ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering &Technology (IJARCET)
Volume 2, Issue 9, September 2013

Mobile Payment Security issues: a Comprehensive Survey

Shikha Nema*,
MCTA Branch
Ganga Ganga College of Technology
Jabalpur (M.P)

Neeraj Shukla*
Dept. of computer science
Gyan Ganga College of Technology,
Jabalpur (M.P)

Abstract

Using a mobile phone to make payments introduces traditional and trusted payment methods in the U.S. It also introduces several new technologies to support mobile payments. The unfamiliarity and complexity of the mobile device and associated technologies create security concerns for consumers who want to be confident that their personally identifiable information and actionable financial information are protected in storage and while being used to process a mobile payment transaction, whether that storage is on the mobile device or in the cloud. They want that their data cannot be intercepted at any time. About sensitive payment information being captured 'over the air,' or mobile phones being lost or stolen and personal data being shared inappropriately need to be addressed by stakeholders to satisfy consumers, merchants, and regulators. The security of each mobile technology platform will be a major contributor to its success and the ultimate broad adoption of mobile payments.

I. Introduction

The Near field communication1 (NFC) and cloud [2] technologies are widely address security for mobile payments at the retail point-of-sale (POS). It also provides a brief overview of security for two other mobile technology platforms, QR code [3] and direct carrier billing DCB [4]. Each technology manages and processes information uniquely hence security practices and issues will vary with the technology deployed by each payments platform provider. This can be used by consumers, regulators, and possibly other mobile stakeholders.

A key concept tied to the various mobile payment technologies is the wallet.

There are 3 types of wallets:-
1) Mobile wallet
2) Digital wallet
3) Hybrid wallet

This paper distinguishes between a mobile wallet and a digital wallet. A mobile wallet (e.g. for NFC), is a software application stored on the physical mobile phone to manage and initiate payments. The mobile wallet accesses the payment credentials (e.g., payment cards, bank account, coupons, loyalty, transit tickets, etc.) or actionable financial information, which are stored on the mobile phone in a trusted environment known as the secure element. The consumer must have the physical phone with him to enable the payment transaction by waving or tapping the mobile phone over an NFC- enabled terminal at a retail location.

A digital wallet stores the payment information on a secure remote server, also known as the cloud. A cloud-based or digital wallet stores actionable financial information remotely from the mobile device, and sends only tokens or authorizations to the actual mobile phone to initiate and authorize the payment at the point-of-sale (POS). Wireless service, either cellular or Wi-Fi, is needed to complete the digital wallet transaction. The primary difference from the NFC mobile wallet is that sensitive financial information is stored in the cloud, not on the mobile phone.

A hybrid wallet combines features of the mobile and digital wallets. The mobile payments provider leverages the security aspects of NFC with the added protection of storing the real payment credentials in the cloud. The consumer's financial information in the cloud is linked to a mobile phone through a unique identifier in the device. Account credentials used when making POS mobile purchases are accessed from the cloud when needed, but the payment transaction is still initiated using the NFC protocol to communicate from the mobile phone to the POS terminal.

II. NFC Mobile Payment

In the U.S., two primary mobile phone system standards are used—Global System for Mobile Communications (GSM) and Code Division Multiple Access (CDMA). The major difference between the two technologies is how they turn voice data into radio waves and how the carrier connects to the mobile phone. Other differences include the coverage area, data transfer speeds, and the type of hardware used. AT&T and T-Mobile use GSM technology, while Verizon and Sprint use CDMA in the U.S.[5] Generally, consumers are unaware of the differences between GSM or CDMA phones when making calls, sending text messages, or using other basic phone features, but there are some differences when applied to mobile payments.

III. NFC Mobile Payment Options

There are three NFC approaches for processing and storing sensitive consumer data in the mobile phone. Mobile payment stakeholders, including mobile network operators (MNO), financial institutions, card issuers, merchants, and payment processors, decide which option(s) to implement. Each approach is hardware-based and differs primarily on the placement of the secure element in the mobile phone.

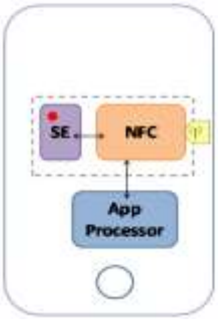
The secure element is essentially the component within the mobile device that provides the application, the network and the user with the appropriate level of security and identity management to assure the safe delivery of a particular service. It is an encrypted smart card chip that contains a dedicated microprocessor with an operating system, memory, an application environment, and security protocols, built to exacting standards and developed and delivered in controlled white room manufacturing environments. The secure element is used to safely store and execute sensitive applications, such as payment applications, on a mobile device, and store associated payment credentials and financial data.

