XVII International Scientific Conference on Industrial Systems (IS'17)
Novi Sad, Serbia, October 4. – 6. 2017.
University of Novi Sad, Faculty of Technical Sciences,
Department for Industrial Engineering and Management
Available online at http://www.iim.ftn.uns.ac.rs/is17

Guidelines for Overcoming some IoT Security Issues

Marija Rakic-Skokovic
(Lecturer, University of Novi Sad, Faculty of Technical Sciences, Trg Dositeja Obradovića 6, 21101 Novi Sad, Serbia, marijars@uns.ac.rs)

Abstract

The Internet of Things (IoT) has become a ubiquitous term to describe wildly diverse range of devices that are connected to each other via the Internet and have sensing or actuation capabilities. For many industries, the IoT offers significant new opportunities, but it also exposes them and their customers to a number of security issues as the previously closed systems are opened up to remote access and control. This paper illustrates some of the security issues that organizations should be aware of and proposes guidelines of how to overcome them and reduce risk across systems.

Key words: *IoT, Guidelines, Security Issues*

1. INTRODUCTION

The transition from closed networks to enterprise IT networks and than to the public Internet is accelerating and along the way raising awareness about security. Since 2009 the number of "things" connected to the Internet surpassed the number of people. Experts estimate that there will be 26 billion connected devices by the end of 2020 and that more than 25 % of identified attacks in enterprises will involve IoT, [3].

According to Gartner [3] "The IoT introduces a wide range of new security risks and challenges to the IoT devices themselves, their platforms and operating systems, their communications, and even the systems to which they're connected. Security technologies will be required to protect IoT devices and platforms from both information attacks and physical tampering, to encrypt their communications, and to address new challenges such as impersonating 'things' or denial-of-sleep attacks that drain batteries. IoT security will be complicated by the fact that many 'things' use simple processors and operating systems that may not support sophisticated security approaches."

The technologies and principles of IoT will have a very broad impact on organizations, affecting business strategy, risk management and a wide range of technical areas such as architecture and network design. IoT Security is listed to be be one of the top 10 IoT technologies for 2017 and 2018, ([3],[7],[8]).

Given these developments, IoT presents a variety of potential security risks that could be exploited to harm consumers by: (1) enabling unauthorized access and misuse of personal information; (2) facilitating attacks on other systems; and (3) creating risks to personal safety, ([7],[8],[10],[12]).

Businesses surveyed by the World Economic Forum identified cyber-attack vulnerabilities as their most important IoT concern. Threat hotspots include critical aspects of operational security, the diverse number of communication protocols in use today, vulnerable software patches and unsecure access management practices, ([10],[12],[14]).

The IoT materializes a vision of a future Internet where any object possessing computing and sensorial capabilities is able to communicate with other devices using Internet communication protocols, in the context of sensing applications. Many of such applications are expected to employ a large amount of sensing and actuating devices. As the Internet communications infrastructure evolves to encompass sensing objects, appropriate mechanisms will be required to secure communications with such devices, in the context of future IoT applications. Throughout their survey [5], Granjal et al, analyse existing protocols and open research issues with focus on security for communications on the IoT. According to their survey, the security mechanisms designed to protect communications with the previously discussed protocols must provide appropriate assurances in terms of confidentiality, integrity, authentication and non-repudiation of the information flows. Security of IoT communications may be addressed in the context of the communication protocol itself, or by external mechanisms, ([5],[12]). Other relevant security requirements that are stated as fundamental for the social acceptance of most of the future IoT applications employing Internet integrated sensing devices are: privacy, anonymity, liability and trust, ([1],[5],[11]).

Symantec's research on cyber security [13] has revealed how cybercriminal networks are taking advantage of vulnerabilities of IoT device security to spread malware

and carry out distributed denial of service (DDoS) attacks on more profitable targets, usually large companies.

