Yalvaç Akademi Dergisi

https://dergipark.org.tr/tr/pub/yalvac

# IOT SECURITY AND SOFTWARE TESTING

Osman Can ÇETLENBİK[1], Ahmet Ali SÜZEN[2*], Burhan DUMAN [2]

[1] Isparta University of Applied Sciences, Graduate Education Institute, Computer Engineering, Isparta
[2] Isparta University of Applied Sciences, Faculty of Technology, Computer Engineering, Isparta

**Corresponding Author**: ahmetsuzen@isparta.edu.tr

## ABSTRACT

The Internet of Things (IoT) symbolizes the era of increased information exchange and interaction between devices through Internet of Things technology. However, this fascinating technology brings with it a number of security challenges. Some of the security issues stem from the nature of IoT devices. IoT devices are often designed to be cheap and uncomplicated. As a result, security tests may be neglected and security vulnerabilities may arise. There are other factors that compromise the security of IoT devices. For example, most IoT devices have standard passwords that have not been changed. Attackers can easily seize devices by manipulating them. There are data leaks from compromised devices.

**Keywords**: Internet of Things, Cybersecurity, Smart Device

## 1. INTRODUCTION

IoT is an emerging technological field as one of the precursors of digital transformation. The concept of the Internet of Things is basically defined as a network structure that allows many devices to interact with each other or through the internet [1]. IoT offers a wide range of applications ranging from everyday life to industrial applications. IoT is based on equipping objects in the physical world with sensors, software and network connections. In this way, these objects can collect and share data and perform many tasks. From smart home systems to wearable technology devices, from industrial sensor networks to smart urban applications, many IoT models are used in different aspects of daily life and business [2]. With the widespread adoption of Internet

of Things technology, previously impossible improvements in data analytics, automation systems and user experiences are being experienced. In addition to the advantages of these technologies, cyber security threats are emerging. Cyber security threats are becoming increasingly complex and sophisticated. These threats pose a significant risk to businesses, public institutions and individuals.

## 2. IOT ARCHITECTURE AND LAYERS

IoT architecture is a framework that defines the key factors in IoT systems and how they are integrated with each other. Typically, IoT systems consist of three basic layers:

**Sensing and Collection Layer**: Sensors, devices and other information sources used to monitor environmental conditions and collect data are located in this layer [3]. Generally, devices such as temperature sensors, motion sensors, humidity meters are located in this layer. This layer collects data from the physical world and prepares the data for processing.

**Network and Communication Layer**: It provides the network infrastructure for the transmission and transfer of collected data. It is the layer where wireless communication protocols, gateways, access points and other communication tools are located. It provides secure and reliable data transmission.

**Application and Analysis Layer**: Processing and analyzing the collected data and presenting the results to the user or other systems are carried out at this layer. Technologies such as data analytics, artificial intelligence, cloud computing and application development are key components of this layer. This layer creates the ultimate value of the IoT system and makes it possible for the benefits to be realized by users or other systems.

## 3. INDUSTRIAL INTERNET OF THINGS (IIOT) AND SECURITY

The Industrial Internet of Things (IIoT) encompasses IoT applications used in industrial plants, power plants, logistics distribution channels and other industrial facilities. These applications aim to automate industrial processes, increase productivity, improve production quality and reduce costs. IIoT collects and analyzes large amounts of data and enables optimization of processes based on this analysis.

IIoT systems is critical to increase efficiency and optimize operations in industrial facilities. The systems often collect, transmit and control large amounts of sensitive data, so security measures must be rigorously implemented. Establishing contingency plans, network and device security, and taking measures against malware are important in industrial IoT security [18].

## 4. IOT SECURITY THREATS

IoT faces significant security threats due to the increasing number and variety of connected devices. These threats can be of various magnitudes and can affect personal privacy and organizational security [4]. Data security and privacy breaches are at the top of the list of threats. IoT devices collect and process mostly sensitive data [5]. In the event of a data security breach, users' personal data becomes vulnerable to cyber-attacks and access by malicious actors. In addition, deficiencies such as insufficient encryption or lack of authentication used in information sharing on devices put data security at risk. Authentication and authorization issues pose a significant risk to IoT security. Devices often communicate over a complex network, and unless authentication and authorization processes are done correctly, their security is greatly compromised. In order to understand the potential risks posed by IoT and to determine effective security strategies, studies in this field should be handled meticulously.

Secure software development processes are of great importance in detecting security vulnerabilities of IoT devices and applications. Secure software development tests are carried out to detect vulnerabilities in IoT devices and applications, identify possible attack points and eliminate these vulnerabilities. It is of great importance in increasing the resilience of the developed software against attacks, ensuring data security and ensuring the safe operation of the devices.

## 5. SOFTWARE TESTING SECURITY AND LITERATURE REVIEW

IoT technology security is becoming an increasingly important priority in today's complex and dynamic threat landscape. In this context, the adoption and effective implementation of secure software development processes play a critical role in detecting and remediating security vulnerabilities in IoT devices and applications. Below are the testing processes used in IoT technologies and the results of the literature review.

