UDC 621.391

SECURING INTERNET OF THINGS DATA

[1]Larysa S. Globa, [2]Julia S. Yamnenko, [1]Vasyl V. Kurdecha, [1]Danylo V. Trokhymenko

[1]Institute of Telecommunication Systems
Igor Sikorsky Kyiv Polytechnic Institute, Kyiv, Ukraine

[2]Faculty of Electronics
Igor Sikorsky Kyiv Polytechnic Institute, Kyiv, Ukraine

Background. The Internet of Things as a concept and as a network is a multitude of objects, which can be either static or dynamic in nature. Those objects also must be identifiable and should be able to be integrated into communication networks related to both the physical world and the information world, Data provided by things is often personal. It can contain our environment, the status of our homes and cities, or our personal health and activities. That’s why mechanisms to provide and guarantee the security and privacy of data are crucial issues in IoT. However, protecting the Internet of Things is a complex and difficult task. To handle the detection of intrusion in IoT is hard task too. This opens up exciting new business opportunities and a trail for economic growth.

Objective. The purpose of the paper is creating concept of data securing in the Internet of things networks.

Methods. Analysis of publications on data security of the Internet of Things. Integration of existing data protection solutions (at the node, network) level with software management systems.

Results. The possible way is combining the current passive protection such as encryption, and integrating them within more active and dynamic applications, such as AIS-based systems shown in the article or any other similar system.

Conclusions. The paper proposes the concept of data protection in the Internet of Things, which is based on the combination of several solutions into a single system and allows ensuring data protection at a guaranteed level.

Keywords: Internet of things; data security.

I. Introduction

In various research groups and communities the concepts of smart things such as smart devices, smart cars, smart cities, and smart homes, and other concepts of Internet of Things have sparkled great interest in the last few years. The Internet of Things as a concept and as a network is a multitude of objects, which can be either static or dynamic in nature. Those objects also must be identifiable and should be able to be integrated into communication networks related to both the physical world and the information world, Data provided by things is often personal. It can contain our environment, the status of our homes and cities, or our personal health and activities. That’s why mechanisms to provide and guarantee the security and privacy of data are crucial issues in IoT. However, protecting the Internet of Things is a complex and difficult task. To handle the detection of intrusion in IoT is hard task too. This opens up exciting new business opportunities and a trail for economic growth.

Most IoT devices present themselves as "closed systems". Buyers will not be able to add security software after the device leaves the factory. Such an intrusion cancels any guarantee or insurance, and often simply does not seem possible. For this reason, the security features must first be embedded in the IoT so that they are safe in their architecture. Common in information and data security appliances, such "internal security", that is, security which is built into device already at the factory, provides same measures of securing devices, like the classical security technologies such as encryption, authentication, integrity checking, intrusion prevention, and the ability to safely upgrade.

Considering rather close relationship between hardware and software parts of the IoT model, it is sometimes easier for protection programs to use the extension of hardware functions and create "external" security levels. It's great that many chip manufacturers already have built-in security features in their hardware. But the hardware level is just the first layer required to keep communications and devices secure. Viable security also employs different methods and functions, like key management, host security, OTA operation ability and also methods to constantly analyze and monitor state of devices and itself.

The lack of even one of the cornerstones in the foundation of security will leave a wide scope for the actions of intruders. Since the industrial IoT and IoT bring the network intelligence into physical things around us, we must carefully consider their safety issues. For example, in applications related to aircraft, trains and cars we ride in, health and civilian infrastructures that in which we live and work. It's easy to imagine how illegitimate manipulation of something as mundane as traffic lights, or something more personal as medical equipment, or countless other devices spawns a possibility of some kind of a disaster – either personal or affecting group of people. It is clear that none of ordinary citizens and IoT buyers want unfamiliar people to break their houses or cars or that someone will do harm to them by arranging failures on automated industrial sites. In this situation, we will try to propose some recommendations and approaches that help build IoT as secure network, while having it stay rather effective and easy to implement.