Advantages and Disadvantages of Secure Element Placement Options

The most common secure element includes:
a) Embedded (hard-wired) in the mobile phone,
b) Loaded on a SIM8 card and
c) Loaded on a microsd card.

a) Embedded Secure Element

In the embedded NFC model, the secure element is soldered onto hardware in the mobile phone. The original equipment manufacturer (OEM) procures space on the secure element for issuing banks or other mobile payment providers, and is responsible for safely distributing the secure elements in the mobile handsets to consumers, who purchase embedded NFC mobile phones at various mobile retailers. MNOs coordinate with the handset manufacturers to ensure that authorized operating systems/applications work with the secure element.



1.1 Embedded secure element

An embedded secure element provides a common architecture for application developers, independent of the mobile phone technology
GSM or CDMA. A larger antenna built into the handset also offers a stronger communication signal between the mobile phone and merchant terminal. And, because secure elements are built

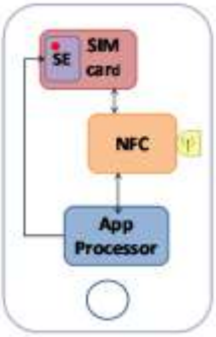
into mobile devices during the manufacturing process, they are relatively tamper-proof and less costly to produce relative to SIM and microsd options [9].

Disadvantage

1) One disadvantage of an embedded secure element is that it is not portable, making it difficult to transfer mobile payment applications and credentials between handsets.
2) This may be inconvenient for consumers when they need to transfer credentials and applications from an old phone to a new one.

b) Secure Element in the SIM Card

A SIM (Subscriber Identity Module) is a removable smart card used in many mobile phones. Each SIM card can hold multiple applications. GSM phones use the SIM card, while CDMA phones use their own version called CSIM. For mobile payments, the SIM card performs the secure element function.

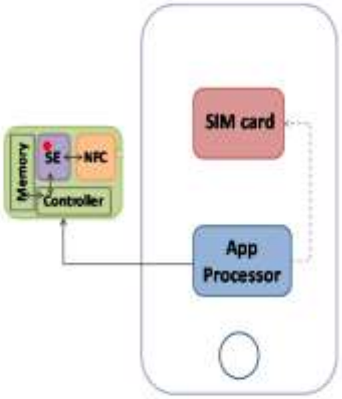


1.2 secure elements in sim card

c) Secure Element in microsd card

The third option is to put the secure element in a microsd card, which is a memory card used to store data. It is designed to integrate with the mobile phone by fitting into a specially designed slot on the device.

In the third option, payment card data is also encrypted and stored in the secure element, but the secure element resides in the microsd card. The portability of a microsd card is done through moving the secure element and associated payment data to any other mobile phone that has a microsd card slot with a microsd slot that fits over the phone.



1.3 microsd card based secure element

IV. Benefits & challenges of NFC mobile payment

According to a report from the Smart Card Alliance, “NFC-based contactless payment offers many security benefits” these are :-

(1) Payment credentials are stored in the secure element in the mobile wallet. Different passwords can be set-up to log on to the mobile device, and to activate the payment application that accesses the payment credentials in the secure element.

(2) When not in use, the NFC antenna can be disabled until needed so that unauthorized users cannot access the wallet.

(3) NFC is an extension of EMV15 chip technology, with the radio interface added.

(4) NFC payments include eliminating the cost of plastic card using the existing clearing and settlement channels.

Challenges

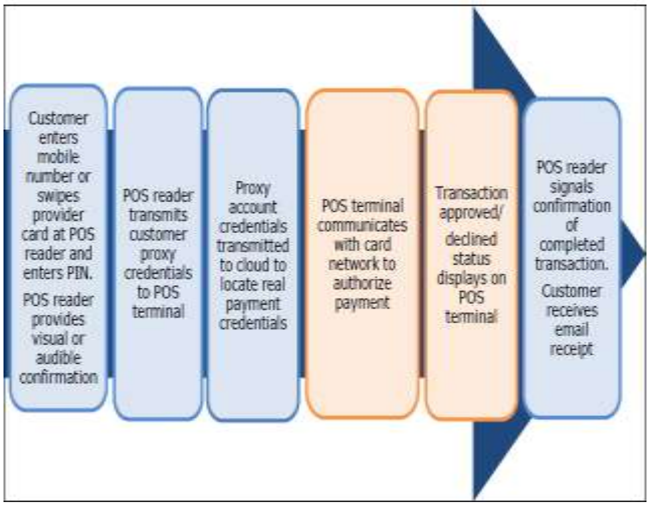
Work still needs to be done to develop an agreed upon set of technology standards for mobile phones, chips, and secure elements, and standards for provisioning and maintaining mobile payment credentials. Number of cross-industry participants engaged in the mobile payment process/value chain continues to grow, further complicating business models and customer-ownership. Finally, we need to remember that many consumers are still unfamiliar with NFC technology and require not only incentives, but also education regarding its safety and security when used for mobile payments, particularly with a mobile wallet.

