DOI 10.15622/sp.2020.19.2.5

G. TSOCHEV, R. YOSHINOV, N. ZHUKOVA

SOME SECURITY ISSUES WITH THE INDUSTRIAL INTERNET OF THINGS AND COMPARISON TO SCADA SYSTEMS

Tsochev G., Yoshinov R., Zhukova N. **Some Security Issues with the Industrial Internet of Things and Comparison to SCADA Systems.**

Abstract. An issue of the Internet of Things security which does not belong to the traditional problem of cybersecurity, as it is a local or distributed monitoring and/or monitoring of physical systems state connected via the Internet, is considered. An architecture of Supervisory Control and Data Acquisition system (SCADA) was considered in previous authors studies. Due to SCADA systems implementation, vulnerabilities and various options of cyberattacks on them were analyzed. As an example, a case study based on trees was considered, and the obtained results were summarized and visualized.

The purpose of the paper is to compare new industrial technology of the Internet of things (Industrial Internet of Things) with the previously studied traditional SCADA systems.

The Industrial Internet of Things is a network of devices which are connected through communication technologies. Some of the most common security issues for the Industrial Internet of Things are presented in this paper.

A brief overview of the structure of the Industrial Internet of things is presented, basic principles of security and the main problems that can arise with devices of the Internet of things are described. Based on research and analysis of the risk of threats in the field of the Industrial Internet of things, a specific case of destructive impact based on a tree analysis is considered as the main approach. A description of an attack tree leaf node value creation and an analysis of results are provided. Analysis of the electronic record change scenario to increase the infusion rate of an overflow pump using a complexity index is performed. The consequences compared to a previous study of SCADA systems are analyzed, and respective conclusion is made.

Keywords: Internet of Things, Industrial Systems, Scada, Attack Tree, Cyber Security, Network and Information Security.

1. Introduction.

In modern society, information and communication technologies have penetrated deeply and have become the basis of all activities in the economy, administration, society and privacy. Digital infrastructures are turning from a supportive environment into a major and critical factor for the management and proper functioning of all resources and systems [1].

The so-called digital transformation of the industry has emerged in the overall development of the digital society [2] in recent years, which is the result of the increasing penetration of the Internet of Things (IoT), robotics, 3D printing, cloud solutions, and artificial intelligence-based cognitive technologies. All these technologies form the so-called Industry 4.0, driven not only by design and production, but also by its relationship with the market and consumers.

Industrial technologies are among the top 5 priority areas in the EU's 2020 development strategy.

According to the Concept for Digital Transformation of Bulgarian Industry: Industry 4.0 [3] is a collection of related digital technological solutions that support the development of automation, integration and real-time data exchange in production processes. In essence, this reflects an industrial and technological transformation process that naturally follows the development of scientific and production practices. The fourth industrial transformation is a natural extension of the digitization and automation of production and includes Internet connectivity and interaction of cyber-physical systems without human involvement, processing and analysis of large information arrays, and decision making from artificial intelligence, digital modeling and simulation of production processes through virtual reality, smart automation, mass production of individualized products, the emergence of new technologies, the creation of new businesses divisible.

The future of industrial automation is evolving in such a way that robots replace humans. In the course of Industry 4.0 revolution, a new term for technological automation of processes, the Industrial Internet of Things, was introduced.

A previous study looked at the nature of the supervisory control and data acquisition (SCADA) system [4]. Through the introduction of Scada systems, vulnerabilities and various options for attacking it were analyzed. A case study based on trees was considered as an example and the results were summarized and visualized. The effects were analyzed and a conclusion was reached.

This article is intended to make a comparison with the new Industrial Internet of Things technology and to compare the results obtained with a previous study on traditional SCADA systems.

2. IoT – Definition protocols, architecture and standards. IoT is a set of technologies and applications that make devices capable of generating any kind of information, connecting these devices for instant data analysis and ideally for "smart" action (Fig. 1) [5]. Conceptually, IoT means that physical entities can use protocols to send information about their status, position, or other data.

The whole end-to-end communication of the IoT consists of three main components: embedded devices, gateways and end applications. Embedded devices connect to their local gateway through protocols such as 6LoWPAN, ZigBee, ZWave, Thread, Bluetooth and Bluetooth LE, WiFi and WirelessHART, etc. There are also a number of remote IoT protocols such as LoRaWAN, NB-IoT, etc. Sector home automation The Home Network Automation Protocol (HNAP) is adopted by many vendors as the preferred protocol for device management. The protocol was originally patented by Pure Networks, but is now owned and developed by Cisco. At the low

power level of the application, Constrained Application Protocol (CoAP) is an IETF protocol designed for RESTful applications and uses HTTP semantics (and transmitted via HTTP a wider network) but with a much smaller footprint and binary, not text, exchange. CoAP is intended for use over UDP. MQTT, The Message Queue Telemetry Transport, is an alternative to CoAP and is deployed as a protocol for publishing messages on wireless sensor networks**.**

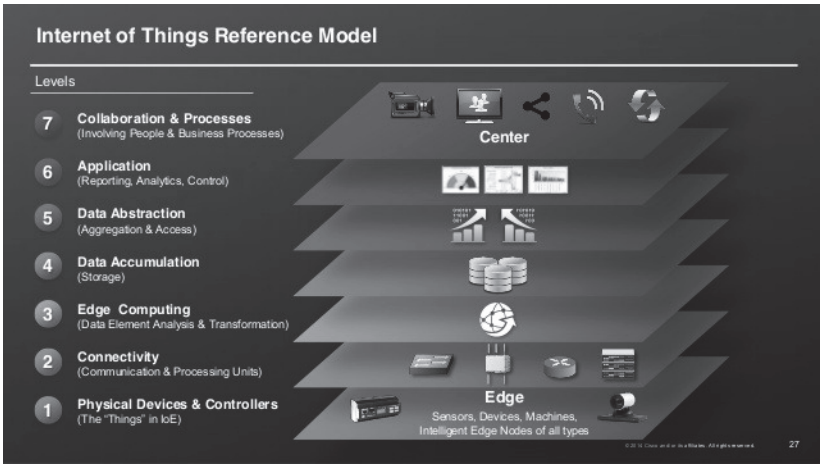


Fig. 1. Internet of Things illustration [6]

The DNS Multiple Transmission Service (mDNS) is often used by IoT devices to detect hostnames to IP addresses within small networks that do not include a local name server. The development of Internet interoperability standards known as Hypercat is encouraged. This standard is intended to improve data discoverability and interoperability and to enable device catalogs and capabilities to be published as web storage for connected metadata devices. This is currently one of the preferred interoperability options. As with any new technology, there are many protocols and standards that are tested and offered for inclusion in IoT, they will form part of the detailed IoT reference structure. They will probably be supported in a timely manner by case-specific implementation profiles. The IoT security architecture is part of the broader IoT reference architecture. It starts with business results and stems from the security and control requirements that can be followed for those results. Given the widespread adoption of IoT, specific arguments for on-demand security architecture will be developed using standard building blocks. The nature of IoT technology (Fig. 2) will place unusual requirements on architecture such as low power algorithms, cryptographic algorithms and low latency communications [7]. Identity and

access management is another challenge that requires quite different solutions to traditional corporate understandings. Secure interoperability will lead to the need for security standardization and account standardization.

