISBN 978-3-902734-07-5, ISSN 1726-9679, Austria, 2016, pp.0731-0740.

[8] Cisco, The Internet of Things: Reduce Security Risks with Automated Policies, White paper, *Cisco*, USA, 2016.

[9] Gartner, "2016 Gartner Magic Quadrant for Security Information and Event Management (SIEM)", *Gartner publications*, USA, 2016.

[10] McMillan, Rob. "Definition: Threat Intelligence". *Gartner Publications*, USA, May, 2013.

[11] Gartner, "Magic Quadrant for Enterprise Network Firewalls", *Gartner Publications*, USA, 2016.

[12] ITU-T, "Y.2060: Overview of the Internet of things," *ITU-T*, Y.2060, June, 2012.

[13] Healey, Jason, Pollard, Neal, and Woods, Beau, "The Healthcare Internet of Things - Rewards and Risks", *Atlantic Council of the United States*, USA, ISBN: 978-1-61977-981-5, 2016.

Marjeta Pučko Marjeta Pučko received the B.S., M.S. and Ph. D. degrees in computer science from the University of Ljubljana, Slovenia, in 1988, 1991, and 1995, respectively. In 1988 she joined Jožef Stefan Institute, Department of digital communications and networks in Ljubljana as a researcher. From 1998 to 2009 she was with IskraTEL, Telecommunications Systems, Ltd., initially as an expert for telco systems design and testing, and later held different management positions in research, development and business improvement. In 2010 she joined Vzajemna health mutual insurance as head of IT department, information security manager and CIO deputy. Currently, at private consultancy, lecturing and managing different research and applicative projects, her interests concern ICT, business intelligence and data, information security, eHealth, e-learning systems and process management.

Andrej Kos (SM'98) received the Ph.D. degree in electrical engineering from the University of Ljubljana, Ljubljana, Slovenia, in 2003. He is a full professor at the Faculty of Electrical Engineering, University of Ljubljana, Slovenia, head of the Laboratory for Telecommunications and the chair of University of Ljubljana Innovation Commission. He started working in the field of telecommunications in 1996. Since 1999 he has specialized in modeling and design of high-speed networks and services. Currently, at the center of his work are broadband systems and applications of the Internet of things. Prof. Kos was part of the team that set up the MakerLab.

Matevž Pustišek (VM'01) received the Ph.D. degree in electrical engineering from the University of Ljubljana, Ljubljana, Slovenia, in 2009. He is a senior lecturer at the Faculty of Electrical Engineering, University of Ljubljana, Slovenia. His research is focused on the Internet services and applications, including mobile, Web, and IoT. A special interest is oriented towards the IoT architectures and security aspects. Recently additional focus is set on use of block-chain technologies in the IoT. At present he is collaborating in the Ekosmart project (http://ekosmart.net/en/ekosmart-2/) on smart cities and communities.