UNIVERSITI TEKNOLOGI MARA

JIIICaS 2024
JOHOR INTERNATIONAL INNOVATION, INVENTION COMPETITION AND SYMPOSIUM

PROCEEDINGS OF JOHOR INTERNATIONAL INNOVATION INVENTION COMPETITION AND SYMPOSIUM 2024 (JIIICaS 2024)

"Flourish and Nurturing Sustainable Innovation for a Prosperous Nation"

JIICOS 2024
JOHOR INTERNATIONAL INNOVATION, INVENTION COMPETITION AND SYMPOSIUM

Editorial Board

e ISBN: 978-967-0033-25-9

Published in Malaysia by
Universiti Teknologi MARA Cawangan Johor
Kampus Pasir Gudang
81750 Masai

Preface

In the name of Allah, the Almighty who gives us the enlightenment, the truth, the knowledge and with regards to Prophet Muhammad (peace be upon him) for guiding us to the straight path. We thank to Allah for giving us guidance and strength to write this e-book.

This e-book compiles the extended abstracts that submitted to Johor International Innovation Invention Competition and Symposium 2024 (JIIICaS2024), where JIIICaS2024 is a virtual platform for all creative minds to share and present their invention and innovation. Each abstract gives a brief background on the innovation or project.

We hope that this e-book will help the readers to get to know the innovation done by the students and get some ideas to develop future innovation products.

Foreword Rector

Assalamualaikum warahmatullahi Wabarakatuh, Salam Sejahtera, Salam Malaysia MADANI and Salam UiTM Dihatiku.

In the name of Allah, the Most Gracious, the Most Merciful.

It is a great honor to welcome you to the Johor International Innovation, Invention, Competition, and Symposium 2024 (JIIICaS 2024). This event connects various disciplines, focusing on education and engaging educators, students, researchers, and innovators from all walks of life.

Innovation is not just about ideas; it demands perseverance, creativity, and determination to turn those ideas into reality. The remarkable projects showcased today highlight the dedication and spirit of all participants. Initiatives like this not only explore new technologies but also cultivate skills and leadership among our youth. At Universiti Teknologi MARA (UiTM) Johor Branch, we are fully committed to fostering a dynamic culture of innovation, promoting the commercialization of new products, and encouraging meaningful collaborations with industry and society.

As we celebrate this event, I would like to extend my heartfelt gratitude to all sponsors, judges, the College of Computing, Informatics and Mathematics, UiTM Pasir Gudang Campus as the event organizer, as well as to the researchers and participants for their hard work in making this event a success. Let us continue striving for innovation and excellence. May the ideas presented today inspire us and lay the groundwork for future achievements.

Thank you.

Associate Professor Dr. Saunah Zainon
Rector
Universiti Teknologi MARA (UiTM)
Johor Branch

(A-ST102) SECURING ARUDINO-BASED SYSTEM USING SECURE CODING & IDS

Wan Maryam Nadzirah Murshid [1], Nurul Azma Zakaria[1*], Zaheera Zainal Abidin[1]

[1]Fakulti Teknologi Maklumat dan Komunikasi,
Universiti Teknikal Malaysia Melaka,
Hang Tuah Jaya, 76100 Durian Tunggal, Melaka

Corresponding author: azma@utem.edu.my (Nurul Azma Zakaria)

ABSTRACT

Arduino platforms are popular for their user-friendliness and adaptability, making them common in various projects. However, their widespread use also exposes them to security vulnerabilities. This paper addresses these threats by focusing on secure coding practices and developing a robust intrusion detection system (IDS). It begins with an analysis of potential security flaws in Arduino systems, identifying areas prone to exploitation. By emphasizing best practices in secure coding, the project aims to strengthen Arduino applications against malicious attacks. The IDS will play a critical role by continuously monitoring Arduino systems for unusual activities that could indicate a security threat. The study seeks to enhance the security of Arduino-based systems through a comprehensive framework combining secure coding and IDS, offering valuable insights for developers to create more secure and resilient systems.