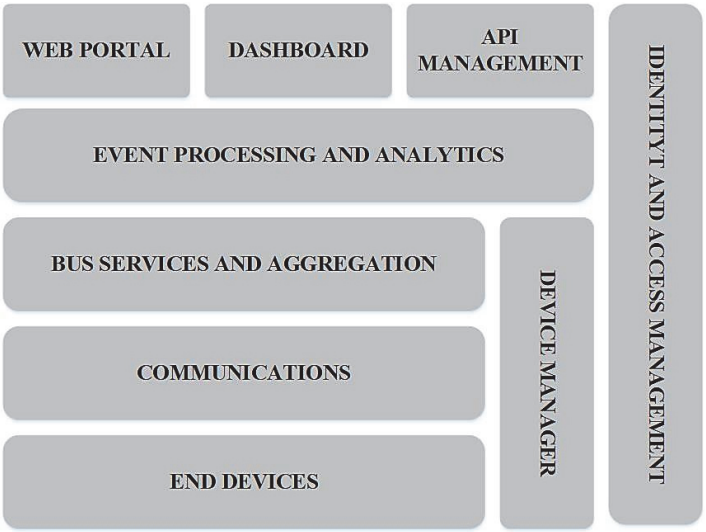


Fig. 2. Architecture of IoT

3. IoT Security and privacy. A key part of the growing interconnectivity response is to ensure that the systems provided are available on request and can be trusted to protect the user's privacy. Given the commodity nature of many IoT devices and the implications of security and privacy, a stable framework of trust is required that is incorporated into product design [2]. The approach should be based on an open and integrated business model, an IT oriented architecture, and a user oriented trust model.

Data needs to be more open and interconnected, but privacy and security must be at the heart of how it is stored and used. In particular, data centralization and reconciliation can be met with suspicion on the part of users and must be managed with care. There is a set of devices that require identity; they totally have a different model of trust [8]. Identity is a complex and deeply personal concept with individuals with multiple overlapping identities, each with different rights and permissions. Some identities must be kept separate and some must be consolidated. Therefore, it must be considered on a case-by-case basis whether the identities are kept separate or united, subject to the requirements set out in the Personal Data Protection Act and all other applicable laws. New ways of introducing identity protection mechanisms (passwords, PINs, digital signatures) have in practice become barriers to the de-

ployment of digital services. Traditional IT systems implement security based on 25 years of security control standards that are difficult to relate to current cyber security requirements; they are quite inadequate to use as a basis for security and trust in IoT. The use of enterprise security controls is not well-functioning in the industrial control systems sector, where the requirement for continuous operation is incompatible with routine updating and restarting. In the same way, it is unlikely that a home light bulb will constantly check for updates, apply updates, and monitor cyber-attacks [9]. The evolution of IoT requires an approach to security and privacy that is flexible and supports unforeseen changes across a wide range of completely different technologies and applications. It requires an approach that recognizes the global ecosystem, made up of different sectors, using common solutions developed independently, in accordance with a common set of principles, but introducing a sector-specific interpretation of security. A common basis for this could be a data layer security application. An end-to-end security model between a device and an application that has reliable data analysis can be considered as part of the solution. Identity management needs to be developed as carefully as security.

4. IoT Resilience. As all sectors of government, industry, and society reap the benefits that can be realized through IoT, so is the dependency on real-time connectivity. This means that networks must not only become resilient [10], but must also strive for security to allow continued operation in the event of a cyber-attack. Internet connection communications offer some new challenges with the use of ultra-low power protocols and algorithms. While some research has been done to ensure security, resilience is an embryonic discipline that urgently needs a lot of attention.

4.1. Cybersecurity vs. IoT and cyber-physical security. The Internet of Things security is not traditional cybersecurity, but a merger of cybersecurity with other engineering disciplines. It addresses much more than just data, servers, network infrastructures and information security [8]. Rather, it involves the direct or distributed monitoring and / or control of the condition of physical systems connected via the Internet. In other words, what distinguishes IoT from cybersecurity is called "cyber- physical systems" [11]. Cybersecurity does not usually address the physical security aspects of a hardware device or the interactions in the physical world that it may have. Digital control of physical processes on networks makes unifying IoT, since security is not limited to the principles of providing basic information in terms of confidentiality, integrity, etc., but also of physical resources and machines that originate and receive information in the physical world. In other words, IoT has many real analog and physical elements.

IoT devices are physical systems, many of which are safety related. Therefore, the compromise of such devices can lead to physical damage to

persons and property, even death. Therefore, the object of IoT security is not to apply a single, static set of meta-security rules, as they apply to network devices and hosts. This requires a unique application for each system and system of systems in which Internet devices are involved. IoT devices have many different options, but an IoT collective device has almost all of the following features:

— Manipulates or monitors something physical (in the device or in the middle or middle of the device), the job itself or the direct connection to something;

— Ability to communicate directly or indirectly via the Internet.

Knowing these two properties, any physical system can be an IoT device because everything physical can be connected to the Internet with appropriate electronic interfaces. IoT device security (Fig. 3) is a function of device usage, physical process, or the state affected by or controlled by the device, and the sensitivity of the systems to which the device connects.

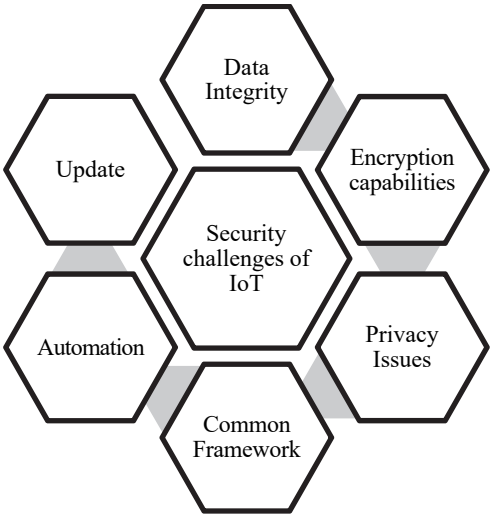


Fig. 3. Cybersecurity of IoT

5. IoT Security Principles. Security has traditionally been considered in terms of confidentiality, availability and integrity. There is no best internet security design. There are many different IoT devices and security needs to be considered in the context of how the device will be used. The device itself will not provide complete security; it must be supported by good end-to-end architecture. While the business requirements are best de-

signed for each use case, the IoT Security Foundation has identified a number of IoT security principles [12]:

— Establishing Principles for Internet of Things Security

— Does the data need to be trusted?

— Is the safe and/or timely arrival of data important?

— Is it necessary to restrict access to or control of the device?

— Is it necessary to update the software on the device?

— Will ownership of the device need to be managed or transferred in a secure manner?

— Does the data need to be audited?

They are grouped into three areas (Fig. 4).

