A NEED FOR PEER-TO-PEER STRONG LOCAL AUTHENTICATION PROTOCOL (P2PSLAP) IN MOBILE BANKING

Bossi Masamila

School of Computing, Dublin Institute of Technology, Dublin, Ireland

ABSTRACT

Mobile phones are considered to be the most common devices in history of humankind. They have involved in financial transaction such as mobile banking and mobile payment, which include sensitive information. Public key cryptography is the proven solution that can provide secure transaction at every point of interaction in mobile banking value chain. This paper proposes a need for peer-to-peer Strong Local Authentication Protocol (p2pSLAP) for Mobile Banking Transaction that implements a peer-to-peer architecture to provide local authentication mechanism between the customer and the agent. It employs public key infrastructure (PKI).

KEYWORDS

Local Authentication Protocols, Security, Mobile Banking, Mobile Payment

1. INTRODUCTION

Mobile phone is without doubt one of the most explosive developments ever to have taken place in the telecommunications industry. As the result of proliferation of mobile phone, more sophisticated applications such as SMS, Internet, MMS, mobile commerce, mobile marketing and mobile banking are becoming commonplace [1]. For the world's poorest countries, mobile phone presents the best chance of bringing the power of telecommunications to economically disadvantaged or isolated communities.

Financial services provided through mobile banking technologies have multiple configurations, goals, and characteristics. Depending on the combinations of agents, technologies and objectives they may have banking features, which results mobile banking services. They may have transaction payment features, which are know as mobile payments. They may be called mobile money if they replicate the concept of digital money [3].

This proliferation of mobile banking solutions has led to lack of cohesive technology standards that can provide a universal mode of payment. This lack of common standard creates local and fragmented versions of mobile banking offered by different stakeholders, which leads to lack of end-to-end security [4]. For instance, mobile banking service providers depend on agents to support customer acquisition and manage cash withdrawal and deposits. During customer registration, agents are exposed to customer's sensitive information such as name, mobile number, Identity Card details, passport details and other credentials that are used for identification and authentication purpose. This present a huge problem as these sensitive information can be compromised. Any misuse of this information can result in serious business damage, repercussion

DOI : 10.5121/ijnsa.2013.5603

for non-compliance with various governmental rules and regulations and can also lead to the loss of customer confidence. This prompts the need to enhance security at the point of interaction between the customer and the agent.

On the other hand, mobile payment systems involve the integration of different industries such as mobile network operator, bank, Merchants, retailer, agents, and utility companies. These industries handle different information systems that vary in size, they are exposed to different security threats, and they have different security schemes. However, interconnecting these industries gives some common advantage characteristics, but the costs of poor security are often distributed [1]. In this paper we propose a peer-to-peer Strong Local Authentication Protocol (p2pSLAP) for Mobile Banking Transaction. p2pSLAP is designed to authenticate participants (i.e. customer and agent) with mobile phones at point of interaction without disclosure of their identification and authentication credentials. p2pSLAP will provide a common local authentication mechanism that can pave a way to open-loop mobile banking services.

This paper is structured as follows: Section one present an introduction to mobile payment, section two present the proliferation of mobile payment services, it discussed the mobile payment landscape. Section three presents related works. It explores works of other rearchers that are closely related to this work. Section four presents security concern in mobile payment services. Section five presents the design requirement for a proposed (p2pSLAP) mobile payment model for developing markets and section five presents concluding remarks for this paper.

2. PROLIFERATION OF MOBILE PAYMENT SERVICES

The spreading of mobile phone and increasing values of their applications across the world depends on the number of factors such as technology change, economic difference, technology adaptability, culture and regulations [5]. Equally, the spread and application of mobile payment across the world are not uniform.

This section will give a brief discussion on the proliferation of mobile payment, starting with few cases in developed countries, which will be followed by cases from developing countries.

