Analyzing IOT Software Testing Methodologies Intermes of Achieving Security and Interoperability with a Prospect of IOT Testing Framework

A research Proposal for Research Methodology

By Yaregal T.

Introduction

the Internet of Things (IoT) is "a system of interrelated computing devices, mechanical and digital machines, objects, animals, or people 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". The IoT encompasses a large range of devices ('things'), among which everyday household electronics, such as dishwashers, fridges, smart cameras, smartwatches, smart glasses, smart TVs, and smart light bulbs. Wearable devices can monitor heart rate, steps, and spent calories to name just a few 'smart' features introduced by IoT devices

Security in IoT software is not a joke anymore since the IoT systems are improving day-to-day life in a way that our day-to-day life depended on it. In this rise of the Internet of Things (IoT), where billions of devices are expected to be integrated into horizontal applications [4][5]. Security problems are massively increasing because the amount of linked smart devices constantly grows with their use of different standards, the heterogeneity of the devices, their different implementation way [6]- [8], making the security testing operations daunted. imagine your smart TV is hacked by someone and its record audio in your Salone or bedroom, imagine your IoT connected car is hacked, or imagine an intruder successfully hacked your IoT supported door, from these simple cases you can imagine the consequence that successful penetration of security holes in an IoT supported devices will case to the society in a variety of aspects. Since every device such as your watch, washing machine, your doorbell, your ovens, etc. is being able to connect to the internet which increases your vulnerability to security. Since the vulnerability of these devices cause a series of impact, securing IoT devices is a must done task

The main cause of many software attacks is a flow in the software that happened during development which will produce a vulnerability in the system of course it's impossible to develop a 100% flow free system but minimizing the flows in the system have high contribution to reducing the possible vulnerabilities in the system and the best time to capture those flows and fix them before they cause any damage is done during testing, unfortunately, the attacks that happen in IoT software level are mostly caused by software flows in the system. In this regard research has been done focusing on developing IoT security testing methodology, framework and techniques have been developed []. But they didn't start by analyzing the cause and move towards finding a solution to the cause they just developed a methodology, a framework, or a technique to perform IoT security testing and the problem still exists.

Problem Statement

Over the last few years, IoT devices and IoT-enabled solutions have become significantly popular both for consumers and industries. IoT is not just about embedded devices, but also comprises an ecosystem of device hardware, system integration, connectivity, data storage, security, IoT platform providers, IT and communication service providers, and application development. Currently, there are more IoT devices connected to networks than the number of human beings on the earth. These IoT devices carry a lot of sensitive data which remains insecure. IoT security has become the subject of strong consideration after several high-profile incidents where a common IoT device was used to infiltrate and attack a larger network, hacking of internet-connected devices, surveillance concerns, and privacy.

The main cause of a security problem is a flaw or bug in the design and implementation of the program that runs the IoT system and these flaws and bugs have to be detected and fixed before the system is delivered to customers this is done through testing in which security tested doesn't get the attention it deserves due to this the security problems are causing a lot of problems not only on the IoT system in which the flaw or the bug is found but also big systems I which this buggy IoT system is communicating.

As said in the introduction part IoT security is still a sensitive issue several studies have been made in the last time which focuses on developing a testing strategy, their main focus is on prevention when they happen. Since the traditional testing mechanisms are not suitable for IoT systems because of their Heterogeneity, distributed-ness, resource-constrained environment, and use of different platforms. So, using the old software testing didn't fit the IoT for this reason adapting or developing a new testing framework is mandatory. In this perspective, a lot of studies have been made [list the papers on security testing and frameworks] and different frameworks and methodologies have been designed. but still, the problem existed and IoT systems still have a lot of vulnerabilities after these all-testing methodologies have been adopted and new frameworks are developed [list papers which tell the security problem still exists]

Whatever a great testing methodology, framework, tool, or techniques have developed the developed IoT security testing methodology, framework, tool, or techniques will be embedded inside the general IoT testing methodology which also includes another testing like interoperability testing, conformance testing, Scalability testing and platform independence testing and of course security testing. So, if this general testing methodology didn't give enough emphasis on the security testing whatever security testing methodology, technique, or tool is developed it didn't affect the result because the problem is not on the Security testing methodology, technique, or tool rather on the general testing methodology.

