UDC 004.62

SECURING INTERNET OF THINGS DATA

Trokhymenko D.V., Kurdecha V.V.
Institute of Telecommunication Systems,
Igor Sikorsky Kyiv Polytechnic Institute, Ukraine
E-mail: theelico@gmail.com

Захист даних в мережах "Інтернету речей"

Безпека в мережах Інтернету речей завжди була дуже серйозною проблемою, тому що дані, що подорожують через мережу часто гетерогенних джерел, йдуть через різні пристрої, які можуть мати якусь вразливість безпеки. Ці дані можуть бути використані хакерами, як в вигляді крадіжки, так і у вигляді зловмисної маніпуляції, що може призвести до негативних наслідків. В роботі було досліджено різні підходи та методи формування надійної системи безпеки в контексті хмари та "речей" мережі Інтернету речей.

In recent years, the Internet of Things (IoT) concepts such as smart devices, smart cars, smart cities, and smart homes have received great interest in different research communities. The IoT encompasses both static and dynamic objects of the physical world and the information world, which can be identified and integrated into communication networks (See Fig. 1). Data provided by things are often personal. It can contain our environment, the status of our homes and cities, or our personal health and activities. That is why mechanisms for providing and guaranteeing the security and privacy of data are crucial issues in IoT. However, because of its nature protecting the Internet of Things is a complex and difficult task. This opens up exciting new business opportunities and a trail for economic growth.

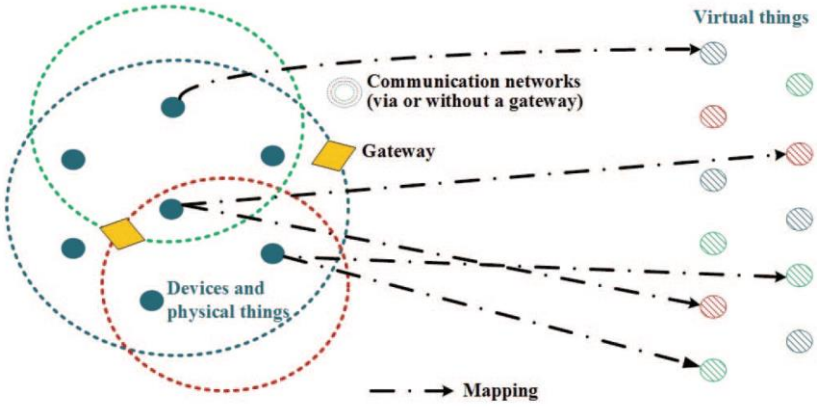

Fig.1 Technical mapping of the IoT

Threats to the security in the Internet of Things. Potential threats to the IoT have basically endless vectors and possibilities. Generally, they are roughly divided by their initial attack target: Attacks Against IoT Devices For an attacker, it is possible that an IoT device with pre-sets is an easy and valuable prey for many reasons. Attacks Against Communications Monitoring and altering the messages while they are being communicated can be a method to endanger the security of IoT. Attacks Against the Master of Devices. The masters including manufacturers, CSPs, and IoT solution providers – when attacked can be inflicted with severe damage. Attacks on Perception Layer Security issues can be found in physical sensing devices and collection of information. Security attacks on WSN, which sense and control the environment can be

Secrecy and authentication, service integrity and network availability. Attacks on Physical Layer Selection and generation of carrier frequency are performed by this layer. Attacks on Network Layer Illegal access, eavesdropping of confidential data, virus etc. are done in network layer. Attacks in Application Layer Eavesdropping and tampering are major security issues in application layer. Traffic management is done in this layer.

The current technologies for IoT security primarily come from the concepts of traditional network security. Most of them focus on identity authentication, access control, privacy protection, encryption, security protocol, and etc. For example, let's look at OAuth 2.0 and oneM2M security frameworks. OAuth 2.0 framework is used to provide authentication and authorization, and Fig. 1 shows general OAuth 2.0 flow.

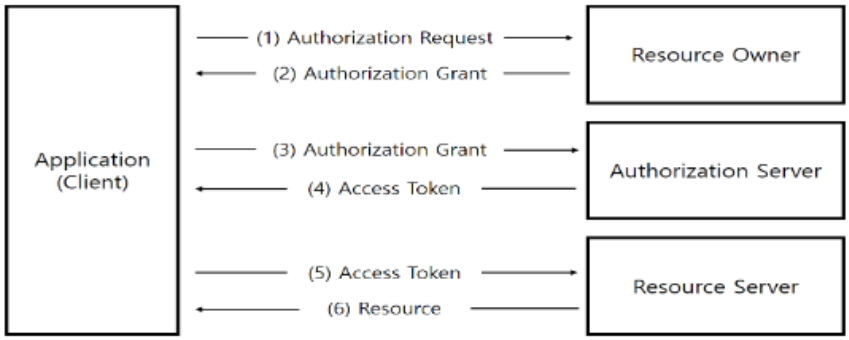

Fig.2 General OAuth 2.0 Flow

The oneM2M security architecture is divided into three layers: Security Functions Layer provides security functions. Secure Environment Abstraction Layer provides key distribution, encryption/decryption, and creation and validation of certificate, Secure Environments Layer contains one or more security environments that provide various security services.

