University of Pittsburgh | School of Computing and Information

Dissertation Defense

Doctor of Philosophy in Information Science

"**Trust Evolution in IoT Networks with Multiple Attributes**" by **Nuray Baltaci Akhuseyinoglu**

Date: April 3, 2023
Time: 11:00 AM – 12:30 PM
Place: Room 502/IS Building, 135 N Bellefield Ave Pittsburgh PA 15260
RSVP for Zoom:
https://pitt.co1.qualtrics.com/jfe/form/SV_2afpEz9qSW4jtAO

Committee:

- Dr. Prashant Krishnamurthy, Professor, School of Computing and Information
- Dr. Konstantinos Pelechrinis, Associate Professor, School of Computing and Information
- Dr. Amy Babay, Assistant Professor, School of Computing and Information
- Dr. Mai Abdelhakim, Assistant Professor, Department of Electrical and Computer Engineering, Swanson School of Engineering

Abstract:
The Internet of Things (IoT) is a communication paradigm comprising millions of devices, a.k.a things or nodes, growing in number. Things are interconnected smart devices that operate with or without human intervention, such as sensors, actuators, RFID devices, wearable devices, or more powerful computing systems. The heterogeneity of devices, software components, and network infrastructure in IoT leads to increased attack surfaces. One of the significant security threats for IoT is untrustworthy data and operations that may arise due to device compromise, vulnerable transmission medium, or faulty sensors. It is essential to ensure trust in the data and operations in IoT, as it is fundamental for people to overcome perceptions of uncertainty and risk in using IoT services and applications. The lack of trust may have dire consequences for IoT. For example, an attacker compromising an IoT device can generate or report bogus data, boost the reputation of malicious nodes, and ruin that of benign nodes.

There are security mechanisms to defend against external attacks in IoT, such as cryptographic algorithms. Yet, they cannot identify internal attacks as a benign node could turn into a malicious node any time after joining the network through a successful exchange of cryptographic keys and behaving benign for some period. Trust management solutions are essential for detecting misbehaving legitimate nodes in IoT when cryptographic measures are not available or applicable. IoT brings extra challenges to trust management due to ever-changing network topology, heterogeneity in devices and network topology, and limited resources of constrained devices. Promising solutions have been proposed for IoT trust management to address these challenges. Yet, they are limited in accommodating key trust properties and automated trust computation needs for IoT environments.

The research in this dissertation focuses on trust evolution in IoT networks, drawing upon trust research in social sciences. Towards this, we distill significant aspects of trust evolution in social sciences and capture them in solutions for IoT trust management through automated trust computations. Specifically, we propose an automated trust computation framework based on the Multi-Attribute Decision Making (MADM) approach and Evidence-based Subjective Logic (EBSL) to account for the multi-dimensionality and uncertainty aspects of trust. We evaluate the

performance of the proposed MADM-EBSL framework concerning varying levels of network connectivity and trust problem size. Additionally, we propose to extend the trust model of this framework with trust attributes based on our review of social sciences trust literature. We compare the two frameworks to investigate the effect of including additional attributes in trust computations. Finally, we explore trust repair strategies for IoT and a model to reflect these on automated trust computations. We present the findings of our evaluation of the proposed trust repair model.