B-POS Secure Mobile Payment System

Antonio Grillo
Università di Roma "Tor Vergata", Italy

Alessandro Lentini
Università di Roma "Tor Vergata", Italy

Gianluigi Me
Università di Roma "Tor Vergata", Italy

INTRODUCTION

The B-POS (Bluetooth Point of Sale) is the prototype of a secure, mobile macropayment system. Since heterogeneous wireless network technologies such as PANs, LANs, and WANs have well-known security weaknesses, it is mandatory to enforce security services, such as authentication, confidentiality, integrity, and non-repudiation. This article describes a Java-based macropayment system prototype featuring security and independence from an e-money third party acting as an intermediary. This system can rely on the existing financial network infrastructure (e.g., credit card, ATM networks).

BACKGROUND

Currently, most of m-payment (payment performed with a mobile device) systems rely upon mobile WAN (wide area network, e.g., GSM/GPRS/UMTS), enabling the customer to buy contents (by mobile carrier) or goods billed to the mobile phone contract account or to a prepaid card (in a business model called "walled garden"). The widespread diffusion of Bluetooth-enabled mobile phones, however, can possibly boost the deployment of new application paradigms based on personal area networks (PANs) and NFC (near field communications), enlarging the payment paradigm to financial and banking systems and circuits (e.g., EFC —electronic financial circuits), so achieving two major benefits: (1) to escape from the "walled garden," so acquiring the capability to buy every good and every service, not only those from the mobile carrier; and (2) collecting the payment capabilities in a personal trusted device (PTD, e.g., the smartphone) without dealing with the ATM/credit cards in the wallets, supporting both micropayments and macropayments (Me, 2003).

There has been a considerable amount of research focusing on the adoption of mobile payments using a POS (Me & Schuster, 2005). Most of the research effort on usability led to description of the adoption factors influencing the consumer in the adoption of the payment solution (Dahlberg, Mallat, & Oorni, 2003; Mallat, 2004; Pousttchi, 2003; Zmijewska, Lawrence, & Steele, 2004). Other research has focused on finding the most critical factor of success and the different requirements of mobile payment systems (Hort, Gross, & Fleisch, 2002; Muller, Lampe, & Fleisch, 2004). Many more studies focused on the adoption intentions of the consumers and the merchants toward a new electronic payment system (Plouffe & Vandenbosch, 2001). Early local mobile payment systems (cash like, micropayments) were pioneered by Chaum CAFÉ-IR (www.chaum.com/CAFE_Project.htm) based on public-key encryption and the blind signature scheme of Ecash: this system uses a smartcard and an electronic prepaid "wallet" to complete transactions via the InfraRed technology. The work of Blaze, Ioannidis, and Keromytis (2001) on microchecks (over the InfraRed links) is (somewhat) similar to ours, except for (at least) its minor concerns with fraudulent transactions (due to their small amount). Another important difference is that the payer is not required to authenticate the merchant during a transaction. Several other e-check systems have been implemented during recent years, but they were never customized for mobile/local transactions (e.g., SET, echeque, First Virtual). The foremost e-check system, Kerberos based, was NetCheque (http://gost.isi.edu/info/NetCheque/).

Currently, several countries have adopted mobile payments: in the Asian market, Singapore, South

Korea, and Japan reached an advanced market stage, for example, the FeliCa contactless payment system, currently the de-facto standard method in Japan with over 20 million users, counts over six million FeliCa-enabled handsets and POS installed in all the major shop chains (www.sony.net/Products/felica). Europe is following close behind with successful m-payment services already launched in Austria, Croatia, and Norway, and in Italy, Telecom Italia Lab unveiled in December 2005 a contactless system called Z-SIM, where mobile phones can communicate with any terminal or object by very simple interaction. As a rule, a mobile payment system can be operator independent, where billing is based on an association between a credit card or bank account to the mobile phone (e.g., the Italian major credit card distributor CartaSi has recently launched its own mobile payment system).

MAIN FOCUS OF THE ARTICLE

B-POS aims to be a secure mobile macropayment system for local, contactless, and operator-independent payment systems, involving three different entities—bank, shop, and customer (smartphone)—communicating via secure channels, as shown in Figure 1. Due to well-known mobile vulnerabilities, especially regarding Bluetooth (Nichols & Lekkas, 2001, 402-415; Jacobson & Wetzel, 2001), it is mandatory to enforce security, firstly on wireless links. For this reason, the requirement of macropayment system security is met at the application layer, avoiding various communication layer vulnerabilities, (e.g. E3—electromagnetic environmental effects) or new, unpredictable vulnerabilities (e.g., wireless transport layer security (WTLS) gap in versions prior to WAP 2.0). This task is performed using an asymmetric keys schema for the authentication with a derived symmetric session key. A mutual authentication is implemented among B-POS's communication parties, so the entities involved can trust each other.

The Bluetooth link connects the smartphone to the shop (1). Information exchanged between the shop and the bank happens on a secure channel. The customer refers to his own bank through a virtual private network (VPN), taking advantage of both these channels (3).

Since the end user trust should be placed into a customer-reliable authority, we centralized all the responsibilities into the bank, whose former task was to release and setup the BPOS mobile application on the customer device.

In order to achieve a widespread diffusion between customers, the prototype is suited for devices as PDAs and smartphones equipped with Kilo Virtual Machine (KVM). Former benefits in adoption of J2ME reside in advantages to use cross-platform code and embedded security mechanisms (safe box). Several further considerations suggest the J2ME platform as appropriate to support m-payments (Sun Microsystems, 2000a; Cervera, 2002):

- **Broad user experience:** The J2ME API provides enhanced possibilities to present GUI, for example, event handling and rich graphics.
- **Comprehensiveness:** The details of the machine architecture, operating system, and display environment are all handled transparently by the Java virtual machine (JVM). The same Mobile Information Device Profile (MIDP) m-payment client can run on all the MIDP-compliant devices (Sun Microsystems, 2000a, 2000b; Cervera, 2002). This allows the m-payment system providers to target a wider range of end-users.
- **Reduced network and server load:** The J2ME-based applications can operate when disconnected, and they only interact with a server when necessary. J2ME has its own runtime environment and the capability to store data in the mobile device.

Figure 1. BPOS architecture