Secure contactless smart card transactions on mobile devices

Adeola O. Poroye, William D. Tucker and Michael Norman
Department of Computer Science, University of the Western Cape, Private Bag X17 Bellville, 7535
Telephone: +(27) 21 959-2461, Fax: + (27) 21 959-3006, Email: {**2561906**, btucker and mnorman}@uwc.ac.za

Abstract—This paper presents work in progress to explore the utility of Near Field Communication technology to secure mobile financial services. The objective is to evaluate the potential of this approach as an upcoming technology for mobile cash transactions. The paper argues that Near Field Communication technology offers a feasible solution and can be integrated into a standard cellular handset to turn it into a contactless smart card. The motivation is to create a new secure way for the unbanked to perform financial transactions. A prototype has been developed and tested with participants in a laboratory environment. This paper also reports on preliminary results.

Index Terms—Secure, mobile, virtual cash, Near Field Communication (NFC)

I. INTRODUCTION

Research initiatives involving the use of mobile devices to offer financial services for those without access to traditional ways of banking (the unbanked) is fast gaining momentum in the developing world[1]. The inability to carry out banking, especially among those residing in rural areas, stalls development and further leads to poverty, illiteracy and a decline in the general standard of living for many people in the developing world. In a bid to provide access to alternative solutions to banking, many people have to resort to insecure, inconvenient and, often times, loss-making forms of money transactions[2].

Financial institutions such as banks will not venture investment in areas that yield low return on investment (ROI). In addition, hidden charges in the form of interest rates and transaction fees, for example, contribute to enlarging the unbanked population. Today, the growing numbers of the 'unbankable' is an unfortunate one, but this situation also creates opportunities. Mobile handsets are in an excellent position to become the primary digital channel for providers of banking and related financial services. This is especially true for emerging markets. Mobile phones are the most ubiquitous information and communication technology (ICT) that is available, useable and affordable to the bottom of the economic pyramid. Mobile transaction systems appear to exhibit the markers of an innovation waiting to be diffused; to be adopted by a growing number of mobile phone users in developing regions[2].

The following section provides a brief overview of work related to mobile banking and transaction technologies. Section III reports on a preliminary survey about mobile banking conducted with university students from rural areas. The results from that survey caused us to propose an experimental design, described in Section IV, to investigate the design of a contactless smart card system for a mobile phone using Near Field Communication (NFC). Section V concludes the paper with a view toward future work.

II. RELATED WORK

Although mobile telephony has spread rapidly, it does not mean that transaction services hosted by mobile devices can necessarily penetrate low-income markets just as quickly. A number of obstacles need to be overcome. Perhaps the most important challenge is the development of suitable virtual and actual cash in and out mechanisms [3].

In Kenya, an innovative payment mobile solution called M-PESA enables customers to transfer money with their mobile phones [4]. M-PESA is aimed at mobile customers who do not have a bank account because they do not have access to a bank, or because they do not have sufficient income to justify a bank account. A slightly different mobile financial service called WIZZIT exists in South Africa. Unlike M-PESA, WIZZIT is interoperable with any Maestro labelled Automated Teller Machine (ATM) and customers are given a branded debit card as an alternative means to access the service. However, WIZZIT has the drawbacks of charges, fees and minimum deposits that frustrate the use by the bottom of the economic pyramid [4].

Mobile phones are extraordinarily ubiquitous in developing regions. Smart cards are cards with memory and a processor, and are ideal for authentication and secure applications. The combination of these two technologies is quite compelling. Smart card standards exist for proximity cards (ISO 14443) or vicinity cards (ISO 15693)[3]. Both standards use the popular Radio Frequency Identification (RFID) technology. FID was developed for automatic identification systems. RFID systems have two components: transponder (tag) and transceiver (reader or writer). The transceiver emits an electromagnetic signal that activates the tag and enables it to read from and write to the tag. RFID readers are small enough to integrate them into mobile phones[5]. Near Field Communication (NFC) is an extension of RFID. NFC is a short-range radio technology that operates at 13.56 MHz and covers distances up to 10 cm with possible data rates of up to 424 Kbit/sec. A 'classic' NFC transaction takes about 200-500ms. NFC was standardized in ISO 18092 and is compatible to ISO standards 14443 and 15693 mentioned above, and also to Sony's FeliCa contactless smart card system[3]. NFC provides for easy and intuitive interaction. NFC communication is triggered when two NFC-compatible devices are brought within close proximity, around four centimetres. Because the transmission range is so short, NFC-based transactions are inherently secure[3][5].

When compared to other short-range radio technologies, NFC is extremely short range. This makes it *people-centric*. Other short-range communication technologies, like RFID, have similar characteristics, while others are completely different yet complimentary to NFC. For example, Bluetooth and infrared can be combined with NFC in innovative ways. The main value of a secure NFC connection is that it can guarantee the confidentiality of data stored in secured memory. Authentication support is provided by encrypting transmitted data with a private key stored in the secured memory of the device. Secure storage is required for services like virtual money transfer, electronic ticketing, and electronic keys.

