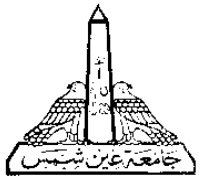
بسم الله الرحمن الرحيم

∞∞∞

تم رفع هذه الرسالة بواسطة / سامية زكى يوسف

بقسم التوثيق الإلكتروني بمركز الشبكات وتكنولوجيا المعلومات دون أدنى مسئولية عن محتوى هذه الرسالة.

ملاحظات: لا يوجد



Ain Shams University
Faculty of Engineering
Computer and Systems Engineering Department

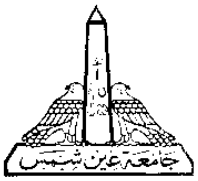
Trust Coding for IoT

A Thesis
Submitted in partial fulfillment of the Requirements
For the Degree of Doctor of Philosophy in Electrical Engineering
(Computer and Systems Engineering)

Submitted by
Alyaa Abdou Hamza Abd El-Rahman
Master of Science in Electrical Engineering
(Computer and Control Systems Engineering)
Faculty of Engineering, Mansoura University, 2017

Supervised by
Prof. Dr. Ayman Mohamed Bahaa-Eldin Sadeq
Assoc. Prof. Mohamed Ali Ali Sobh
Dr. Islam Tharwat Abdel Halim

Cairo – Egypt
2022



Ain Shams University
Faculty of Engineering
Computer and Systems Engineering Department

Approval Sheet

Name: Alyaa Abdou Hamza Abd El-Rahman

Thesis: Trust Coding for IoT

Degree: Doctor of Philosophy in Electrical Engineering (Computer and Systems Engineering)

Examiners' Committee

Name and Affiliation	**Signature**
1- Prof. Dr. Hesham Arafat Ali Professor at Computer Engineering and Systems Department Faculty of Engineering, Mansoura University, Egypt.	…… **(Examiner)**
2- Prof. Dr. Ahamed Hassan Yousef Professor at Computer and Systems Engineering Department Faculty of Engineering, Ain Shams University, Egypt.	…… **(Examiner)**
3- Prof. Dr. Ayman Mohamed Bahaa-Eldin Sadeq Professor at Computer and Systems Engineering Department Faculty of Engineering, Ain Shams University, Egypt.	…… **(Supervisor)**
4- Assoc.Prof. Dr. Mohamed Ali Ali Mostafa Sobh Associate Professor at Computer and Systems Engineering Dept. Faculty of Engineering, Ain Shams University, Egypt.	…… **(Supervisor)**

Examination Date: **21 / 7 / 2022**

Statement

This thesis is submitted to Ain Shams University in partial fulfilment of the requirements for the degree of Doctor of Philosophy in Electrical Engineering (Computer and Systems Engineering).

The work included in this thesis was carried out by the author at the Computer and Systems Engineering Department, Faculty of Engineering, Ain Shams University.

No part of this thesis has been submitted for a degree or a qualification at any other scientific entity.

Alyaa Abdou Hamza Abd El-Rahman
Computer and Systems Engineering Department
Faculty of Engineering
Ain Shams University
Cairo, Egypt
2022

Signature
……...…….
Date: … / … / ……

Researcher Data

Name: Alyaa Abdou Hamza Abd El-Rahman

Date of birth: 11/03/1989

Place of birth: Saudi Arabia

Last academic degree: Master's degree

Field of specialization: Electrical Engineering

University issued the degree: Mansoura University

Date of issued degree: 27/9/2017

Current job: Assistant Lecturer & Electronic Coordinator at Faculty of Engineering and Technology - Badr University in Cairo (BUC)

Thesis Summary

Alyaa Abdou Hamza Abd El-Rahman

Trust Coding for IoT

Doctor of Philosophy in Electrical Engineering
(Computer and Systems Engineering)

Ain Shams University, 2022

The Internet of Things (IoT) provides the ability for humans and computers to learn and interact from billions of things, including devices, sensors, actuators, services, and other Internet-connected objects. IoT devices enable massive opportunities to automate everyday tasks by increasing machine-to-machine interaction. These smart devices have been used in several domains like healthcare, transportation, smart home, smart city, and more. However, this technology has been exposed to many vulnerabilities, which may lead to cybercrime. Since the number of incidents related to IoT devices is alarming, a new investigation approach is needed to handle the crime associated with IoT devices.

Recently, IoT systems are being rapidly developed with adequate consideration of the increasing need to face security challenges. This could be justified because IoT is an open invitation to hackers to control and attack connected IoT devices. In this context, the programming analysis (static and dynamic) technique is used to achieve a trusted coding for IoT that focuses on defending against attacks on these systems. Also, this technique is responsible for analyzing applications' behavior accurately to support security & privacy.

Program Analysis (PA) is one of the essential security factors which has more than analysis techniques. These techniques successfully build perfect security analysis system (SAS) that can detect malware. There is a struggle remains between security analysts and malware developers. It is a battle that does not end quickly, because malware is always complex as fast as discovery grows. Analysis techniques examine IoT app source code to recognize applications' security.

Consequently, this thesis focuses on two significant contributions:

-The first is to follow the principles of systematic literature reviews to present a detailed and objective overview of a new taxonomy of the program analysis techniques and their related topics. It explains how to build SAS based on various program analysis techniques. Also. It covers SAS types, which play an essential role in identifying the suitable program analysis techniques to be used.

PA and its related topics have been introduced in the presented survey and taxonomy: the sensitivity and analysis characteristics. It gives a new classification of PA techniques. This classification has been created by examining the implemented security analysis system (SAS) that detect various malware applications. More importantly, this survey presents the three types of SAS that used PA methods for the first time. Also, It discussed the related surveys, the performance metrics of PA, IoT Security Issues, and Challenges.

-On the other side, the second contribution is to provide a new hybrid (static and dynamic) SAS based on the model-checking technique and deep learning, called an HSAS-MD analyzer, which focuses on the holistic analysis perspective of IoT apps. It aims to analyze the data of IoT apps by (i) converting the source code of the target applications to the format of a model checker that can deal with it. (ii) detecting any abnormal behavior in the IoT application. (iii) extracting the main static features from it to be tested & classified using a deep learning (CNN algorithm). (iv) verifying app behavior by using model-checking technique. HSAS-MD gives the best results in detecting malware from malicious smartThings applications compared to other SASs. The experimental results of HSAS-MD show that it provides 95%, 94%,91%, and 93%for accuracy, precision, recall, and F-measure, respectively. It also gives the best results in comparing with other analyzers from various criteria.

Keywords:

Formal Verification, IoT Security, Malware Detection, Program Analysis, Security Analysis System, Smart Homes, Triggers/Actions.

Acknowledgment

First of all, I deeply thank God for providing me the strength and patience all the way and inspiring me from the beginning of my thesis.

I want to express my gratitude to ***Prof. Dr. Ayman Mohamed Bahaa-Eldin*** *for his encouragement, patience, and for giving me time, experience, and support. Also, I would like to extend my gratitude to* ***Assoc. Prof. Mohamed Ali Ali Sobh*** *and* ***Dr. Islam Tharwat Abdel Halim*** *for their guidance and insightful comments.*

Finally, I must express my gratitude to ***my family*** *for providing unfailing support and continuous encouragement throughout my years of study. I wouldn't accomplish anything without their support and love.*

I can only say: May God bless them and give them all health, happiness, and whatever they wish.

Alyaa Abdou Hamza

Contents