Initial Trust Establishment for Personal Space IoT Systems

A thesis submitted in fulfilment of the requirements for
the degree of Doctor of Philosophy
in the Faculty of Engineering and Information Technology
at the University of Technology Sydney

by

Thi Tham Nguyen

Supervised by

Professor Doan B. Hoang

2019

Certificate of original authorship

I, Thi Tham Nguyen declare that this thesis, is submitted in fulfilment of the requirements for the award of the degree of Doctor of Philosophy, in the Faculty of Engineering and Information Technology at the University of Technology Sydney.

This thesis is wholly my own work unless otherwise reference or acknowledged. In addition, I certify that all information sources and literature used are indicated in the thesis.

This document has not been submitted for qualifications at any other academic institution.

Signature: Production Note: Signature removed prior to publication. Thi Tham Nguyen

Date: 03, January 2019

Dedication

To my parents, my sisters and my brothers

Thank you for your love and support

Acknowledgments

I wish to express my profound gratitude and sincere thanks to my principal supervisor, Professor Doan B. Hoang for leading me along the way to this point and educating me on both academic research and life lessons. He has taught me how to look at problems from different perspectives, how to always come up with the best possible solutions, and how to deliver research results to different audiences effectively. He has been outstanding in providing insightful feedback and creating the balance between working and living. I am grateful to him for his constant advice on various aspects of a Ph.D. student's life, both inside and outside academia. He has not only advised me on technical issues but also given me many lessons in dealing with problems in life. Without his critical comments, suggestions and encouragement, none of my work would have been possible.

My special thanks to Data61-CSIRO for offering me the Ph.D. and Top-up Scholarships, to the University of Technology Sydney (UTS) for offering me the International Research Scholarship (IRS). I am also grateful to Professor Aruna Seneviratne in Data61-CSIRO for his support during my Ph.D. He has always been very encouraging and a continuous source of support and encouragement. I am grateful for his constant guidance and invaluable intellectual insight, and thankful to him for introducing me to great researchers and colleagues at Data61. I wish to thank the School of Electrical and Data Engineering, the Vice-Chancellor's Postgraduate Research Students Conference Fund at UTS and the Networks Research Group at Data61-CSIRO for providing me funding for attending international conferences.

I would also like to thank Dr. Diep Nguyen for his valuable feedback, discussions, and comments on my work on "Binary Initial Trust Establishment Model for Personal Space IoT systems," which is part of this thesis.

I wish to thank my colleagues and friends, who have influenced my views and efforts during my time here at UTS and Data61, including Chau Nguyen, Sara Farahmandian, Ngoc Le, Kathick Thiyagarajan, Ashish Nanda, Prashanthi Jayawardhane, Suranga

Seneviratne, Mosarrat Jahan, Harini Kolamunna, Rahat Masood, and Sara Khalifa. I would also like to thank all my wonderful friends inside and outside UTS and Data61 for bringing happiness and wisdom to my life.

Finally, I would like to thank my parents, my sisters and my brothers for their love and support during these years. My parents have made many sacrifices for me and have provided me with steady guidance and encouragement. This dissertation is dedicated to them.

Sydney, January 2019.

The Author's Publications

International Conference Publications and Proceedings:

- **Tham Nguyen**, Doan Hoang, Aruna Seneviratne, "Challenge-Response Trust Assessment Model for Personal Space IoT," in Proc. of *the 2016 IEEE International Conference on Pervasive Computing and Communications Workshops* (PerCom 2016), Sydney, Australia, 2016, pp. 1-6.
- **Tham Nguyen**, Doan Hoang, Diep Nguyen, Aruna Seneviratne, "Initial Trust Establishment for Personal Space IoT Systems," in Proc. of *the 2017 IEEE International Conference on Computer Communications Workshops* (INFOCOM 2017), Atlanta, USA, 2017, pp. 846-851.
- **Tham Nguyen**, Doan Hoang, Aruna Seneviratne, "Dirichlet-based Initial Trust Establishment for Personal Space IoT Systems," in Proc. of the *2018 IEEE International Conference on Communications* (ICC 2018), Kansas City, MO, USA, 2018, pp. 1-6. ERA: B
- **Tham Nguyen**, Doan Hoang, Aruna Seneviratne, "Exploring Challenge-Response Mechanism Designs for IoT Initial Trust Establishment," in Proc. of *the 2018 IEEE International Conference on Communications Workshops* (ICC 2018), Kansas City, MO, USA, 2018, pp. 1-6. ERA: B

Journal papers:

- **Tham Nguyen**, Doan Hoang, Aruna Seneviratne, "Information Design for Challenge-Response-based Initial Trust Establishment for Personal Space IoT Systems," submitted to *IEEE Transactions on Information Forensics and Security*. (Under Review) IF: 4.332 (2016)
- **Tham Nguyen**, Doan Hoang, Aruna Seneviratne, "Initial Trust-aware BLE Protocol for Personal Space IoT Systems," submitted to *IEEE Transactions on Mobile Computing*. (Under Review) IF: 3.822 (2016)