Keywords: Security vulnerabilities, Secure coding practices, Intrusion detection systems (IDS), Application security, Arduino

1.0 INTRODUCTION

The rapidly evolving landscape of the Internet of Things (IoT) and microcontrollers, particularly Arduino-based systems, has led to their widespread use in various applications, from industrial systems to hobbyist projects. However, as these systems become integral to larger industrial and residential networks, they also become prime targets for cybercriminals, exposing significant security vulnerabilities. These weaknesses could lead to data theft, unauthorized access, or even physical harm if exploited. Despite the popularity of Arduino due to its flexibility, affordability, and user-friendly nature, a comprehensive understanding of its security flaws and mitigation strategies remains limited. Current security measures often focus on network security while overlooking potential hardware and software vulnerabilities.

One of the main challenges is the lack of secure coding practices. Many developers may neglect secure coding guidelines, such as the principle of least privilege, proper error handling, and input validation, due to Arduino's simplicity, leaving systems exposed to attacks. Additionally, the absence of Intrusion Detection Systems (IDS) in Arduino-based setups further worsens the security risks. IDS are crucial for monitoring systems for malicious activity or policy violations and alerting users to potential security breaches. Without IDS, attackers could exploit vulnerabilities in Arduino-based systems undetected, leading to significant damage, especially in critical applications like automotive systems, industrial machinery, and home security.

2.0 OBJECTIVE

This study aims to identify vulnerabilities in Arduino-based systems by thoroughly examining their architecture, setup, and coding standards. Once identified, the study will develop secure coding practices, including guidelines on error management, secure data storage, and input validation, to mitigate these risks. Additionally, the study will implement an IDS to detect and alert administrators of suspicious activity. The effectiveness of these mitigation techniques will be evaluated through various attack scenarios to assess the system's resilience. Ultimately, the goal is to provide developers and administrators with practical guidelines for securing Arduino-based systems.

3.0 METHODOLOGY

In order to protect Arduino-based systems, this study employs a comprehensive approach that includes evaluating the state-of-the-art security measures, creating secure coding guidelines, and the implementing IDS into place. The study's materials include the documentation of developed guidelines, software tools for security analysis and intrusion detection, and Arduino hardware. In addition to deploying IDS to monitor system activities for possible intrusions, the goal is to identify common security weaknesses and build a set of best practices for secure coding. With the support provided by these methods, IoT devices' security framework should be strengthened and made more resilient to attacks via the Internet. Figure 1 depicts the flow of the system.

