

Recent Challenges, Trends, and Concerns Related to IoT Security: An Evolutionary Study

Chalee Vorakulpipat*, Ekkachan Rattanalernusorn*, Phithak Thaenkaew*, Hoang Dang Hai**

*Cybersecurity Laboratory, National Electronics and Computer Technology Center, Pathumthani, Thailand

**Post and Telecommunication Institute of Technology, Hanoi, Vietnam

chalee.vor@nectec.or.th, ekkachan.rat@nectec.or.th, phithak.tha@nectec.or.th, haihd@ptit.edu.vn

Abstract—Network security has become a critical issue in recent years. A drastic increase in the use of devices for accessing corporate networks could expose these systems to major security risks. As the use of personal computers moves to mobile devices and now IoT devices, it is highly desirable to gain more services and more accessible channels for corporate information. In addition, the scope and definition of IoT security have changed from time to time in response to technology changes and market needs. This paper presents a review of recent challenges, trends, and concerns related to IoT security, and discusses three generations of IoT security from past to future. IoT service platforms, values created out of customers' transaction data, industry and market driven approaches, the replacement of smartphone or BYOD, and IoT policies will all become more important.

Keywords— Internet of Things (IoT), Security, Challenges, Trends, Concerns

I. INTRODUCTION

Information security is an important topic in many organizations and industries. Network security is one of the information security domains. A corporate network must be protected from data interception, theft, and attack by unauthorized persons or hackers. Numerous countermeasures have been introduced and adopted to reduce this vulnerability risk, and today these are the must-have solutions in any organization to strengthen their network security. One of the widely accepted solutions is a preventive action that includes a system for monitoring and detecting attacks and threats in computer systems within an organization or across organizations. The Internet of Things (IoT) has become well-known over the last decade. The reasons may include the fact that an IoT device is easy to implement, portable, and lightweight [1,2]. However, although the use of IoT devices has drastically increased, security practices in most IoT devices are not yet in place [3]. Many studies have expressed concerns about security issues, and these concerns continue to change in response to

technology trends and industry demands [4,5]. Although there have been studies of the challenges, trends, and concerns related to IoT security, it is difficult to find an evolutionary study of these. Therefore, there is a need to study IoT security concerns with an emphasis on the recent challenges and trends.

The objective of this paper is to provide a holistic understanding of IoT security, with a focus on the recent challenges, trends, and concerns. The presentation will be divided into several categories related to technology trends and industry demands. The paper first provides a general description of information security, network security, and IoT security, followed by the challenges, trends, and concerns related to IoT security. The following sections present the generation of IoT security, along with some conclusions.

II. INFORMATION SECURITY AND IOT SECURITY

Information security is categorized into numerous domains, including security and risk management, asset security, security engineering, communications and network security, identity and access management, security assessment and testing, security operations, and software development security. All of these focus on the protection of data and information assets. Communications and network security, or simply network security, deals with how to protect data from end to end (data at the source, during transmission, and at the destination), and it is considered to be one of the most important security domains.

Information security can be categorized into three groups, including confidentiality, availability, and integrity [6]. Confidentiality deals with how to protect data from unauthorized access. Access control is used to preserve the confidentiality and

privacy. Access control can include a username and password, token, biometric authentication, or multi-factor authentication. Cryptography is employed to prevent data interception. In network security, end-to-end encryption like a virtual private network (VPN) is generally used when transmitting sensitive data. Availability ensures that the data system is available when needed. Redundancy and backup systems are adopted to secure availability. In terms of integrity, this ensures that the data stored in a system are not modified or deleted by unauthorized persons or malware. An intrusion detection/protection system is a good example of how to strengthen the system integrity.