V. Cloud Based Mobile Payment

In a cloud-based payment solution, both the consumer and the merchant must download the cloud-based application and subscribe to the service. Mobile payment credentials and account information stored on remotely located network servers – "in the cloud." Payment credentials accessible via an app on mobile phone with a phone number and PIN, or a physical card.

The mobile device becomes an extension of the POS terminal, which communicates information about the mobile payment transaction to the cloud for authentication. Consumers can access their account information in the cloud via mobile phone, e-mail address, mobile phone number, mobile browser, or mobile application. Once a cloud payment is completed, payment notification can be communicated via e-mail or SMS text messages.

Generally digital wallet uses the cloud based mobile payment.


Customer enters mobile number or swipes provider card at POS reader and enters PIN.
POS reader provides visual or audible confirmation
POS reader transmits customer proxy credentials to POS terminal
Proxy account credentials transmitted to cloud to locate real payment credentials
POS terminal communicates with card network to authorize payment
Transaction approved/ declined status displays on POS terminal
POS reader signals confirmation of completed transaction.
Customer receives email receipt

5.1 The cloud model

VI. Benefits & Challenges of Cloud Based Mobile Payment

Consumer familiarity -Consumer experience with use of other mobile apps may help them transition more quickly to a cloud-based mobile payment solution than an NFC mobile solution.

Portability - Cloud model is hardware agnostic, a consumer does not need to move his data if he switches mobile devices or upgrades his phone.

Improved security - The cloud solution provides security for payment credentials when they are stored for back-up. Because account credentials and sensitive data are stored in the cloud, no hardware secure element is needed. cloud can provide secure backup storage for NFC mobile payments transaction data.

Broader availability. Cloud apps are web or browser-based and accessible across different device/OS platforms, enabling the apps to run on many different mobile phones.

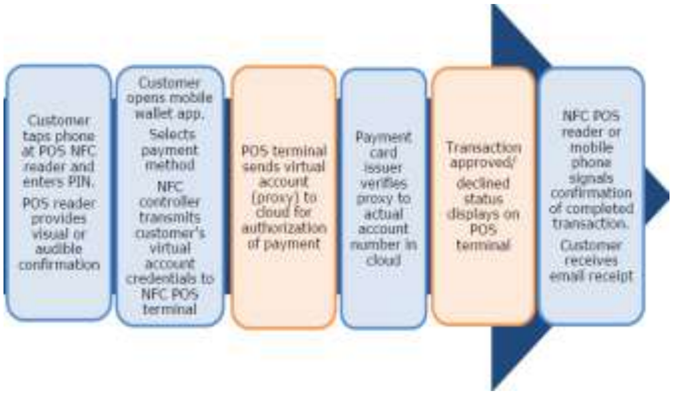
Challenges

Use of cloud-based mobile payment services requires both the merchant and the consumer to subscribe. While merchants do not need to implement NFC ,merchants must work with the mobile payments providers to implement additional infrastructure to accept cloud payments at the POS, and the customer must register with each individual merchant before making a payment.

Cloud payments require Internet connectivity. A transaction may not work or be interrupted due to connectivity issues, particularly if access to the cloud fails and there are no back-up payment credentials stored on the mobile phone. The most notable problem is the lack of quick mobile Internet access. Transactions may be slow depending on how the wallet is accessed, what the connection speed is, and how much data must be entered. A payment transaction may require more time because transmission to the cloud is slower than NFC to POS.