In most of the developed economies people have wide and easy access to the banking system, with an extensive usage of internet systems and credit cards. Most retail establishments have facilities that can accept both internet based and credit card transaction in addition to cash and such facilities can be easily accessed in local service areas such as taxi cabs and even parking meters. For example, in Japan the giant mobile operator DoCoMo extended the functionality of the SIM card by including credit card services. By using contactless FeliCa Technology, the account represented by the chip in the phone can be charged by waving the phone in close proximity to FeliCa point of sale device. FeliCa technology, is deployed in mass transit system in Japan, by NFC vendors such as Mobile Suica, Osaif-Keita system. In South Korea where the mobile market access is almost saturated, consolidations between mobile carriers and banks have been formed for different business strategies. Subscribers exploit their mobile phones to shop in virtual malls, and online boutiques and are able to use their handsets for almost any type of payment; credit card, cash, prepaid vouchers and post-paid subscribers billing [6].

In developed markets, there is a large number of prepaid users who use their phone for text and voice as well as recharging handsets on the prepaid based system. These users are an ideal target for mobile payment services. They have no access to any bank, and they are not connected to the internet or credit card systems, but the can perform financial transactions that evidence their ability to purchase and activate prepaid cards for additional credit and transfer air-time credit to their friends, and comrades [5]

In Philippines, a middle income developing country, major mobile service provider Globe Telecoms and Smart Communications have developed a larger scale mobile banking services. Their product such as G-cash and Smart Money are used to transfer money around the country and circumventing the banking system [6]. Smart is associated with Banco D'Oro in offering SmartMoney and Maestro debit card that can enable SMART client to use conventional ATM and POS devices and can be used for mobile payment services. Globe Telecoms provides G-cash product that supports local and international remittances transfers and payments. M-Pesa is the mobile banking services offered by Safaricom in Kenya [5]. M-Pesa services are available to subscribers with or without a bank account, and supports subscriber to deposit cash, transfer money, withdraw money through M-Pesa urgent or participating ATM network, buy Safaricom airtime, pay bills and manage M-PESA account [7].

Most of these successful deployments have been through consolidations. Consolidation provides shared access that creates the opportunity to gain greater returns from all sorts of infrastructure investments. For instance, Vodafone partnered with Safaricom in Kenya for M-Pesa product and has extended the same version to Tanzania and Afghanistan. AirtelMoney and Western Union are working together to deliver mobile money transfer services in Africa and the Middle East through AirtelMoneys Zap platform. In Philippines, Western Union service allows mobile subscribers to receive funds sent from selected Western Union Agent locations directly into their mobile phone. MoneyGram International and SMART Communications enable SMART subscribers to receive money transfer to their SMART Money account on their mobile phones. Globe Telecoms has partnered with a number of financial institutions in the Philippines, in order to mitigate the legal constraints of running the financial service while holding a telecommunication license [8]. In India, the Nokia Money initiative based on Obopays platform for developing market is designed to work in partnership with multiple network operators and banks, involving distributors and merchants in a dynamic open ecosystem.

With current trend of mobile phone penetration rate and availability of mobile banking platforms, the spread and use of mobile payment services in developing markets is encouraging.

3. RELATED WORKS

Literature has a fair amount of past work looking at mobile payment and mobile banking on aspects such as business markets, payment processes, payment methods and standards in wireless payments [9]. [10] offers topologies of different mobile banking business models on which p2pSLAP falls under the non-banklead mobile banking business model. [10] also highlights mobile banking technologies. [2] a site that is dedicated for tracking all mobile deployment in the world, publishes bank penetration statistics, mobile banking deployments and their corresponding technologies. Currently, mobile banking are based on SMS, USSD, WAP or IVR (interactive Voice Response) as the trusted channel to carry mobile banking transactions [10]. For instance, M-Pesa, AirtelMoney, SmartMoney all depends on GSM/3G networks.