An IoT device can work as a computer or cyber-physical system that stores and transmits data from one machine to others [7]. Thus, IoT security should be handled, as well as computer security, especially network security. However, the IoT cannot purely focus on network security. An application layer must be included [8]. The IoT not only involves data transmission in a network, but also contains the data, storage, and processor. Therefore, data protection during storage is also important. There are many issues in IoT security. Privacy is a common concern. This is because the IoT has not yet really been standardized, which creates a problem for developers [9]. In many cases, IoT devices are out of control and cannot be monitored by system administrators [10,11]. Some IoT devices are not protected by sufficient access control [12]. Therefore, the use of an IoT may not be under an organization's information security policy. Some authentication process limitations inhibit IoT security [13]. For example, an IoT device cannot use a web authentication system to obtain access to a corporate network, but instead must use an outside network (3G/4G) without authentication, leading to security breaches and security compromises. Moreover, because there are too many devices, many problems emerge without control [14]. This is the same as in the case of Bring Your Own Device (BYOD) like smartphones and tablets, which people can use freely through a corporate network and are not monitored by the organization. In fact, a BYOD device is perceived to be replaced by an IoT device because they share common functions [15]. Thus, most security

concerns are similar. These days, cloud-based IoT platforms have been heavily introduced to help developers implement IoT-based systems in an easy way [16]. For example, the platform provides libraries that facilitate coding. Because the platform is based on the cloud, the security concerns can relate to those in cloud computing. Privacy concerns are usually raised with the cloud or a third-party platform. Therefore, the security responsibility will mostly go to the platform providers, who will be tasked with building the developers' or customers' trust and confidence.

III. RECENT CHALLENGES, TRENDS, AND CONCERNS RELATED TO IOT SECURITY

Information security concepts periodically change due to technology and market changes. For example, in the last ten years, people have exhibited concerns about privacy in cloud computing or third-party public clouds, whereas today using a cloud service is much more widely accepted because cloud providers have more security readiness than in the past, and business sectors are satisfied with the benefits of the cloud, e.g., the low cost and elasticity [17]. At the beginning of the IoT era, the security issues are similar to common network security issues. Intrusion and malware detection is the must-have countermeasure to combat attackers. Although data interception during transmission is a concern, most IoT devices use the same network as other computers. Thus, the security level is not different. However, protecting data in an IoT device is more serious. This is because data storage security is not designed during the beginning stage of the development. Developers may not be familiar with an IoT device and its operating system. Moreover, most of them focus on functionality rather than security, similar to other computer application developers.

In the past, people developed in their own way without a standardized development guideline. It was difficult to control all of the devices and their security. Although there is no single de facto standardized IoT protocol, developers today find an easy way to develop. MQTT is widely accepted and used as a protocol for data communication between devices. Numerous IoT platforms have been introduced to allow IoT developers to implement in

a shorter time. Platform providers offer developers a cloud-based infrastructure, platform, and libraries and allow them to write shorter lines of code. Privacy concerns are mentioned less frequently because people have more trust and confidence in the providers. Moreover, most providers today are aware of the need for a security standard in the scope of data center, such as the ISO/IEC 27000 standard in particular. Because this service is centralized, providers can collect rich data about user (device) behavior and logs or transactions. This can be useful for security reasons (incident detection) and business purposes (customer analytic).

Because the number of IoT devices has drastically increased over the last five years, most devices are out of control, similar to wireless devices or BYOD in the past. Using de facto standards and a centralized platform can reduce this problem. This could be monitored by a system administrator, and the transactions could be recorded. However, in most cases, because of technical problems or constraints, some IoT devices cannot use the organization's authentication system (e.g., web authentication). Thus, they choose to use an outside network like a mobile 3G/4G network. In this case, these devices will not be under the same security policy, which will be problematic when an incident occurs because a system administrator cannot monitor them. Recently, many organizations have included BYOD security issues in their security policy. If a BYOD device is indicated as a subset of IoT, IoT security issues should be added to the policy.