II. Internet of things vulnerabilities

Due to the very concept and nature of the network that is IoT, attackers have basically endless vectors or opportunities to perform malicious attacks against network. Although, generally they can be roughly divided by their initial attack target:

A. *Attack on Device*

For an attacker and IoT device with open access points presents itself as an easy prey.

B. *Attack on Master*

Tampering or sometimes just monitoring any messages or commands while they are exchanged greatly endanger the IoT network. Vulnerabilities in manufacturing process, CSPs, or IoT solution providers – when chosen as a vector of attack can lead to severe damage to the network.

C. *Attacks on Perception*

Even the way devices collect information can be tampered with. Hacker attacks on WSN, which are most often used in an industrial of civil IoT applications to monitor the environment, can greatly undermine networks service integrity.

D. *Attack on Physical Interface*

Attacks such as jamming, or carrier frequency hijacking are performed on this layer.

E. *Attacks on Software*

Things such as illegal access to confidential data via eavesdropping or trojan viruses are main concerns here. Eavesdropping and tampering with confidential data is the most crucial issue security systems are trying to prevent.

Therefore, for each of the described network attack vectors, the security system must have some kind of counteraction or prevention of the possibility of an intruder penetrating into the system, or vice versa, the leak of confidential data outside.

A. *Communication security*

Any channel devices speak to each other have to be secure, employing authentication protocols, so that devices know if they can trust the remote party A rather important task here is to manage the keys to establish the authenticity of both the channel and the data being exchanged. Thankfully, modern technologies in cryptography, such as ECC (Elliptic Curve Cryptography), work much better than their precursors on nodes and IoT sensors. Leading Certification Centers (CAs) have already issued special "Device Certificates" for more than a billion IoT devices, enabling them a wide range of IoT devices and sensors to be able to work over secured channels.

B. *Device security*

Device security primarily means the integrity of the embedded software. When implemented, the cryptographic signature of the software ensures that it has not been tampered with and is safe. The software signing is enough to confirm software is safe to run, however additional runtime protection is required so that attackers cannot override any part of software during its execution. Runtime protection can be implemented at application and firmware levels. All critical sensors, controllers, or other devices should be capable to run only the signed code. Devices must be protected in the following steps, even after the code is started. The host can also provide software hardening, system resources access control, connection control, sandbox, various types of behavioral-based protection, blocking, logging of alerts and events for various IoT operating systems.

C. *Device monitoring*

It's sad, but the vulnerabilities in IoT devices will still be, they will need to be closed by patches and modifications, and this can happen for a long time even after the transfer of equipment to the consumer. For example, code with the use of obfuscation in critical systems can eventually be reconstructed, and malicious people can still find vulnerabilities in it. Nobody wants, and often cannot, arrange a solution on-site to each IoT network node for software and firmware updates, especially when it comes to, for example, a truck fleet or a network of hundreds of kilometers of control sensors. For this reason, the necessary precautions, such as OTA ability have to be implemented before devices reach the end user.

D. *Monitoring network interactions*

Some threats can overcome any measures taken regardless of how well everything is protected. It is therefore extremely important to have an IoT security analytics capability. Security analytics systems will help you detect an anomaly that can potentially be suspicious or malicious.

II. IoT DEVICE PROTECTION

Hackers abuse mentioned vulnerabilities to install software, benefitting them, like backdoor, sniffer, other data acquisition software for extracting any kind of confidential information from the system. Sometimes the target could be even the command & control infrastructure (C & C) which can lead to a situation where attacker can alter system's behavior. The ability of some intruders to exploit vulnerabilities to install malware directly into memory already running IoT systems can be particularly disturbing. And sometimes it is chosen such a method of infection, in which the malicious program disappears after rebooting the device but manages to cause great harm. This works because some IoT systems and many IoTs are almost never restarted. For the security department, in this case, the task of detecting vulnerability in the system and investigating the origin of the attack becomes rather complicated. Often attacks occur from an Internet or local IT network, to which the IoT network is connected to. Other times it can be direct physical access to the device. Regardless of what was the source of the intrusion, if compromised device stays undetected, then it is still trusted, hence becoming a “guide” for tampering with other parts of the network, be it the automotive network of the vehicle or the whole production chain of the plant. Therefore, IoT security should be comprehensive. Unacceptably close the windows, leaving the door open. All vectors of threats must be suppressed.