### 5.1. Penetration Testing

Penetration testing is the process of evaluating IoT devices through the eyes of a malicious intruder. These tests are carried out to identify potential vulnerabilities, identify vulnerabilities and strengthen defense mechanisms for these issues. By evaluating the effectiveness of security controls within the system, strategies are developed to improve against cyber-attacks.

Haddadpajouh et al. Haddadpajouh et al. focused on a survey study addressing the requirements, issues and solutions for IoT security, and this study is an important resource for understanding the general requirements and issues in IoT security. [6].

Yadav et al. Yadav et al. developed a scalable, flexible and automated penetration testing framework called IoT-PEN, which utilizes target graphs to explore all possible ways in which attackers can find vulnerabilities in target systems [7].
Akhilesh et al. developed an automated penetration testing framework for smart home-centric IoT devices and this work emphasizes the importance of automating security testing of IoT devices [8].

Süren et al. presented a four-step IoT vulnerability research methodology called PatrIoT, which is based on a logical attack surface decomposition, compilation of the top 100 vulnerabilities, lightweight risk scaling, and step-by-step penetration testing guidelines [9].

### 5.2. Vulnerability Analysis

Weak point analysis is defined as a method that identifies potential vulnerabilities in software. This analysis reveals errors that arise from the design of the software or occur during the implementation phase. Vulnerability analysis provides a preventive approach to correct these errors and prevent future security problems.

The study titled "Vulnerabilities in LPWANs - An Attack Vector Analysis for the IoT Ecosystem" by Torres et al. examines the vulnerabilities of IoT devices over LPWAN technologies [10].

"Multi-Source Knowledge Reasoning for Data-Driven IoT Security" by Zhang et al. presents an analysis and decision making method for IoT security [10].

In the paper "CorrAUC: A Malicious Bot-IoT Traffic Detection Method in IoT Network Using Machine-Learning Techniques" by Shafiq et al. a method for anomaly detection in IoT networks is presented [12].

### 5.3. Test Automation Processes

Test automation is used to make secure software testing more comprehensive and efficient. Automation is used to perform repeatable test cases, process large datasets and continuously inspect for potential security vulnerabilities. In this way, security tests are performed more frequently and in a planned manner. Reliable software testing is crucial to minimize security threats in the IoT ecosystem and to ensure end-user security. Periodically repeating and updating these processes is essential to create an effective security strategy suitable for changing threat environments.

The article "IoT Testing-as-a-Service: A New Dimension of Automation" by Malik et al. discusses automated IoT testing processes as a service model that performs distributed interoperability testing, security testing and verification of IoT devices [13].

"Cybersecurity Model Based on Hardening for Secure Internet of Things Implementation" by Echeverria et al. discusses a certification approach using security risk assessment and testing methodologies for IoT devices [14].

## 6. APPLICATION PRINCIPLES IN IOT SECURITY

Implementation guidelines in IoT security aim to prepare users and organizations for potential threats. These guidelines cover key elements such as awareness, tracking updates, security policies, data encryption and contingency plans. Below are considerations for the implementation of these guidelines:

### 6.1. Awareness Raising and Training

It is an important element in IoT security. The application of this principle emphasizes the importance of preparing users and organizations for potential threats as well as adopting safe behaviors. Awareness programs aim to continuously inform users about IoT security. Trainings and programs aim to make users and organizations aware of potential threats and adopt safe behavioral habits [15]. Informed user behavior aims to improve users' security habits. In this context, behaviors such as avoiding potentially suspicious connections and using strong passwords should be consciously encouraged. Building a security culture involves creating a security culture within the organization and adopting it as a security value supported by management. It is important to encourage conscious behaviors such as learning from, responding to, and avoiding security incidents. This is important in order to respond quickly and effectively to security incidents. In this context, it is necessary to increase end-user awareness and to carry out training activities for end-users meticulously.

### 6.2 Systematic Monitoring of Device and Software Updates

IoT devices and software are being integrated to make life easier for a wide audience and optimize the operations of organizations [16]. However, this rapid adoption process increases the possibility of security vulnerabilities. Systematic tracking of device and software updates is one of the important fundamentals in IoT security [17]. This principle involves the systematic inspection of smart devices and the software used, and the tracking of their updates. The path-method relationship regarding this principle is given in Table 1 below.

**Table 1.** Systematic Inspection Of Smart Devices And The Software Used

| Code of Practice | Method |
|---|---|
| Establishing Update Tracking Process | Deciding on the criteria to be followed (e.g. software version, security patches, etc.). Creating follow-up reports and scheduling regular update meetings. |
| Creating the Update Schedule | Determining and sharing scheduled update dates. Create a dedicated calendar for emergency updates. Identify a communication mechanism that can quickly communicate changes to the calendar. |
| Use of Automatic Update Tools | Selecting and installing automatic update tools. Configure settings and design update policies. |
| Determination of Update Policies | Creating update policies and reducing the risk of business interruption. |
| Risk Assessment and Emergency Plans | Assessing the potential risks of the update process. Identifying emergency scenarios and creating plans for these situations. |

In Table 1, it is important for institutions and organizations to put into effect the application-based method relations. As a result of data losses that may occur as a result of any cyber attack, institutions and organizations may face loss of reputation and high amounts of financial losses.

