SECURITY THREATS IN IOT TECHNOLOGIES

Vasiyeva Dilfuza
Shahrisabz State Pedagogical Institute
Vasiyevadilfuza1997@gmail.com

ABSTRACT

IoT technology is one of the key issues that need to be addressed. There are various configurations of issues that need to be addressed in the physically connected part of the IoT and in the network domain. IoT automation programs have special requirements in real time, they have a high level of reliability and security in a stable environment. These requirements strengthen security and high security measures.

This article discusses security threats that may arise in various layers of iot architecture, especially in the automation domain. Impact mitigation methods are discussed with security in mind, with equipment in the field, communication infrastructure resulting in a variety of physical solutions and measurements for data processing applications.

Keywords: IoT (Internet of Things), data processing, cyber security, CPS(cyber-physical systems) , CPSS(cyber-physical production systems), DoS(Denial of service).

INTRODUCTION

Information and communication technologies are widely used in many areas around us. The evolution of IoT technology is leading to increased automation in many areas. More and more people are replacing computer tasks with computer tasks. This trend combines a variety of goals, such as diversity, compatibility, distributed processing, and security.

The Internet of Things (IoT) competency aims to bridge the gap between low-cost technologies and the use of non-slip sensors. This competence is governed by cyber-physical systems such as industrial systems (automation (CPS), cyber-physical production systems (CPPS), the fourth industrial revolution). CPSS connects industrial systems and has the ability to optimize and automate production [2]. CPPS is used in the fourth industrial revolution for mass privatization, co-production, and end-to-end digital integration [3]. IoT is a concept for simple Internet technologies to interconnect low-power devices, such as sensors and actuators (so-called things). IoT requires both customized technology and hundreds of thousands of devices. IoT is not defined as the technology itself, but as a concept for the expansion of Internet technologies through

Wireless Sensor Networks (WSN). Wireless sensors networking is the interconnection of protocols and low-power devices such as ZigBee, IEEE 802.15.4, WirelessHART, ISA100.11, IETF 6LoW-PAN, IEEE 802.15.3, Wibree, which use wireless. This poses problems such as maintaining confidentiality [4]. As technology becomes cheaper, devices with simple limited processing power will connect to each other and to the IT cloud as well [5]. In IoT automation, great importance is attached to safety. uses IoT automation despite the narrow limit for processing and power-limited devices and security tasks. Between security, sales, performance, and costs need to be evaluated. There is a demand for lightweight and autonomous safety solutions with subsequent self-mitigation capabilities [6].

This article discusses security issues for the automation IoT space. This article was written for IoT Technology: Sensors and Actuators, Gateways and Networking, Data Processing, and Finally, Application Layers [7].

In this article, our contribution is a layered analysis of the approach to security issues of IoT automation and the provision of possible mitigation and detailed development solutions.

II. Security of IoT automation systems

It provided a taxonomy for security-related terms in this context for IoT. This reflects vulnerabilities arising from the Machine to-Machine (M2M) communication features used in IoT automation. M2M operates without human control [8]. In automation issues, limited devices with no power and special processing, limited security capabilities are used in sensors nodes. The IoT world is vast regarding application [9] areas, small and complex concerning complexity. Requirements for IoT systems also vary in the field of application. Requirements for the operation of systems within the IoT automation system and the IoT domain are as follows [10]:

- interoperability between devices and systems;
- dimensionality;
- real-time operation;
- security;
- engineering simplicity;

Automation is also developing in industry. Industrial systems have separate, stricter safety requirements than IT systems. These requirements can be characterized by well-known goals of the CIA: confidentiality, integrity, and availability. There is a difference between the IT industry, and the IT industry depending on what the priority is. This industry has aroused great interest in the topic of 4.0 and IoT automation systems [11]. Industry 4.0, is an interaction of several technologies. Industry 4.0, is an interaction of several technologies. Like IoT, it is known for its diversity. Therefore, the need to determine what these existing technologies will look like is combined, e.g.

reference architecture is required. To date, there have been several initiatives. The Industrial Internet Consortium (IIC) is developing the Industrial Internet Recording Architecture (IIRA), a building on industrial Internet systems (IIS) defined by four levels of "point of view".