Authentication and manageability are the backbone of lasting secure network. There are excellent open source libraries that allow hardware encryption even in IoT devices, having their limited computing resources. But, unfortunately, most companies are still at risk, assuming errors in key management for the IoT. E-Commerce transactions of up to $4 billion a day are secured just by a simple and reliable credibility model that serves billions of users and more than a million companies around the world. This credibility model help systems safely verify the reliability of other party and interact with them over secure communication channels.

III. Trust in IoT

The already existing technologies used in IoT security primarily are borrowed concepts of more or less traditional network security, used current in IT or telecommunication networks. That comes from the fact that most of such concepts focus on identity authentication, access control, privacy protection, encryption, etc. often without considering any of IoT network features.

To take a perspective on it let's look at OAuth 2.0 and oneM2M security frameworks as an example of passive approach to IoT network security. OAuth 2.0 is a framework developed for being used in authentication and authorization processes. Fig. 1 depicts the usual OAuth 2.0 workflow.

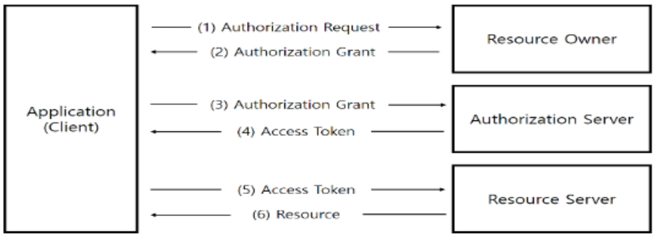

Fig. 1. General OAuth 2.0 Flow

Additionally, Mobius, which is the open source IoT server platform based on the oneM2M standard, is used to provide common services functions (e.g. registration, data management, subscription/notification, security). Mobius can also be used as a middleware to IoT applications of different service domains, even not specified by oneM2M.

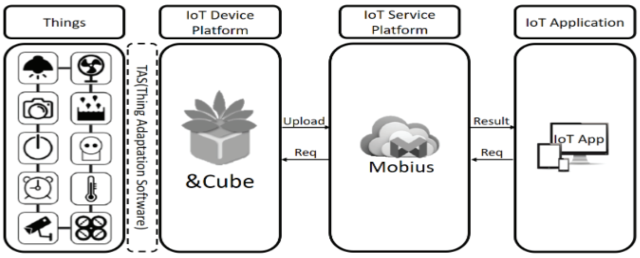

Fig. 2. Connectivity Structure of Mobius

Fig. 2 shows that, IoT devices like a CCTV, a drone or a lamp could be connected to Mobius through the special piece of software called TAS (Thing Adaptation Software). TAS most often works over special IoT device platform (&Cube for example, as shown on the figure), and IoT application can control managed things by making use those systems. The important thing to know here is that commands issued by the application are the form of REST API, more specifically a subset of CRUD (Create, Read, Update and Delete) used in Mobius. The use of REST API means the access, execution and management right can be reliably authorized through the use of OAuth2 framework.

The oneM2M security architecture is divided into three layers:

- Security Functions Layer - provides main security functions
  - Identification and Authentication,
  - Authorization,
  - Identity Management,
  - Sensitive Data Handling,
  - Security Administration.
- Secure Environment Layer - contains several implementations of various security services for providing sensitive data or execution of critical function.
- Secure Environment Abstraction Layer - handles key distribution, encryption/decryption, and creation and validation of certificate. Also, any credentials which are created or verified inside Secure Environments layer are handled by this level.

Fig. 3 depicts a basic example of using oneM2M in IoT networks.