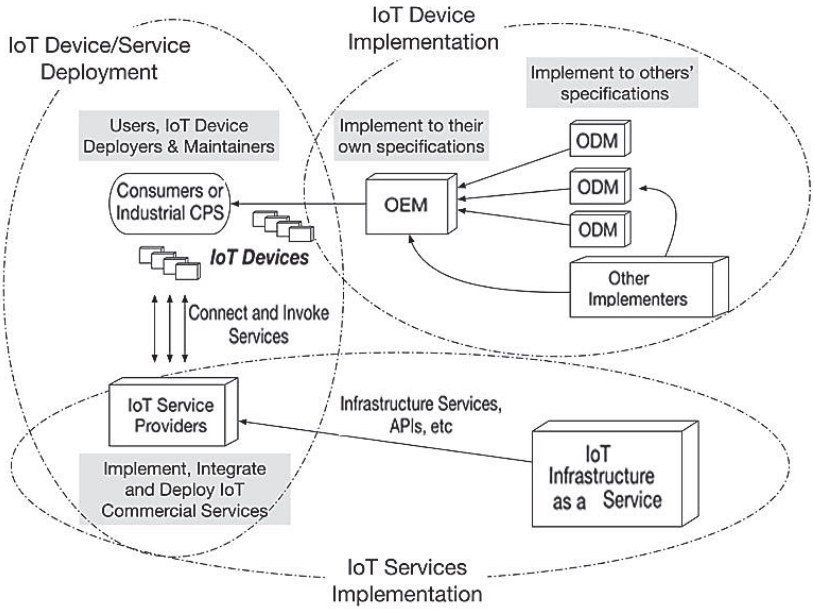


Fig. 4. Connections between IoT devices

5.1. Application layer. CoAP uses Datagram Transport-Layer Security (DTLS) to secure messages in CoAP – a TLS variant that can take on the unreliable nature of UDP communications. It has a small number of compulsory configurations identified as suitable for restricted environments. This provides support for confidentiality, authentication, integrity, denial and protection against repressive attacks. CoAP has four security modes for key management: NoSec, PreSharedKey, RawPublicKey and Certificates.

The DTLS connection for authentication and key consent has a significant impact on the resources of restricted devices, especially the requirement for encryption with an elliptical curve. Studies in DTLS optimization continue in the middle of the Internet of Things and incorporate elliptical curve cryptography into hardware.

5.2. IoT communication. In most cases, an IoT device communicates with a gateway, which in turn communicates with a controller or web service (Fig. 5).

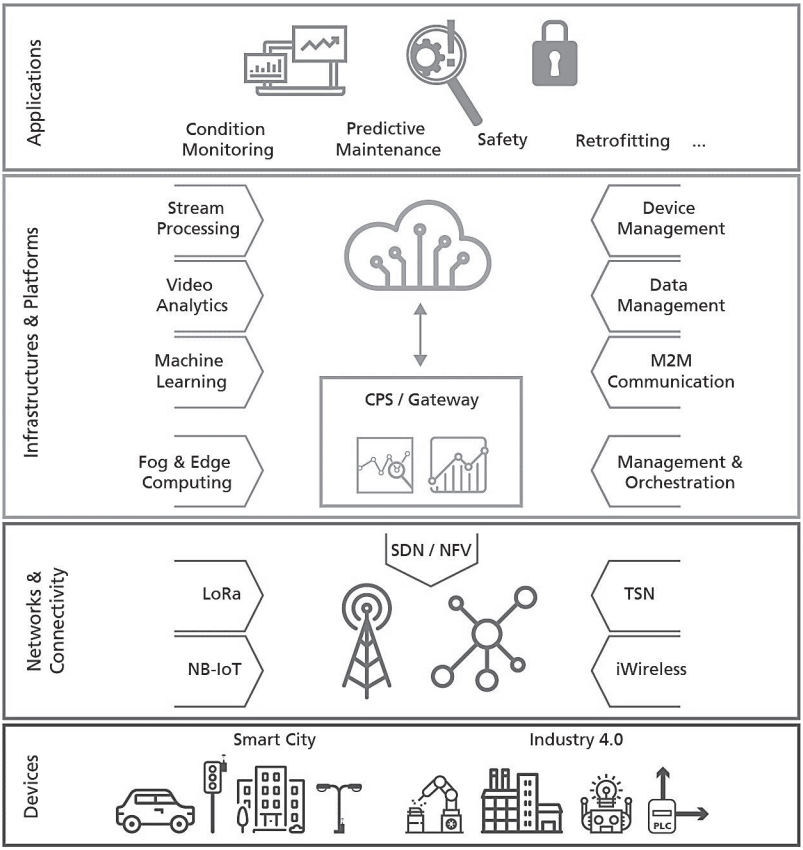


Fig. 5. Different IoT layers

There are many options for gateways, some of which are as simple as a mobile device (smartphone) positioned together with an IoT endpoint and communicating via RF such as Bluetooth -LE, ZigBee or Wi-

Fi. Gateways like this are sometimes called edge-edge gateways. Others may be more centrally located in data centers to support any number of special or proprietary IoT protocols, such as MQTT or Representational State Transfer (REST). The web service may be provided by a device manufacturer or an enterprise or public cloud service that collects information from manually operated devices. In many situations, the end-to-end connection between the load device and the web service can be provided by a series of field and cloud gateways, each of which integrates large amounts of data. Dell, Intel and other companies have recently introduced internet gateways to the market. Companies like Systech offer multiple protocol gateways that allow connecting different types of devices to IoTs using multiple antennas and receivers. There are also user-focused gateways, also called commercially available hubs that support intelligent home communication.

One of the main aspects of IoT is how small power supplies self-organize and exchange information (route information and data) with each other. Although these sensor devices are energy-limited, they must store and process data, dynamically connect to the network, and interact with other devices. Some devices may act as internal or border routers. There are five key issues to consider secure route creation, automatic recovery and stabilization, malicious detection, hardware-based calculations, and node location confidentiality.

5.3. Message protocols. At the top of the IoT communication packet are stored protocols that support the exchange of formatted messages between two endpoints, usually client-server or client-client. Protocols, such as MQTT, CoAP, The Data Distribution Service (DDS), Advanced Message Queuing Protocol (AMQP), and The Extensible Messaging and Presence Protocol (XMPP), which work on lower layer communications and enable effectively contract clients and servers to share data. Possible communications can be done very efficiently and in many Internet systems. Today, communications based on REST and MQTT appear to be leading the way.

5.3.1. MQTT. MQTT (Fig. 6) is a publish/subscribe model where clients subscribe to topics and maintain a TCP connection to a broker server. As new messages are sent to the broker, they include the subject of the message, which allows the broker to determine which clients receive the message. Messages are sent to customers through a constantly working connection.

5.3.2. XMPP. XMPP is XML-based (Extensible Markup Language) and is an open source real-time communication technology. It is developed by the Jabber Instant Messaging (IM) protocol. XMPP supports the transmission of XML messages over TCP transport, which allows IoT developers to effectively detect and troubleshoot defects.