Statistics based on the location of IP addresses to launch malware attacks, shows that more than half of all IoT attacks originate from China and the U.S. There are also high numbers of attacks from Germany, the Netherlands, Russia, Ukraine and Vietnam. In some cases, IP addresses may be proxies used by attackers to hide their true location.

IoT devices are a prime target, since they are designed to be plugged in and forgotten after basic set-up. Attacks originating from multiple IoT platforms simultaneously may be seen more often in the future, as the amount of the embedded devices connected to the Internet rises, ([5],[8],[13]).

2. OVERVIEW OF SECURITY ATTACKS

The IoT comprises a complex network of smart devices, which frequently exchange data through the Internet. IoT is using smart objects and network connectivity to get the information and it has to allow the reliable transmission and incorporate intelligent processing in order to maintain the high accuracy and real time of the systems function smartly, ([4],[16]).

There are several types of attacks on IoT [10] such as:

- Spoofing/Altering/Replay Routing,
- Denial of Service (DoS): Distributed Denial Of Service (DDoS) and Ordinary DoS,
- Sybil attack,
- Based on Device Property: Low-end and High-end device class attacks,
- Based on Access Level: Passive and Active attacks,
- Based on Adversary Location: Internal and External attacks,
- Based on Strategy: Physical and Logical attacks,
- Based on Information Damage Level: Interruption, Eavesdropping, Alteration, Fabrication, Message Replay, Man-in-the-middle,
- Host-based: User-compromise, Software-compromise, Hardware-compromise,
- Protocol based: Deviation from protocol, Protocol disruption.

In the case of layer-based attack and the attempt by an adversary to attack through communication protocol stack, where the attacker tries to compromise the objects of IoT, there are five levels involve, [15]. Some of the proposed methods/strategies for mitigating these attacks are presented in **Table 1**.

Table 1. Layer Based Attacks with Their Attacks Strategies in IoT Systems

Layer	Attacks	Strategies
Physical	Jamming	Creating radio interference and exhaustion on IoT devices.
	Tampering	Creating compromised nodes.
Data link	Collision	Simultaneously transmit two nodes of the same frequency.
	Exhaustion	Repetitive collision the nodes.
	Unfairness	Repeated application of exhaustion or collision based MAC layer attacks or an abusive use of cooperative MAC layer priority mechanisms
Network	Spoofed, altered or replayed routing information	Create routing loops, extend or shortening sources routes, attracting or repelling network from selected nodes.
	Selective forwarding	Selectively forward only some messages.
	Sinkhole	Create compromised node by forging routing information – all traffic information flow through adversary's node.
	Sybil	Creating duplicate identities on multiple locations of single node.
	Wormholes	Selectively tunnelling or transmitting information to the IoT devices.
	HELLO flood	Use HELLO packets as weapon to launch the attack on IoT system.
	Acknowledgement spoofing	Spoof the link layer acknowledgement of overhead packets destined for neighbouring nodes.
Transport	Flooding	Repeating the request of a new connection until the IoT system reach maximum level.
	De-synchronization	Disruption of an existing connection.
Application	False data filtering	Attack on data aggregation point in order to corrupt data.
	Clock unsynchronization (skewing)	Send falsified synchronization message so that nodes calculate incorrect phase offset and skew.
	False data injection	Launch attack by sending own packets to inject data or by comprising several sensor nodes and using them to inject false data into network.

3. EMERGING THREATS

When moving from the enterprise networks to networks built from a different type of end devices (handheld devices, embedded devices, isolated sensors) together with operation centre computers, organization is facing with two security issues: a) new attack surfaces appearing, and b) the old defence strategies no longer being valid.

3.1 New attack surfaces

The number of attack groups focusing on IoT has multiplied over the past years, [13]. Only in 2015, eight new malware families targeting IoT emerged.

Poor security on many IoT devices makes them soft targets and often victims may not even know they have been infected. Attackers are now highly aware of weak

IoT security and many pre-program their malware with commonly used and default passwords.