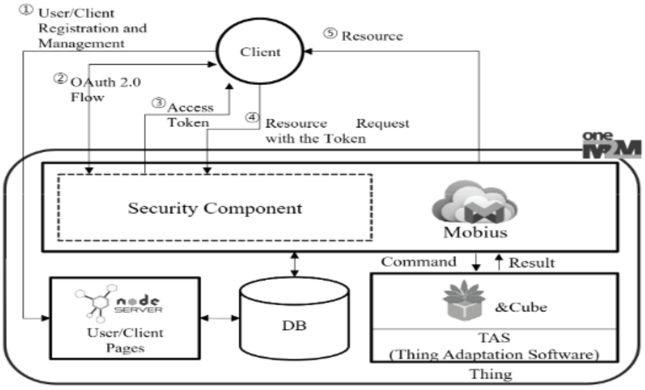

Fig. 3. Connectivity Structure of Mobius with oneM2M Security Component

There exist different data encryption algorithms and methods each with their own features. Increasing the level of security for stored sensitive and critical data thereby can assure its content integrity, availability and authenticity. However, as mentioned before the traditional security architectures consist of traditional protection measures and do not make full use of the other features possible to implement in network security system. That means they cannot be copied blindly to construct the IoT security system because of the special attributes and features of IoT as a network.

IV. Device Security

Even after protecting communication and having a secure and well-managed device, additional protection may be needed during the operation phase. IoT devices face many threats that can be exploited by attackers and distributed through connections, which are compromised, but seem secure. Weak signing, poor verification model is often exploited in such attacks, using anything that could be circumvented. Fortunately, in combination with a reliable signature of the code and verification model, host-based protection can help protect the device from a host of dangers. The host-based protection consists of malware protection, system resources access management, sandboxing, hardening, behavioral protection, and encryption. In a particular IoT system, the right combination of these technologies can provide the best level protection for each and every part of the network. Hardening, delimitation of access to resources and sandboxing will protect all the "doors" into the system. They limit network connections to applications and regulate the incoming and outgoing traffic flow, protect against various exploits, buffer overflow, targeted attacks, regulate the behavior of applications, while allowing control over the device. That solution still can be used to prevent unauthorized use of device, by locking device settings, or even removing user privileges, if needed. Host protection has the ability to audit and alert, helping to track event logs. Policy control technologies can handle working in environments without connection to the outside network, with the limited computing power. Reputation technologies can be used to determine the nature of files by age, prevalence, location, and the rest to identify hazards that are not detected by other means, and to give an idea of whether to trust the new device even with a successful authentication. This way, you can spot threats that use a mute code or go as far as adapting encryption scheme by simply separating files at high risk, forming a fast, safe and accurate malware detection system, in spite of all hackers' tricks. Of course, the proper combination of technologies is highly dependent on the situation, but the combination of above methods can be created to secure devices, even having environment with limited computing resources.

V. Blockchain in IoT

Blockchain technology is used in different ways, most known of them are proof of work electronic currency systems. So the concept of decentralized secure system may prove themselves as a very valuable asset for any field of research and development.

An IoT network implementing such concepts inside their security system may seem a very easy and effective solution to the security and privacy problems. A blockchain infrastructure consists of decentralized nodes, which exchange blocks of information, encrypted by some form of asymmetric encryption, more recently ECC-based. Common among them is for example are 32 bytes random keys based on the secp256k1 curve. The node address is also usually equal or is derived from its public key. The main blockchain features are the following:

- No separate management and control entity, network is decentralized and self-governing.
- Every transaction ever executed is stored in the database and can be accessed by any peer at any time.
- No centralized storage for all the ledger components, i.e. transactions and blocks, so each node has to keep their own copy.
- Every transaction is validated by each node separately – which means consensus also has to be decentralized.

IoT infrastructures, sensor data are usually not stored on the devices themselves, but instead sent to cloud. Usually neither data itself, nor communication channels are taking care about authentication or reputability of such transactions. Blockchain can help solve such issue, providing networks a way to authenticate the data distributed inside the system, to ensure that it was not tampered in any way. However, Blockchain itself has gives no guarantee of data being correct in a sense that in case of IoT devices source of data itself can be tampered even before the data from it enters the network. This and the need to store the transaction history are the main issues that have to be considered when designing security systems.

