Uluslararası İleri Doğa Bilimleri ve Mühendislik Araştırmaları Dergisi
Sayı 7, S. 16-19, 2, 2023
© Telif hakkı IJANSER'e aittir
Araştırma Makalesi

IJANSER

https://as-proceeding.com/index.php/ijanser
ISSN: 2980-0811

International Journal of Advanced Natural Sciences and Engineering Researches
Volume 7, pp. 16-19, 2, 2023
Copyright © 2023 IJANSER
Research Article

The Best Software Security Practices for Internet of Things

Maha Al Wahaibi [*1] and Zuhoor Al Khanjari [1]

[1]*Computer Science Department, Sultan Qaboos University, Muscat, Saltant of Oman*

[*]*(S128560@student.squ.edu.om) Email of the corresponding author*

(Received: 10 March 2023, Accepted: 16 March 2023)

(2nd International Conference on Scientific and Academic Research ICSAR 2023, March 14-16, 2023)

ATIF/REFERENCE: Al Wahaibi, M. & Al Khanjari, Z. (2023). The Best Software Security Practices for Internet of Things. *International Journal of Advanced Natural Sciences and Engineering Researches*, 7(2), 16-19.

Abstract – The Internet of Things (IoT) is one of the most modern technologies of the twenty-first century. Technology for the Internet of Things has been rapidly developed and applied, allowing for a wide range of technological advancements in various sectors of life [1]. This paper intends to explore different software security frameworks that offer recommendations for securing software, such as the IoT Security Maturity Model (SMM) and the Software Assurance Maturity Model (SAMM), Based on these frameworks, the study will identify the most effective practices for securing IoT software. Ultimately, this paper aims to provide valuable insights for software developers, security professionals, and organizations that seek to secure their IoT software and devices.

Keywords – Internet of Things (IoT), Software Security, Security Model, Best Practices

I. INTRODUCTION

In the 1999s, kevin Ashoton introduced the terms of Internet of Thing. The main objectives of IoT technologies are to simplify processes in various fields, to ensure that systems (technologies or processes) are more efficient, and ultimately, to increase the quality of life. [6]

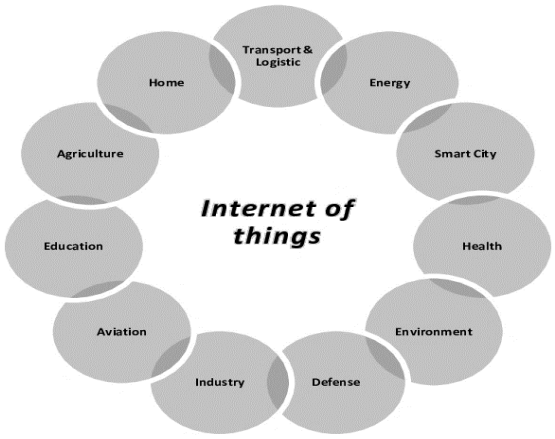

Fig. 1 Areas of IoT

The Internet of Things (IoT) technology is working in many areas: industrial, intelligent transportation system (ITS), agriculture, healthcare, smart environment (such as homes, networks, vehicles), food supply chain, and mission-critical applications. [10]

While the Internet of Things has many advantages in various fields, there are still challenges that are primarily related to security concerns, including interoperability with assistive technologies, lack of standards, legislative challenges, and regulatory issues for data sharing and authorization. [15]

Therefore, the need for a security standard for the use of this technology is an urgent need for the development and spread of this technology because these standard security practices will provide quality assurance in terms of security of use and data privacy. [11] Also, it is important to speed up the pace of work on finding a security standard that is suitable for the different segments of users of IoT technology.

This paper will first introduce the related work. Second, go over the best practices for IoT software security. Finally, a conclusion and future work are given in the last section.

COMPONENT OF THE IOT

Internet of Things (IoT) is a technology consist of IoT devices/ sensors which collect data this data is transmitted throw gateway to the cloud to analyze and process the output data is useful for automated decision making and be useful for the end users. [17]

Fig. 2 Main Components of an IoT System.