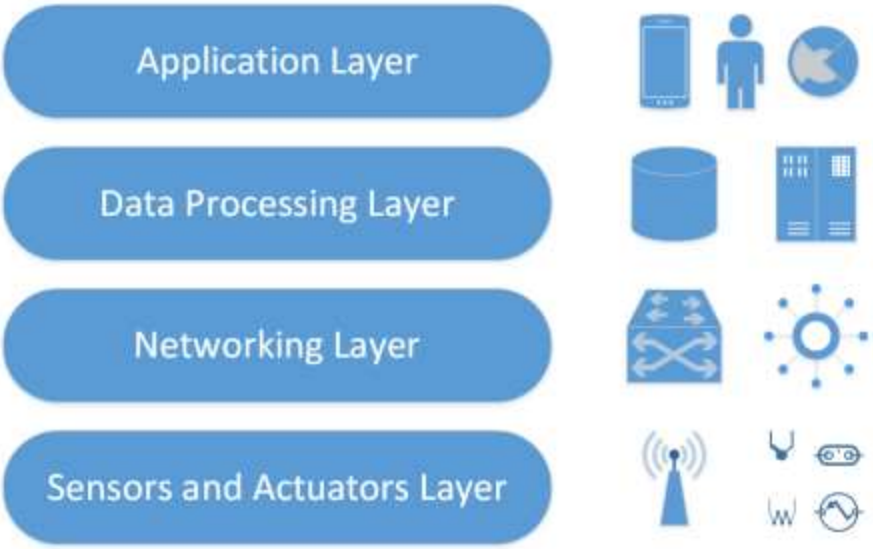


Fig 1. The architectural layers of IoT systems

While RAMI 4.0 is primarily focused on industrial automation, IIRA aims to bring IoT to a wider target area such as energy, healthcare, and transportation. There are many similarities between these two architectural concepts. Security is of great importance in CPSS, especially in the modernization of industrial systems controlled by interconnected ICT components. Although current reference architectural models do not deal with security sufficiently, the link should include security aspects. Explored the possibility of setting a security perspective in RAMI 4.0. To integrate security through a hierarchical axis, we need to consider the threats that arise in an automation scenario [12]. Therefore, in this paper, we provide a layered overview of security threats and possible mitigation in industrial IoTs.

III. LAWYER APPROACH FOR IoT SYSTEMS

In general, although IoT is standardized, typically agreeing on a layered structure for IoT systems, future records for the industry will be Architectural models 4.0 layered. This supports our view that such a structure is useful in describing security threats. First, it presents us with a four-tiered architecture built on threat analysis. As mentioned in the previous chapter, similar, layered architectures are offered by different vendors and research teams. However, they are not technical architectures because [4] they are usually also involved in business views and processes. In addition, the access (or collection) network and the transport network are sometimes recommended to be in different layers because they use different network technologies.

1. Application layer

2. Data processing layer

3. Network layer

4. Layer of sensors and actuators

The “Data Processing” layer covers all the methods, technologies, and equipment that help extract meaningful information from the collected data. The “Application” layer includes the ultimate management mechanisms based on the entire IoT architecture - the highest level of logic, along with the configuration of the system and the [5] presentation of its state.

IV. SAFETY AND ACTUATOR SAFETY LAYER

The IoT Sensors and Actuators layer is vulnerable to direct physical access through the following types of attacks: physical disruption of end devices and communication tools, link and denial of service (DoS) attacks.

A. Tampering

This physical layer provides an excellent attack surface. Device elements can be accessed in case of identity violation, theft of keys, violation of privacy and integrity. One way to prevent this is to tamper-resistant fragmentation.

However, this can be very expensive considering cheap low-power sensors or consumer devices, which are the main driver of IoT. Violation of a [11] communication link can take the form of disconnection or modification of a physical connection, which is a denial-of-service attack or alteration of transmitted data, which is a condition of a secondary attack.

B. Denial of service

In most cases, IoT devices communicate over the radio access to technologies in the physical layer. Wireless communication They are very prone to denial of service (DoS) attacks may take their forms in signal distortion or compression. DoS attacks can disrupt system availability. Although spectral methods against wireless interference can be used,

There is no general solution to avoid DoS attacks. There are even approaches require a lot of processing because IoT does not have limited devices. Maybe solutions need to monitor and interpret traffic, but it works in the upper layers.