VI. Dynamic security

Such approach to securing network devices and channels consists of dynamically detecting any irregularities in dataflow, because they can possess a threat to such network integrity. One of such approaches employs Artificial Immune Systems (AIS) special complex systems that borrow characteristics and mechanisms such as self-learning, self-adaptation, robustness, distribution, etc., implementing them similarly to Biological Immune Systems (BIS). Due to this AIS has the potential to use bionics principles of detection and reaction in networks or other computer systems.

The dynamic AIS-based system works by monitoring and capturing of IoT network traffic and analyzing it against different known or developed signatures to determine if dataset can pose a threat to the system. Use of AIS allows the system to be more flexible against unusual security threats. Because of highly dynamic nature of IoT network, employing features found in Biological Immune Systems can allow the system to be adaptable enough to provide necessary security level to the devices, and respond to any potential breach in the network.

Essentially, system built on that approach must have the following attributes, which qualify it as AIS:

- antigen simulation
- detector simulation
- match mechanism
- evolution mechanism
- self-tolerance

The antigen, for AIS being the original data set to be analyzed by the system can be defined by following formula.

$$A = \{a \| a| = l, a = bSring(D)\} \quad (1)$$

Where A represents the antigen, $l \geq 0$ is the length of the data set and $bSring(\ )$ is some kind of a parsing or converting function, in this example representing data set as binary string.

In this dataset to find and recognize abnormalities in antigens the simulative AIS immune mechanisms called detectors must exist. Such detectors can be defined as follows.

$$D = \{\ a, t_a, n, f\ \} \quad (2)$$

Where: a is the antibody data, t_a is living time, n is the number of recognizable antigens, and f is the class of antigen.

Some quantitative representation of danger caused by security threats also has to be considered in the system. Danger computation links are employed for this function. They require some elements of harmfulness of security threats that can be easily translated into numerical parameters, such as importance or sensitivity of data handled in or by the device. Another major factor could be asset cost. Memory detectors' thickness generated in the previous link also has to be considered in computation. The danger assessment process can be summarized in formulas below.

$$A_{harm} = \{a | \forall a \in A, \exists d \in D; \cap f_{matching}(d,a) = true\} \quad (3)$$

$$f_{danger}(r) = f(r.t, r.h, c) \quad (4)$$

Where A_{harm} is a recognized data set, D is a known harmful data, $f_{matching}$ – matching function (feasible matching methods can include Euclidean, *r*-Contiguous, Hamming, etc.), f_{danger} – danger calculating function $r.t, r.h$ - is harmfulness, c is a cost of IoT asset.

In order of this system to function properly it needs some way to detect and properly process antigens of itself. In BIS, the mechanism of self-tolerance is used to prevent cells from recognizing self-antigens as harmful data, but instead ignore or take another non-destructive action. In the proposed approach, the AIS may develop new detectors which must have the ability to recognize and properly handle self-elements. It can be shown as an additional detection function defined the way shown below.

$$f_{self}(D) = \{r \vee r \in D, r.t_a \geq t, \forall s \in S \wedge f_{matching}(r,s) = false\} \quad (5)$$

Where D is immature detector, t is time threshold for self-tolerance, and S is the self-set

However, such detectors usually cannot and should not be used to detect security threats directly.

After performing the recognition and danger computation of the antigen system then has an option of assigning it security response grade. Then it can choose corresponding security response polices or offload this task to some kind of management device. Additionally, those policies not only could be set in stone based on prognosed system needs and value of the network assets, but they also could be dynamically changed to reflect on the possible change in the network.

VII. Application protection

Each device runs a specific executable code. It is extremely important for us to be confident that the devices will do only what we have programmed, and that third parties cannot reprogram them. That is, the first step in protecting the devices is the protection of the code, so that it is guaranteed to load and only the code that we need is launched. Fortunately, many manufacturers have already built support for the ability to download safely into their chips. Similarly, things come with high-level code - various open source client libraries, such as OpenSSL, can be used to verify signature and authorization of a code from an authorized source only.

