Risk Identification for Low Capacity IoT Device

Nurul Azma Zakaria[1], Fatin Zahidah Shamsudin[2], Zaheera Zainal Abidin[3], Fairul Azni Jafar[4], Zuraida Abal Abas[5]
[1, 2, 3, 5] Fakulti Teknologi Maklumat Dan Komunikasi, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka.
[4] Fakulti Kejuruteraan Pembuatan, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka.
azma@utem.edu.my

Abstract

Risk assessment is required in order to eliminate the security risks that harmful to IoT device. Based on previous studies, there has no detail content relate to low capacity device in ISO standard document. The ISO Standard focuses on equipment in general device but not for general low capacity device. This concern motivates the development of the study. Thus, this study focuses on the risk identification process which is the initial stage of risk assessment. In this case, low capacity IoT device namely Raspberry Pi was used as the key component. Documents and articles analysis approach was used to extract and identify potential security risks from past related works. The study focuses on port scanning and vulnerability test outcomes which contains threats and vulnerabilities to produce the risk rating. There are 10 potential risks listed for low capacity IoT device with three level risk rating (high, medium and low). This study provides guidance to analyze security risk and document the identified risks of low capacity IoT device. In the future, the outcomes support in producing supplementary information relate to the content of ISO Standard specifically on risk assessment of low capacity device.

***Keywords*:** *Risk Identification, Risk assessment, Security risks, IoT device.*

1. Introduction

Low capacity device contains low storage and has low price in the market such as Beaglebone, Arduino and Raspberry Pi. It is widely used in Internet of Things (IoT) technology. The IoT is an is a system of interrelated registering gadgets, computing, mechanical, electrical or electronic devices, or objects of various sizes and capability that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. IoT has developed and extended to different domains and applications, for example, healthcare, energy, smart cities, industry, environment and entertainment (Seliem & Elgazzar, 2018). Yang et al. (2017) indicates that security is still massive issues for IoT and these issues will lead to a security and privacy concerns for users. The same concern is highlighted by Tabrizi and Ibrahim (2016) which states that despite of the innovative technologies of IoT, the security issues is one of the big challenges.

Consequently, because IoT devices are widely used, security of these devices need to be considered and all threats need to be minimized. Thus, risk assessment is required to eliminate the security risks that would be harmful to the devices. In this case, the study focuses on one of the microprocessor type device namely Raspberry Pi. Due to its benefits, Raspberry Pi becomes very popular than other types. International Federation of the National Standardizing Associations (ISO), Information Technology Infrastructure Library (ITIL), Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), Escal Institute of Advanced Technologies (SANS Institute) and National Institute of Standards and Technology (NIST) are key organizations that

play significant roles and involve in various risk assessment matters such as providing standard, policy and guidance to cater the risk assessment solutions.

In this study, ISO standard was used since the standard is widely used by industry. The standard focuses on equipment in general but no detail content related to low capacity device. Thus, this motivates the development of this study to provide supplementary content of ISO standard for risk assessment information that provides guidance for analyzing security risk of the related device.

The main objective of this study is to explore what are the possible security risk for IoT device. This paper also aims to identify the rating of the possible risk. In order to achieve these objectives, the study addresses the following research questions:
RQ 1 – What is the list of threats related to the low capacity device?
RQ 2 – What are the vulnerabilities?

The reminders of this paper are organized as follows. Section 2 provided the explanations related key areas. The methodology and the result and discussion are described in Section 3 and 4 respectively. The paper concludes with conclusion and future work.

2. Related key areas

2.1 Information Security

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction (NIST). Other similar phrases that normally being used interchangeably with information security are computer security and information assurance. The goals of information security is to protect the confidentiality, integrity and availability (CIA) of information. The CIA triad as shown in Figure 1 is a security model that has been developed to help people think about various parts of IT security.

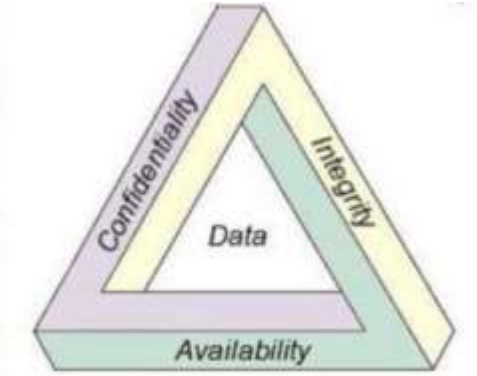

Figure 1: The CIA Triad (Farooq et al., 2015)