C. Sensors as Security Treats

On the other side of the coin are IoT sensors. The biggest security threat, because if broken - they can be source nodes for Distributed Denial (DDoS) attacks. Access to their management is due to vulnerability the practice of negligently placing [10] weak authentication pairs. Most devices are easy to break username / password pairs can cause a very large attack surface. If damaged, these devices can be used for the flood type DDoS attacks. Such attacks do not require high scores power output from any device and high network throughput byte payload is sufficient. This is the sum of the packets sent towards the target infrastructure leading to their DoS.

V. NETWORK LAYER SECURITY ISSUES

In the case of automated IoT, here is real-time data flow is important, network attacks can be particularly harmful. The IoT network layer is exposed to various security threats

known in the computer networking community. There are specialized attacks for Wireless Sensor Networks (WSN),collection network (often referred to as Gateway or Bond layer), and network between junction points and cloud and its applications, in this section they are referred to in the usual way because they are poses a risk to data transportation. The following sections are brief possible network threats and attacks are summarized significant impact on IoT systems.

A. Denial of Service attacks

1) Exhaustion: network sources, such as buffers, computing power and performance may run out a targeted attack of a given source, i.e., a given node.

2) Collision: A deliberate collision can lead to an attack because it usually targets awireless connection. part of the data, especially its data link layer. Even if the attackers don’t completely squeeze out the signal, they are reduced good network performance or even communication impossible [9].

3) Unfairness: Data Link layer attacks often target corruption Justice mechanisms of WSNs. Their method includes the following stopping or colliding target WSN sources. These are subsequent methods [8] lead to poor rejection of the service; though his the effect is magnified by the number of nodes involved.

4) Spoofed routing information: payload information, the packages are usually drained, diverted and no other [7] title information is available. Data obtained within the routing protocol - in our case: IP - is often the primary one the purpose of the fraud. Attackers can break, modify, or replay IP addresses or access protocol information (UDP, TCP ports, etc.) to disrupt network traffic. As a result, routing is possible loops, extended (or shortened) routes, fake error [1] messages and more.

5) Selective forwarding: In multi-hop networks, a queen or broken node can change traffic messages, selectively redirect others. Information that is, the address is incomplete.

6) Sinkhole attack: Some nodes in this type of attack or routes are more attractive for transport (e.g. by route management information is corrupted), other, normal nodes. When you reach a sinking node, there may be messages unload modified by content or other means.

7) Wormhole attack: piercing worms prepared in a harmful way, a low delay link where the attacker can listen to messages again. In a worm attack, the attacker receives

packets at one point the "tunnels" in the network lead them to another point in the network, and then reposts them to the network [2] from that point.

8) Sybil attack: Sybil type attackers are from nodes or devices with multiple identities. They generate traffic seems to be multi-source or even distributed. This method is broken the concept of using available resources in the infrastructure, redundancy or voting.

9) Flooding: Floods in the network and their possible levels have extensive literature due to their complexity and breadth their impact on the life of our systems. DDoS is currently under water attacks are the most annoying attacks; The authors support a comprehensive survey on their algorithms and protections mechanisms.

10) Node replication: can copy the attacker ID node and create another (virtual) node with the same identification. He can then send false information to his name via random routes network disruption.

B. Man-in-the-Middle attacks

Man-in-the-Middle attacks is when an attacker has access for information sent between nodes and which can be used its advantage. Encrypt your data to avoid the risk of this attack should be applied. The following three attacks relate to this category:

1) Eavesdropping: Eavesdropping is a moment the attacker may have access to the communication channel. Here it is a passive attack if the attacker does not slightly change what is accepted packages and sends back to any participant. This method called a repeat attack, this is a very common subtype of deception.

2) Routing Attack: Typical router information an unencrypted attacker can change route information thereby creating route cycles that significantly deteriorate quality of service.

3) Replay attack: the attacker takes my signed package, and even if he can’t decrypt it, he can gain his trust the person whose package is to be sent later. Replay attacks can be bypassed using a sequence of messages numbers and message confirmation code (MAC).

