Paying with a Selfie: A Hybrid Micro-payment Framework Based on Visual Cryptography

Stelvio Cimato[1], Ernesto Damiani[1,2], Fulvio Frati[1(✉)], Joël T. Hounsou[3], and Judicaël Tandjiékpon[3]

[1] Department of Computer Science, Università degli Studi di Milano, Milan, Italy
{stelvio.cimato,fulvio.frati}@unimi.it
[2] Etisalat British Telecom Innovation Center, Khalifa University, Abu Dhabi, UAE
ernesto.damiani@kustar.ac.ae
[3] Institut de Mathématiques et de Sciences Physiques, Porto Novo, Benin
joelhoun@gmail.com, judicaeltandjiekpon@yahoo.fr

Abstract. In developing countries, the mobile revolution is happening in these days, and technology is now improving life conditions and providing new opportunities for the developing of the economies. In this paper, we provide a micro-payment framework that can be used to conclude everyday financial transactions. The novelty of the approach relies on the usage of techniques of easy understanding and application, even for uncultured people. The security of the system is also ensured by exploiting visual cryptography schemes, whose reconstruction phase requires no particular technical skills and relies only on human activities. The description of usage scenarios and the prototypal architecture of the framework are provided together with the initial plan for the experimental deployment.

Keywords: Micro-payment · Visual cryptography · Mobile

1 Introduction

A common feature of nowadays is the ubiquitous usage of information and communication technologies for different activities in everyday life. In developed economies, mobile phones are considered a normal part of the life, and the functions they provide extend the usual way in which customers do business, get educated or informed, and socialize, getting in touch with family and friends through emails, messaging, and social networks [9].

Even in developing countries, where satisfying basic needs often is an issue, the number of people accessing to mobile phones is surprisingly increasing from year to year. According to a report from IAMAI (Internet and Mobile Association of India), in 2012 there were 120 million people connected to the internet each week (doubling the total population of the UK, but getting less than 10 % of Indian population). According to recent reports, there are currently more than four billion mobile phones across the world, of which 64 % are used in a developing country [1].

The possibility to have easily simple voice and text communication has started a revolution in accessing financial, health, agricultural, and educational services for many

R. Glitho et al. (Eds.): AFRICOMM 2015, LNICST 171, pp. 136–141, 2016.
DOI: 10.1007/978-3-319-43696-8_15

communities, increasing the working opportunities. As an example, many people living in rural areas of Africa and Asia have started using SMS services to find out daily prices of agricultural goods, to improve their bargaining position in local markets, and to select markets that offer the maximum income [2]. Another example of the possibilities offered by the connection to remote services comes from the UNICEF's RapidSMS initiative, which is a SMS-based open-source framework for the collection of dynamic data. Thanks to this initiative across six countries in Sub-Saharan Africa, 200,000 users in some of the most underserved and rural communities can access health services and receive support from the central places, saving money and, sometimes, lives. In Ghana, the same service is used by a local entrepreneur to monitor the sales of cook stoves around the country [2].

The process that in the rest of the world is replacing many paper-based procedures with digital information processing, is of utmost importance in the developing economies, where it can support the creation of new business opportunities and overcome some of the constraints coming from the cultural and social context. A field that is in rapid expansion is the development of mobile digital-money frameworks, giving the possibility to conclude transactions and/or transfer small amounts of money among users. Airtime [3] and MPESA [4] are two examples of mobile cash transfer systems that are being used in different countries to provide citizens with financial services that can significantly improve their lives. Still several challenges remain to be solved, including the need to overcome cultural barriers and support trust in non-traditional financial services. Applications need to be developed taking into account a better analysis of the ways in which people interact with money in developing countries, being flexible enough to be customized to different cultural patterns. In this paper, we present a mobile payment framework that leverages on face-to-face exchanges, where pictures taken with mobile phones are used to support the successful conclusion of a financial transaction. Trust is enhanced by relying on Visual Cryptography (VC) schemes that make possible the creation of shares, whose ownership ensures the correctness of the transaction [5]. The novelty of the proposed approach relies on the usage of simple techniques such as taking pictures and over-stacking images. Such actions are of easy understanding also for uncultured people. Today, people of all cultural backgrounds take pictures or selfies, since even the cheapest smartphones enable photo taking and require virtually no training or technology awareness. The human visual system has always been used by humans to establish the context (purchaser/supplier roles, object of the transaction, price) of commercial transactions. In our system, group selfies are used as context representations, where all the parties participating in a payment protocol can be represented in a self-validating way: the purchaser, the supplier, the purchased goods or service, the amount, time, and place of the transaction. On the other side, visual cryptography is used as a tool to build systems where the degree of trustworthiness that the user needs to have in the system is reduced. VC is a technique where a secret image is split into random-looking images printed on transparencies [6]. The most relevant property of VC schemes is that the reconstruction of the original image can be performed by simply stacking the shares, using the human visual system to perform the decoding operation, releasing any need for trust in the hardware. Furthermore, the computation of the shares requires simple procedures and low computational power. In literature, an

example of hybrid systems, where visual cryptography is used as a tool to provide additional trust without leveraging on the digital equipment is Chaum's voting system [7], while a complete survey of applications of VC can be found in Cimato and Yang (2011).