According to (Chai, 2021), confidentiality measures are designed to prevent sensitive information from unauthorized access attempts. Protecting confidentiality is dependent on being able to define and enforce certain access levels for information. Integrity involves maintaining the consistency, accuracy and trustworthiness of data over its entire lifecycle. It is designed to protect data from deletion or modification from any unauthorized party. Data must not be changed in transit, and steps must be taken to ensure data cannot be altered by unauthorized people. Authentication mechanisms, access channels and systems have to work properly to protect the information and available when it is needed. Availability means information should be consistently and readily accessible for authorized parties. This involves properly maintaining hardware and technical infrastructure and systems that hold and display the information. High availability systems are the

computing resources that have architectures that are specifically designed to improve availability. Any breaches in any of these three areas would cause serious security issues to the IoT ecosystem (Farooq et al., 2015).

2.2 Risk Assessment

Security risk assessments are performed to survey, distinguish and change the general security act and to empower security, operations, and hierarchical administration. This procedure is required to improve security arrangements in any organization. It is important to recognize the information that are valuable to the organization, the capacity systems of the related information and its vulnerabilities. In other words, a risk assessment is a comprehensive look at the workplace to recognize things, circumstances, structures, and others that maybe harmful to the organization. The assessment can be quantitative or a subjective. In a quantitative evaluation, numerical qualities to the likelihood an occasion will happen are used. These numerical qualities determines an occasion's danger component. However, subjective evaluations do not include numerical probabilities. The objective of a subjective approach is to provide risk rating to indicate level of risk from low to high.

2.3 ISO Standard

The ISO standard is a standard used for the development of a country. ISO 31000:2009 gives gages and non-specific principles on risk association. ISO 31000:2009 can be used by any public or private organization, and individual. It is proposed that the standard can be used to orchestrate risk administration forms in existing and future models. Figure 2 shows the process phase for risk assessment based on ISO standard and this study focus on risk identification part only.

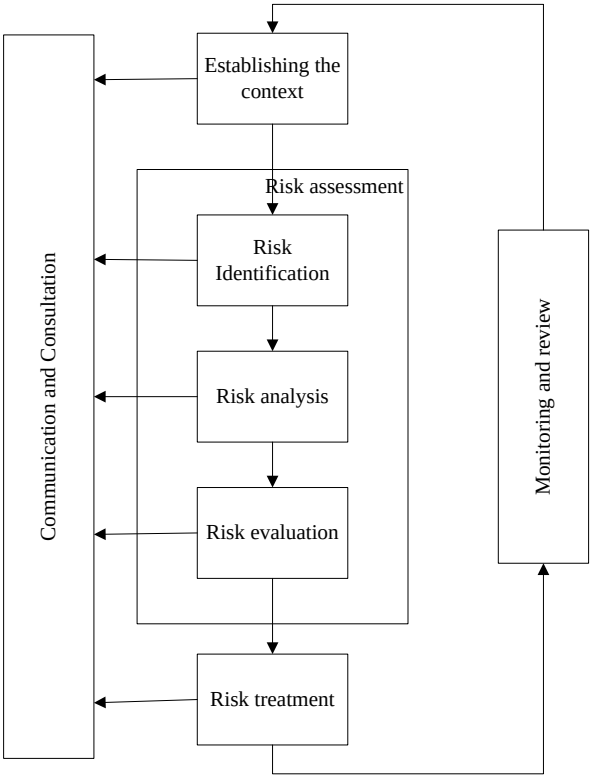

Figure 2: Process Phase for Risk Assessment (ISO, 2009)

3. Methodology

The aim of this study is to identify the risk for low capacity device for future guidance. In order to achieve the objective, a qualitative research method (i.e., a document review) was performed by referring to several previous studies as a literature review. This method was used because it is a systematic procedure to review and evaluate printed documents and electronic materials (Sallabaş, 2013). Literature studies from journals, reports, and working papers were used as materials and resources for our document analysis.

In this study, the framework for the risk assessment process was guided by the ISO 31000:2009 standard. The scope for the risk assessment process was established and the context was defined, and the criteria against which the risks were assessed was set. Details of the study were provided from past literatures review about risk assessment, risk identification and Raspberry Pi. The related experiments were port scanning and vulnerability test. Since the study employed qualitative method, data from past researches were extracted and compared to create the content of risk assessment specifically on low capacity device. The list of security risks related to Raspberry Pi were identified for further analysis.

In port scanning, all ports are scanned and detected which were filtered, opened and closed. During scanning port, security scanner software like Zenmap detects the total of packets sent during the scanning process. For the vulnerabilities test, Open Vulnerability Assessment System (OpenVAS) software can be used to scan the vulnerabilities in Raspberry Pi. Figure 3 shows the conceptual framework for the experiment. All identified risks were analysed and rated.

