AUTOMATIC TESTING OF SMART SPEAKER APPS

J.L.A.I.A.Sandaruwani
198772M

Faculty of Information Technology
University of Moratuwa

July 2022

AUTOMATIC TESTING OF SMART SPEAKER APPS

J.L.A.I.A.Sandaruwani
198772M

Dissertation submitted to the Faculty of Information Technology, University of Moratuwa, Sri Lanka for the partial fulfillment of the requirements of Degree of Master of Science in Information Technology

July 2022

Declaration

I declare that this thesis is my own work and has not been submitted in any form for another degree or diploma at any university or other institution of tertiary education. Information derived from the published or unpublished work of others has been acknowledged in the text and a list of references is given.

Name of Student — Signature of Student

UOM Verified Signature

J.L.A.I.A.Sandaruwani …….

Date:

Supervised by

Name of Supervisor — Signature of Supervisor

Dr. Kulani Mahadewa ……

Date:

Acknowledgment

This research behind it would not have been possible without the exceptional support of my supervisor, Dr. Kulani Mahadewa. Her enthusiasm, knowledge, and exacting attention to detail have been an inspiration and kept my work on track.

And also, thank you to Ms. Rrubaa Panchendrarajan for her guidance, supervision, advice, sparing valuable time, and help in keeping my development on track with the NLP part of the research project.

Furthermore, a special thanks should be extended to Dr. Mohamed Firdhous, who taught the subjects of Research Methodology, Literature Reviews, and thesis writing, which formed the foundation for this research, and thank you to the examiners for their insights and their valuable comments.

I am so grateful to My colleagues who provided insight and expertise that greatly assisted the research.

Nobody has been more important to me in the pursuit of this project than the members of my family. I would like to thank my parents and sisters, whose love and guidance are with me in whatever I pursue. They are the ultimate role models.

Abstract

With the emergence of the Internet of Things (IoT), Smart Speakers open up a new world where we can talk to a machine for getting help in our day-to-day lives. The Smart Speaker Apps (SSA)s provide a user-friendly vocal experience to the customers by allowing them to dictate commands to the speaker through voice commands. Amazon Alexa is one of the most prevalent smart speakers which allows third-party developers to write SSAs called Skills. Due to the prevalence of Alexa, it has become vulnerable to security and privacy threats by malicious skill developers. In particular, Alexa skills could be overprivileged such that they collect more data than necessary or specified by the privacy policy in the skills description. In this research, we systematically explore skills to test whether the behaviors of the skills adhere to the privacy policy provided in the skill description. We extracted the utterances related to privacy-sensitive behavior of the skills through Natural Language Processing (NLP) techniques. Second, we implemented a dynamic testing tool Test case Generator & Invocator based on the fuzzing technique to automatically manipulate the inputs to the skills and observe the output to identify the skills which accept the privacy-sensitive information. During the study, we discovered that 21% of the tested skills accept privacy-sensitive data. We have simply focused on the real or actual behavior of the skills during the research. The claimed behavior of the skills is covered by our study, which will be the focus of further work.

Index Terms - **Alexa skills, Amazon Alexa, vulnerabilities, Internet of Things, privacy, security, Automatic testing**

Table of Contents

List of Figures

List of Tables