Embedded devices are often designed to be plugged in and forgotten after a very basic setup process. Many don't get any firmware updates or owners fail to apply them and the devices tend to only be replaced when they've reached the end of their lifecycle. As a result, any compromise or infection of such devices may go unnoticed by the owner and this presents a unique lure for the remote attackers.

Cybercriminals are hijacking home networks and everyday consumer connected devices to help carry out DDoS attacks on more profitable targets, usually large companies. To succeed, they need cheap bandwidth and get it by stitching together a large web of consumer devices that are easy to infect because they lack sophisticated security.

Most IoT malware targets non-PC embedded devices such as web servers, routers, modems, network attached storage devices, closed-circuit television systems, and industrial control systems. Many are Internet-accessible but, because of their operating system and processing power limitations, they may not include any advanced security features.

The most common passwords IoT malware used to attempt to log into devices was, unsurprisingly, the combination of 'root' and 'admin', indicating that default passwords are frequently never changed. Although the IoT malware is becoming more sophisticated, the DDoS attacks still remain its main purpose. With the increased processing power in devices and growth of IoT, attackers may change tactics in future, with branching out into cryptocurrency mining, information stealing, and network reconnaissance.

3.2 Staying protected

Having all these in mind, it is advisable to consider some simple security practice when employing IoT devices:

- Research the capabilities and security features of an IoT device before purchase.
- Perform an audit of IoT devices used on network.
- Change the default credentials on devices. Use strong and unique passwords for device accounts and Wi-Fi networks.
- Use a strong encryption method when setting up Wi-Fi network access (WPA).
- Many devices come with a variety of services enabled by default. Disable features and services that are not required.
- Disable Telnet login and use SSH where possible.
- Modify the default privacy and security settings of IoT devices according to organization's requirements and security policy.
- Disable or protect remote access to IoT devices when not needed.
- Use wired connections instead of wireless where possible.
- Regularly check the manufacturer's website for firmware updates.
- Ensure that a hardware outage does not result in an unsecure state of the device.

4. PROTOCOLS AND MECHANISMS TO SECURE COMMUNICATIONS

Connotations currently relating to the IoT include concepts such as Wireless Sensor Networks (WSN), Machine-to-Machine (M2M) communications and Low power Wireless Personal Area Networks (LoWPAN), or technologies such as Radio-Frequency Identification (RFID). As with the current Internet architecture, IP-based communication protocols will play a key role in enabling the ubiquitous connectivity of devices in the context of IoT applications. Such communication technologies are being developed in line with the constraints of the sensing platforms likely to be employed by IoT applications, forming a communications stack able to provide the required power-efficiency, reliability, and Internet connectivity. As security will be a fundamental enabling factor of most IoT applications, mechanisms must also be designed to protect communications enabled by such technologies.

IoT wireless protocols are potentially vulnerable to the following attacks, ([1],[5]):

- Sniffing network traffic,
- Injection,
- Tampering/Forging,
- Jamming,
- Exhaustion of battery,
- Collision and Unfairness (link layer),
- Greed, homing, misdirection, black holes (network layer),
- Flooding, desynchronization (transport layer).

Some of existing protocols and mechanisms to secure communications in the IoT are presented in **Table 2**., [5].

5. IOT SECURITY FRAMEWORK AND GUIDELINES

The Industrial Internet Consortium® (IIC), the global, public-private organization formed to accelerate adoption of the Industrial Internet of Things (IIoT), in September 2016 published the Industrial Internet Security Framework (IISF), a common security framework that addresses security issues in IIoT systems. The IISF emphasizes the importance of five IIoT characteristics – safety, reliability, resilience, security and privacy – that help define "trustworthiness" in IIoT systems. The IISF also defines risk, assessments, threats, metrics and performance indicators to help business managers protect their organizations, [6].