VII. Hybrid model for Both Digital & Mobile Wallet

Initiating a hybrid NFC-cloud mobile payment is the same process as an NFC-only payment, but the payment credentials are not stored locally on the mobile phone. Instead, a virtual account number or proxy is stored in the secure element and used in communication from the mobile phone to merchant's POS system, which is then used to identify the customer's real payment credentials which are encrypted and stored remotely on servers (the cloud). Neither the merchant nor the mobile phone's operating system has the real payment card information


Customer taps phone at POS NFC reader and enters PIN.
POS reader provides visual or audible confirmation
Customer opens mobile wallet app.
Selects payment method
NFC controller transmits customer's virtual account credentials to NFC POS terminal
POS terminal sends virtual account (proxy) to cloud for authorization of payment
Payment card issuer verifies proxy to actual account number in cloud
Transaction approved/ declined status displays on POS terminal
NFC POS reader or mobile phone signals confirmation of completed transaction.
Customer receives email receipt

7.1 Hybrid model

VIII. Task Ahead

Hybrid model can provide security of both types means it combines features of both digital & mobile wallet in a one wallet. It achieves the security using both NFC & cloud.

IX. Comparison between mobile Payment Technologies

		Advantage/ disadvantages
NFC Non Removable Secure Element	Embedded	1)OS platform independent 2) Additional hardware costs 3) Might cause issue user upgrades a handset
NFC Non Removable Secure Element	SIM/UICC	1) OS platform Independent 2) NO additional hardware costs
	Microsd	1)OS platform independent 2)Additional hardware costs for micro SD card 3)Needs SD card slot 4) No issues with handset upgrades
Cloud		1)Leverages existing payment terminals 2)No special consumer device needed 3)Strong link to online channels

References

[1] Mobile Phone Technology: “Smarter” Than We Thought Marianne Crowe and Elisa Tavilla Federal Reserve Bank of Boston November 16, 2012.

[2]. An architecture based on Internet of Things to support mobility and security in medical environments Antonio J. Jara, Miguel A. Zamora and Antonio F. G. Skarmeta *IEEE Member* University of Murcia, Computer Science Faculty, Murcia, Spain. jara@um.es.

[3]. Antonio J. Jara, Alberto F. Alcolea, Miguel A. Zamora, Antonio F. G. Skarmeta ‘Evaluation of the security capabilities on NFC-powered devices’ Department of Information and Communications Engineering,Computer Science Faculty, University of Murcia, Murcia, Spain

[4].Near Field Communication, White paper, ECMA international, December 2003

[5].Teddy Mantoro (Member IEEE), in “smart card authentication for internet applications using NFC enabled phone”Admir Milisic at Department of Computer Science, Kulliyyah (Faculty) of Information and Communications Technology, International Islamic University Malaysia.

[6]. Paillès, J.C. Gaber, C. Alimi, V. Pasquet, M, “ Payment and Privacy: A key for the development of NFC mobile“,ENSICAEN, GREYC Lab., Univ. of Caen, France , June 2010.

[7]. Haselsteiner, S. & Breitfuß, K. (2006). Security in near field communication (NFC). Philips semiconductors.In *Proceedings of workshop on RFID security 2006*, Graz, Austria, 12–14 Jul 2006.

[8].NFC Forum, "Near Field Communication and the NFC Forum: The Keys to Truly Interoperable Communications", White Paper, 2007.

[9]P5CN072 Secure Dual Interface PKI Smart Card Controller. http://www.nxp. com/acrobat download/other/identification/SFS107710.pdf..

[10].Helsinki metropolia university of applied sciences bachelor of business administration degree programme in European management may 2012

[11]. Haselsteiner, S. & Breitfuß, K. (2006). Security in near field communication (NFC). Philips semiconductors.In *Proceedings of workshop on RFID security 2006*, Graz, Austria, 12–14 Jul 2006,

[13]. Leng, X. (2009). Smart card applications and security. *Information Security Technical Report.*

[14] Jara, A. J., Zamora, M. A., Skarmeta, A. F. G.,"NFC/RFID applications in medicine: security challenges and solutions", Sth International Conference on Intelligent Environments (lE'09), RFID Technology: Concepts, Practices & Solutions, Barcelona, July, 2009.

[13] Jara, A. J., Zamora, M. A., Skarmeta, A. F. G., "Secure use of NFC in medical environments", Sth European Workshop on RFID Systems and Technologies, Bremen (Germany), June, 2009.

[14] Madlmayr, Gerald et aI, "NFC Devices: Security and Privacy", The Third International Conference on Availability, Reliability, 2008.

[15] Ernst Haselsteiner and Klemens BreitfuB, "Security in Near Field Communication (NFC)". Workshop on RFID Security 2006, RFIDSec06, 2006.