III. PRELIMINARY SURVEY

We conducted a preliminary survey to learn about the needs for such mobile services amongst rural inhabitants in South Africa. We interviewed forty students from rural areas enrolled at the University of the Western Cape (UWC) in a controlled environment in the laboratory. We showed them MIDlet applications using the NFC manager with Nokia 6212 Classic and 6313 emulation on a PC. We observed their interaction with the demo and conducted semi-structured interviews to get their feedback. 39 of 40 users found the system user friendly, effective and efficient. 34 users thought it had good performance and only 25 said they would trust such a system enough with their own money. When asked for additional comment, fifteen users said they would like to see more speed and nineteen users indicated that they had fears of security breaches, but admitted that the system worked.

IV. EXPERIMENTAL DESIGN

Based on positive feedback from the preliminary survey, we began to model a contactless smart card architecture with NFC. We have performed a requirements analysis of WIZZIT, shown in Figure 1, in order to produce a clone that we can work with in the laboratory. We intend to perform experimentation with the WIZZIT clone prototype in a controlled environment, similar to how we conducted the preliminary survey.

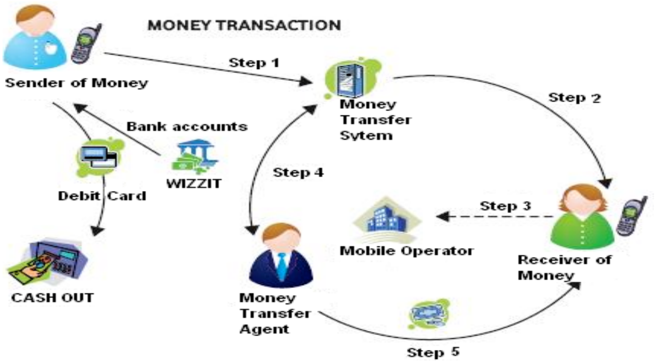

Figure 1: MTN WIZZIT system high-level design for money remittance

The prototype will require an NFC application programmatic interface (API). The API will use a contactless communication API and the Generic Communication Framework (GCF). J2ME and Java Card technology will help ensure secure interoperability when programming the mobile device.

Figure 2 shows a possible deployment scenario. The sender residing in an urban area purchases virtual cash with physical money at a registered agent outlet (AO). An AO can be any tuck shop owner who has an account with the mobile web server. To purchase virtual cash, both the AO and the sender need the software on their mobile devices that they bring close to a third NFC-enabled authentication device. The reverse transaction is the case when the receiver provides the authentication identification number of a transaction done by a sender and wants to trade virtual cash for physical cash with the AO. This means the AO provides physical cash for virtual cash. The third NFC device communicates with the server in place of human input and output. The device is fast and accurate, and allows for intuitive user interaction with a simple touch of a cell phone to the authentication device.

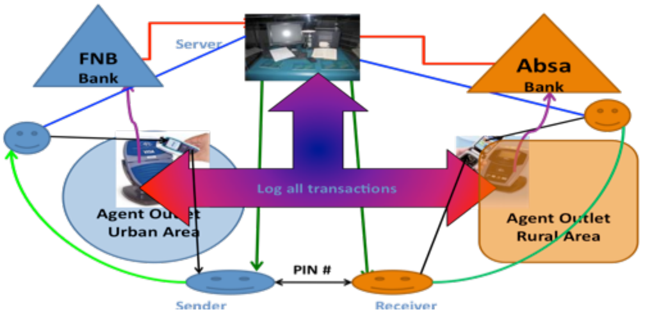

Figure 2: Use case scenario for mobile cash transfer.

V. CONCLUSION AND FUTURE WORK

According to related work and a preliminary survey conducted with UWC students from rural areas, mobile phones appear to offer an intriguing way to bank the unbanked. We argued that NFC can be a useful technology to design and provide mobile financial services. For the laboratory experiment, we also intend to develop a second clone for M-PESA. Both M-PESA and WIZZIT services are proprietary and we must infer their architecture. Our system will be fully open source. With two clones, we envision the provision of middleware to enable secure interoperability between the two different NFC-enhanced clones.

REFERENCES

[1] J. Donner & C.A. Tellez, Mobile banking and economic development: linking adoption, impact, and use, *Asian Journal of Communication*, 18, 2008, 318-332.

[2] R. Duncombe and R. Boateng, Mobile phones and financial services in developing countries: A review of concepts, methods, issues, evidence and future research directions,*Centre for Development Informatics*, 2009.

[3] S. Ortiz Jr., Is near-field communication close to success?,*IEEE Computer*, 39, 2006, 18-20.

[4] N. Hughes and S. Lonie, M-PESA: Mobile money for the unbanked: Turning cellphones into 24-Hour tellers in Kenya," *Innovations: Technology, Governance, Globalization*, 2:1-2, 2007, 63-81.

[5] N. Ichinose, Mobile e-ticket and e-membership services,*NEC Journal of Advanced Technology*, 1(3), 2004, 184-187.

Adeola O. Poroye is an MSc student in computer science at the University of the Western Cape (UWC) with the Bridging Applications and Networks Group (BANG).

William D. Tucker is a senior lecturer in computer science at UWC and leads BANG research there.

Michael Norman is a senior lecturer in computer science at UWC. His main interest is software engineering.