Table 2. Security Mechanisms and Proposals for IoT Communication Technologies

Operational layer	Security properties an functionalities supported	Context of application security	Method
6LoWPAN adaptation	Confidentiality, integrity, authentication, non-repudiation	Transparent end-to-end (network layer) security	Compression of AH and ESP security headers for 6LoWPAN; security in tunnel and transport nodes; pre-programmed keys with varying size
6LoWPAN adaptation	Resistance against fragmentation attacks	Communications between 6LoWPAN devices using fragmentation	Addition of a timestamp plus a nonce to the 6LoWPAN fragmentation header to support security against unidirectional and bidirectional fragment replays
6LoWPAN adaptation	Resistance against fragmentation attacks	6LoWPAN communications between sensing devices or end-to-end communications with external devices	Usage of mechanisms to support per-fragment sender authentication using hash chains and purging of messages from suspicious senders based on the observed behaviour
Transport layer	Confidentiality, integrity and replay protection	Security for CoAP multicast communications	Adaptation of the DTLS record layer to enable multiple senders in a multicast group to securely send CoAP messages using common group key
Transport layer	Confidentiality, integrity, authentication, non-repudiation	Transparent end-to-end (transport layer) security	Compression of the DTLS headers in the context of 6LoWPAN using IPHC; End-to-end DTLS using mutual authentication with hardware support provided by specialized trusted-platform modules supporting RSA cryptography; Transparent interception and mediation of the DTLS handshake, enabling the offloading of ECC pubic key computation to the gateway
Transport layer	TLS and DTLS mapping for end-to-end secure communications	Transparent end-to-end (transport layer) security	Mapping between TLS and DTLS using a gateway also providing HTTP to CoAP mapping
Transport layer	Support of end-to-end transport layer security for sleepy devices	Transparent end-to-end (transport layer) security for inactive devices	Usage of a proxy to support end-to-end communications and data retrieval from devices that may be inactive
Transport layer	Confidentiality, integrity, authentication, non-repudiation	End-to-end (transport layer) security with certificates and sessions managed at the gateway	Usage of the certificate pre-validation and session resumption to offload public key authentication to the gateway
Routing layer	Confidentiality, integrity, authentication, non-repudiation	Protection of RPL routing control messages	Definition of secure version of the RPL routing control messages, together with two security modes to protect routing updates
Routing layer	Security framework for ROLL routing protocols	Identification of security measures appropriate to the RPL routing protocol	Identification of security measures that can be activated in the context of RPL and of the system aspects that may impact on routing, as well as potential approaches in addressing them
Routing layer	Resistance against internal attacks	Protection of RPL routing operations against falsified routing updates	Usage of version number and rank authentication security scheme based on one-way hash chains providing security against internal attackers; Usage of a security mechanism combining parent fail-over with a rank authentication scheme to combat sinkhole attacks
Application layer	Confidentiality, integrity authentication, replay protection	Protection of CoAP application-layer messages using DTLS and the transport layer	Definition of bindings to DTLS to protect CoAP messages, together with three security modes with different approaches to cryptographic key management
Application layer	Support of the DTLS handshake using CoAP communications	Support authentication and initial key agreement with sensing devices employing DTLS	DTLS handshake messages are transported in the payload of CoAP application layer messages using CoAP block wise transfers to reduce 6LoWPAN fragmentation
Application layer	Confidentiality, integrity, authentication, non-repudiation	Transparent and granular end-to-end (application layer) security	CoAP security options allow for granular security, authentication of clients and secure transversal of multiple security domains

Security programs encompass a range of technologies and activities essential to a comprehensive, robust security posture. The National Institute of Standards and Technology (NIST) 'Framework for Improving Critical Infrastructure Cybersecurity' for example, has been adopted across many industrial sectors internationally, [9].

It identifies five essential program activities:

- **Identification**: Developing the organizational understanding to manage security risk to systems, assets, data and capabilities.
- **Protection**: Developing and implementing the appropriate safeguards to ensure delivery of critical infrastructure services.
- **Detecting**: Developing and implementing appropriate activities to identify the occurrence of a security event.
- **Responding**: Developing and implementing the appropriate activities to take action regarding a detected security event.
- **Recovering**: Developing and implementing the appropriate activities to maintain plans for resilience and to restore any capabilities or services impaired due to a security event.