[11] provides a summary of various wireless technologies for mobile payment such as 2G, 2.5G, 3G, infrared, NFC, and Bluetooth. In his work, we leverage our work on Bluetooth as it is almost available to every make of mobile phone as we focus on local communication between mobile phones for mobile banking transaction. Our work focuses local authentication between the agent and the customer. [12] presented Signet: Low-cost auditable transaction Using SIMs and Mobile phone that can securely enable in-personal transactions in developing markets. It provides a ground work for developing mobile financial transactions in a trusted environment in a close range independent of the main network. Their solution can accommodate network outage issues through the provision of a local receipt. However, this solution is suitable for digital money it

does not address mobile banking transactions. [13] presented an interested paper that is centered on the application of Bluetooth for building trusted mobile device as an authenticator. It aims to improve usability, as there is no password required, enhance security, since most common attacks (such as social engineering) are ineffective, and with a quasi-free features for zero login time. It can be extended to accommodate applications such as payment systems, remote control of appliances and services, and transactions on unattended dispensers of goods such as packing meters, and petrol stations. This work together with [14] are appropriate on the design requirement mobile phone as the authenticator, they provide the required components and other access mechanisms. mFerio: [15] mFerio, a secure peer-to-peer (P2P) mobile cash payment system that uses NFC technology. With mFerion a user uses Fingerprint to authenticate him/her to mFerio MIDlet application for transaction. The authentication between participating parts is based on the assumption that NFC require the two devices to be very close, that the closest device is the actual device the participating part is communication with. The work given in [16] presents a peer-to-peer m-payment system (P2P) to allows mobile users to conduct mobile payments over the Bluetooth communications and to perform related secured transactions. P2P-Paid system uses 2-dimensional secure protocol integrated several security solutions which involve the use of Payment authority in authentication phase of participating parties prior to the transaction.

Most mobile banking systems relay on authentication provided by the third party for example mobile network operators (MNO) and banks. They depend on online support to complete authentication. According to [17] authentication only verifies the names and users have difficulty to link the authenticated name the image of the desired entity in their minds. For example, the problem of faking the third party system, spoofing, as it appended to the agent in M-Pesa mobile banking platform [18]. Therefore online authentication does not meet the need for secure mobile banking transactions. In order to provide end-to-end security on which users can transact securely from anywhere any time, method of bootstrapping security directly between the customer and the agent is necessary.

4. SECURITY CONCERNED IN MOBILE PAYMENT SYSTEMS

Security is the major concern in the adoption of mobile payment. As such the adoption and wide spread application of mobile payment depends on the strength of security. The following are security concerns in mobile payment systems for developing markets:

- Larger network that have emerged as the result of consolidation are prone to security implications. Applications for mobile payment solutions are complex in nature with mismatching set of possibilities that are caused by the involvement of multiple players [19, 20]. The lines differentiating these players have become blurred with the crossover of mobile phone. The benefit of consolidation and sharing infrastructure are apparent, but the costs of poor security are often distributed.
- Proliferation of mobile payment technologies has led to lack of cohesive technology standards that can provide a universal mode of payment. This lack of common standard creates local and fragmented version of mobile payment offered by different stakeholders, which leads to lack of end-to-end security.
- In developing markets, mobile payment service providers depend on agents for customer acquisition and for managing liquidity. They access customer's sensitive information such as the user name, mobile number and other credentials that are used for identification and authentication purpose. These agents are not well equipped to preserve customer's sensitive information and can easily lead to information leakage. Any loss of control over protected or sensitive information by service providers is a serious threat to business operations as well as, potentially, customer security [21].

- With the current technology and the wide spread of mobile applications, mobile devices that use mobile payments and users cause major risk to the security of mobile payment. Mobile devices can be easily infected with virus that could perform unauthorized payments or send user information such as PIN codes through close range communication technologies such as bluetooth, Radio frequency identification (RFID) and Near Field Communication (NFC) [23].
- Spoofing issues as it was report in M-Pesa platform. The fraudsters' withdrawal cash from the agent and fooled the agent by sending a fakes response from M-Pesa platform [18].

For wide application and usability of mobile money, a proposed p2pSLAP local authentication that is intended for developing market, must address these security concern.