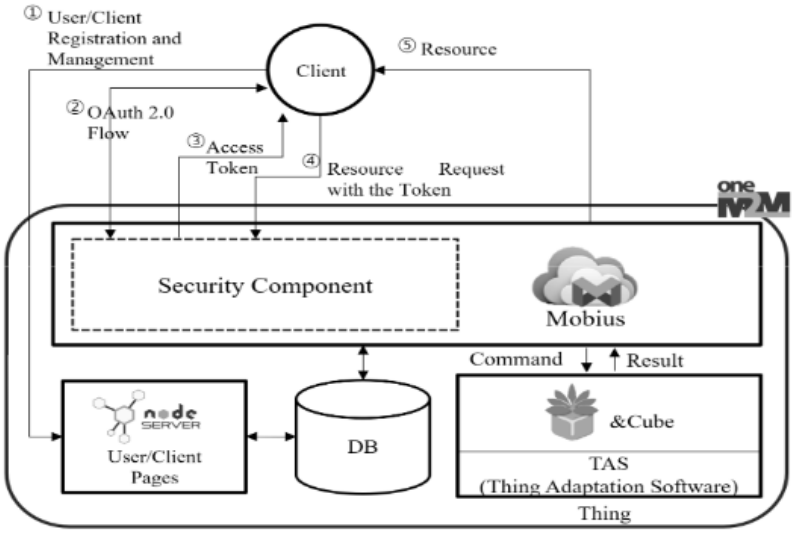

Fig.3 Connectivity Structure of Mobius with oneM2M Security Component

Fig. 3 depicts a basic example of using oneM2M in IoT networks. There are various data encryption techniques which can be different. The level of security for the stored data has been increased that thereby assures content integrity, authenticity, and the availability. Standard and commercial organizations realize the guarantee strategy of network security through the aspects of management and technology. However, the traditional security architectures emphasize simple protection measures and do not make full use of the other links of network security system. They cannot be copied blindly to

construct the IoT security system because of the special attributes of IoT. In the interest of resolving the problems of information security, researchers introduced Artificial Immune System (AIS) which imitates the mechanisms of Biological Immune System. AIS has attributes such as self-learning, self-adaptation, robustness, distribution, etc., it is valuable to use bionics principles of AIS. This approach captures original data from IoT traffic and analyzes the data to judge whether it contains security threats. It simulates the principles and mechanisms of AIS to detect security threats in the original data. The principles and mechanisms have the attributes of self-learning, self-adaptation, etc. They make the approach adapt the dynamic IoT security environments and discover mutated security threats. The approach simulates the following principles and mechanisms: antigen simulation, detector simulation, match mechanism, evolution mechanism, self-tolerance. In the immune systems, antigen is the original data to be recognized. Detectors and the simulative immune mechanisms are used to recognize abnormal antigens from real-time antigens. Danger computation link, the quantitative danger caused by security threats is computed. It needs the elements of harmfulness of security threats, asset cost and memory detectors' thickness which is generated in the previous link. The danger computation process can be summarized in formulas below:

$$A_{harm} = \{a \mid \forall a \in A, \exists d \in D; \cap f_{matching}(d, a) = true\} \quad (1)$$

$$f_{danger}(r) = f(r.t, r.h, c) \quad (2)$$

Where A_{harm} is a recognized data set, D is a known harmful data, $f_{matching}$ – matching function (matching methods include Hamming, Euclidean, *r*-Contiguous, etc.), f_{danger} – danger calculating function, r.t, r.h is harmfulness, c is a cost of IoT asset. The approach then produces security response grades and chooses according to security response polices.

The IoT is expected to integrate advanced technologies of communication, networking, cloud computing, sensing and actuation, and pave the way for groundbreaking applications in a variety of areas, that will affect many aspects of people's lives and bring about many conveniences. Nevertheless, given the enormous number of connected devices which are potentially vulnerable, highly significant risks emerge around the issues of security, privacy, and governance in IoT. The solutions covered in this paper are an important step towards this goal. However, they still require further analyzing and comparing the benefits of using these systems or their combinations onto various IoT network infrastructures, both existing and future.

References

1. Choudhury, T., Gupta, A., Pradhan, S., Kumar, P., & Rathore, Y. S. (2017). Privacy and Security of Cloud-Based Internet of Things (IoT). 2017 *3rd International Conference on Computational Intelligence and Networks (CINE).* doi:10.1109/cine.2017.28.
2. Liu, C., Zhang, Y., & Zhang, H. (2013). A Novel Approach to IoT Security Based on Immunology. 2013 *Ninth International Conference on Computational Intelligence and Security.* doi:10.1109/cis.2013.168.
3. Oracevic, A., Dilek, S., & Ozdemir, S. (2017). *Security in internet of things: A survey. 2017 International Symposium on Networks, Computers and Communications (ISNCC).* doi:10.1109/isncc.2017.8072001.
4. Oh, S.-R., & Kim, Y.-G. (2017). Development of IoT security component for interoperability. 2017 13th International Computer Engineering Conference (ICENCO). doi:10.1109/icenco.2017.8289760.