Data monitoring and detection processes with an IoT are not different from those for a computer. This can make it difficult to differentiate IoT activities from other computer activities in log data. IoT devices and computers may not be assigned real IP addresses, and the IP address assigned to a device can periodically change, which makes it difficult to identify a device. To solve this problem, an IP address or a set of real IP addresses can be allocated for the use of IoT devices, and a system administrator then creates an internal IP and log management system to identify IoT devices by assigning virtual IP addresses to all of the IoT devices. Once an incident occurs by an IoT device,

a real IP address assigned to the IoT can be detected, and a system administrator can identify an IoT device from a virtual IP address assigned under the real IP address. IoT service providers should develop security requirements to help identify devices [18].

Although privacy in a third-party IoT platform is less of a concern, confidentiality issues still exist. Confidentiality for data storage and data transmission is at a high level. Storage in an IoT device may not be designed with security concerns and most manufacturers may overlook these. Data may be transmitted through a secure corporate network. Nevertheless, the data at the source device and destination device (end to end) may not be encrypted or may be in clear text. End-to-end encryption is very crucial when communicating between devices. Network watermarking can be used to hide the identity [19]. It could be applied to the IoT, although it is still rarely used. Today, the IoT is more widely used in the real world, both for home use and industry use. Data therefore becomes more sensitive than in the past, and security countermeasures should be considered more seriously.

IV. GENERATIONS OF IoT SECURITY

It can be argued that an IoT device is viewed as a computer or BYOD due to similar functions and security concerns. In fact, the scope and definition of IoT security that has evolved over the years are understood in a broader way from time to time depending on technology changes and market needs. At present, there are at least three generations of IoT security.

A. First Generation

The first generation was related to traditional computer security concerns, including confidentiality, availability, and integrity, with an emphasis on network security. Most IoT devices were implemented and deployed in a test environment, which not everyone could use. Therefore, the challenges and concerns were limited to developers. The use of several different standards became a problem when developers implemented IoT in different ways, which led to incompatibility and other unexpected incidents. Similar to the early

adoption of cloud computing, the IoT was not known by many people. Thus, many challenges and concerns were mentioned. Privacy protection was a significant challenge during the early stage. Privacy involved end-to-end communication from data storage to data transmission. Cryptography, including encryption, decryption, and PKI, was important to preserve confidentiality in the IoT. Because an IoT communicates between or among devices in a network, there were issues related to protecting the network infrastructure and data. The countermeasures included intrusion detection and protection, malware analysis, and DDOS protection.

B. Second Generation

The second generation is the current generation, where people are more familiar with IoT and use it in a real environment. The challenges and concerns in this generation will go to both developers and users. There are a large number of cloud-based IoT platforms offering infrastructure and libraries. Therefore, developers (or even new developers) find easier ways to implement IoT using these platforms. The easy implementation and fast delivery of products are more important because of market demands. Similar to cloud adoption today, privacy is less of a concern because people are satisfied with the benefits offered by the service providers and have confidence in them. Once using third-party services become well known and widely accepted, developers are forced to implement the same standard in order to be compatible with libraries provided by the platform. Authentication and user (device) identification can be a challenge. Because an IoT is deployed in a real environment, this can create various constraints, which is different from a test environment. For example, when an IoT device connects to a real corporate network, its use must comply with the organization's security policy; it must be monitored by a system administrator; its activities must be recorded in a log file (by law); and finally, it can be viewed as a computer. To accomplish all of these, authentication and identification systems should be implemented. The challenge is how to authenticate a device using the existing authentication system (such as web authentication) and how to identify a device and detect transactions of IoT devices from a

log file. In terms of availability concerns, a large number of IoT devices rely on a centralized platform, as previously mentioned. Thus, more concern should be given to a single point of failure.