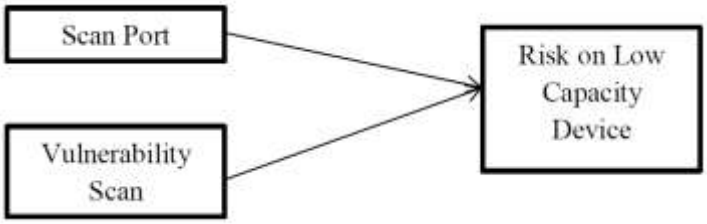

Figure 3: Conceptual Framework of the experiment

4. Metric Measurement - Risk Rating

For metric measurement, rating was used to populate the risks. The rating consists of low, medium and high as shown in Table 1. Risk evaluation involves comparing the level of risk found during the analysis process with risk criteria established when the context was considered. Based on this comparison, further action is taken.

Table 1: Example of risk rating

Risk Rating	
Level of Risk	**Risks**
High	Item1
Medium	Item2
Low	Item3

4. Finding & Discussion

4.1 Risk Identification

Table 2 shows the summary of identified risk that produced from scanning port and vulnerability test. These risks are possible treats and harmful to the Raspberry Pi. The results of the risk were rated accordingly as shown in latter section.

Table 2: Summary of Identified Risks

Scanning Port	Vulnerabilities Scanning	Author
• UDP • SSH	• UPnP • ICMP • SMTP	• Hunt n.d
• HTTP port • ICMP port • Shell • Login • Exec • Microsoft-DS • Netbios-SSN • Sunrpc • HTTPS • SNTP • TELNET • SSH • FTP	• TCP (6) • HTTP (1) • UDP (3) • FTP (1) • SMTP • NTP • Netbios-SSN	• Allen et al. (2014)
• 991 • SSH • MSRPC • KRB524 • Netbios-SSN • Microsoft-DS • HTTP-PROXY • TCP • Blackice-icecap	• HTTP • UDP • FTP • ICMP	• Hutchens (2014)
• Not Applicable	• Unsecure Authentication • Unsecure Network • Location can be tracked • Authentication mechanism not secure	• Ching & Singh (2016)
• TCP • SSH	• SSH • ICMP	• William (2015)
• HTTP • HTTPS • TELNET • SMTP • HTTP(alt/proxy) • DNS	• UPnP • Weak Public Key	• Durumeric et al. (2013)

- FTP
- SSH
- 2-Wire RPC

Risk on low capacity device was short listed to risk that usually exist in scanning process based on previous researches. After completed the process of analyze the risks, there are ten (10) risks that have been found due to frequency occurrence at scanning risks. Figure 4 shows the summary of risks after all the result had been produced. These are the result after been extracted and identified from previous works.

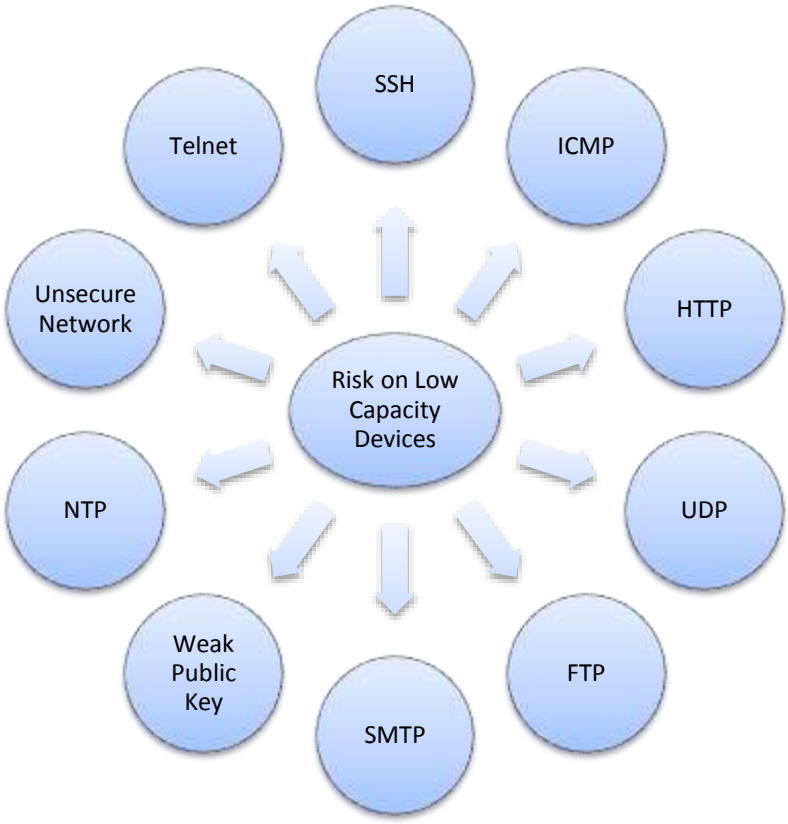

Figure 4: Identified Risk for Low Capacity Device

4.2 Risk Classification

Risk classification is a step for generating the risk levels (high, medium and low). The level of the risk is based on the analyst's or specific personnel's judgement to indicate the risk level. In this research, the level of risks is based on the number of the risk occurrence (frequency).

