Pervasive and Mobile Computing 29 (2016) 113–129

Contents lists available at ScienceDirect

Pervasive and Mobile Computing

journal homepage: www.elsevier.com/locate/pmc

Recovering from a lost digital wallet: A smart cards perspective extended abstract☆

Raja Naeem Akram [a,*], Konstantinos Markantonakis [a], Damien Sauveron [b]

[a] Smart Card Centre, Information Security Group, Royal Holloway, University of London, Egham, United Kingdom
[b] XLIM (UMR CNRS 7252 / Université de Limoges) Département Mathématiques Informatique, Limoges, France

ARTICLE INFO

Article history:
Received 29 May 2014
Received in revised form 11 June 2015
Accepted 26 June 2015
Available online 3 July 2015

Keywords:
Smart card
GlobalPlatform Consumer-Centric Model
Java Card
Multos
Performance measurement

ABSTRACT

Multi-application smart cards enable a user to potentially have a diverse set of applications on her smart card. The growing trend of services convergence fuelled by Near Field Communication and smart phones has made multi-application smart cards a tangible reality. In such an environment, cardholders might have a number of applications on their smart cards and if a card is lost, all of the applications would be lost with it. In addition, consumers might decide to upgrade their smart cards and require a seamless and secure framework to migrate their applications from the old smart card to the new one. Currently, the recovery of a smart card-based service might take from a day to a week at best as each of the lost cards can only be replaced by the respective card issuer, during which time the card issuer might lose business from the user because she is not able to access the provisioned services. Similarly, there is at present no migration mechanism proposed for smart card applications. The proposed framework in this paper enables a user to acquire a new smart card as she desires and then migrate/restore all of her applications onto it—allowing her to recover from her lost digital wallet in a secure, efficient, seamless and ubiquitous manner.

1. Introduction

Smart card technology has the capability to have multiple applications coexisting on a single smart card chip in a secure and reliable manner [1]. Cards with this capability are generally described as multi-application smart cards. Proposals for multi-application smart cards have been around since the latter half of the 1990s. The majority of the deployed smart card platforms like Java Card [2] and Multos [3] support multiple applications; however, a large number of deployed cards only offer a single application (e.g. banking, telecom, or transport) [4].

In recent years, the convergence of multiple services onto a single smart card has gained momentum due to the emergence of Near Field Communication (NFC) [5]. NFC enables a mobile phone to emulate[1] a contactless smart card. Therefore, a user can use her mobile phone to gain access to different smart card-based services (e.g. banking, transport and door access). The Groupe Spécial Mobile (GSM) [6] and GlobalPlatform [7] specifications have also evolved to support the convergence of multiple services in the Issuer Centric Smart Card Ownership Model (ICOM) [8] by including an entity known

☆ Originally published in the 4th IEEE International Symposium on Trust, Security, and Privacy for Emerging Applications (TSP-13).

* Corresponding author. Tel.: +44 758 807 4358.
E-mail address: rnakram@waikato.ac.nz (R.N. Akram).

[1] NFC enables a mobile phone to have three different modes: card emulation, peer-to-peer, and reader/writer mode. However, in this paper the main focus is the card emulation mode.

http://dx.doi.org/10.1016/j.pmcj.2015.06.018
1574-1192/

as the Trusted Service Manager (TSM) [9]. The TSM is (potentially) a neutral third party that has administrative control of the smart card. This administrative control includes the installation and deletion of applications along with enforcement of security policies related to smart cards and applications developed by the partner application providers referred to as Service Provider (SP) in this paper.

In contrast the User Centric Smart Card Ownership Model (UCOM) delegates the ownership of smart cards to their users [8]. The term ownership means the right to install or delete an application according to the smart card user's requirements. In such a dynamic and open environment, where users can have multiple applications of their choice, certain security and privacy issues [8,10] are created. In March 2012, GlobalPlatform announced the initiative of a user centric ownership model for smart cards called the GlobalPlatform Consumer-Centric Model (GP-CCM) [11]. This model is significantly similar to the UCOM; therefore, the proposal in this paper also applies to the GP-CCM.

One of the main features of the UCOM is "dynamism" (wherever, whenever). This allows a user to download a diverse set of applications onto her smart card just to perform mundane tasks (e.g. transport and building access), increasing the potential damage/inconvenience if the device is lost. To expedite the recovery process after theft or loss, customers should be able to have their applications backed up and then restored when required, in a secure and ubiquitous manner, to their new devices. In addition, the UCOM also allows users to acquire a UCOM-supported smart card as they desire—this provision could also lead to a user upgrading or replacing her old smart card. Therefore, similar to the recovery process, the migration of applications from an old smart card to a new one should be seamless and implemented through a secure mechanism.

1.1. Problem statement

The multi-application smart card concept supported and advocated by the ICOM-TSM, UCOM, and GP-CCM has one commonality. They all want to provide a service to the cardholder[2] in which the user can access and use all of her application from a single device with ease. This idea of single device with multiple applications (e.g. telecom, banking, transport, and access control) that a card user requires to perform her daily tasks, also has the potential to negatively disrupt her daily activities if it is lost or stolen. From the point of view of the ICOM-TSM, UCOM and GP-CCM, a quick and user-friendly mechanism to get all the applications back on the new device would be preferable for the card user that has lost her multi-application smart card.

As the ICOM-TSM, UCOM and GP-CCM proposals are still in their early stages, they do not have any potential candidates to provide a quick and user-friendly restoration mechanism. The only existing precedent specific to the smart card industry is the card replacement service in the ICOM environment. In this process, the card user informs the respective card issuer of the loss of her smart card. The card issuer can then initiate the re-issuance of the smart card to the particular card user—that might take from few days to a week depending upon the card personalisation and then postage service to cardholder's address. Where such a mechanism might not be preferable for the models that advocate convergence of different applications onto a single smart card, along with enabling instant access to SP's services via the respective users smart card.

On the other hand, UCOM permits the card user to download any application they require as long as they have the authorisation from the respective SP [12]. The application installation process requires a cardholder to have a set of authorised credentials to access SP and request the application download. Depending upon the SP's security policy, these credentials might only be one-time use only. The application installation process in the UCOM is described in [13]. A simplistic recovery mechanism after the loss of a smart card would be for a user to acquire a new smart card and then request individual SPs to issue her a new set of authorised credentials so she can download the respective applications. Such a solution is possible; however, it seems laborious on the part of the cardholder.

Whereas, in the ICOM-TSM model, depending upon the actual role and responsibility set for each of the stakeholders the card user might download any permitted application by the overall scheme, either from the SP or the designated TSM [14]. Authorised credentials are still required to download or access individual applications from their respective SPs. However, the TSM issues a smart card with pre-installed applications (similar to the card issuer in the ICOM) then the recovery process might takes from few hours to potentially few days. Whereas the potential mechanism for GP-CCM [11] might deploy is still not made public, in this paper we assume that GP-CCM application download mechanism might either be similar to the ICOM-TSM or UCOM mechanisms.

There is potentially no proposal for a smart card backup and recovery process that enables instant access to lost applications while providing the features listed as below:

1. A secure, and reliable application backup (and recovery) process that does not compromise SP's applications and associated intellectual property (IP).
2. A flexible, and ubiquitous process that can be accessed by the authorised card user from anywhere to backup and later restore the smart card applications.

[2] In this paper, the terms cardholder, card user and user are used interchangeably representing the consumer who is in possession of the respective smart card and has the authorisation to utilise the services provisioned by the applications on it.