C. Third Generation

The third generation, or future generation, focuses on value creation in business and industry. IoT implementation on a cloud-based IoT platform will become widespread. Rich data from device transactions will be centrally stored. A service provider can analyze the big data (e.g., customer behavior) to create business values, which will improve productivity. Privacy issues will be related to customers' sensitive data. The IoT in this generation is not only adopted in real situations, but also moves to more industry sectors and links to other technologies. IoT and blockchain technology will enable the exchange of transaction data among users and devices to secure the availability and authenticity of data. The technologies involved in this generation may include big data analytic, deep learning, artificial intelligence, business intelligence, cryptography, blockchain, and watermarking. In the future, the IoT is expected to replace the smartphone or BYOD. In other words, the IoT will be able to work as any computing system and could be used on a regular basis. Therefore, the creation of policies, regulations, standards, and guidelines for IoT security will be necessary.

These three generations of IoT security are summarized in Table 1.

V. CONCLUSIONS

This paper has presented a discussion of IoT security in relation to the challenges, trends, and concerns based on a review and synthesis of a broad range of relevant literature. The first generation of the IoT shared common security practices with general computer usage, while concerns about adopting new technology were raised. In the second generation, today's IoT is widely implemented in a real environment. Cloud-based centralized IoT service platforms have been welcomed by developers because of their ease of implementation. Therefore, trust and confidence increase, whereas privacy concerns decrease. The use of IoT becomes under control. The future generation will focus on

industry and market driven approaches, where more technologies will be involved. Values can be created out of the big data stored in the IoT service platforms, but customers' sensitive data will be taken into account. The IoT will be perceived to

replace the smartphone or BYOD. Thus, IoT security compliance will be reinforced.

TABLE 1. THREE GENERATIONS OF IoT SECURITY

First generation	Second generation	Third generation
• Used in a test environment • Common security practices: confidentiality, availability, and integrity • Concerns in technology adoption • Data privacy • End-to-end encryption • No standard	• Used in a real environment • More standardized protocol • Centralized IoT service platform • Ease of implementation • Less concerns about privacy • More trust and confidence • Authentication and identification • Single point of failure • Under control	• More industry and market driven • Linking to other technologies • Value creation from big data of customer transactions • Privacy of customers' sensitive data • Replacement of smartphone or BYOD • IoT policy

ACKNOWLEDGMENT

This work is part of the output of the ASEAN IVO project "A Hybrid Security Framework for IoT Networks".