2 Usage Scenarios

The mobile payment system we propose is not intended to replace the existing payment infrastructures, but to extend their reach. The goal is to enable commercial transactions in low or no connectivity areas involving non-IT-savvy or even illiterate parties. All parties must do at the time of purchase is *(i)* take a group selfie, *(ii)* compute and exchange shares. Shares are then sent to a trusted service point who reconstructs the image and (interacting with a traditional payment infrastructure) ensures that the supplier gets the cash, and that the buyer gets the goods. The proposed system supports three transaction styles, of which a simplified description is given in the following.

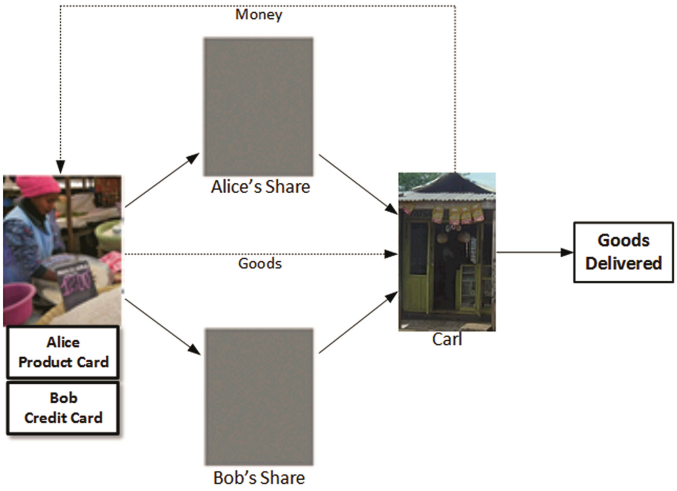

Fig. 1. *Cash and Carry* transaction style.

Cash then Carry. Alice and Bob meet somewhere outside the range of the mobile network. They both carry a simple phone. In order to commit to selling a product/service to Bob, Alice takes out a pre-marked product card (with her name, the product name and an amount, say 10 cents) and gives it to Bob. In turn, Bob takes Alice's product card, puts it and his own micro-credit card side by side and takes a photo with his phone. Bob's phone contains a simple app that computes two visual shares of the picture. One share stays with Bob, the other goes to Alice. Alice gets back her product card and keeps her product. Once Bob and Alice get mobile coverage (without needing to sync and in no particular order), they send their shares to Carl, a trusted operator who runs a point-of-service equipped with a desktop computer and an Internet connection. Carl puts together the two shares, uses the image to debit Bob's micro-credit card, prepares 10

cents cash, and sends a message to Alice. Alice drops by Carl's shop, gets the money and leaves the product, which can be delivered to Bob. If Carl receives only one share, the missing party is blacklisted. The scenario is depicted in Fig. 1.

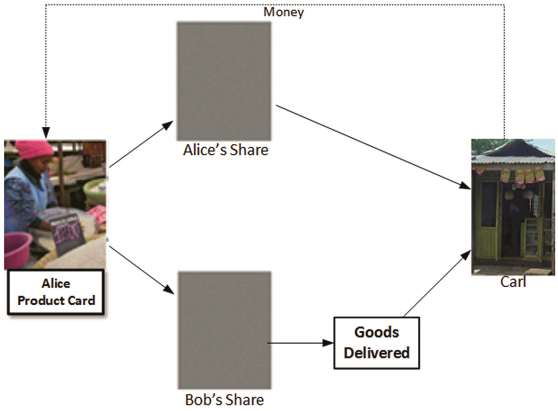

Fig. 2. *Carry then Cash* transaction style.

Carry then Cash. In this style (see Fig. 2), when Alice gets her share, she directly delivers the good to Bob. Alice and Bob later sends their shares to Carl, who notifies Alice to pass by the point of service and redeem the share to obtain the cash. Alice can decide to wait until notified amounts add up to a given value, or leave permanent money transfer instructions to Carl. If Carl receives only one share of the transaction, the missing party is blacklisted and will be excluded from the service.

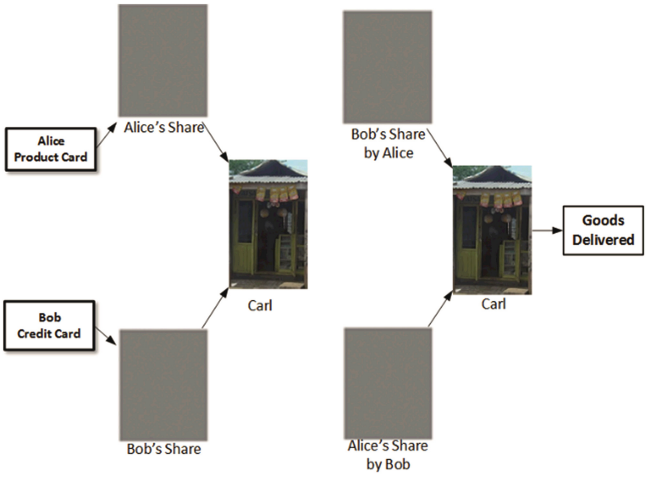

Fig. 3. *Guaranteed Future Contract* transaction style.