As a result, sign-up firmware, download images and higher-level embedded code. And this code includes signed base software components and operating systems. Newer developments should even allow signing not only firmware but just any possible applications able to be executed on the device. Thus, approach ensures that all critical devices in the network like gauges, mechanisms, controllers and hubs are configured correctly – to ever run correctly signed applications and disallowing or being flat out unable to run unsigned applications.

A good manner would be to stick to the principle of "never trust non-signed data." A logical extension would "never trust the data not signed and, moreover, not signed configuration data". The use of modern means of signing up and distribution of hardware implementation of secure download, poses a serious task for many companies - key management and access control keys to sign code and protect software and hardware. Fortunately, some certification centers offer cloud services that make it easier, safer and more reliable to administer code signing applications and guarantee strict control of how and who can sign the code, manage signatures, and how the signature infrastructure cannot be tampered with.

There are situations when the software needs to be updated, for example, for security reasons, but it should consider the impact of battery upgrades. Data rewrite operations increase power consumption and shorten the battery life of the device. There could be a need for partial signing individual blocks or fragments of data, so rather than monolithic images of firmware updates can be applied gradually. Then software, signed at the block level or fragments, can be updated with much finer detail, without sacrificing security or battery charge. This does not have to be built-in hardware feature; such flexibility is possible through a special software environment that is able to work on many embedded devices. And if the issue of battery life raises itself as critically important, it should be possible to just configure a device in a way that nobody can change or tamper with firmware.

Unfortunately, while creating application security system we have to assume that devices in the field are very vulnerable to reverse engineering. After its conduct, vulnerabilities are detected and exploited, which must be closed as soon as possible. Techniques such as obfuscation or runtime encryption potentially significantly slow down the reverse engineering process and possibly even discourage further attacks on most attackers. But hostile secret services or transnational destructive organizations can do this even for programs that are protected by obfuscation and encryption, primarily because unfortunately the devises cannot run encrypted or obfuscated code. So, such hackers can find and use even the most obscure vulnerabilities, provided they were not timely closed or dealt with.

Due to this, remote upgrade capabilities are critical and must be embedded in the device before they leave the manufacturing process. Software and firmware updates distributed through OTA can be extremely important to maintain a consistently high level of security of the device. However, the obfuscation, segmentation of the code signing, and OTA updates must be tightly interconnected with the IoT network to work efficiently.

VIII. Conclusion

Internet of Things as a concept and as a network is expected to integrate a lot of advanced technologies in the fields of telecommunications, cloud and fog computing, sensing thus paving the way for groundbreaking applications in a variety of areas, which will affect many aspects of people's lives and bring about many conveniences. Although considering the nature of IoT network, like the enormous number of connected devices, or the no less enormous volume of data inside the network that is potentially vulnerable, the issues of security, privacy, and governance in IoT raise very significant risks. Solutions covered in the paper are important step forward towards achieving the goal of overcoming those challenges. 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. Although no "one-for-all" solution could be feasibly created in the near future, there still is a possibility to create new and improved approaches and systems that further enhances the security of the IoT network. One possible way the imperfect system could be implemented is combining the current passive protection such as encryption, and integrating them within more active and dynamic applications, such as AIS-based systems shown in the article or any other similar system.

References

[1] S.Suganthi, D.Usha. A SURVEY OF INTRUSION DETECTION SYSTEM IN IOT DEVICES Int. J. Adv. Res. 6(6), 23-3ISSN: 2320-5407

[2] Falguni Jindal, Rishabh Jamar.FUTURE AND CHALLENGESOF INTERNETOF THINGS // International Journal of Computer Science & Information Technology (IJCSIT) Vol 10, No 2, April 2018 DOI:10.5121/ijcsit.2018.10202

[3] D. H. Summerville, K. M. Zach, Y. Chen, Ultra-lightweight deep packet anomaly detection for Internet of Things devices, in: 2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC), IEEE, 2015, pp.1–8.

