New Protocol Layer for Guaranteeing Trustworthy Smart Card Transaction

Zheng Jianwu, Liu Mingsheng, and Liu Hui
Department of Information Engineering,
Shijiazhuang Railway Institute, Hebei 050043, China,
{zhengjw, liums, liuhui}@sjzri.edu.cn

Abstract—**We first point out that trustworthy information exchange between the card application and the smart card should be guaranteed, given the application system wants to leverage the enhanced security and privacy functionality of the smart card to make itself an attack-proof system, then suggest to introduce a new protocol layer for ensuring trustworthy transaction into current smart card protocol stack, and determine the position where the new protocol layer should be in the stack.**

Furthermore, protocol detail of the new layer, i.e. cryptographic policy in essence for establishing trustworthy channel between the card application and the smart card is proposed, specifically, how measures for ensuring transaction information privacy & integrity, and fighting fraudulent transaction are taken and integrated. Moreover, STS (Station to Station) protocol for attestation and authenticated key negotiation, which is the key to the success of the new protocol layer, is introduced.

I. Introduction

Because the smart card is an intrinsically secure computing platform, it is often incorporated in the application system to enhance the security of the system or realize some special security purposes. Fig. 1 depicts two scenarios of the networked application system.

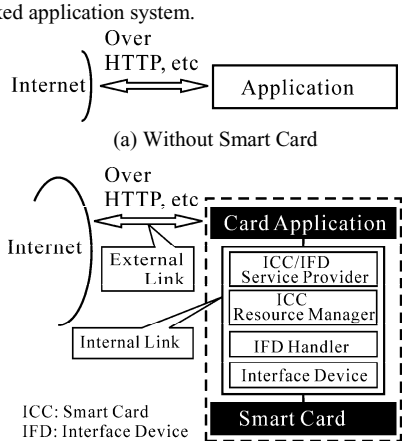


Fig. 1. Two Scenarios of the Networked Application System

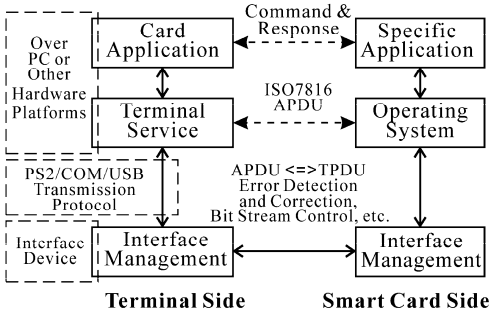
After incorporating the smart card, on the one hand, it is possible for the system to exploit the enhanced security and privacy functionality of the smart card, and on the other hand, the system is complicated, namely, besides the card application and the smart card, so many intermediary parties, including ICC/IFD Service Provider, ICC Resource Manager and so on are involved in the application terminal.

We always pay more attention to the external link (Internet link), such as implementing SSL/TLS, IPSec and so on for securing the traffic between application terminals through Internet, than that to the internal link connecting the card application and the smart card, precisely, it is always neglected to take measures to guarantee trustworthy information exchange between the card application and the smart card. Consequently, attacks initiated by spyware, virus software and so forth find favourite entrances here and bring disastrous consequences to the system.

In reality, two links mentioned above are equally important in terms of the security of the system, and therefore should be thoroughly safeguarded with proper policies and measures. This paper aims to propose measures to secure message exchange between the card application and the smart card in the application terminal.

A. Transmission Model and Protocol Stack

Fig. 2 (taken from PC/SC Specification Version 2.0 [1] with modifications) and Fig. 3 depicts transmission model and protocol stack of smart card transaction executed in the application terminal depicted in the bottom scenario of the Fig. 1 respectively.



(APDU: Application Protocol Data Unit
TPDU: Transmission Protocol Data Unit)

Fig. 2. Transmission Model of Smart Card Transaction

From Fig. 1 and Fig. 2, it is clear that the card application is the entrance to the Internet, connecting the external world over

T. Sobh and K. Elleithy (eds.), Advances in Systems, Computing Sciences and Software Engineering, 377–381.