- Suranga Seneviratne, Yining Hu, **Tham Nguyen**, Guohao Lan, Sara Khalifa, Kanchana Thilakarathna, Mahbub Hassan, Aruna Seneviratne, "A Survey of Wearable Devices and Challenges," *IEEE Communications Surveys & Tutorials,* vol. 19, pp. 2573-2620, 2017. IF: 20.230 (2017)

Table of Contents

List of Figures

List of Tables

List of Abbreviations and Acronyms

6LoWPAN	Internet Protocol v6 & Low-power Wireless Personal Area Network
BLE	Bluetooth Low Energy
CA	Certificate Authority
CIA	Confidentiality, Integrity, Availability
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CSRK	Connection Signature Resolving Key
DDoS	Distributed Denial of Service
ECG	Electrocardiography
EEG	Electroencephalography
EPC	Electronic Product Code
EV	Electric Vehicle
FPGA	Field-Programmable Gate Array
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IFS	Interframe Space
IoT	Internet of Things
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IRK	Identity Resolving Key
ITU	International Telecommunication Union
LL	Link Layer
LTK	Long Term Key
MAC	Media Access Control
MANET	Mobile Adhoc Network
MIC	Message Integrity Check
MIT	Massachusetts Institute of Technology

NFC	Near-field communication
NIST	National Institute of Standards and Technology
OMNet++	Objective Modular Network Testbed in C++
OS	Operating System
P&G	Procter & Gamble
P2P	Peer-to-Peer
PDF	Probability Density Function
PDU	Protocol Data Unit
PKI	Public Key Infrastructure
QoS	Quality of Service
RFID	Radio Frequency Identification
SoA	Service-oriented Architecture
SoC	System on Chip
STK	Short Term Key
TK	Temporary Key
UML	Unified Modelling Language
UPC	Universal Product Code
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UUID	Universally Unique Identifier
UWB	Ultra-wideband
VANET	Vehicular Adhoc Networks

Abstract

Internet of Things (IoT) is becoming a reality with innovative applications, and IoT platforms have been developed to transfer technologies from research to business solutions. With IoT applications, we have greater control over personal devices and achieve more insights into the resource consumption habits; business processes can be streamlined; people are also better connected to each other. Despite the benefits derived from the IoT systems, users are concerned about the trustworthiness of their collected data and offered services. Security controls can prevent user's data from being compromised during transmission, storage or unauthorized access, but do not provide a guarantee against the misbehaved devices that report incorrect information and poor services or avoid conducting a common task. Establishing trust relationship among devices and continuously monitoring their trust is the key to guarantee a reliable IoT system and hence mitigate user's concerns.

In this dissertation, we propose and investigate a novel initial trust establishment architecture for personal space IoT systems. In the initial trust establishment architecture, we propose a *trust evidence generation module* based on a challenge-response mechanism to generate the trust evidence relying on the device's responses to the challenges, a *trust knowledge assessment module* to obtain the knowledge about the device from the generated trust evidence, and a *trust evaluation scheme* to quantify the initial trust level of the devices. We design and investigate a *challenge-response information design* to determine feasible designs of the challenge-response mechanism that ensure meaningful and related trust knowledge about the device's trustworthiness captured from the challenge-response operations. A *new trust-aware communication protocol* is designed and implemented by incorporating the proposed initial trust establishment architecture into existing Bluetooth Low Energy (BLE) protocol to demonstrate the feasibility and efficiency of the proposed initial trust establishment architecture in practice.

In this work, we first study building blocks and possible architectures of the IoT and analyze key requirements of an IoT system. Based on the analysis, we identify the critical role of the initial trust establishment model and the challenges of establishing initial trust in IoT systems due to the lack of knowledge for the trust assessment to work. To address the challenges, we propose a novel initial trust establishment architecture that can generate trust evidence for assessing the initial trust level of new devices by conducting challenge-response operations within a limited time window before they are admitted to the system.

We propose three new initial trust establishment models based on the proposed architecture. An implicit relationship between the responses and the challenges is assumed for the system to judge the initial trustworthiness of the devices. The first model assesses the initial trust value based on a probability associated with the device's behavior captured from the challenge-response process. The second model investigates the initial trust value based on a binary outcome set, and the third model quantifies the initial trust level based on a multiple-component outcome set from the challenge-response process.

Subsequently, we propose the challenge-response information design where the challenge-response process is investigated and designed to determine the information space of the challenger's view on its environment so that the challenge can invite relevant responses from the target environment. Based on the design of the challenge-response mechanism, the system can capture meaningful trust knowledge about the devices from challenge-response operations at their admission phase. We finally design and implement the initial trust-aware BLE protocol which incorporates the proposed initial trust establishment architecture into the existing BLE protocol. The simulation results show the efficiency, feasibility, and dependability of using initial trust-aware BLE protocol for building a trustworthy personal space IoT systems.

The novelty of this research lies in assessing the devices' initial trust level within a limited time window, before their admission to the personal space IoT system, without requiring prior experience or recommendations. The major contribution of this thesis is that it helps the IoT business solution providers to build secure and trustworthy IoT systems by admitting dependable devices, monitoring the trust of admitted devices, detecting maligned devices, and building long-term trust among. As a result, it mitigates the user's concerns about the trustworthiness of IoT systems and encourages broader adoption of IoT applications.