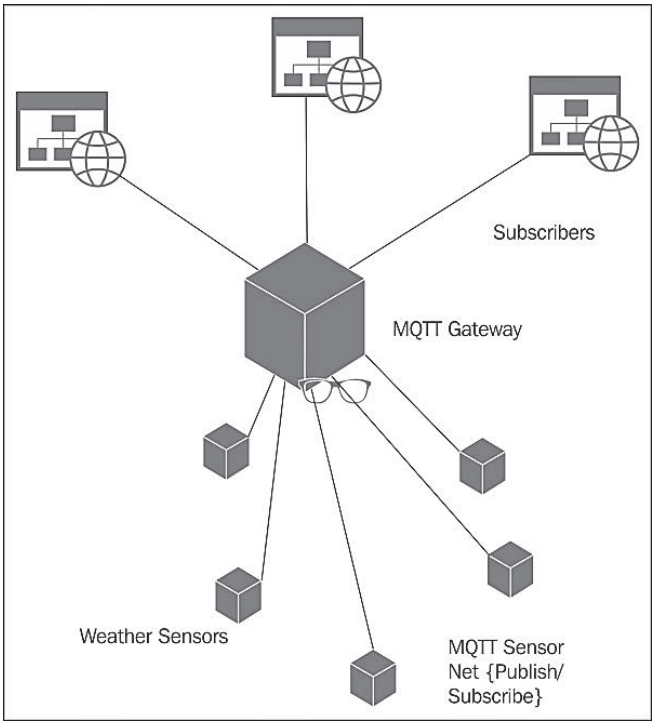


Fig. 6. Architecture of MQTT

5.3.3. CoAP. CoAP (Fig. 7) is another UDP-based IoT message protocol designed to be used on resource-limiting Internet devices, such as WSN nodes. It consists of a set of messages that easily navigate to HTTP: GET, POST, PUT and DELETE.

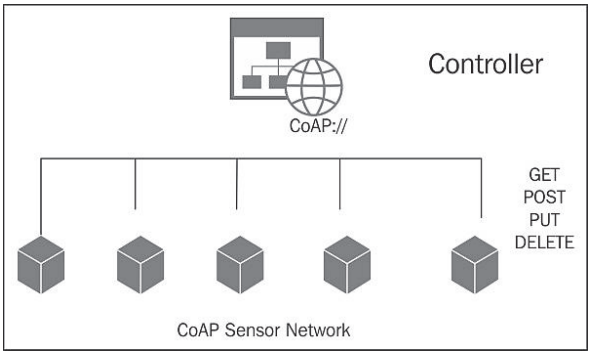


Fig. 7. Architecture of CoAP

5.3.4. DDS. DDS (Fig. 8) is an information bus used to integrate intelligent machines. Like MQTT, it uses a reader publishing / subscription model to subscribe to topics of interest.

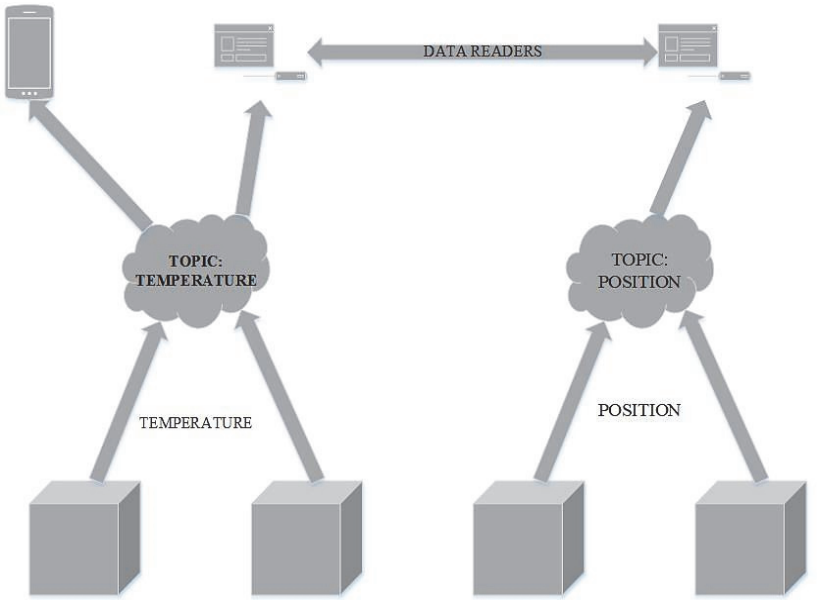
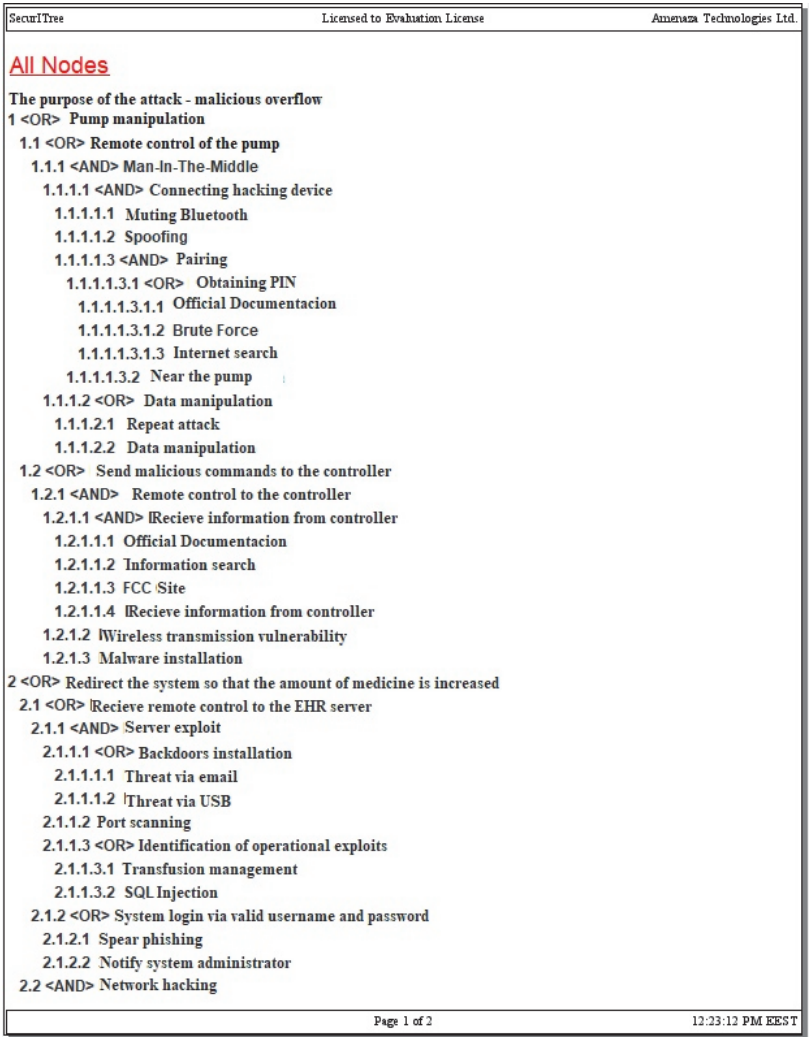


Fig. 8. Architecture of DDS

6. Risk Analysis Method. Data security issues are becoming increasingly important as civilization moves toward a global information age. The information revolution has changed the way of communication all over the world and also drawn unprecedented attention to network security issues [13].

The Internet of Things has a very promising development and its development is very turbulent. The problem with detecting possible attacks or breakdowns in Threat Risk Analysis (TRA) systems. Part of TRA is tree-based analysis. Attack Tree Analysis is a modeling technique for understanding risk in complex situations. Based on the previous study, the method [4] of risk analysis of a security breach based on trees was selected.