5. THE NEED FOR STRONG LOCAL AUTHENTICATION

In order to keep a mobile banking system secure [24] and [25] outlined seven security requirements that any security service should be able to accomplish:

- **Confidentiality:** The confidentiality of sensitive information needs to be protected. Unauthorized people should not be able to gain access to confidential material.
- **Integrity:** Mobile service providers need to protect the integrity of data transmitted over wireless networks from the point of transmission to the point of delivery. The system should be able check that the data is the same at the points of origin and destination.
- **Availability:** This is about ensuring that services are available on demand, which often means 24 hours a day, seven days a week. This is related to with security because a security breach can lead to downtime, for example Denial of Service and virus attacks.
- **Non-repudiation:** Non-repudiation ensures transactions are legally binding. This is critical for electronic banking systems because it prevents complication from regulation violation.
- **Authorization:** Authorization ensures transactions are endorsed and authorized by the parties involved.
- **Authentication:** Authentication is the process of identifying the user to be whom they claim to be.
- **Privacy:** Privacy is a prominent issue in mobile banking. Mobile banking service provider must meet the legal requirements.

With the above security requirements, authentication is a basic building block of security. Once the authenticated communication channels are established, other security services such as confidentiality, privacy, authorization, integrity and non-repudiation can be realised [27]. The compromise of the authentication service breaks down the whole security system on which the provision of other services cannot proceed. Traditionally, authentication has concentrated on the notion of entity authentication, which provides assurance of who is the subject of a secure interaction. Security over the mobile platform is more critical due to the open nature of wireless networks. The vulnerability of mobile banking and underlying infrastructure present a big security threat [28]. So designing a security solution for mobile banking must address the nature of the mobile device and the environment on which it operates.

Most mobile banking systems relay on authentication provided by the third party for example mobile network operators (MNO) and banks. They depend on online support to complete authentication. According to [17] authentication only verifies the names and users have difficulty to link the authenticated name the image of the desired entity in their minds. For example, the

problem of faking the third party system, spoofing, as it appended to the agent in M-Pesa mobile banking platform [18]. Therefore online authentication does not meet the need for secure mobile banking transactions. In order to provide end-to-end security on which users can transact securely from anywhere any time, method of bootstrapping security directly between the customer and the agent is necessary.

6. P2PSLAP DESIGN REQUIREMENTS

This section presents the key components for p2pSLAP:

1. **Cryptographic Design:** Lightweight PKI that are developed specifically for resource constrained devices such as mobile phone are available. Bouncy Castle implements four asymmetric engines in the lightweight API- RSA, ElGamal, Elliptical Curve Cryptography (ECC) and NTRU. The choice on which algorithm to use in constrained environments are given in [29]. With authentication, p2pSLAP should provide other security services such as confidentiality, integrity and non-repudiation, thus Hash function, encryption algorithm are the integral part of p2pSLAP. SATSA is increasing becoming an integral part of handsets is needed to provide a secure environment for p2pSLAP application

2. **Application (MIDlet):** p2pSLAP application is designed with dual mode (i.e. it can be in customer mode or agent mode) will be distributed as the package to users. This package is based on Java ME platform. Java ME is the predominant mobile technology as it is being supported by a wide range of mobile device operating systems. In p2pSLAP setup, the mobile banking service provider, which in most cases is the network operator, will distribute p2pSLAP application as the JAR. Figure 1 shows UML key classes of p2pSLAP.

    - **UserInterface class:** UserInterface class as the method to provide user interface to p2SLAP application.
    - **DSignature class:** DSignature class has the method to read a private key and generate a digital signature.
    - **KStorage class:** KStorage class has the method to read keys from a secure storage
    - **MBPtk class:** MBPtk has the method to access mobile banking toolkit
    - **Controller class:**It is the main class in package. It performs most of the actions and coordinates the tasks done by other classes.

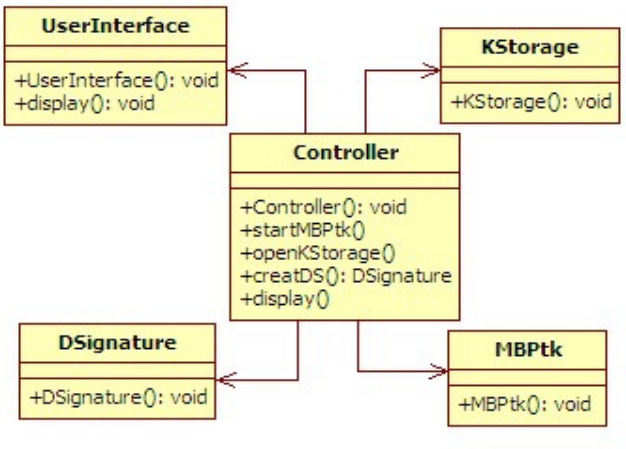

Figure 1. p2pSLAP MIDlet class diagram

3. **Keys Distribution:** The main problem with PKI is the key management: The provider (MNO) with powerful server will host key generator and generate the keys once the customer requests for p2pSLAP algorithm. As with p2pSLAP, the keys will be distributed in JAR file format via over the air (OTA) upon customer request. The keys will be securely stored in the customer's SIM card (see Figure .2).