RELATED WORK

To improve security of IoT product should secure by design that's main have to consider security from the beginning when start developing a such software. That provide more security with less cost. There are some frameworks that defined practices to provide security. [7]

The Lightweight Application Security Process (CLASP) is provided software security process. It can be used by organizations of various sizes with less strict security. [14]

The Microsoft Security Development Lifecycle (MSSDL) is contained more strict security compared with (CLASP). It increases software reliability and reduce maintenance cost. It is used for large organizations. It is used by Microsoft for example vista project. [13]

Different from the previous frameworks the International Organization for Standardization

(ISO 27001) not open source and need auditor to check the security level that main no self-assessment. [8]

The Software Assurance Maturity Model (SAMM) is an open-source project that assists organizations of all sizes in assessing and developing software security. It has three levels of security maturity to indicate the level of security. It supports security at every stage of the software development process. It enables organizations to identify strengths and weaknesses of their software security and enabling the identification of areas for improvement and successful practices. It provides continues improvements. [19]

Building Security in Maturity Model (BSIMM), like SAMM, indicates which security activity the organization follows in the secure software development life cycle (SSDLC). It has a security maturity rating. Governance, intelligence, secure software development life cycle touchpoints, and deployment are the four domains. There are 12 main activities mentioned. The difference between SAMM and BSIMM is that BSIMM is a descriptive model that is created by collecting empirical data. [7]

The IoT Security Maturity Model (SMM) is proved framework for develop secure IoT software. It has three domains and tan practices and eighteen activities. [16]

Most of the identified frameworks represent practices and activities for traditional software security, not specifically for IoT, and have not been updated in a long time. As we all know, security vulnerabilities and attacks are constantly evolving, so this research collects an updated list that includes IoT-related practices.

II. IOT SOFTWARE SECURITY PRACTICES

In this section of the paper, it presents the collected Internet of Things software security practices from different frameworks and describes them.

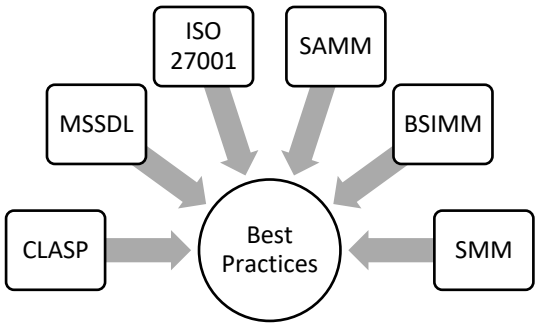

Fig.3 Gathering the best practices from different framework.

By implementing the software security practices shown in Table 1, organizations can reduce the risk of security incidents and ensure the security of their software.

Table 1. The best security practices.

Practices	Declaration
Strategy and Governance	A fundamental step to defining the security goals.
Regulation and Compliance	Build for the purpose of establishing security.
Education and Guidance	Developers' security knowledge should be expanded.
Risk Assessments	Overcoming the risk with the defined risk level.
Security Requirements	Include the security specification for developing software with secure functionality.
Security Design	This practice focuses on designing and building secure software.
Design Review	Make sure the proper mechanisms are used to ensure that it meets the security requirements.
Implementation Review	Evaluating the source code to detect the vulnerability.
Security Test	It is used to find vulnerabilities in software development during runtime
Issue Management	Use to handle and decrease the vulnerability and enhance security.
Configuration and Installation	The IoT is configured and installed in a secure manner.
Monitoring and reporting	Used to quickly respond to the issues before any damage occurred.

Using the previous practices in the previous table, can achieve the main security requirements, which are confidentiality, integrity, authentication, and availability.

Following some declarations for the security requirements

- Confidentiality: Unauthorized parties are not given access to the data.
- Integrity means that the data does not change.
- Authentication: The data came from the right place.
- Availability: The data can be located and obtained when required.