7. IoT Attack Scenario. This section describes how the values of each leaf node of an attack tree are generated [14], as well as an analysis of these data and results (Table 1 and 2) [15, 16]. All nodes of the attack in full view are shown in Figures 9 and 10.



SecurITree | Licensed to Evaluation License | Amenaza Technologies Ltd.

All Nodes

The purpose of the attack - malicious overflow

1 <OR> Pump manipulation

1.1 <OR> Remote control of the pump

1.1.1 <AND> Man-In-The-Middle

1.1.1.1 <AND> Connecting hacking device

1.1.1.1.1 Muting Bluetooth

1.1.1.1.2 Spoofing

1.1.1.1.3 <AND> Pairing

1.1.1.1.3.1 <OR> Obtaining PIN

1.1.1.1.3.1.1 Official Documentacion

1.1.1.1.3.1.2 Brute Force

1.1.1.1.3.1.3 Internet search

1.1.1.1.3.2 Near the pump

1.1.1.2 <OR> Data manipulation

1.1.1.2.1 Repeat attack

1.1.1.2.2 Data manipulation

1.2 <OR> Send malicious commands to the controller

1.2.1 <AND> Remote control to the controller

1.2.1.1 <AND> Recieve information from controller

1.2.1.1.1 Official Documentacion

1.2.1.1.2 Information search

1.2.1.1.3 FCC Site

1.2.1.1.4 Recieve information from controller

1.2.1.2 Wireless transmission vulnerability

1.2.1.3 Malware installation

2 <OR> Redirect the system so that the amount of medicine is increased

2.1 <OR> Recieve remote control to the EHR server

2.1.1 <AND> Server exploit

2.1.1.1 <OR> Backdoors installation

2.1.1.1.1 Threat via email

2.1.1.1.2 Threat via USB

2.1.1.2 Port scanning

2.1.1.3 <OR> Identification of operational exploits

2.1.1.3.1 Transfusion management

2.1.1.3.2 SQL Injection

2.1.2 <OR> System login via valid username and password

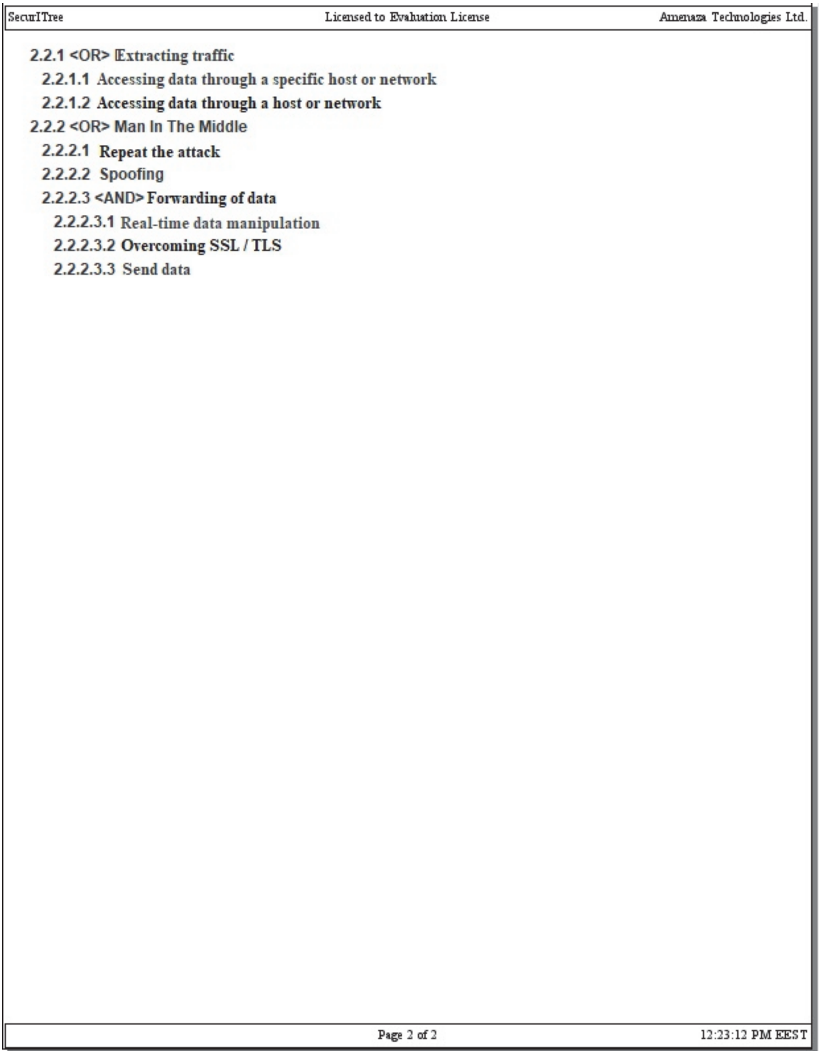
2.1.2.1 Spear phishing

2.1.2.2 Notify system administrator

2.2 <AND> Network hacking

Page 1 of 2 | 12:23:12 PM EEST

Fig. 9. All attack nodes



SecurITree | Licensed to Evaluation License | Amenaza Technologies Ltd.

2.2.1 <OR> Extracting traffic
2.2.1.1 Accessing data through a specific host or network
2.2.1.2 Accessing data through a host or network
2.2.2 <OR> Man In The Middle
2.2.2.1 Repeat the attack
2.2.2.2 Spoofing
2.2.2.3 <AND> Forwarding of data
2.2.2.3.1 Real-time data manipulation
2.2.2.3.2 Overcoming SSL / TLS
2.2.2.3.3 Send data

Page 2 of 2 | 12:23:12 PM EEST

Fig. 10. All attack nodes

Table 1. Attack nodes

Aim	Description of the sub-objective	Attack nodes	Tech. Spec.	Access	Notice	Breakthrough time
Installation of Backdoors	The attacker aims to find a point of entry by installing programs with Backdoors on the EHR server	Transmission of threat by email	Average	High	High	Weeks-Months
		USB threat transmission	Average	Average	High	Weeks-Months
		Port scanning	Low	Average	High	Days-Weeks
Identifying working exploits	The attacker uses several vulnerabilities in EHR server until it is discovered exploit , co her it meets the purpose of the attacker	Spillover management	High	Average	Average	Weeks-Months
		SQL Injection	Average	Average	Average	Days-Weeks
Login with a valid username and password	Once accessed to the hospital network, the attacker may attempt to log in with the administrator name and password	Spear Phishing	Average	High	High	Weeks-Months
		Confusing the administrator	Low	High	High	Days-Weeks
Extracting traffic	The attacker must find means of accessing traffic to or from the network	Accessing data through a host or network	Average	Average	Average	Weeks-Months
		Access data for a specific host or network	Average	Average	Average	Weeks-Months

Table 1 continued

Aim	Description of the sub-objective	Attack nodes	Tech. Spec.	Access	Notice	Breakthrough time
Man in the Middle Attack	The attacker aims to capture the data by moving from the client to the EHR server. Change attack and change packages.	Repeat the attack	Average	Average	Average	Weeks-Months
Forwarding data	When transmitting data to the attacker and intercepting the data, the attacker must change the data so that the modified data will cause physical harm to the patient.	Real-time data manipulation	High	Average	High	Weeks-Months
		Send data	Low	High	High	Days-Weeks
		Overcoming SSL / TLS	Very High	Low	High	Years-Decades

Backdoors installation: The need to install Backdoors is to allow attackers to repeatedly access systems and intranet sites whenever they wish, bypassing normal security controls [17, 18]. During this time, the attacker finds other loopholes in the system that can be operated to achieve the desired goal.

