UNIVERSITI TEKNOLOGI MARA

MUTUAL ATTESTATION AND INTEGRITY VERIFICATION OF RFID SYSTEM USING TRUSTED PLATFORM MODULE (TPM)

MOHD FAIZAL BIN MUBARAK

Thesis submitted in fulfillment of the requirements

for the degree of

Master of Science

Faculty of Computer Science and Mathematics

October 2010

Author's Declaration

I declare that this thesis entitled *"Mutual Attestation and Integrity Verification of RFID System Using Trusted Platform Module (TPM)"* is the result of my own research except as cited in the references. The thesis has not been accepted for any degree and is not concurrently submitted on candidature of any other degree.

Signature :

Name : Mohd Faizal Bin Mubarak

Date : 25th October 2010

Abstract

Radio Frequency Identification (RFID) technology is an advance contactless identification system which communicates through radio frequency between RFID reader and tags. Basically, there are three components in RFID system which consists of reader, back-end server and tags. RFID tags are normally small and can be deployed in many solutions such as goods and luggage tracking, and access control system. The widespread deployment of RFID system across many solutions is a good impact to the community and it's simplifies a lot of business transactions. However, massive deployment of RFID system into several solutions may potentially impose security and privacy threats. Since RFID tag and reader communicate through contactless radio frequency channel, messages can easily be captured by any unknown reader. RFID system without any trust and integrity element poses security threat because secret data can easily be revealed to adversary system due to unverified RFID platform. Numerous works done by several researchers have shown that unprotected RFID platform can be compromised either by malicious codes or man in the middle attack. System integrity verification for RFID reader, tag and back-end server have to be implemented to provide system trust for RFID system. The proposed back-end server and RFID reader with the embedded trusted computing technology will provide the system integrity measurements and verifications. This research utilized Trusted Platform Module (TPM) as a tamper proof hardware to protect the integrity of RFID system. The proposed solution provides mutual attestation and integrity verification for trusted RFID protocol by using TPM and Advanced Encryption Standard (AES) encryption for encrypting data transfers within trusted RFID system. Our scheme offers the most enhanced security feature in RFID system by using mutual attestation technique with respect to protect user privacy. This solution also highlights the importance of trusted computing technology towards solving the privacy and security issues. The experiment results prove that our proposed solution is reliable whereas attack model shows that our proposed solution is more trusted and secured compare to previous RFID protocols.

Table of Contents