[4] 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

[5] 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

[6] 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

[7] 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

[8] M. Tortonesi, J. Michaelis, N. Suri and M. Baker, "Software-defined and value-based information processing and dissemination in IoT applications," NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium, Istanbul, 2016, pp. 789-793

[9] S. K. Sharma and X. Wang, "Live Data Analytics With Collaborative Edge and Cloud Processing in Wireless IoT Networks," in IEEE Access, vol. 5, pp. 4621-4635, 2017.

[10] Tasnuva Mahjabin1, Yang Xiao1, Guang Sun2 andWangdong Jiang, A survey of distributed denial-of-service attack, prevention, and mitigation techniques, International Journal of Distributed Sensor Networks, 2017, Vol. 13(12).

[11] Roman, Rodrigo, Jianying Zhou, and Javier Lopez. "On the features and challenges of security and privacy in distributed internet of things." Computer Networks 57.10 (2013): 2266-2279.

[12] Urien, P. (2018). Blockchain IoT (BIoT): A New Direction for Solving Internet of Things Security and Trust Issues. 2018 3rd Cloudification of the Internet of Things (CIoT). doi:10.1109/ciot.2018.8627112

[13] Lu, X., Li, Q., Qu, Z., & Hui, P. (2014). Privacy Information Security Classification Study in Internet of Things. 2014 International Conference on Identification, Information and Knowledge in the Internet of Things. doi:10.1109/iiki.2014.40

[14] Narang, S., Nalwa, T., Choudhury, T., & Kashyap, N. (2018). An efficient method for security measurement in internet of things. 2018 International Conference on Communication, Computing and Internet of Things (IC3IoT). doi:10.1109/ic3iot.2018.8668159

[15] S. Geetha, R. Hariharan and V. P. Venkatesan, "Secured Indexing and Tagging of IoT Based Device Nodes for Service Based Licensing and Secured Access," 2017 World Congress on Computing and Communication Technologies (WCCCT), Tiruchirappalli, 2017, pp. 6-10. doi: 10.1109/WCCCT.2016.12

[16] S. J. Johnston, M. Scott and S. J. Cox, "Recommendations for securing Internet of Things devices using commodity hardware," 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, 2016, pp. 307-310. doi: 10.1109/WF-IoT.2016.7845410

[17] M. Singh, A. Singh and S. Kim, "Blockchain: A game changer for securing IoT data," 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 2018, pp. 51-55. doi: 10.1109/WF-IoT.2018.8355182

[18] Globa L. Method for resource allocation of virtualized network functions in hybrid environment / L. Globa, M. Skulysh, S. Sulima // 2016 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), 6–9 June 2016 : conference proceedings. — Varna, Bulgaria, 2016. — P. 1–5.

[19] Mariia S., Svitlana S. Service deployment aspects in the systems with network function virtualization //Radio Electronics & Info Communications (UkrMiCo), 2016 International Conference. – IEEE, 2016. – С. 1-7.

[20] Skulysh M. Management of Multiple Stage Queuing Systems / M. Skulysh, S. Sulima // CADSM 2015 : 13-th International conference, 24–27 February 2015 : conference proceedings. — Lviv–Polyana, 2015. — P. 431– 434.

[21] Benazzouz, C. Munilla, O. Günalp, M. Gallissot and L. Gürgen, "Sharing user IoT devices in the cloud," 2014 IEEE World Forum on Internet of Things (WF-IoT), Seoul, 2014, pp. 373-374. doi: 10.1109/WF-IoT.2014.6803193

[22] Globa, L., Kurdecha, V., Ishchenko, I., Zakharchuk, A., Kunieva, N."The Intellectual IoT-System for Monitoring the Base Station Quality of Service", 2018 IEEE International Black Sea Conference on Communications and Networking, BlackSeaCom 2018, 8433715