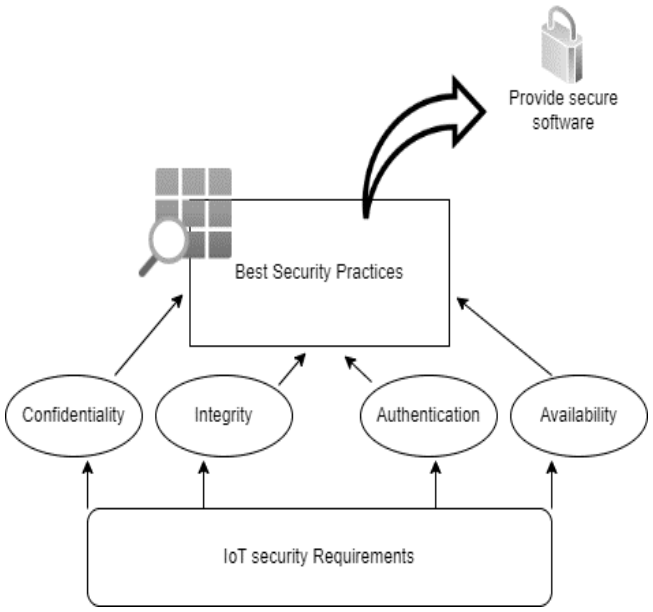

Fig.4 Best practices help to reach the security goals.

III. CONCLUSION AND FUTURE WORK

The practices of different frameworks used to develop IoT software security have been studied and

analysed. It can be used by any organization to plan and assess software security.

For future work, there is a plan to propose a comprehensive and up to date IoT software security framework that will allow organizations to assess whether they have met their objectives or need additional guidance to improve security to the highest level.

REFERENCES

[1] Aakanksha Tewari, B.B. Gupta. (2021). Security, privacy and trust of different layers in Internet-of-Things. Future Generation Computer Systems, 909-920.

[2] Alliance. (2016). Future-proofing the Connected World: 13 Steps to Developing Secure IoT Products.

[3] Arbia Riahi Sfar,Enrico Natalizio,Yacine Challal,Zied Chtourou. (2018). A roadmap for security challenges in the Internet of Things. Digital Communications and Networks, 118-137.

[4] C. Sandescu et al. (2018). Why IoT security is failing. The Need of a Test Driven Security Approach. IEEE, 1-6.

[5] D. Miorandi, S. Sicari, F. De Pellegrini, I. Chlamtac. (2012). Internet of things : Vision, applications and research challenges. Ad Hoc Networks, 1497–1516.

[6] Daniele Miorandia,Sabrina Sicarib Francesco,De PellegriniaImrich Chlamtac. (2012). Internet of things: Vision, applications and research challenges. Ad Hoc Networks, 1497-1516.

[7] Gary McGraw, Ph.D., Sammy Migues, and Jacob West. (2018). Building Security In Maturity Model.

[8] ISO/IEC 27001. (2013). International Organization for Standardization and the International Electrotechnical Commission.

[9] J. Viega and G. McGraw. (2002). Building Secure Software: How to Avoid Security Problems the Right Way. Addison-Wesley.

[10] M. Farooq, M. Waseem, A. Khairi, S. Mazhar. (2015). A critical analysis on the security concerns of internet of things (IoT). Int. J. Comput. Appl., 1-15.

[11] Mark Mbock Ogonji a, George Okeyo, Joseph Muliaro Wafula. (2020). A survey on privacy and security of Internet of Things. Computer Science Review, 1-19.

[12] McGraw, G. (2006). Software Security: Building Security In. Addison-Wesley.

[13] Michael Howard and Steve Lipner. (2006). Microsoft Security Development Lifecycle. United States of America: Microsoft Press.

[14] OWASP. (2006). lightweight application security process.

[15] Sandro Nizetic a, Petar Solic, Diego Lopez-de-Ipina Gonzalez-de-Artaza, Luigi Patrono. (2020). Internet of Things (IoT): Opportunities, issues and challenges towards. Journal of Cleaner Production, 1-32.

[16] Sandy Carielli, Matt Eble, Frederick Hirsch, Ekaterina, Rudina, and Ron Zahavi. (2020). IoT Security Maturity Model (SMM). An Industrial Internet Consortium.

[17] Society, I. C. (2019). IEEE Standard for an Architectural Framework for the Internet of Things . IEEE.

[18] Z. Ling et al. (n.d.). IoT Security: An End-to-End View and Case Study.

[19] Chandra, p. (2018). Software Assurance Maturity Model. OWASP

[20] J. R. C. Nurse, S. Creese, and D. De Roure. (2017). Security Risk Assessment in Internet of Things Systems. IEEE, 20-26.