4. **Short-range Communication Technologies:** Most of short-range communication technologies such as RFID, NFC and Bluetooth are integral part of mobile phone. In this case, Bluetooth is preferred because it provides an adaptable platform for short-range wireless communication that is robust, easy to use, and secure. Its simple and extendible implementation allows it to be used for a wide range of applications mobile to mobile communications. Bluetooth technology provides a path to free portable devices from the restrictions of cables while retaining usability and reliability.

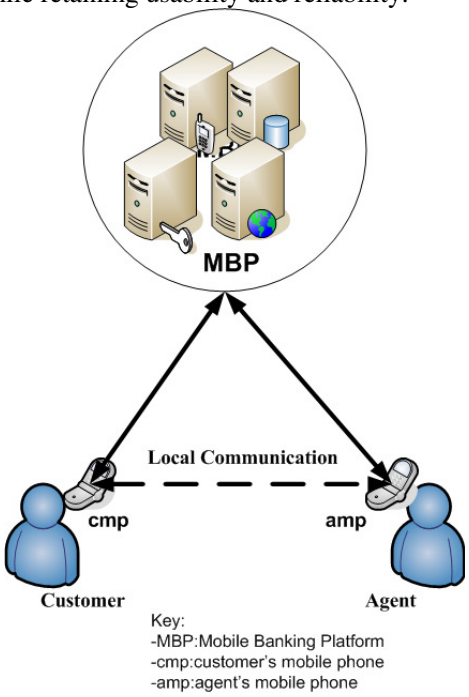

Figure 2. Mobile Payment Platform

7. CONCLUSION

The solution proposed by p2pSLAP provides security during the transmission process and can authenticate participants at the point of interaction (i.e between the customer and the agent). The implementation of p2pSLAP is based on the use of digital signature using asymmetric lightweight cryptographic algorithm. Through the use of lightweight public key cryptography, the p2pSLAP uses customer's/agent's private key to create the digital signature. The resulting signature has the key properties of non-repudiation and verifying the message integrity since signing. In order to provide for a valid digital signature it is imperative to keep a user's private key secure. Lightweight cryptography contributes to the security of smart objects networks because of its efficiency and smaller footprint. Another important thing to note in the design is that only Java ME can offer an independent device system operative solution as well as SIM card native possibilities.

REFERENCES

[1] Jenkins, B.: "Developing mobile money ecosystems", Washington, DC: International Finance Corporation and Harvard Kennedy School. (2008)

[2] MobileMoneyExchange,: Deployment tracker. http://www. wirelessintelligence.com/mobile-money/. (2012)

[3] Diniz, E. H., De Albuquerque, J. P., and Cernev, A. K.: "Mobile Money and Payment": a literature review based on academic and practitioner-oriented publications (2001-2011)."

[4] Lyman, T., Pickens, M., and Porteous, D.: "Regulating transformational branchless banking: mobile phones and other technology to increase access to finance," Focus Note, vol. 43. (2008)

[5] Donner, J.: Research approaches to mobile use in the developing world: A review of the literature. The Information Society 24(3), 140-159. (2008)

[6] Porteous, D.: The enabling environment for mobile banking in Africa. Bankable Frontiers Associates, Boston, USA, (2006)

[7] Ivatury, G., Mas, I.: The early experience with branchless banking. Consultative Group to Assist the Poor (CGAP), (2008)

[8] Mirembe, D., Kizito, J., Tuheirwe, D., Muyingi, H.: Model for Electronic Money Transfer for Low Resourced Environments: M-Cash. In Proc. Third International Conference on Broadband Communications, Information Technology Biomedical Applications, pp. 389-393. (2008)

