Information & Security

E. Staneva & M. Rachev
vol. 47, no. 1 (2020): 135-140
https://doi.org/10.11610/isij.4709

Published since 1998 ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Tactical Approach for Cyber Defence in IoT Computer Networks

Elisaveta Staneva **(✉), *Mariyan Rachev*** **(✉)**

Nikola Vaptsarov Naval Academy, Varna, Bulgaria,
https://www.naval-acad.bg/en

ABSTRACT:

Securing Internet of Things' devices has been an ongoing struggle since the technology's recognition. Finding methods to prevent or counter those threats through the experience of the hackers themselves is a promising way of securing these devices. The approach described in this article uses that experience and transforms it into useful models and algorithms for IoT security.

ARTICLE INFO:

RECEIVED: 16 JUNE 2020
REVISED: 28 AUG 2020
ONLINE: 21 SEP 2020

KEYWORDS:

Internet of Things, security, vulnerabilities, authentication, architecture

Introduction

With the advancement of technology, significant attention is given to the Internet of Things (IoT). The latter is based on the connectivity of devices to the network, but these devices are not only computers, tablets and smartphones. It is no coincidence that it was decided to call the technology the Internet of Things. These so-called "things" can interact both with the user and other device. The growing use of IoT technology is seen not only in people's daily routine, but also in the industry. The main reason is process automation. In 2013, Cisco Systems defines a new term – Internet of Everything (IoE), which describes a system in which people, things, data and processes participate. The information from this system turns into actions that create new opportunities,

✉ E-mail: e.staneva@naval-acad.bg; m.rachev@naval-acad.bg

richer experience and unprecedented economic opportunity for businesses, individuals and countries.[1]

As already mentioned, IoE is a kind of system that consists of:

- *People* – all users of devices that monitor physical condition (health sensors), activity, location, interests.
- *Things* – devices using IoT technology - phones, tablets, computers, household appliances, industrial machines and more. By means of their sensors - they collect information about users.
- *Data* – received data is accumulated in order to inform the user about the state of the system and assist decision-making (and possibly drives alone to make decisions).
- *Processes* – the accumulated data is systematized and processed to enable users to easily handle the information.

IoE removes the boundaries that IoT sets. The presence of more IoT devices creates a kind of ecosystem, so the transition to IoE is absolutely necessary. Customers and vendors are already looking for advanced features (for example - machine learning algorithm, which is in the cloud) to be able to optimize processes and quality. The following protocols are used for communication - Machine-To-Machine (M2M), Machine-To-People (M2P) and People-To-People (P2P).[2]

These "things" take an important part in our daily lives without us even realizing it. Last but not least, the vendors are obliged to provide some security features to said devices. The IoT devices can provide unauthorized access for the intruders, if the level security is not high enough. As a result, a well-known CIA (Confidentiality, Integrity, Availability) triad in the field of information security could not be achieved. These three elements define the security of every information system. To consider a network to be secure – the information should not be accessed by unauthorized personal in order for it to remain confidential, complete, accurate and so that authenticated users can access it if necessary.

The purpose of this paper is to describe some of the IoT threats and security mechanisms which could be used against threats. Vulnerabilities, attacks and consequences will also be considered. The mandatory countermeasures to these threats will also be discussed.

IoT architecture

IoT devices are all around us, whether we notice them or not. They are not only part of our daily lives – smart watches, fitness bracelets, refrigerators, lighting, etc., but they are also part of the industry, medicine, even smart cities. Interest in such devices is growing, but the growth rate of their number cannot be predicted.

IoT technology is already involved in many areas and industries. This means that it would be difficult to define a uniform structure. In general, the following components could be distinguished:

- Devices (“things”)
- Network
- Gateway
- Cloud/ Storage

Communication between devices is organized mostly by wireless network and a significant part of the process is automated.

In the industry, the information from the sensors is for monitoring the state of objects and through the received information to make a decision. Decisions can also be made from the device itself, i.e. it takes action when a certain condition is met.

In the paper Internet of Things (IoT) - A Vision, Architectural Elements, and Security Issues the authors have presented architecture as a structure for the specification of a network's physical components and their functional organization and configuration, its operational principles and procedures, as well as data formats used in its operation.[3] Layers are defined as:

- Perception Layer - in this layer are the devices and sensors that receive the information – about conditions, state, etc.
- Network Layer - the medium and technology used to transfer data from the device to the device (3G, LTE, WLAN, etc.) that will store and process it.
- Middleware Layer - stores and manages information from devices.
- Application Layer - for application management. The information that middleware stores and processes is used.
- Business Layer - this layer provides already processed information in a form that helps users make their decisions.

Vulnerabilities and Threats

The more the number of IoT devices grows, the more the interest of hackers in organizing attacks grows. Many vulnerabilities in the networks in which these devices are involved, where they are also sought after and identified. In other words - the disadvantage of the system becomes the advantage of the hacker.
The architectural elements of IoT were discussed above, but three of them are always present. It is possible to assume that the architecture is consisted of either three, four or five layers. The original architecture has only three layers, more layers can be added to ensure security. If only the three basic layers present (Application Layer, Network Layer, Perception Layer), the system is considered susceptible to intrusions.

Figure 1 shows the three layers that consist the basic model of the IoT architecture and their security options.

The paper will look at all three layers along with their characteristic vulnerabilities and possible attacks.

Perception/Sensor Layer - as already mentioned - this layer is responsible for receiving data, i.e. the device collects information.