— Email threat transmission – An attacker can send an infected file through an attachment to an email or group of people in the hospital. Once the file is opened on a computer on the hospital network, a back door can be created that allows the hacker to connect to that computer from a remote

location. This method is highly accessible because emails are sent over the Internet and there are no restrictions.

— USB threat transmission – An attacker can transmit malware to the target EHR server via a USB device. Alternative USB devices for hospital staff or tricking a doctor into sharing a file from a computer system may be an alternative. Low technical ability to perform this attack is required.

— Port Scanning – Upon successful access to the hospital network, the attacker will scan for open network ports that can be used to get started. It takes a very low technical skill to perform this attack as there are numerous online tutorials explaining how this can be done [19].

Table 2. Nodes weight

Attack nodes	Technical ability	Accessibility	Landmark	Breakthrough time
Transmission of threat by email	3	3	2	3
USB threat transmission	2	2	2	3
Port scanning	2	3	2	2
Spillover management	4	2	3	3
SQL Injection	2	2	3	2
Login with a valid username and password	2	3	4	1
Accessing data through a host or network	3	2	3	3
Access data for a specific host or network	3	2	3	3
Repeat the attack	3	2	3	3
Real-time data manipulation	4	2	2	3
Send data	2	3	2	2
Overcoming SSL / TLS	5	1	2	5

Identifying working exploits: Once an attacker has established himself in the system, the next objective of the attack is to detect vulnerabilities in the system.

— SQL Injection – The purpose of an attacker is to request a database that can change the electronic records in the database.

— Spillover management – Upon entering the hospital network, the attacker may decide to execute arbitrary operating system commands through a vulnerable application.

Login with a valid username and password: An attacker who can access the server may try to use different combinations of username and passwords to gain access to the system.

Extracting traffic: In order to compromise a network, an attacker must retrieve the traffic as it passes between the client and the server [20].

— Accessing data through a host or network – An attacker may attempt to retrieve data destined for the hospital network.

— Access to data destined for a particular host or network – The attacker may attempt to retrieve data coming from the hospital network.

Repeat Attack: The attacker may decide to forward already captured data so that the EHR server receives authentic data in real time. If successful, this will result in incorrect transfer of the record, since the original data are not the same as the repeated data.

— Real-time data manipulation – An attacker must capture and modify incoming packets during real-time transmission to capture SSL flow.

— Data Transmission – Data forwarding is the least that an attacker can do. An attacker may attempt to apply additional techniques to ensure that the attack is critical enough when transmitting modified data.

— Overcoming SSL / TLS – This attack node has a very high technical result as a high level of understanding of the basic principles of encryption is required to launch an attack. The attacker must have access to real-time data to capture the SSL stream.

8. Comparative analysis. SecurlTree software provides a tool that allows identifying threat profiles [1].

Attack scenarios that fall under threat level 1 have the highest level of attack complexity [21]. The level of complexity of attacks decreases from threat level 1 to threat level 5. While attacks that are below threat level 1 are the most complex, threat level 5 may lead to attack against infrastructure, with less complexity and good result. In the SCADA attack scenario, it can be seen that only attackers under threat 1 and 3 can carry out the attack.

Comparing both results (Table 3), it can be seen that the level of threat 4 and 5 may lead to an attack on infrastructure, but not on the industrial SCADA system. This means that the skills required to attack an IoT application, such as a drug overflow pump, are less than an industrial SCADA system.

Analysis of the electronic record change scenario to increase the infusion rate of an overflow pump – using a complexity index (CI).

Table 3. Comparison of threat levels between IoT and SCADA

IoT System		SCADA attack	
Level of threat	Scenario	Level of threat	Scenario
1	11	1	36
2	5	2	0
3	9	3	36
4	9	4	0
5	2	5	0
6	0	6	0
7	0	7	0
8	0	8	0

An attacker can modify electronic records by attacking the EHR server, EHR client, or network. In order to attack the server, it is assumed that the attacker exploits the existing vulnerabilities. In order to carry out the attack, the attacker must combine elements of social engineering, insubordination, remote administration and APT. This makes CI the value of this attack scenario 4. In the network attack scenario, it has been suggested that if an attacker wants to compromise a server that correctly implements SSL / TLS data encryption, a Zero- Day vulnerability must be used. This increases the complexity of this attack to 5, otherwise the CI score for an attack on the network layer is considered to be 4. The lowest complexity attack against an EHR is an attack against a client machine. The script here introduces an attacker who gains remote access to the client machine after using social engineering techniques to obtain vital access information. The CI result for such an attack is 2. Table 4 illustrates the attack in detail.

Table 4. Determination of CI coefficient for IIoT

Types of features	Attack on the server	CI	Network Attack	CI
Social engineering	Email Threat, USB Threat	1	Access data from / through a host or network	1
Remote administration	Overflow Management, SQL Injection	1	Access data from / through a host or network	1
Landmark	Install backdoors	1	Access data from / through a host or network	1
Zero-Day Vulnerabilities	None	0	Overcoming SSL / TLS	1
APT	Installing Backdoors	1	Access data from / through a host or network	1
		Total = 4		Total = 5
Types of features	Client attack	CI	Network Attack	CI
Social engineering	Spear Phishing	1	Access data from / through a host or network	1
Remote administration	Overflow Management, SQL Injection	1	Access data from / through a host or network	1
Landmark	There is no	0	Access data from / through a host or network	1
Zero-Day Vulnerabilities	None	0	None	0
APT	There is no	0	Access data from / through a host or network	1
		Total = 2		Total = 4

10. Results of an IIoT attack. Using indicators related to the complexity of attacks to analyze the capabilities at each threat level, it is observed that the threat level 5 is the lowest threat level that can attack an infrastructure. Attacking can lead to a physical impact, such as endangering a

patient's life. Two attacks can be achieved through threat level 5. The purpose of both attacks is to successfully replicate the transmitted data between the patient's device and the EHR server. Repeated attack would result in incorrect data being recorded in normal data, if the physician starts treating a patient based on this data, the result could be catastrophic.

The result of the analysis also shows that threat level 1 is the highest threat level for IoT infrastructure. Threat Level 1 aims to change the encoded data during transmission. This may include changing patients 'names, changing patient's blood type, and modifying the data used to determine the patient's rate of transfusion, etc.

Some of the attack nodes include network traffic capture, real-time data manipulation, SSL/TLS encryption processing before the final forwarding of the data.

For the system attack tree, five scenarios can be performed with a threat level of 2. These attacks consist of an attack that is designed to trick the physician into introducing medical records into a false domain, a spy phishing attack that is the precursor to receiving a custom username and password to remotely access the EHR and find the vulnerability in the server for remote server operation. The same attack scenarios can be performed from threat level 3 and threat level 4. These attacks include the Man-In-The-Middle attack of the overflow pump itself, the controller attack, and the server operation of the EHR server. These attacks cannot be carried out by a second level threat because of their reduced technical ability. At the end of the analysis it can be seen that none of the attacks can be carried out with a threat level of 1, 2 and 3.