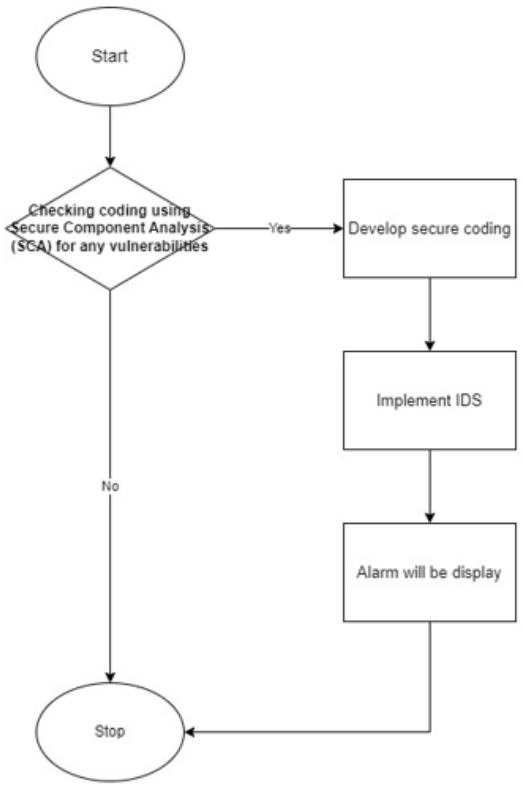

Figure 1: Flow of the study

4.0 RESULTS

4.1 Security Evaluation of Arduino Projects

The literature research indicates that when developers initially begin working with Arduino, many of them lack a firm grasp of ICT security fundamentals. Due to this unfamiliarity, their projects can be vulnerable. This gap is especially troubling in the context of Arduino projects for a number of reasons. Due to the nature of open systems, Arduino projects commonly being shared publicly on sites such as GitHub, where other developers can use them as models or templates. Security flaws in the original code may spread to other projects if they exist. A thorough grasp of potential threats, vulnerabilities, and mitigation techniques is necessary in the complicated field of security. Without this understanding, programmers could unintentionally add security risks into their systems. Table 1 shows the comparative analysis of security evaluation.

Table 1: Comparison of Security Evaluation

Author	Objective	Proposed Approach	Result
Corno & Mannella, 2023b	To identify security issues in these projects and categorize them based on security concepts	The approach involves categorizing the identified security issues based on fundamental security concepts	The research provides insights into the security concerns present in Arduino projects created by hobbyist programmers.
Bakhshi et al., 2024	To review IoT firmware vulnerabilities and auditing techniques.	Various tools like Firm-AFL and FIRMCORN employ fuzzing approaches to find vulnerabilities in IoT firmware	It categorizes IoT firmware vulnerabilities across eight axes, detailing susceptibility triggers and domain limitations based on prior literature
Alrawi, A. N., Ammar, M., & Campbell, R.,2020	Evaluate the security of IoT devices, including Arduino-based systems	Systematic security evaluation framework including threat modeling, attack surface analysis, and security testing	Identification of common security issues in home IoT devices, leading to improved security guidelines for manufacturers
Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A.2015	Address security, privacy, and trust issues in IoT deployments	Propose a multi-layered security architecture combining encryption, access control, and trust management	Improved security and privacy for IoT deployments, fostering greater user trust in IoT technologies

4.2 Intrusion Detection System (IDS)

Table 2 presents the related works applying IDS to Arduino-based systems. There are four (4) types of IDS, namely signature-based, anomaly-based, hybrid, and behaviour-based.

Table 2: Comparative Analysis of IDS for Arduino-based systems

Author	IDS Type	Strengths	Features
Reeves et al., n.d.	Signature-based IDS	High accuracy for known threats, low false positives	Uses known attack patterns for detection
Nowroozi et al., 2018	Anomaly-based IDS	Can detect new and unknown attacks, adaptable	Detects deviations from normal behavior patterns
Zarpelão et al., 2017	Hybrid IDS	Balances accuracy and coverage	Integrates signature-based and anomaly-based methods
Mitrokotsa et al, 2017	Behavior-based IDS	Adaptable, detects sophisticated attacks	Analyzes behavior patterns over time

4.3 OWASP Secure Coding Practices

This guide offers a comprehensive checklist of technology-agnostic software security coding practices that can be seamlessly integrated into the software development lifecycle. Rather than focusing on specific vulnerabilities and exploits, the guide emphasizes secure coding requirements, making it an essential resource for developers aiming to mitigate common software risks through best practices. It covers a broad range of topics, including input validation, output encoding, authentication, session management, access control, cryptography, error handling, data protection, communication security, system configuration, database security, file management, and memory management. The OWASP guide (Canedo et al., 2024) provides crucial guidelines to ensure that Arduino-based systems are developed with security at their core. The principles outlined are applicable to any software development project, including those involving Arduino, offering a solid framework for research focused on evaluating and mitigating security vulnerabilities.

