UNIVERSITI TEKNOLOGI MARA

A NEW TECHNICAL FRAMEWORK FOR SECURITY, TRUST AND PRIVACY (STP) OF RFID SYSTEM

MOHD FAIZAL BIN MUBARAK

Thesis submitted in fulfilment
of the requirements for the degree of
Doctor of Philosophy

Faculty of Computer and Mathematical Sciences

January 2015

ABSTRACT

Future trend of RFID system is moving towards integration with other devices, and hence making it more pervasive. Even though RFID technology brings numerous benefits, it also comes with potential security and privacy threats. In this thesis, we investigate how the integration and interconnection of RFID system with other devices introduce security vulnerabilities which could be exploited by attackers and adversary systems equipped with advanced techniques and attacking tools to achieve their evil objectives. We examined past works on RFID with privacy-preserving solutions dealing with issues on system integrity and availability. We found out that these unprotected RFID system without integrity verification could also be subjected to malicious code attacks and impersonation attacks. We found a solution that could exactly protect the RFID system in three main protection areas, namely security, trust, and privacy (STP). We believe that we have used a unique approach in our research study because we have taken into account all potential issues and we tackle them in a unified and integrated way. Our main contribution is that we proposed a unified STP protection in RFID framework which protected against unauthorized access and adversary attacks. We call this framework as MF-JaSa2 RFID framework. The framework offers enhanced unified STP features in RFID system advanced techniques such as encrypted-based attestation, integrity verification techniques with respect to protect user privacy, utilization of Trusted Platform Module (TPM), a tamper proof hardware to provide integrity verification for RFID system and utilization of MJS-Watcher as runtime integrity-checker, elliptic curve cryptography (ECC) for security protection and anonymizer for privacy-preserving protection. Based on formal method analysis, we proved that MF-JaSa2 RFID protocol always maintains its platforms in trusted and secured mode and keeps tags anonymous. Based on experiments, we proved MF-JaSa2 framework is able to protect RFID system against any attack especially the runtime-based attack and impersonation attack. Finally, MF-JaSa2 RFID framework is considered as trusted, secured and privacy-preserved RFID system.

ACKNOWLEDGEMENT

I wish to express my gratitude to my supervisors, Prof. Dr. Saadiah Yahya from the Faculty of Computer and Mathematical Sciences, UITM and Dr. Jamalul-lail Ab Manan from MIMOS Bhd., for their continuous support and supervision during the year of my study. It is their brilliant ideas and expertise that led this study to its successful outcome.

Special thanks to my parents, Mubarak Md. Arshad and Bisah Hassim and my family, Nurul Haryanie, Akmal Firdaus, Hannah Khadeeja, Luqman Hamzah and Haziq Fahmee for all their love and support.

My special thanks also to the two of my bosses, Mr Azhar and Mr Azuddin for their support and allowing me to visit my supervisor regularly. Not to forget that they also encourage me to complete my study especially in my thesis writing.

Last but not least my appreciation also goes to all my friends especially Anuar Isa, Fazli Mat Nor, Sazali Musa and Zaid Ahmad for their input and friendships.

TABLE OF CONTENTS