10. Conclusion. For the IIoT infrastructure, each node is described in detail, and for SCADA, the infrastructure relies on data provided by different reports.

After using the data correlation, the introduction of the corresponding value of each leaf attack into the securITree system was continued and a table was created to categorize the threat level. Amenaza's methodology is also used to generate a complexity index for all attacks. This makes it possible to compare the level of complexity of SCADA and IoT infrastructures. Such attacks can be carried out to an IoT application, with lower complexity requirements and still produce a physical result.

The safe and secure deployment of IoT is a major challenge, given the unique characteristics of these systems, their ability to impact events in the physical world, and the diversity of IoT applications.

References

1. Checharova N., Chehlarova K. Verification and Improvement of Digital Competence and Common Culture through Symmetries. Electronic Collection of “Instruments for Attractive Education. 2015.

2. Chechlarova N. Online competition “Rosette” for the development of digital competence. Pedagogical Forum. 2016. Issue 3.
3. Ahmedova S. Digital transformation of the Bulgarian industry. IOP Conference Series: Materials Science and Engineering. 2020. vol. 709. no. 2. pp. 022061.
4. Tsochev G.R., Yoshinov R.D., Iliev O.P. [Key Problems of the Critical Information Infrastructure through Scada Systems Research]. *Trudy SPIIRAN – SPIIRAS Proceedings.* 2019. vol. 18(6). pp. 1333–1356.
5. Rouse M. Internet of things (IoT). IOT Agenda. Available at: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT (accessed: 14.08.2019).
6. Wang B. The internet of things world forum unites industry leaders in Chicago to accelerate the adoption of iot business models. Available at: http://www.marketwired.com/press-release/internet-things-world-forum-unites-industry-leaders-chicago-accelerate-adoption-iot-nasdaq-htm (accessed: 21.03.2020).
7. Nedyalkova A., Bakardjieva T., Nedyalkov K. Application of Digital Cybersecurity Approaches to University management – VFU Smart Student. International Association for Development of the Information Society. 2016. pp. 173–180
8. Trifonov R. et al. A Survey of Artificial Intelligence for Enhancing the Information Security. *International Journal of Development Research.* 2017. vol. 07. no. 11. pp. 16866–16872.
9. Garvanov I., Garvanova M. *V"vedenie v MATLAB i SIMULINK* [Introduction to MATLAB and SIMULINK]. Za bukvite – O pismenekh'. 2014. 122 p. (In Bulg.).
10. Nikolov B., Tcholakova V. Aspects of risk management in logistics activities of enterprises. application of fault tree analysis (FTA). *Innovations.* 2015. vol. 3. no. 2. pp. 34–38.
11. Trifonov R., Yoshinov R., Pavlova G., Tsochev G. Artificial neural network intelligent method for prediction. AIP Conference Proceedings. 2017. vol. 1872. no. 1. pp. 020021.
12. IoT Security Foundation. “Establishing Principles for Internet of Things Security”. Available at: https://www.iotsecurityfoundation.org/establishing-principles-for-internet-of-things-security/ (accessed: 01.03.2020).
13. Trifonov R. et al. Conceptual model for cyber intelligence network security system. *International Journal of Computers*. 2017. vol. 11. pp. 85–92.
14. Amenaza Technologies Ltd., "Introduction to SecurITree". 2017. Available at: https://www.amenaza.com/demos/introduction_to_securitree.html (accessed: 14.08.2019).
15. Gershfang E. Ransomware and Healthcare – OWASP Montreal. 2016. Available at: https://ca.linkedin.com/in/eduard-gershfang-cissp-ceh-cnda-ccsp-608a1811 (accessed: 14.08.2019).
16. Stoyanov D. Neurorehabilitation: Public Health and Health Care in Greece and Bulgaria: the Challenge of the Cross-border Collaboration. *Asklepij. Mezhdunarodno spisanie po istoriya i filosofiya na medicinata.* 2010. vol. IV. pp. 170–170.
17. Trifonov R. et al. Increasing the level of network and information security using artificial intelligence. Fifth Intl. Conf. Advances in Computing, Communication and Information Technology. 2017. pp. 2–3.
18. Lecture notes. Available at: https://www.cs.fsu.edu/~redwood/OffensiveComputerSecurity/lectures.html (accessed: 16.12.2019).
19. Nikolov D., Kordev I., Stefanova S. Concept for network intrusion detection system based on recurrent neural network classifier. 2018 IEEE XXVII International Scientific Conference Electronics (ET). 2018. pp. 1–4.
20. Morris T., Gao W. Industrial control system traffic data sets for intrusion detection research. International Conference on Critical Infrastructure Protection. 2014. pp. 65–78.

21. Moore A., Ellison R.J., Linger R.C. Attack Modeling for Information Security and Survivability. Carnegie-Mellon Univ Pittsburg Pa Software Engineering Inst. 2001. No. CMU-SEI-2001-TN-001.

Tsochev Georgi — Ph.D., Chief Assistant Professor, Laboratory of Telematics, Bulgarian Academy of Sciences (BAS). Research interests: computer science, computer networks and communication, neural networks, deep learning, application of mathematics and informatics in cybersecurity. The number of publications — 25. gtsochev@cc.bas.bg; bl. 8, Acad. Georgi Bonchev str., 1113, Sofia, Bulgaria; office phone: +359895589861.

Yoshinov Radoslav — Head of Laboratory, Laboratory of Telematics, Bulgarian Academy of Sciences (BAS). Research interests: computer science, medical systems, computer networks and communication, deep learning, cybersecurity, E-Government cybersecurity of computer networks. The number of publications — 191. yoshinov@cc.bas.bg; 8 bl., Akad. G. Bonchev str., 1113, Sofia, Bulgaria; office phone: +359888627190.

Zhukova Nataly — Ph.D., Associate Professor, Senior researcher, Laboratory of Information and Computing Systems and Programming Technologies, St. Petersburg Institute of Informatics and Automation of the Russian Academy of Sciences (SPIIRAS). Research interests: intelligent systems, data analysis. The number of publications — 70. nazhukova@mail.ru; 39, 14th line V.O., 199178, St. Petersburg, Russia; office phone: +7(812)328-08-87; fax: +7(812)328-44-50.

Acknowledgements. This research is supported by ICT in NOS.

УДК 006.72 **DOI** 10.15622/sp.2020.19.2.5

Г.Р. Цочев, Р.Д. Йошинов, Н.А. Жукова

ПРОБЛЕМЫ БЕЗОПАСНОСТИ ИНДУСТРИАЛЬНОГО ИНТЕРНЕТА ВЕЩЕЙ И СРАВНЕНИЕ С СИСТЕМАМИ SCADA

Цочев Г.Р., Йошинов Р.Д., Жукова Н.А. **Проблемы безопасности индустриального интернета вещей и сравнение с системами SCADA.**

Аннотация. Рассматривается проблема безопасности Интернета вещей (Internet of Things), которая не относится к традиционной проблеме кибербезопасности, так как связана с локальным или распределенным мониторингом и/или контролем состояния физических систем, подключенных через Интернет. Предыдущее исследование авторов рассматривало архитектуру системы диспетчерского контроля и сбора данных (SCADA). Благодаря внедрению систем SCADA, были проанализированы уязвимости и различные варианты кибератак на них. В качестве исследовательского примера было рассмотрено тематическое исследование, основанное на деревьях, результаты которого были обобщены и визуализированы.