C. Safety precautions for the network layer

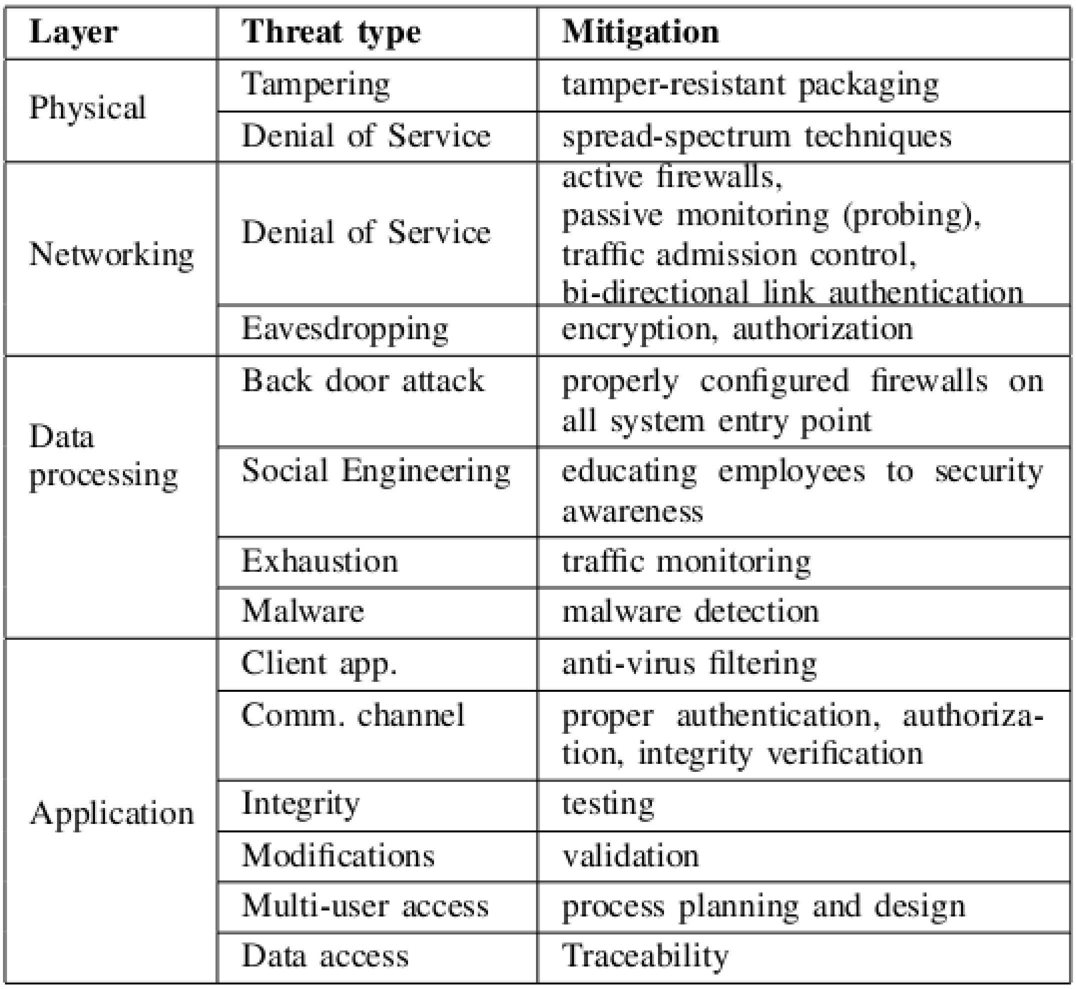
The attacks mentioned above can be eliminated as needed network security measures. Defensive methods are included active firewalls that filter traffic, passive surveillance (verification) to raise signals, control access to vehicles through authentication, and two-way link confirmation. IoT sensors are often simple, low-power end devices.

Security due to the limited functional capabilities of IoT sensors additional processing such as encryption. This it is also best to perform encryption at the lowest layer possible because the payload of the protocol layer can only be encrypted in the protocol layer below. layer, lightweight encryption method presented to validate RFID tags in IoT.

CONCLUSION

IoT is the Internet of Things because of its success in the world of things access to automation and industrial systems.