Table 3 shows the level of risk accordingly. For the low level risk, the frequency is 1 and it usually happened for unsecure network, which are NTP and weak public key. For the medium level risk, the risks occurred in 2-3 times which in this case are telnet, SMTP and FTP. For the high level risk, the frequency is between 4 to 5 occurrence which are SSH, ICMP, HTTP and UDP.

Table 3: Level of risks

Level of Risk	Risks
Low (Frequency– 1)	Unsecure Network, NTP, Weak Public Key
Medium (Frequency– 2-3)	Telnet, SMTP, FTP
High (Frequency - 4-5)	SSH, ICMP, HTTP, UDP

5. Conclusion and Future Recommendation

As low capacity device is common and popular in IoT application, its security aspect must be considered. By identifying the potential risks of the device, the security of the IoT device can be improved. In this study there are 10 potential risks for low capacity IoT device with SSH, ICMP, HTTP and UDP are in the high risk level. After the high risks have been recognized, the counter measure for all risks can be further explored and some has been suggested by Allen et al. (2014). Information generated from this study support and provide supplementary guidance for risk assessment of low capacity device based on ISO standard. Since the results produced from the study mainly based on secondary data, further experimentation need to be carried out in this area. This assessment is important as it shapes part of security administration arrangement.

Acknowledgement

A high appreciation to Ministry of Higher Education, Malaysia for sponsoring this research under the fundamental research grant with grant number: FRGS/2018/FTMK-CACT/F00392. Utmost gratitude also goes to Fakulti Teknologi Maklumat Dan Komunikasi (FTMK) and Universiti Teknikal Malaysia Melaka (UTeM).

References

Allen, L., Heriyanto, T. & Ali, S. (2014), Kali Linux – Assuring Security by Penetration Testing, Network Security, http://linkinghub.elsevier.com/retrieve/pii/S1353485814700777.

Chai, W. (2021). Confidentiality, integrity and availability (CIA triad), https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

Ching, K.W. & Singh, M.M. (2016). Wearable Technology Devices Security and Privacy Vulnerability Analysis. *International Journal of Network Security & Its Applications*, 8(3), 19–30.

Cobb, M. (2016). Confidentiality, integrity and availability (CIA triad), https://searchsecurity.techtarget.com/definition/physical-security

Durumeric, Z., Wustrow, E. & Halderman, J.A. (2013). ZMap: Fast Internet-wide Scanning and Its Security Applications. *Proceedings of the 22nd USENIX Security Symposium*, 605–619.

Farooq, M. U., Waseem, M., Khairi, A. & Mazhar, S. (2015). A Critical Analysis on the Security Concerns of Internet of Things (IoT), International Journal of Computer Applications, 111(7), 1–6,

Hunt, A., Raspberry MoCA : an Automated Penetration Platform.

Hutchens, J., 2014. Kali Linux Network Scanning Cookbook,

ISO (2009). ISO 31000:2009 Risk management —Principles and guidelines, https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en

National Institute of Standards and Technology (NIST). Glossary: INFOSEC, Computer Security Resource Center. U.S Department of Commerce, https://csrc.nist.gov/glossary/term/INFOSEC

Sallabaş, M. E. (2013). Analysis of Narrative Texts in Secondary School Textbooks in Terms of Values Education, *AcademyJournals*, 8(8), 361–366.

Seliem, M. & Elgazzar, K. (2018). IoTeWay : A Secure Framework Architecture for 6LoWPAN based IoT Applications, *IEEE Glob. Conf. Internet Things*, 1–5.

Tabrizi, S. S. & Ibrahim, D. (2016). Security of the Internet of Things: An Overview, *Proceedings of the 2016 International Conference on Communication and Information Systems*, 146–150.

Williams, M.G. (2015). A Risk Assessment on Raspberry PI using NIST Standards, 15(6), 22–30.

Yang, Y., Wu, L., Yin, G., Li, L. & Zhao, H. (2017). A Survey on Security and Privacy Issues in Internet-of-Things, *IEEE Internet of Things Journal*, 4662(c), 1–10.