Цель настоящей статьи – сравнить новую индустриальную технологию Интернета вещей (промышленный Интернет вещей, Industrial Internet of Things) с ранее исследованными традиционными системами SCADA.

Промышленный Интернет вещей (Industrial Internet of Things) – это сеть устройств, которые связаны между собой с помощью коммуникационных технологий. В настоящей статье представлены некоторые из наиболее распространенных проблем безопасности устройств промышленного Интернета вещей.

Представлен краткий обзор архитектуры промышленного Интернета вещей, описываются основные принципы безопасности и основные проблемы, которые могут возникать с устройствами Интернета вещей. Основываясь на исследованиях и анализе риска угроз в области промышленного Интернета вещей, в качестве главного подхода рассмотрен конкретный случай деструктивного воздействия, основанный на древовидном анализе. Дается описание создания значений каждого конечного узла дерева атак, а также приводится анализ полученных результатов. Анализ сценария изменения электронной записи для увеличения скорости инфузионного насоса был выполнен с использованием индекса сложности. Результаты были сравнены с предыдущим исследованием систем SCADA и представлены результаты и выводы.

Ключевые слова: Интернет вещей, промышленные системы, SCADA, дерево атак, кибербезопасность, сетевая и информационная безопасность.

Цочев Георги Руменов — канд. техн. наук, главный ассистент, лаборатория телематики, Болгарская академия наук (БАН). Область научных интересов: информатика, информационные технологии, нейронные сети, глубинное обучение, киберзащита. Число научных публикаций — 25. gtsochev@cc.bas.bg; ул. Академика Георги Бончев, бл. 8, 1113, София, Болгария; р.т.: +359895589861.

Йошинов Радослав Даков — заведующий лабораторией, лаборатория телематики, Болгарская академия наук (БАН). Область научных интересов: информатика, информационные технологии, модели, связанные с обучением, решения для поддержки электронного управление. Число научных публикаций — 191. yoshinov@cc.bas.bg; ул. Академика Георги Бончев, 8 бл., 1113, София, Болгария; р.т.: +359888627190.

Жукова Наталия Александровна — канд. техн. наук, доцент, старший научный сотрудник, лаборатория информационно-вычислительных систем и технологий програм-

мирования, Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН). Область научных интересов: интеллектуальные системы, анализ данных. Число научных публикаций — 70. nazhukova@mail.ru; 14-я линия В.О., 39, 199178, Санкт- Петербург, Россия; р.т.: +7(812)328-08-87; факс: +7(812)328-44-50.

Поддержка исследований. Работа выполнена при финансовой поддержке ИКТ in HOC.

Литература

1. *Checharova N., Chehlarova K.* Verification and Improvement of Digital Competence and Common Culture through Symmetries // Electronic Collection of "Instruments for Attractive Education. 2015.
2. *Chechlarova N.* Online competition "Rosette" for the development of digital competence // Pedagogical Forum. 2016. Issue 3.
3. *Ahmedova S.* Digital transformation of the Bulgarian industry // IOP Conference Series: Materials Science and Engineering. 2020. vol. 709. no. 2. pp. 022061.
4. *Tsochev G.R., Yoshinov R.D., Iliev O.P.* Key Problems of the Critical Information Infrastructure through Scada Systems Research // Труды СПИИРАН. 2019. Т. 18(6). С. 1333–1356.
5. *Rouse M.* Internet of things (IoT). IOT Agenda. URL: https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT (дата обращения: 14.08.2019).
6. *Wang B.* The internet of things world forum unites industry leaders in chicago to accelerate the adoption of iot business models. URL: http://www.marketwired.com/press-release/internet-things-world-forum-unites-industry-leaders-chicago-accelerate-adoption-iot-nasdaq-htm (дата обращения: 21.03.2020).
7. *Nedyalkova A., Bakardjieva T., Nedyalkov K.* Application of Digital Cybersecurity Approaches to University management – VFU Smart Student // International Association for Development of the Information Society. 2016. pp. 173–180
8. *Trifonov R. et al.* A Survey of Artificial Intelligence for Enhancing the Information Security // International Journal of Development Research. 2017. vol. 07. no. 11. pp. 16866–16872.
9. *Гарванов И., Гарванова М*. Въведение в MATLAB и SIMULINK // За буквите – О писменехъ. 2014. 122 с.
10. *Nikolov B., Tcholakova V.*, Aspects of risk management in logistics activities of enterprises. application of fault tree analysis (FTA) // Innovations. 2015. vol. 3. no. 2. pp. 34–38.
11. *Trifonov R., Yoshinov R., Pavlova G., Tsochev G*. Artificial neural network intelligent method for prediction // AIP Conference Proceedings. 2017. vol. 1872. no. 1. pp. 020021.
12. IoT Security Foundation. "Establishing Principles for Internet of Things Security". URL: https://www.iotsecurityfoundation.org/establishing-principles-for-internet-of-things-security/ (дата обращения: 01.03.2020).
13. *Trifonov R. et al*. Conceptual model for cyber intelligence network security system // International Journal of Computers. 2017. vol. 11. pp. 85–92.
14. Amenaza Technologies Ltd., "Introduction to SecurITree". 2017. URL: https://www.amenaza.com/demos/introduction_to_securitree.html (дата обращения: 14.08.2019).
15. *Gershfang E.* Ransomware and Healthcare – OWASP Montreal. 2016. URL: https://ca.linkedin.com/in/eduard-gershfang-cissp-ceh-cnda-ccsp-608a1811 (дата обращения: 14.08.2019).
16. *Stoyanov D.* Neurorehabilitation: Public Health and Health Care in Greece and Bulgaria: the Challenge of the Cross-border Collaboration // Асклепий. Международно списание по история и философия на медицината. 2010. № IV. С. 170–170.

17. *Trifonov R. et al*. Increasing the level of network and information security using artificial intelligence // Fifth Intl. Conf. Advances in Computing, Communication and Information Technology. 2017. pp. 2–3.
18. Lecture notes. URL: https://www.cs.fsu.edu/~redwood/OffensiveComputerSecurity/lectures.html (дата обращения: 16.12.2019).
19. *Nikolov D., Kordev I., Stefanova S*. Concept for network intrusion detection system based on recurrent neural network classifier // 2018 IEEE XXVII International Scientific Conference Electronics (ET). 2018. pp. 1–4.
20. *Morris T., Gao W*. Industrial control system traffic data sets for intrusion detection research // International Conference on Critical Infrastructure Protection. 2014. pp. 65–78.
21. *Moore A., Ellison R.J., Linger R.C.* Attack Modeling for Information Security and Survivability // Carnegie-Mellon Univ Pittsburg Pa Software Engineering Inst. 2001. No. CMU-SEI-2001-TN-001.