So since even after several studies have been made on security testing and security methodology, technique, tool, and frameworks are developed still the problem is not solved [put the reference here] in this study we will answer the question are the general testing frameworks give enough emphasis to security testing and if so what's the solution and if not, what is the solution will be answered in this paper

testing methodology on IoT devices but still the security problem exists. So maybe the security problem rises not only

Objectives

General Objective

identify the root causes of IoT Security problems that exist in current IOT systems in the aspects of testing the security and propose a solution to mitigate the cause of the problem.

Specific Objective

- Analyze state-of-the-art IoT system testing methodologies with respect to their capability of handling security testing with a comparative approach.
- Develop a novel IoT testing framework that can add the capability of Security testing.

Research Questions

- Did the current IoT system Testing methodologies give enough emphasis to testing the security of the system?
- If the answer to the above question is yes so why is the known security problem still a problem?
- If the answer to the 1st question is no, how can we make the methodologies give to the security testing of the IoT system

Methodology

In this paper I discuss and analyze state of the art IoT System testing methodologies and their effectiveness on testing the IoT system for security with a comparative approach with respect to their effectiveness in terms of unveiling security problems in the IOT software.

From the testing methodologies discussed and analyzed we will identify did the IoT testing methodologies give enough emphasis to test the security of the system and if they didn't give enough emphasis see how we can include security on the testing methodology which will lead us to the development of new testing framework which includes testing the security of the system and if they have given enough emphasis why is the security problems still existing in the IoT Systems

I will do this by surveying the current IoT testing with respect to their ability to test the security perspective of the IoT system so that I can be able to identify the root cause of why the security problems are not pre detected before installation during the testing phase so that I can answer why the well-known security problems are still security problems for IoT devices

Literature Review

G. Murad et.al[9] examines the trends in software testing approaches using different types of IOT environments and uncovers various issues that must be to enhance testing in IOT environment

Abbas Ahmad et al[10] an IOT-TaaS(Internet of Things Testing as a Service) frame work that aims to solve problems such as the scalability of traditional software testing, the heterogeneity of IoT devices increases costs and the complexity of coordination of testing due to the number of variables which arises due to The amount of IoT devices and their collaborative behavior. The aim of the testing framework is to resolve constraints regarding coordination, cost and scalability issue of traditional software testing in the context of standard based development of IOT devices. It is composed of distributed interoperability testing, scalable automated conformance testing and semantic conformance testing.

Pedro Martins Pontes et al[11] in their papers named IZinto a pattern based IOT Testing framework they stated that there are several solutions for testing IOT systems which follows different testing approaches and focus different focus level(),u it, integration and acceptance) covering different layers(cloud layer, fog layer, edge layer) however they have their own limitations such as failing to account for the heterogeneity of the IOT field by focus on specific platform, language, or standards and lack the possibility of improvement or functionality extension, and also not providing out of box functionality by mentioning this limitations they proposed a pattern based test automation framework for integration testing. This framework also have limitation since it only solves the integration testing which didn't solve other testing's like interoperability, scalability and security

Brian Ramprasad et al[12] have also discussed the challenges of IOT testing they stated the main challenges with heterogenous IOT network is maintaining the quality of service(QOS) because of the fluctuation in the number of active devices and the data they produce [13],[14],[15]. Fluctuations occur because IoT devices may operate under different time of use policies to save energy, IoT devices may fail in the network or their up link to the Internet may be temporarily down. Being able to reliably predict resource utilization in a dynamic heterogeneous IoT environment can help overcome some of the QoS challenges associated with scaling IoT networks. Prediction with high accuracy allows us to plan ahead in preparing for changes in demand on the IoT network. In this paper, they develop a novel resource utilization prediction engine for IoT applications based on a Smart Testing Framework for Adaptation. This allows to execute repeatable experiments to learn about IoT device resource utilization so that we can trigger adaptations to add or remove computing resources.