[23] S. Suhail, C. S. Hong, Z. U. Ahmad, F. Zafar and A. Khan, "Introducing Secure Provenance in IoT: Requirements and Challenges," 2016 International Workshop on Secure Internet of Things (SIoT), Heraklion, 2016, pp. 39-46. doi: 10.1109/SIoT.2016.011

[24] T. Shah and S. Venkatesan, "Authentication of IoT Device and IoT Server Using Secure Vaults," 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), New York, NY, 2018, pp. 819-824. doi: 10.1109/TrustCom/BigDataSE.2018.00117

[25] M. Singh, A. Singh and S. Kim, "Blockchain: A game changer for securing IoT data," 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Singapore, 2018, pp. 51-55. doi: 10.1109/WF-IoT.2018.8355182

[26] Liu, C., Zhang, Y., Li, Z., Zhang, J., Qin, H., & Zeng, J. (2015). Dynamic Defense Architecture for the Security of the Internet of Things. 2015 11th International Conference on Computational Intelligence and Security (CIS). doi:10.1109/cis.2015.100

Глоба Л.С., Ямненко Ю.С., Курдеча В.В., Трохименко Д.В.

Захист даних мережі Інтернету речей

Проблематика. Інтернет речей як поняття і як мережа - це безліч об'єктів, які можуть мати статичний або динамічний характер. Ці об'єкти також повинні бути ідентифікованими і повинні бути здатні інтегруватися в комунікаційні мережі, пов'язані як з фізичним світом, так і з інформаційним світом. Дані мережі Інтернету речей часто є особистими - наприклад персональні дані, інформація про діяльність, фінанси, здоров’я, довкілля тощо. А тому механізми забезпечення та гарантії безпеки та конфіденційності даних є вирішальними питаннями Інтернету Речей. Однак захист даних Інтернету речей є складним завданням, що з одного боку потребує створення концепції захисту даних, а з іншого відкриває нові можливості виробництва.

Мета досліджень. Створення концепції захисту даних в мережі Інтернет речей.

Методика реалізації. Аналіз публікацій, присвячених безпеці даних мереж Інтернет речей. Інтеграція існуючих рішень захисту даних (на рівні вузла, мережі)з програмними системами управління.

Результати. Результат заключается в сочетании текущей пассивной защиты, такой как шифрование, и интеграции их в активные и динамичные программы, такие как системы на основе AIS.

Висновки. В роботі запропоновано концепцію захисту даних в мережі Інтернету речей, що базується на поєднанні кількох рішень в єдину систему та дозволяє забезпечити захист даних на гарантованому рівні.

Ключові слова: Інтернет речей; захист даних.

Глоба Л.С., Ямненко Ю.С., Курдеча В.В., Трохименко Д.В.

Защита данных сети Интернета вещей

Проблематика. Интернет вещей как понятие и как сеть - это множество объектов, которые могут иметь статический или динамический характер. Эти объекты также должны быть идентифицированы и должны быть способны интегрироваться в коммуникационные сети, связанные как с физическим миром, так и с информационным миром. Данные сети Интернета вещей часто являются личными - например персональные данные, информация о деятельности, финансы, здоровье, окружающая среда и тому подобное. Поэтому механизмы обеспечения и гарантии безопасности и конфиденциальности данных являются решающими вопросами Интернета Вещей. Однако защита данных Интернета вещей сложной задачей, с одной стороны требует создания концепции защиты данных, а с другой открывает новые возможности производства.

Цель исследований. Создание концепции защиты данных в сети Интернет вещей.

Методика реализации. Анализ публикаций, посвященных безопасности данных сетей Интернет вещей. Интеграция существующих решений защиты данных (на уровне узла, сети) с программными системами управления.

Результаты исследований. Результат заключается в сочетании текущей пассивной защиты, такой как шифрование, и интеграции их в активные и динамичные программы, такие как системы на основе AIS.

Выводы. В работе предложена концепция защиты данных в сети Интернета вещей, основанный на сочетании нескольких решений в единую систему и позволяет обеспечить защиту данных на гарантированном уровне.

Ключевые слова: Интернет вещей; защита данных.