REFERENCES

- [1] G. Tanganelli, C. Vallati, C., and E. Mingozzi, "Coapthon: easy development of coap-based iot applications with python", in Internet of Things (WF-IoT), IEEE 2nd World Forum on, pp. 63-68, 2015.
- [2] Z. Sheng, C. Mahapatra, C. Zhu, and V. C. Leung, "Recent advances in industrial wireless sensor networks toward efficient management in IoT", IEEE access, vol. 3, pp 622-637, 2015.
- [3] M. M. Hossain, M. Fotouhi, and R. Hasan, "Towards an analysis of security issues, challenges, and open problems in the internet of things. in Services (SERVICES)", 2015 IEEE World Congress on, pp. 21-28, 2015.
- [4] C. M. Medaglia, and A. Serbanati, "An overview of privacy and security issues in the internet of things". in The Internet of Things, pp. 389-395. Springer, New York, NY, 2010.
- [5] K. Zhao, and L. Ge, "A survey on the internet of things security", in Computational Intelligence and Security (CIS), 2013 9th International Conference on, pp. 663-667, 2013.
- [6] J. Andress, "The basics of information security: understanding the fundamentals of InfoSec in theory and practice. Syngress, 2014.
- [7] X. Li, R. Lu, X. Liang, X. Shen, J. Chen, and X. Lin, "Smart community: an internet of things application. IEEE Communications Magazine, vol. 49, 2011.
- [8] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the internet of things: a review", In Computer Science and Electronics Engineering (ICCSEE), 2012 international conference on, 2012.
- [9] H. Zhang, and L. Zhu, "Internet of things: key technology, architecture and challenging problems", in Computer Science and Automation Engineering (CSAE), 2011 IEEE International Conference on, 2011.
- [10] J. Bloomberg, "7 Reasons Why the Internet of Things Is Doomed", <https://www.wired.com/insights/2014/07/7-reasons-internet-things-doomed/>, 2014.
- [11] A. Matthews, "The 'unknown unknowns' of IoT security", <http://www.electronicsspecifier.com/blog/the-unknown-unknowns-of-iot-security>, 2016.
- [12] R. Sagy, "Internet of things security: new connections, new threats", <https://developer.ibm.com/open/2016/01/20/internet-of-things-security-new-connections-new-threats>, 2017.
- [13] X. Xiaohui, "Study on security problems and key technologies of the internet of things", in Computational and Information Sciences (ICCIS), 2013 Fifth International Conference on, 2013.
- [14] G. Eastwood, "4 critical security challenges facing IoT", <https://www.networkworld.com/article/3166106/internet-of-things/4-critical-security-challenges-facing-iot.html>, 2017.
- [15] L. Colombus, "Internet Of Things On Pace To Replace Mobile Phones As Most Connected Device In 2018", <https://www.forbes.com/sites/louiscolombus/2016/07/09/internet-of-things-on-pace-to-replace-mobile-phones-as-most-connected-device-in-2018>, 2016.
- [16] P. P. Ray, "A survey of IoT cloud platforms", Future Computing and Informatics Journal, vol. 1, pp. 35-46, 2016.
- [17] S. Pearson, and A. Benameur, "Privacy, security and trust issues arising from cloud computing", in Cloud Computing Technology and Science (CloudCom), 2010 IEEE Second International Conference on, pp. 693-702, 2010.
- [18] D. H. Kim, J. Y. Cho, J. Lim, and B. G. Lee, "Developing IoT security requirements for service providers", International Information Institute (Tokyo). Information, vol. 19, 2016.
- [19] M. A. Nematollahi, C. Vorakulpipat, and H. G. Rosales, "Digital Watermarking", Springer, Berlin, Germany, 2016.
- [20] O. Barzilay, Can Blockchain and AI Accelerate the Arrival of the IoT Economy? <https://www.forbes.com/sites/omribarzilay/2017/11/02/can-blockchain-and-ai-accelerate-the-arrival-of-the-iot-economy/#5bc06a4140d8>, 2017.



Chalee Vorakulpipat earned a PhD in information systems from the University of Salford, an M.S. in information technology from Kasetsart University, and a B.Eng. in electronics engineering from King Mongkut's Institute of Technology Ladkrabang. He is currently the head of Cybersecurity Laboratory at the National Electronics and Computer Technology Center (NECTEC), Thailand. He has been involved in several projects in information security (including ThaiCERT), national e-science, mobile device management, social networking, context-aware computing, e-health, and mobile application development. He has over forty refereed publications in these areas. He also serves as a subcommittee member on issues regarding national information security of Thailand. He holds professional certificates including CISSP, CISA, PMP, and IRCA (ISMS Lead Auditor).



detecting system.

Ekkachan Rattanalerdnusrn received M.S. and B.S. degrees in computer science from Chulalongkorn University. He is currently a senior research assistant at the National Electronics and Computer Technology Center (NECTEC), Thailand. He has been involved in several projects in information security, and particularly network security. His current research focuses on an IoT monitoring and



and e-science projects. His current research includes an IoT monitoring and detecting system and a job monitoring system in HPC.

Phithak Thaenkaew received the M.S. degree in computer science from Thammasat University and a B.Eng. in electrical engineering from King Mongkut's University of Technology, North Bangkok. He is currently an engineer at the National Electronics and Computer Technology Center (NECTEC), Thailand. He has been involved in information security, high performance computing (HPC),



Hoang Dang Hai, A/Prof. Dr. DSc., received PhD (1999) and DSc (2002) from TU Ilmenau, Germany. His current institution is Posts and Telecommunication Institute of Technology, Hanoi, Vietnam. His research interests include communication networks, IoT networks, information security, and network security.