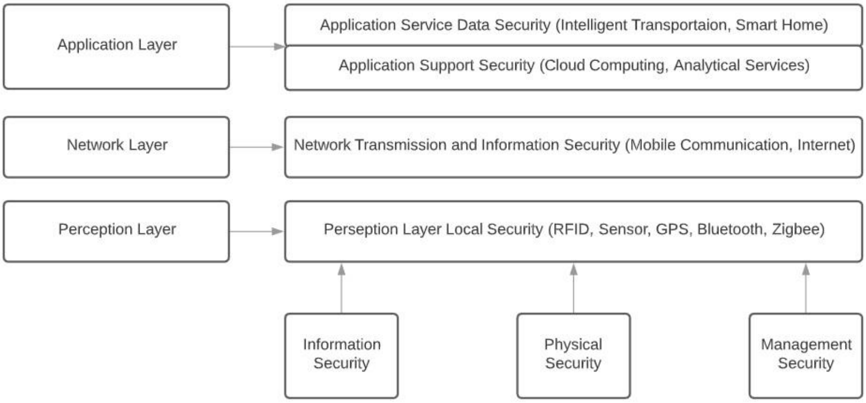
Application Layer
Application Service Data Security (Intelligent Transportaion, Smart Home)
Application Support Security (Cloud Computing, Analytical Services)
Network Layer
Network Transmission and Information Security (Mobile Communication, Internet)
Perception Layer
Perseption Layer Local Security (RFID, Sensor, GPS, Bluetooth, Zigbee)
Information Security
Physical Security
Management Security

Figure 1: Three basic layers of IoT technology.[4]

As shown in figure 1 - physical security is mandatory, otherwise – the intruder could conduct the following attacks:

- Eavesdropping - all information from the network can also be obtained from third parties. In any case - the information is considered sensitive because it contains data about individuals and companies, correspondence, as well as the state of certain systems;
- Node Capturing – the intruder take control over the sensor and manage the system;
- False Data Injection Attacks - once one of the sensors is used by the attacker - he can use it and send wrong data;
- Sleep Deprivation Attacks - these attacks use the ability to drain the edge IoT device's battery. This will cause a Denial of Service attack.

All of mentioned attacks are usually followed by a Denial of Service attack or Distributed Denial of Service attack.

Transportation/Network Layer - the name of the IoT technology suggests that devices are expected to communicate via the Internet, which means that network vulnerabilities must be taken under consideration. The network can be both wired and wireless. The latter predisposes to hacker attacks, because everyone in its range can be actively or passively involved, i.e. only to gather information or actively attack. Transportation Layer is responsible for connectivity and different methods can be used to disrupt the IoT networks normal functionality. The main challenge for any new technology is to devise a method to authenticated its appropriate users. A single unprotected device, that provides unsupervised access, can lead to serious consequences. We will examine some of the potential attacks:

- A Denial of Service (DoS) Attack – as the name suggests, the attackers' intention is that users cannot use services or resources. It is executed by creating a huge number of requests that network devices cannot fulfil – so the system fails to process requests from users who are authorized. This can be especially dangerous, because for some systems it is extremely important to be able to be controlled, and in such an attack – the control cannot be performed. A derivative attack is DDoS, which, unlike DoS, uses much more network resources – it creates more network connections, it is also more difficult to track.
- A Man-in-The-Middle (MiTM) Attack - the man in the middle is actually the attacker. In this attack, all the information goes through a third person, who can actually steal information, but it is also possible to change it. In this attack, the third person may not be found for a long time, especially if he is passive and only receives data.
- Data Transit Attacks – as already mentioned, the information is stored in the cloud or storage where, if not stored according to certain rules, can become a victim of the attack, which may lead to replacement, deleting or copying.

Application Layer – this layer interfaces with the end-user (track heart rate, smart home management, etc.).

- Access control attacks – attackers want to compromise the system and make access control unreliable;
- DoS/DDoS attacks – they are typical for this layer, too;
- A XSS attack – by injecting a script, hackers can change the content of a site, i.e. the information that users will use is changed;
- A Sniffer attack – if the hacker uses a tool to capture network traffic, he may receive sensitive information.

The four-layer model has an additional level – Support Layer. This level is situated before the Application Layer, and its purpose is to check whether users are authorized and if the information required by the application layer is reliable.

The five-layer model consists of not only the three main layers - Perception, Transport, Application Layer, but it also has two new layers – Middleware/ Processing and Business Layer. The Middleware/Processing Layer processes the information and removes the redundant one. The Business layer serves for process management and decision making.

References

[1] Cisco, "The Internet Of Everything – Global Private Sector Economic Analysis," 2013, https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoE_Economy_FAQ.pdf [accessed June 09, 2020].

[2] Atef Zaki Ghalwash, Nashaat El Khameesy, Dalia A. Magdi, and Amit Joshi, "Internet of Things – Applications and Future," *Proceedings of ITAF 2019*, *Lecture Notes in Networks and Systems book series 114,* 2019, pp. 125-136, https://doi.org/10.1007/978-981-15-3075-3.

[3] Shivangi Vashi, Jyotsnamayee Ram, Janit Modi, Saurav Verma, and Chetana Prakash, "Internet of Things (IoT) A Vision, Architectural Elements, and Security Issues," *International Conference on I-SMAC, 2017*, https://doi.org/10.1109/I-SMAC.2017.8058399.

[4] Mohamed Elhoseny and Amit Kumar Singh, "Smart Network Inspired Paradigm and Approaches in IoT Application," (Springer, 2019) https://doi.org/10.1007/978-981-13-8614-5_5.

[5] Jungwoo Ryoo, Soyoung Kim, Junsung Cho, Hyoungshick Kim, Simon Tjoa, and Christopher DeRobertis, "IoE Security Threats and You," *2017 International Conference on Software Security and Assurance (ICSSA), Altoona, PA, USA, 2017*, https://doi.org/10.1109/ICSSA.2017.28.