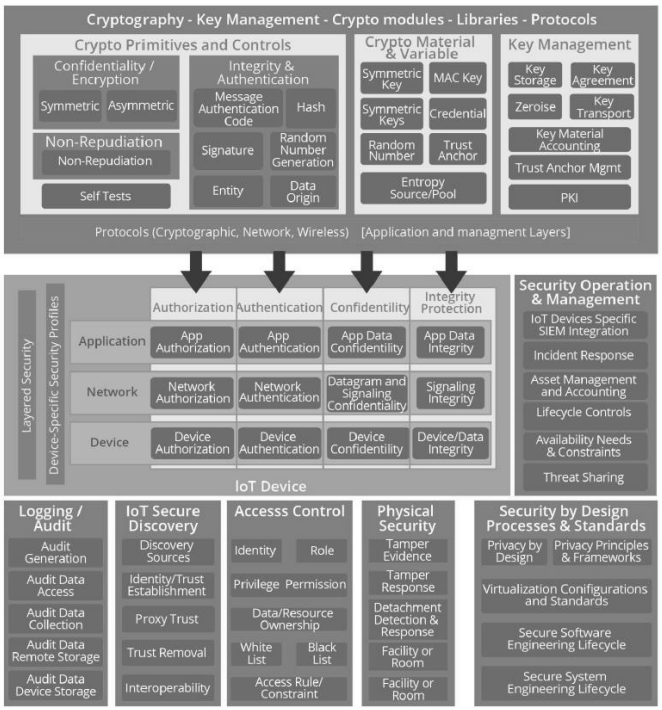
IIoT security cannot be considered in isolation. It comprises a complex set of industrial processes and applications as well as significant safety and reliability requirements. The IISF delivers security from business, functional and implementation perspectives. It helps business managers within industrial organizations make informed decisions based on well-designed risk assessments.

The mobile telecommunications industry, on the other hand, has a long history of providing secure products and services to their customers. Some of the representatives of this domain has therefore created set of security guidelines for the benefit of providers who are looking to develop new IoT products and services.

There are more different guidelines for adopting IoT. In [2] there can be found security controls recommended

for organizations implementing IoT capabilities (see **Table 3**). These controls have been tailored to IoT-specific characteristics to allow early adopters of the IoT to mitigate many of the risks associated with this new technology.

Table 3. Cloud Security Alliance - Security Guidance



A fragmented environment of proprietary IoT technical implementations will inhibit value for users and industry. While full interoperability across products and services is not always feasible or necessary, purchasers may be hesitant to buy IoT products and services if there is integration inflexibility, high ownership complexity, and concern over vendor lock-in.

In addition, poorly designed and configured IoT devices may have negative consequences for the networking resources they connect to and the broader Internet. Appropriate standards, reference models, and best practices also will help curb the proliferation of devices that may act in disrupted ways to the Internet. The use of generic, open, and widely available standards as technical building blocks for IoT devices and services (such as the Internet Protocol) will support greater user benefits, innovation, and economic opportunity.

6. ADITIONAL ISSUES TO CONSIDER

To improve its security profile while also pursuring value of IoT adoption, organization should consider the following suggestions:

1. Engineer trust into connected products - by applying “secure by design” principles throughout a product’s development, from concept ideation to series manufacturing instead of addressing security issues at the end of the cycle.

2. Adopt a new operational mind set - While attacks may not be preventable, it can be detected quickly and their effectiveness can be limited.