## 7. CONCLUSION

The rapid proliferation and increasing use of IoT technology has greatly increased the exchange of information and interaction between devices. However, in addition to its benefits, this

technology also brings serious security risks. Software testing and security play a critical role in making the IoT ecosystem sustainable and secure. In this article, the main components of IoT security are discussed, focusing on topics such as determining the update tracking process, creating an update schedule, using automatic update tools, determining update guidelines, risk assessment and creating contingency plans. It is critical to carefully follow these steps to minimize vulnerabilities in IoT devices and applications and to be prepared for potential threats.

## 8. REFERENCES

[1] Gürfidan, R., & Ersoy, M. (2022). A new approach with blockchain based for safe communication in IoT ecosystem. Journal of Data, Information and Management, 4(1), 49-56.
[2] Kamsin, I. and Zainal, N. (2021). A comprehensive review on smart iot applications.. https://doi.org/10.2991/ahis.k.210913.069
[3] Fedullo, T., Morato, A., Peserico, G., Trevisan, L., Tramarin, F., Vitturi, S., & Rovati, L. (2022). An iot measurement system based on lorawan for additive manufacturing. Sensors, 22(15), 5466. https://doi.org/10.3390/s22155466
[4] Wang, F. (2023). Mitigating iot privacy-revealing features by time series data transformation. Journal of Cybersecurity and Privacy, 3(2), 209-226. https://doi.org/10.3390/jcp3020012
[5] Abomhara, M. and Køien, G. (2014). Security and privacy in the internet of things: current status and open issues.. https://doi.org/10.1109/prisms.2014.6970594
[6] HaddadPajouh, H., Dehghantanha, A., Parizi, R., & Aledhari, M. (2021). A survey on internet of things security: requirements, challenges, and solutions. Internet of Things, 14, 100129. https://doi.org/10.1016/j.iot.2019.100129
[7] Yadav, G., Paul, K., Allakany, A., & Okamura, K. (2020). Iot-pen: an e2e penetration testing framework for iot. Journal of Information Processing, 28(0), 633-642. https://doi.org/10.2197/ipsjjip.28.633
[8] Akhilesh, R., Bills, O., Chilamkurti, N., & Chowdhury, M. (2022). Automated penetration testing framework for smart-home-based iot devices. Future Internet, 14(10), 276. https://doi.org/10.3390/fi14100276
[9] Süren, E., Heiding, F., Olegård, J., & Lagerström, R. (2022). Patriot: practical and agile threat research for iot. International Journal of Information Security, 22(1), 213-233. https://doi.org/10.1007/s10207-022-00633-3
[10] Torres, N., Pinto, P., & Lopes, S. (2021). Security vulnerabilities in lpwans—an attack vector analysis for the iot ecosystem. Applied Sciences, 11(7), 3176. https://doi.org/10.3390/app11073176
[11] Zhang, S., Bai, G., Li, H., Liu, P., Zhang, M., & Li, S. (2021). Multi-source knowledge reasoning for data-driven iot security. Sensors, 21(22), 7579. https://doi.org/10.3390/s21227579
[12] Shafiq, M., Tian, Z., Bashir, A., Du, X., & Guizani, M. (2021). Corrauc: a malicious bot-iot traffic detection method in iot network using machine-learning techniques. Ieee Internet of Things Journal, 8(5), 3242-3254. https://doi.org/10.1109/jiot.2020.3002255
[13] Malik, B., Khalid, M., Maryam, M., Nauman, M., Yousaf, S., Mehmood, M.,& Saleem, H. (2019). Iot testing-as-a-service: a new dimension of automation. International Journal of Advanced Computer Science and Applications, 10(5). https://doi.org/10.14569/ijacsa.2019.0100545

[14] Echeverria, A., Cevallos, C., Ortiz-Garcés, I., & Andrade, R. (2021). Cybersecurity model based on hardening for secure internet of things implementation. Applied Sciences, 11(7), 3260. https://doi.org/10.3390/app11073260
[15] Lowry, P., Dinev, T., & Willison, R. (2017). Why security and privacy research lies at the centre of the information systems (is) artefact: proposing a bold research agenda. European Journal of Information Systems, 26(6), 546-563. https://doi.org/10.1057/s41303-017-0066-x
[16] Celik, Z., Fernandes, E., Pauley, E., Tan, G., & McDaniel, P. (2019). Program analysis of commodity iot applications for security and privacy. Acm Computing Surveys, 52(4), 1-30. https://doi.org/10.1145/3333501
[17] Abdulmalek, S., Nasir, A., Jabbar, W., Almuhaya, M., Bairagi, A., Khan, M., & Kee, S. (2022). Iot-based healthcare-monitoring system towards improving quality of life: a review. Healthcare, 10(10), 1993. https://doi.org/10.3390/healthcare10101993
[18] Gürfidan, R., Ersoy, M., & Kilim, O. (2022, May). AI-Powered Cyber Attacks Threats and Measures. In The International Conference on Artificial Intelligence and Applied Mathematics in Engineering (pp. 434-444). Cham: Springer International Publishing.