Guaranteed Future Contract. This style, depicted in Fig. 3, requires two photos, one of the micro-credit card and the other of the product card. First, Carl collects one share of Bob's micro-credit card and of Alice's product card.

At the time of transaction, Alice collects the other share of Bob's credit card and gives Bob the other share of her product card. When Alice comes to Carl's point of service, she matches the other share of Bob's card held by Carl. Carl debits Bob's micro-credit account, beyond Bob's control to pull out from the transaction. In turn, Bob matches the product card share with the one stored by Carl on Alice's behalf and will collect the product without Alice being able to pull out.

3 Architecture of the Framework

The mobile payment framework presented in this paper will be implemented as a simple software toolkit that includes three components (Fig. 4):

- **The share generator and share stacker utilities.** The share generator utility will create the shares and will target cheap smartphones, including the ones designed with developing countries in mind, in the line of Mozilla's $25 smartphone idea. The share stacker will be available under smartphone, tablet, and desktop platform, and it will reconstruct the image using the available shares.
- **The integrator tool.** This component will be installed at the point of service and act as a glue between share stacker and the current systems handling e-payments and money transfers in developing countries. The integrator prototype will be built according to West Africa specifications (Benin, Ghana, Togo and Nigeria)[1] [8].

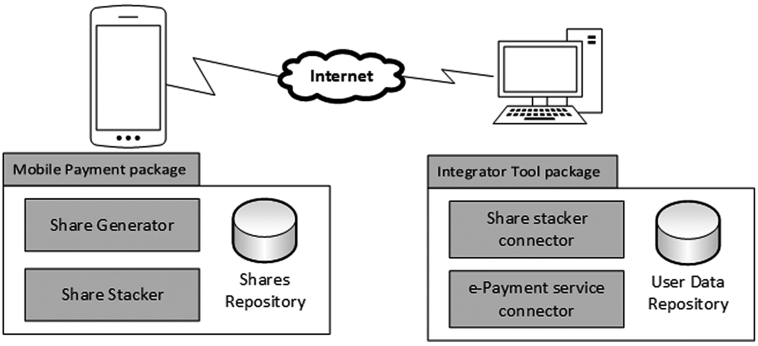

Fig. 4. Mobile payment framework component diagram.

4 Conclusions and Future Work

The continuing growth of mobile devices in developing countries represents a tremendous business opportunity. The features of this new potential market differ completely

[1] Source: http://www.itu.int/ITU-D/cyb/publications/archive/wmrcjune00/ntoko.html.

from the ones of the occidental world, where, for example, companies in Silicon Valley are fighting to develop the top app in a certain category. In developing countries, business developers are required to be able to think the design of their applications from a different viewpoint, considering the different contexts, environmental constraints and scenarios, and the motivations, experiences, needs of end users. The mobile payment framework we propose faces some of these challenges, not requiring any specific technological skill for its use, and, at the same time, relying on strong security techniques such as visual cryptography. We plan to perform functional and acceptance tests in collaboration with mobile phone companies operating in the rural area of Porto Novo (Benin), where many of the features above described are present. Although the illiteracy level in Benin reaches 60 % in rural areas, virtually everyone has a mobile phone. The framework will be tested out by a selected group of students of the local University, coordinated by graduate students and professors. Specific acceptance test and survey will be administered in order to evaluate the quality of the service and the user experience, to evaluate how and in which measure such service could be useful in rural areas. In particular, the test will report the number of transactions, the amount of exchanged money, and the number of users that have been blacklisted for misusing the service.

References

1. Business case studies: using technology to improve economies (2015). http://businesscasestudies.co.uk/vodafone/using-technology-to-improve-economies/
2. Kochi, E.: How the future of mobile lies in the developing world (2012). http://techcrunch.com/2012/05/27/mobile-developing-world/
3. The Economist: Airtime is money (2015). http://www.economist.com/news/finance-and-economics/21569744-use-pre-paid-mobile-phone-minutes-currency-airtime-money
4. Safaricom: M-PESA (2015). http://www.safaricom.co.ke/personal/m-pesa
5. Cimato, S., Yang, C.-N.: Visual Cryptography and Secret Image Sharing. CRC Press Inc., Boca Raton (2011)
6. Naor, M., Shamir, A.: Visual cryptography. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 1–12. Springer, Heidelberg (1995)
7. Chaum, D.: Secret-ballot receipts: true voter-verifiable elections. IEEE Secur. Priv. **2**(1), 38–47 (2004)
8. Jagun, A., Heeks, R., Whalley, J.: The impact of mobile telephony on developing country micro-enterprise: a nigerian case study. Inf. Technol. Int. Dev. **4**(4), 47–65 (2008)
9. Brazier, C.: Computers and cellphones in the developing world (2013). http://newint.org/books/reference/world-development/case-studies/2013/03/14/computers-cellphones-in-developing-world/