On paper "Secure SDLC Using Security Patterns 2.0"paper written in 2022[18] they proposed "Secure SDLC using **Security Patterns 2.0 (SSDLC using SPs2.0)**", and this framework enhances security by minimizing the known vulnerability. Identifying the security requirements using security discoverer process, selection of security pattern for security requirements, design security requirements using security building blocks, creating test templates to support pattern implementation during development stage, vulnerability scanning

Large Scale IoT Security Testing, Benchmarking and Certification(07_chapter_07)[20] describes the challenges in IOT security testing and presents a model based approach solution here what they want to solve is what are the challenges when security testing of IoT system is performed or what are the challenges during the implementation of any selected testing strategy then the proposed a model based approach to solve the challenges(read the methodology part)

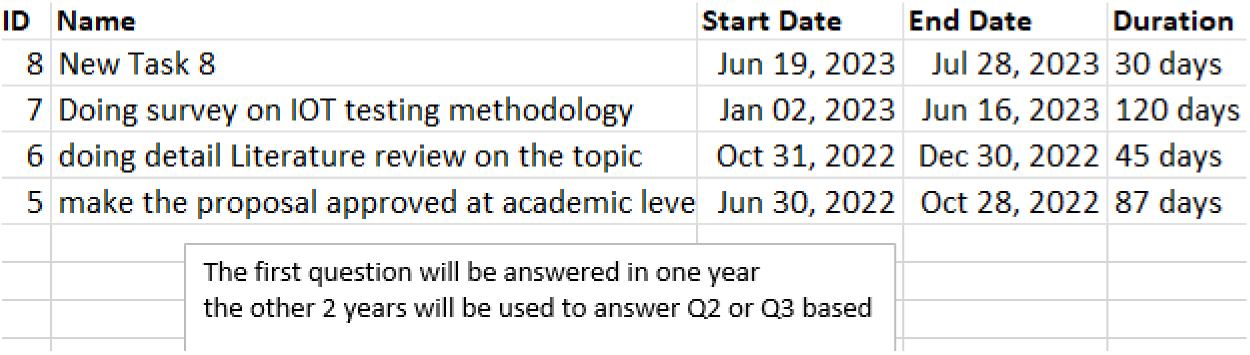
Consumer IoT: Security Vulnerability Case Studies and Solutions[19] in this paper the researchers try to describe the common attacks to the consumer IOT devices and suggests their mitigation strategy which helps to reduce the severity of the attack

Artorias: IoT Security Testing Framework in this paper the researchers introduce the IoT Security Testing Framework named Artorias which is an automated testing tool to test the TOP 10 security issues identified by OWASP then they show how it tests those areas, how to setup and run Artorias and how Artorias should be used. As we see above this paper selected top 10 OWASP selected security issues, introduces an automated testing tool named Artorias and show how this tool is used to test those security problems.(Read The Methodology part)

The Open Web Application Security Project, or OWASP, evaluated and derived a list of the top 10 vulnerabilities associated with IoT devices in 2014; insecure web interfaces, insufficient authentication or authorization, insecure network services, lack of transport encryption, privacy concerns, insecure cloud interfaces, insecure mobile interfaces, insufficient security configuration, insecure software or firmware and poor physical security [2].

Improving Software Testing, Verification and Reliability in the Software Development Life Cycle (ImprovingSoftwareTesting.pdf) make a detail methodology review on this paper

Time Schedule



ID	Name	Start Date	End Date	Duration
8	New Task 8	Jun 19, 2023	Jul 28, 2023	30 days
7	Doing survey on IOT testing methodology	Jan 02, 2023	Jun 16, 2023	120 days
6	doing detail Literature review on the topic	Oct 31, 2022	Dec 30, 2022	45 days
5	make the proposal approved at academic leve	Jun 30, 2022	Oct 28, 2022	87 days

The first question will be answered in one year
the other 2 years will be used to answer Q2 or Q3 based