3. Develop threat models - Prioritize threats with models that are specific to organization.

4. Apply lessons learned - Gain insights from other industries and follow emerging standards.

5. Establish privacy by design - Maintain data security at collection and over the entire life cycle.

6. Educate system users - increase their ability to respond to sophisticated attack methods.

7. INEXPENSIVE STEPS TO SECURE IOT

One of the common reasons that IT managers state for organizations not to invest in additional security of their systems against intruders is that their IT assets are of little value. Manufacturers, for example, do not believe their control systems are of any value to hackers, as they do not hold critical information and are easily reset to factory defaults if hacked. Hackers view such targets as precious resources. Unsecured IoT devices are a treasure trove for botnet operators. It is the responsibility of IT managers to ensure these devices remain protected against botnet enlistment. IT security vendors offer expensive protection products. Alternatively, here are three simple steps to protect enterprise IoT against compromise, even on a limited budget.

7.1 Identification of IoT devices

Common IoT devices include security cameras, industrial lighting systems, and manufacturing controllers managed by a web-based solution. An example is an IP-phone provided by a cloud-based PBX. However, an IoT device is any non-traditional endpoint with an IP address. It is these systems that may become targets.

Some commonly overlooked IoT devices include multi-function printers, security scanners, and inventory scanners. A high-level place to start to identify non-traditional IoT devices is to look at IP addressing system. If there are tight controls around IP addresses, the IP address inventory is a good place to start identification. Administrators should audit their IP address system for unmanaged systems. Another IP address source is the DHCP system.

7.2 Isolation of the systems

Another best practice is to change default passwords and apply security updates to devices. In the case of some of the devices compromised in the Dyn attack, updates or changing the default password isn't an option.

A potential security mitigation technique is to isolate the devices from the production network. There's rarely a good reason for unmanaged, or even managed, IoT devices to reside on the same logical network as end-user devices and servers.

A solid approach is to create VLAN specifically for IoT devices. By placing the devices in an isolated network, administrators have the ability to apply layer 3 security

policies to large swaths of the network. Layer 3 network isolation allows the use of existing access control lists on routers and traditional firewalls to control the flow of communication between IoT devices and the production network. The approach allows for mitigation of risk associated with IoT devices attacking production systems, such as workstations and servers, [13].

7.3 Limited internet access

Placing IoT devices into an isolated network also provides the ability to deny internet access by default. Botnet operators want system resources that they can point toward targets on the internet. If the isolated devices neither have the ability to access the internet, nor infect other devices with an internet connection, administrators reduce the desirability of these devices to intruders.

8. CONCLUSION

The IoT promises to deliver substantial productivity improvements over the coming decade, but very few IoT assets feature adequate security. To guarantee security in IoT, properties such as confidentiality, integrity, authentication, authorization, availability and privacy must be assured for entire IoT system.

Operation of IoT relies on security at both the device and network levels. Implementing intelligence that enables devices to recognize and counteract threats it does not require any new inventive approach, but rather an evolution of measures and best practices that have proven successful in IT and mobile networks, adapted to constraints of connected devices and challenges of IoT. There are number of guidelines for IoT security challenges, covering the different types of threats, product and service development, work processes and device categories.

Security is not just about creating a right system from the start (i.e., ensuring that communication protocols offer the appropriate level of protection and having sufficient authentication mechanisms). At a minimum, it also requires continuous software updates, policies for key and password management and renewal, staff training and mechanisms for monitoring system integrity. Underestimating the risks of cyberattacks can lead to serious damages if they do occur and overestimating them will probably result in unnecessary investments in security products, personnel costs, and consultancy services. Moreover, if organization is focusing on the wrong type of threats it could lead to both of these negative effects.

Having in mind that attacks can never be fully prevented, companies should advance their cyber threat detection capabilities so they can respond appropriately and proactively. The challenge of learning how to stay ahead of cyberattacks takes time, but it brings considerable benefits for the organization by enable it to exploit the opportunities offered by the digital world, and at the same time minimizing exposure and the cost of dealing with the risks.