4.4 Testing Scenario: Arduino Uno RFID Security System

The Arduino Uno RFID security system aims to secure access to a PC or laptop using RFID technology integrated with Arduino which involves several key scenarios to validate its functionality and security measures. The scenario centres around implementing a secure access control system using an Arduino Uno board and RFID technology to protect access to PC or laptop systems. Authorized users approach the Arduino Uno RFID reader module and present their RFID tags. The reader module detects the RFID tag and reads its unique identifier (ID), which is then transmitted to the Arduino Uno microcontroller. The microcontroller compares this ID against a pre-defined list of authorized RFID tag IDs stored in its memory. Upon successful validation, the Arduino Uno triggers an action to grant access to the connected PC or laptop, typically by sending a command via USB serial communication to simulate

unlocking the device or controlling an output pin for external locking mechanisms. The system provides immediate feedback to the user regarding the authentication outcome through LED indicators or messages displayed on a serial monitor.

The scenario defines a practical application of RFID technology integrated with Arduino Uno for secure access control. It aims to authenticate users based on authorized RFID tags, demonstrating the system's ability to prevent unauthorized access to sensitive PC or laptop environments. The scenario exemplifies the implementation of secure coding practices within the Arduino sketch, ensuring secure handling of RFID tag data and validation processes to mitigate potential security vulnerabilities. Additionally, the scenario can extend to incorporate IDS principles, testing the system's capability to detect and respond to anomalous activities, such as repeated unauthorized access attempts or abnormal RFID tag behaviours.

4.5 Metric Measurement

Metrics measurement in this study involves the quantitative assessment of various security aspects, focusing on specific, measurable indicators to evaluate the effectiveness of secure coding practices and the performance of intrusion detection systems. These metrics are essential for determining how well the system is protected against vulnerabilities and how effectively it responds to potential security threats. They offer a means to track progress, pinpoint areas for improvement, and validate the security measures implemented. In this project, key metrics might include vulnerability detection rate, false positive rate, system performance overhead, response time, and code coverage.

5.0 CONCLUSION

This study addressed essential areas of security in Arduino-based systems by focusing on secure coding practices and IDS, with the goal of improving Arduino-based system security and mitigating common vulnerabilities caused by developers' lack of security awareness. This combined strategy of proactive prevention with secure code and reactive monitoring with IDS creates a comprehensive security framework. It ensures that Arduino-based systems are not only functional, but also resistant to cyber threats, protecting both their functionality and the data they handle. These techniques aim to increase Arduino-based systems' defences against potential intrusions by preventing common security flaws. This study enhances the topic of IoT security academically while also providing practical benefits. It provides crucial insights about the security of embedded systems and serves as a foundation for future research and development in the field.

References

1. Alrawi, A. N., Ammar, M., & Campbell, R. (2020). SoK: Security evaluation of home-based IoT deployments. IEEE Internet of Things Journal, 7(11).
2. Bakhshi, T., Ghita, B., & Kuzminykh, I. (2024). A Review of IoT Firmware Vulnerabilities and Auditing Techniques. In Sensors (Vol. 24, Issue 2). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/s24020708

3. Canedo, G., Silva, P., & Gadsden, J. (2024). OWASP Secure Coding Practices-Quick Reference Guide. OWASP. https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/
4. Corno, F., & Mannella, L. (2023a). Security Evaluation of Arduino Projects Developed by Hobbyist IoT Programmers. Sensors, 23(5). https://doi.org/10.3390/s23052740
5. Mitrokotsa, A., Dimitriou, T., & Giannetsos, T. (2017). Behavior-Based Intrusion Detection in IoT: Challenges and Solutions. IEEE Internet of Things Journal, 4(6), 1935-1945.
6. Nowroozi, A., Shahriari, H. R., & Behniafar, M. (2018). A Survey of Anomaly Detection Approaches in Internet of Things (Vol. 10, Issue 2). http://www.isecure-journal.org
7. Reeves, J., Ramaswamy, A., Locasto, M., Bratus, S., & Smith, S. (n.d.). Chapter 3 Lightweight Intrusion Detection for Resource-Constrained Embedded Control Systems.
8. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. Computer Networks, 76, 146-164.
9. Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & de Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. In Journal of Network and Computer Applications (Vol. 84, pp. 25–37). Academic Press. https://doi.org/10.1016/j.jnca.2017.02.009