References

1. C.H.R.I.S.T.O.P.H.E.R.S.Y.O.O. (n.d.). article on IOT. Cigionline.Org. Retrieved January 31, 2022, from https://www.cigionline.org/articles/emerging-internet-things/?utm_source=google_ads&utm_medium=grant&gclid=Cj0KCQiArt6PBhCoARIsAMF5wagddds86MyMXi-niFl-yx3swGYbPzhqvyGooatrEBmvZdKB-NKO_jQaAneLEALw_wcB
2. B.L.E.G.E.A.R.D. (2019, March 25). Security Testing of IoT systems. In C.V.I.H.O., B.O.U.Q.U.E.T.F.A.B.R.I.C.E., & F.L.E.G.A.L.L. (Eds.), Model-Based Testing for IoT Systems - Methods and Tools (1st ed., Vol. 1, pp. 24–32).
3. Ahmad, A., Baqa, H., Hwang, J., & le Gall, F. (2018, February). IoT-TaaS: Towards a Prospective IoT Testing Framework. 10.1109/ACCESS.2018.2802489, IEEE Access, 1, 1–14.
4. L. Ericsson, “More than 50 billion connected devices,” White Paper, 2011
5. S. Ziegler, C. Crettaz, L. Ladid, S. Krco, B. Pokric, A. F. Skarmeta, A. Jara, W. Kastner, and M. Jung, “IoT6–moving to an ipv6-based future IoT,” in The Future Internet Assembly, pp. 161–172, Springer, 2013.
6. D. Bandyopadhyay and J. Sen, “Internet of things: Applications and challenges in technology and standardization,” Wireless Personal Communications, vol. 58, no. 1, pp. 49–69, 2011.
7. J. Song et al., “Connecting and managing m2m devices in the future internet,” Mobile Networks and Applications, vol. 19, no. 1, pp. 4–17, 2014.
8. P.V. Lingala Thirupathi, N. Rao, Developing a multilevel protection framework using EDF, Intern. J. Advanced Research Eng. Technol. (IJARET) 11 (10) (2020) 893–902.
9. G. Murad, A. Badarneh, A. Qusef. and F. Almasalha, “Software testing techniques in IoT,” in 8th Int. Conf. on Computer Science and Information Technology (CSIT), Amman, Jordan vol. 1, no. 1, pp. 17–21, 2018.
10. Ahmad, A., Baqa, H., Hwang, J., & le Gall, F. (2018, February). IoT-TaaS: Towards a Prospective IoT Testing Framework. 10.1109/ACCESS.2018.2802489, IEEE Access, 1, 1–14.

11. Pontes, P., Lima, B., & Pascoal Faria, J. (2018b). Izinto: a pattern-based IoT testing framework. Conference: Companion Proceedings for the ISSTA/ECOOP 2018 Workshops, 1(1). https://doi.org/10.1145/3236454.3236511
12. Ramprasad, B., Mukherjee, J., & Litoiu, M. (2018). A Smart Testing Framework for IoT Applications. Conference: 2018 IEEE/ACM International Conference on Utility and Cloud Computing Companion (UCC Companion), 1(1), 1–7. https://doi.org/10.1109/UCC-Companion.2018.00064
13. A. Javed, K. Heljanko, A. Buda, and K. Frmling, "CefIoT: A fault-tolerant IoT architecture for edge and cloud," in IEEE WF-IoT, 2018.
14. H. F. Atlam, A. Alenezi, A. Alharthi, R. J. Walters, and G. B. Wills,"Integration of cloud computing with internet of things: Challenges and open issues," in 2017 IEEE International Conference on Internet of Things, 2017.
15. A. Botta, W. de Donato, V. Persico, and A. Pescap, "On the integration of cloud computing and internet of things," in 2014 International Conference on Future Internet of Things and Cloud, 2014.
16. W. Shi and S. Dustdar, "*e promise of edge computing,"Computer, vol. 49, no. 5, pp. 78–81, 2016.
17. X. Xia, F. Chen, Q. He, J. Grundy, M. Abdelrazek, and H. Jin,"Cost-effective app data distribution in edge computing,"IEEE Transactions on Parallel and Distributed Systems, vol. 32,no. 1, pp. 31–44, 2020.
18. Aruna, E. & Reddy, A. & Sunitha, K.V.N.. (2022). Secure SDLC Using Security Patterns 2.0. 10.1007/978-981-16-3945-6_69.
19. T. Alladi, V. Chamola, B. Sikdar and K. -K. R. Choo, "Consumer IoT: Security Vulnerability Case Studies and Solutions," in IEEE Consumer Electronics Magazine, vol. 9, no. 2, pp. 17-25, 1 March 2020, doi: 10.1109/MCE.2019.2953740.
20. Ahmad, Abbas & Baldini, Gianmarco & Cousin, Philippe & Matheu Garcia, Sara Nieves & Skarmeta, Antonio & Fourneret, Elizabeta & Legeard, Bruno. (2017). Large Scale IoT Security Testing, Benchmarking and Certification.