A Secure Mobile Wallet Framework with Formal Verification

Shaik Shakeel Ahamad, Department of Computer and Information Sciences, University of Hyderabad, Hyderabad, India & Institute for Development and Research in Banking Technology, Castle Hills, Masab Tank, Hyderabad, India

V. N. Sastry, Institute for Development and Research in Banking Technology, Castle Hills, Masab Tank, Hyderabad, India

Siba K. Udgata, Department of Computer and Information Sciences, University of Hyderabad, Hyderabad, India

ABSTRACT

This paper proposes a Secure Mobile Wallet Framework (SMWF) using WPKI (Wireless Public Key Infrastructure) and UICC (Universal Integrated Circuit Card) by defining (a) a procedure of personalizing UICC by the client, (b) a procedure of provisioning and personalization (Mutual Authentication and Key Agreement Protocol) of Mobile Payments Application (which is on UICC) by the Bank and (c) our proposed mobile wallet is will have mobile wallet manager managed by CA (acting as TSM), every mobile application is independent, protected by firewalls and encrypted data is stored in the mobile wallet application. Their proposed Mobile Wallet ensures end to end security. The authors’ proposed SMWF is compared with recent works and found to be better in terms of generating client’s credentials, implementation of WPKI in UICC, personalization of mobile payment application by the bank and in ensuring end to end security (i.e., from Mobile Payments Application in UICC to the Bank Server). The proposed mobile payment protocol originating from Mobile Payment Application (which is on UICC) to the Bank Server realizes Fair Exchange ensures Confidentiality, Authentication, Integrity and Non Repudiation, prevents double spending, over spending and money laundering, and withstands replay, Man in the Middle (MITM) and Impersonation attacks. Proposed mobile payment protocol is formally verified using AVISPA and Scyther Tool and presented with results.

Keywords: AVISPA Tool, Scyther Tool, Secure Mobile Wallet Framework (SMWF), Universal Integrated Circuit Card (UICC), Wireless Public Key Infrastructure (WPKI)

INTRODUCTION

A mobile wallet is a complete payment application for NFC-enabled mobile phone that enables consumers to pay at stores at the point of sale with a mobile phone. The digital wallet, which is associated with a credit card, integrates all payment-related services like the management and storage of receipts, coupons and offers, and loyalty cards. With the rapid evolution of
mobile technology, and an expanding base of mobile phone users, the mobile wallet has been recognized as having growth potential in the mobile commerce industry (Au & Kauffman, 2007). The industry strives to develop and build robust mobile commerce applications and at the same time provide an environment for secure, convenient, cost saving and efficient business transactions. A mobile wallet can support various transactions, including consumer-to-consumer, consumer-to-business, consumer-to-machine (i.e., paying for small-value transactions at a device such as a parking meter), and consumer-to-online. In addition, consumers have greater flexibility for settling transactions at the point of sale with mobile phone payments. Our proposed mobile wallet is a much-advanced and versatile application that includes elements of mobile transactions, as well as other items one may find in a wallet, such as debit cards, credit cards, membership cards, loyalty cards and travel cards. It also stores personal and sensitive information like passports, credit card information, PIN codes, online shopping accounts, booking details and insurance policies that can be encrypted or password-protected. Our proposed mobile wallet is loaded inside the UICC (Universal Integrated Circuit Card) of the mobile phone called UICC Wallet, which stores data in a UICC. The UICC is the smart card used in mobile phone in GSM or UMTS networks. Since it is a smart card, it inherits all the security features of smart cards. It provides a secure storage of data.

The remainder of the article is as follows: First, we give a literature review of mobile wallets, gaps found in the literature and contributions made by us. Then we propose a Secure Mobile Wallet Framework SMWF based on NFC. Next we present Security analysis of our proposed mobile payment protocol in SMWF. Followed by a comparative analyses of the proposed framework with the literature review (Table 1). Afterwards we present Formal Verification of the Proposed Protocol’s Security using AVISPA and SCYTHE. Finally we then conclude our work. We provide some explanations of notations and abbreviations in the Appendix (Tables 2 and 3).

LITERATURE REVIEW

Mobile Wallets were proposed by NTT DoCoMo and Google Wallet (2011) but there are many flaws in their proposed mobile wallets

Gaps Found in Literature

- NTT DoCoMo’s Mobile Wallet is implemented in the memory of mobile phone.
- NTT DoCoMo’s Mobile Wallet needs a special mobile phone which supports NTT DoCoMo’s Mobile Wallet.
- Digital forensics firm via Forensics has found may flaws in Google Wallet (Block, 2011) such as,
  - Significant amount of data is stored unencrypted within Google Wallet.
  - While Google Wallet does a decent job by securing all users credit cards numbers (it is not insecurely stored and a PIN is needed to access the cards to authorize payments), the amount of data that Google Wallet stores. unencrypted on the device is significant (pretty much everything except the first 12 digits of your credit card) which can lead to social engineering attack.
- Privacy of the consumers is not ensured.
- Authors of Labrou et al. (2004) propose a wireless wallet in the memory of mobile phone.
- Authors of Steffens, Nennker, Ren, Yin, and Schneider(2009) propose a SIM based mobile wallet in SIM which cannot be personalized by the bank using OTA.
- Current mobile wallet solutions (Labrou et al., 2004; Steffens et al., 2009; Zhao & Muftic, 2011) store client’s credentials in the memory of Mobile Phones, on the SIM or UICC, Mobile Phones and SIM with PKI functionality is personalized by the Issuer (Usually by MNSP) and Service...
Related Content

RFID Technologies and Applications
www.igi-global.com/chapter/rfid-technologies-applications/37776?camid=4v1a

Ontology Based Context-Aware Adaptation Approach
www.igi-global.com/chapter/ontology-based-context-aware-adaptation/7115?camid=4v1a
A Multi-Agent System for Improving the Resource Allocation on Programmes in Higher Education
www.igi-global.com/chapter/multi-agent-system-improving-resource/76783?camid=4v1a

Image Reconstruction Algorithm Based On PCA and WNN for ECT
www.igi-global.com/article/image-reconstruction-algorithm-based-on-pca-and-wnn-for-ect/108528?camid=4v1a