Although the use of technology for IT is reliable applications, the uniformity of the technologies that can be used, and the result is a lack of standardized methods for net use the cases reveal many unanswered questions. Industry exists there is a very narrow limit to the acceptable risk it can cause not to mention that there may also be security risks involved. From a security and safety standpoint, IoT cannot be called mature because its heterogeneous structure contains a large amount overcoming vulnerabilities that may not yet be fully understood. Security to manage a safe and secure IoT system and protection should be applied through thorough planning, implementation, placement and processing cycle:



Layer	Threat type	Mitigation
Physical	Tampering	tamper-resistant packaging
	Denial of Service	spread-spectrum techniques
Networking	Denial of Service	active firewalls, passive monitoring (probing), traffic admission control, bi-directional link authentication
	Eavesdropping	encryption, authorization
Data processing	Back door attack	properly configured firewalls on all system entry point
	Social Engineering	educating employees to security awareness
	Exhaustion	traffic monitoring
	Malware	malware detection
Application	Client app.	anti-virus filtering
	Comm. channel	proper authentication, authorization, integrity verification
	Integrity	testing
	Modifications	validation
	Multi-user access	process planning and design
	Data access	Traceability

- selection of technologies, architecture and tools;
- project configuration, programming and verification;
- deployment and commissioning;

•operation and maintenance.

For IoT, the issue of cyber security has always been relevant. To solve the problem of cyber security, it is important to consider the different types of attacks on the system, to determine the protection measures depending on their characteristics. If the planned IoT system pays attention to cyber security within its architecture, significant results will be achieved.

REFERENCES:

1. Kabulov, A.V., Normatov, I.H., Karimov, A.A., Navruzov, E.R. “Algorithmization of constructing control models of complex systems in the language of functioning tables” European Journal of Molecular and Clinical Medicine, 2020, 7(2), стр. 758–771.

2. Kabulov, A., Normatov, I., Urunbaev, E., Ashurov, A. “About the problem of minimal tests searching” Advances in Mathematics: Scientific Journal, 2020, 9(12), стр. 10419–10430.

3. Anvar Kabulov, Firdavs Muhammadiyev, and Inomjon Yarashov. "ANALYSIS OF INFORMATION SYSTEM THREATS" Science and Education, vol. 1, no. 8, 2020, pp. 86-91.

4. A.V.Kabulov, I.K.Yarashov, and M.T.Jo‘Rayev. "COMPUTER VIRUSES AND VIRUS PROTECTION PROBLEMS" Science and Education, vol. 1, no. 9, 2020, pp. 179-184.

5. Dilrabo Madrahimova, and Inomjon Yarashov. "LIMITED IN SOLVING PROBLEMS OF COMPUTATIONAL MATHEMATICS THE USE OF ELEMENTS" Science and Education, vol. 1, no. 6, 2020, pp. 7-14.

6. Kabulov, A.V., Normatov, I.H., Karimov, A. “Algorithmization control of complex systems based on functioning tables” Journal of Physics: Conference Series, 2020, 1441(1), 012141.

7. Kabulov, A., Kalandarov, I., Boltaev, S. “Development of mathematical models of problems of management the production division with a discrete unit type production” Journal of Advanced Research in Dynamical and Control Systems, 2020, 12(6 Special Issue), стр. 778-791.

8. Kabulov, A.V., Normatov, I.H., Boltaev, S., Saymanov, I. “Logic method of classification of objects with non-joining classes” Advances in Mathematics: Scientific Journal, 2020, 9(10), стр. 8635-8646.

9. Kabulov, A.V., Urunbaev, E., Normatov, I., Ashurov, A. “Synthesis methods of optimal discrete corrective functions” Advances in Mathematics: Scientific Journal, 2020, 9(9), стр. 6467-6482.

10. Kabulov, A.V., Urunbaev, E., Ashurov, A. "Logical method for constructing the optimal corrector of fuzzy heuristic algorithms" International Conference on Information Science and Communications Technologies: Applications, Trends and Opportunities, ICISCT 2019, 2019, 9011906.

11. Kabulov, A.V., Normatov, I.H. "About problems of decoding and searching for the maximum upper zero of discrete monotone functions" Journal of Physics: Conference Series, 2019, 1260(10), 102006.

12. Kabulov, A.V., Normatov, I.H., Ashurov, A.O. "Computational methods of minimization of multiple functions" Journal of Physics: Conference Series, 2019, 1260(10), 102007.