[9] Streff, K. and Haar, J.: An Examination of Information Security in Mobile Banking Architecture. Journal of Information System Applied Research, 2(6). (2009)

[10] Krugel, G.: Mobile Banking Technology Options. FinMark Trust. (2007)

[11] Zmijewska, A.: Evaluating wireless technologies in mobile payments-a customer centric approach. In Mobile Business, 2005. ICMB 2005. International Conference on, pages 354362. (2005)

[12] Paik, M., Subramanian, L.: Signet: low-cost auditable transactions using SIMs and mobile phones. SIGOPS Oper. Syst. Rev. 43(4), pp. 73–78. (2009)

[13] Dellutri, F., Me, G., Strangio, M.: Local authentication with bluetooth enabled mobile devices. Proceedings of the Joint International Conference on Autonomic and Autonomous Systems and International Conference on Networking and Services', IEEE Computer Society, pp. 72. (2005)

[14] Kunyu, P., Jiande, Z., and Jing, Y.: An identity authentication system based on mobile phone token. In IEEE International Conference on Network Infrastructure and Digital Content, 2009. IC-NIDC 2009, pages 570575. (2009)

[15] Balan, R., Ramasubbu, N., Prakobphol, K., Christin, N., and Hong, J.: mFerio: the design and evaluation of a peer-to-peer mobile payment system. In Proceedings of the 7th international conference on Mobile systems, applications, and services, pages 291304. ACM. (2009)

[16] Gao, J., Edunuru, K., Cai, J., and Shim, S.: P2P-paid: a peer-to-peer wireless payment system. In Mobile Commerce and Services, 2005. WMCS05. The Second IEEE International Workshop on, pages 102111. (2005)

[17] Bangdao, C., Roscoe, A., Kainda, R., and Nguyen, L.: The missing link: Human interactive security protocols in mobile payment. In Proceedings of the 5th International Workshop on Security, IWSEC.(2010)

[18] Gmeltdown: M-pesa fraud - agents beware! http://www.gmeltdown.com/2010/02/ m-pesa-fraud-agents-beware.html (2010)

[19] Nie, J., Hu, X.: Mobile Banking Information Security and Protection Methods. International Conference on Computer Science and Software Engineering. (2008)

[20] Mallat, N., Rossi, M., Tuunainen, V.: Mobile banking services. Communications of the ACM, ACM New York, NY, USA 47(5), pp. 42–46. (2004)

[21] Pickens, M., Porteous, D., Rotman, S.: Scenarios for Branchless Banki in 2020. Technical report, CGAP and DFID. (2009)

[22] Krugel, G., Solin, M.; Desai, S., Paul, L., White, A.: Mobile Money for the Unbanked; Annual Report 2009. Technical report, GSMA (2009)

[23] Wang, P., Gonzalez, M., Hidalgo, C., Barabasi, A.: Understanding the spreading patterns of mobile phone viruses, Science 324(5930), 1071. (2009)

[24] Emmanuel, A. and Jacobs, B.: ”Mobile Banking in Developing Countries: Secure Framework for Delivery of SMS-banking Services,” Radboud University Nijmegan, The Netherland. (2007)

[25] Tang, J., Terziyan, V., and Veijalainen, J.: ”Distributed PIN verification scheme for improving security of mobile devices,” Mobile Networks and Applications, vol. 8, pp. 159–175. (2003)

[26] Creese, S., Goldsmith, M., Roscoe, B., and Zakiuddin, I.: “Authentication for pervasive computing”, Security in pervasive computing, pp. 439–488. (2004)

[27] Luo, H., Kong, J., Zerfor, P., Lu, S., and Zhang, L.: “Providing robust and ubiquitous security support for mobile ad-hoc networks.”(2001)

[28] Agarwal, S., Khapra, M., Menezes, B., and Uchat, N.: “Security Issues in Mobile Payment Systems,”Citeseer. (2007)

[29] Forns Rumbao, J. Rodriguez Rubio, F.: Digital Signature Platform on Mobile Devices MOBILITY 2011, The First International Conference on Mobile Services, Resources, and Users, 151-157. (2011)