9. REFERENCES

[1] Asplund, M. and Nadjm-Tehrani, S. (2016), *"Attitudes and Perceptions of IoT Security in Critical Societal Services"*, IEEE Access journal, 2016. doi:10.1109/ACCESS.2016.2560919.

[2] Cloud Security Alliance (2015), *"Security Guidance for Early Adopters of the Internet of Things (IoT)"*, available at: https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf, (accessed: 30 August 2017)

[3] Gartner Inc. (2016), Gartner Special Report *"Internet of Things - IoT's Challenges and Opportunities in 2017"*, available at: http://www.gartner.com/technology/research/internet-of-things/report/?cm_sp=sr-_-iot-_-link (accessed: 30 August 2017)

[4] Gou, Q., Yan, L., Liu, Y. and Li, Y. (2013), *"Construction and Strategies in IoT Security System"*, Green Computing and Communications (GreenCom), 2013 IEEE and Internet of Things (iThings/CPSCom), IEEE International Conference on and IEEE Cyber, Physical and Social Computing. IEEE, 2013, pp. 1129–1132.

[5] Granjal, J., Monteiro, E. and Sá Silva, J. (2015), *"Security for the Internet of Things: A survey of existing protocols and open research issues"*, IEEE Communication Surveys & Tutorials, vol. 17, no. 3, third quarter 2015, pp. 1294-1312, doi: 10.1109/COMST.2015.2388550

[6] Industrial Internet Consortium (2016), *"THE INDUSTRIAL INTERNET CONSORTIUM DELIVERS THE INDUSTRIAL INTERNET SECURITY FRAMEWORK"*, available at: http://www.iiconsortium.org/press-room/09-19-16.htm, (accessed: 30 August 2017)

[7] Maddox, T. (2017), *"9 IoT global trends for 2017"*, available at: http://www.techrepublic.com/article/9-iot-global-trends-for-2017/ (accessed: 30 August 2017)

[8] McLellan, C. (2017), "*Cybersecurity in 2017: A roundup of predictions*", available at: http://www.techproresearch.com/article/cybersecurity-in-2017-a-roundup-of-predictions/, (accessed: 30 August 2017)

[9] National Institute of Standards and Technology (2014), *"Framework for Improving Critical Infrastructure Cybersecurity"*, Version 1.0, available at: https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf, (accessed: 30 August 2017)

[10] Nawir, M., Amir, A., Yaakob, N. and Lynn, O. B. (2016), *"Internet of Things (IoT): Taxonomy of Security Attacks"*, 3rd International Conference on Electronic Design (ICED), August 11-12, 2016, Phuket, Thailand, pp. 321-326

[11] Sadeghi, A. R., Wachsmann, C. and Waidner, M. (2015), *"Security and privacy challenges in industrial Internet of Things"* in Proc. 52nd Annu. Design Autom. Conf. (DAC), Jun. 2015, pp.1-6, doi: 10.1145/2744769. 2747942.

[12] Shantha Mary Joshitta, R. and Arockiam, L. (2016), "Security in IoT Environment: A Survey", Int. Journal of Information Technology & Mechanical Engineering - IJITME, Vol.2 Issue. 7, July- 2016, pg. 1-8, ISSN: 2349-2865

[13] Symantec Corp. (2016) *"IoT devices being increasingly used for DDoS attacks"*, available at: https://www.symantec.com/connect/blogs/iot-devices-being-increasingly-used-ddos-attacks, (accessed: 30 August 2017)

[14] World Economic Forum (2017), *"The Global Risks Report 2017"*, 12th Edition, available at: http://www3.weforum.org/docs/GRR17_Report_web.pdf, (accessed: 30 August 2017)

[15] Zhang, Y. and Kitsos, P. (ed) (2009), *Security in RFID and Sensor Networks*, Auerbach Publications 2009. ISBN: 978-1-4200-6839-9.

[16] Zhang, Y. W. and Zhang, X. (2012), *"Internet of Things"*, in [International Workshop, IoT], © [Springer] 2012,Changsha, China, August 2011.