Security Protocol for NFC Enabled Mobile Devices Used in Financial Applications

By

Osama Bin Faridoon

2012-NUST-MS-CCS-05

Supervisor

Dr. Abdul Ghafoor Abbasi

Department of Computing

A thesis submitted in partial fulfillment of the requirements for the degree of Masters of Science in Computer and Communication Security (MS CCS)

In
Department of Computing (DoC)
School of Electrical Engineering and Computer Science (SEECS),
National University of Sciences and Technology (NUST),
Islamabad, Pakistan
(Jan, 2015)

Dedication

Dedicated To My Father

Lt Col Faridoon Khan Jadoon

Without whose persuasion it would not have been possible to complete it.

Abstract

The fostering of NFC in everyday tasks and with growth in applications involving contactless transactions based on NFC; there is a requirement from users and industry to address the security issues affecting mobile payments. The current NFC security standards are inadequate to address most of the security concerns such as privacy infringements, unauthorized access to financial data, theft of mobile data exchanged between terminal and mobile device. We designed a NFC based security protocol for financial applications, which addresses security requirements holistically and provides local and remote mutual authentication, confidentiality, integrity and non-repudiation. It is based on some common and extended security features which help to increase the reliability of NFC based systems. After designing, we verified our protocol using formal verification tools like Scyther and established that it protects against spoofing attack, man-in-the-middle attack, replay and skimming attacks. It ensures the secrecy of transaction data, privacy of the users and also ensures that only authenticated and authorized NFC device holder and PoS terminals are securely exchanging financial data to perform the transaction. Furthermore, it may be beneficial to the financial organizations in increasing their user's trust, for secure usage of their mobile devices for financial transactions.

As a proof of concept, we designed and implemented our solution using java technology for android based NFC mobile devices and successfully deployed it in our local environment to test its correctness and behavior. We also provided a comprehensive comparison of our protocol with other NFC based financial protocols. We found that the mutual authentication, confidentiality, integrity, authorization and non-repudiation services help to protect against most of the security attacks related to mobile financial transactions. Since this protocol is flexible, generalized and reliable, so the whole system is not depended on the third parties and any prior knowledge.