Security in Mobile Payments

Alessandro Vizzarri
Department of Enterprise Engineering
University of Rome Tor Vergata
Rome, Italy
alessandro.vizzarri@uniroma2.it

Francesco Vatalaro
Department of Enterprise Engineering
University of Rome Tor Vergata
Rome, Italy
vatalaro@uniroma2.it

Marco Vari
Department of Enterprise Engineering
University of Rome Tor Vergata
Rome, Italy
marco.vari@uniroma2.it

***Abstract* — Mobile Payments are getting more and more popular in the Information Society (E-Society). These new payment systems allow a user to pay in every condition, especially if she/he is moving around with a pad, a smartphone or a mobile phone. This paper presents some main characteristics of Mobile Payments, in terms of requirements and benefits for the end user. Mobile procedures are also presented, underlining relationship and interactions between involved players. In fact, analysis of Mobile Payment systems and procedures is affected by security issues to be carefully considered. Main requirements to be respected and main policies to be followed in case of frauds are here within presented, together with possible solutions to prevent them.**

Keywords: Mobile Payment, Security, NFC, Attacker

1. Introduction

Payment systems have undergone an incredible evolution passing from a physical transfer of goods or money (a transmission of information between two or more parts) to exchanging digital data transaction. However in modern electronic payment systems the number of involved players is still increasing. In fact, from a traditional "buyer-seller" exchange we passed to new methods which also include network providers, the institutional authorities of privacy and finance companies for money transaction management (generally a credit card or debit card company or other similar institutions, e.g. Paypal). [8]

Requirements for security able to ensure interoperability and privacy, as well as ease-of-use and execution speed, increased their importance in this context. The current stage of evolution of payment systems deals with mobile payment systems. The term Mobile Payment, or simply “m-payment”, refers to a system of payment or money transfer via a mobile device. The result of a Mobile Payment is the transition of money between the purchaser (person making the purchase) and the merchant (person selling the good or service). Mobile Payments are made using one or more technologies including SMS, Near Field Communication (NFC), Interactive Voice Response (IVR), Unstructured Supplementary Service Data (USSD), SDK libraries, cellular networks, WAP protocols, i-mode protocols, wireless networks and JAVA applications. The systems that provide the possibility to carry out a Mobile Payment are expanding very quickly. The goal of many operators is to make these forms of payment systems suitable for daily use. [8]

We can provide a simple taxonomy for mobile payments (Fig. 1).

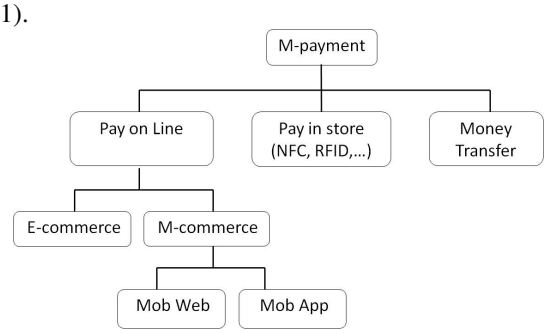

Fig. 1: Taxonomy of Mobile Payments.

2. Mobile Payment systems

2.1 Architecture

A general architecture of a Mobile Payment System is composed by two main context areas: one customer area and one merchant area. Each area is characterized by two main elements:

- Mobile Terminal (e.g. mobil phones, tablet,...)
- Payment Circuit (e.g. bank, credit card,...)

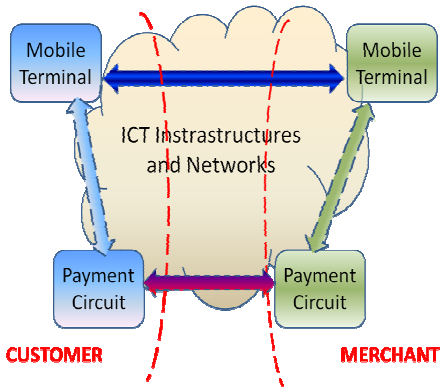

Fig. 2: Reference architecture of a m-payment system.

The general architecture of a Mobile Payment system is composed of four modules, as shown in Fig. 3 (a): a data transfer module, one Security Element (SE), HW/SW components, and, finally, the payment circuit module. The

data transfer module is in charge of managing connections among terminal devices in order to enable transactions. It can provide remote (on-line) or proximity connections, using different technologies.

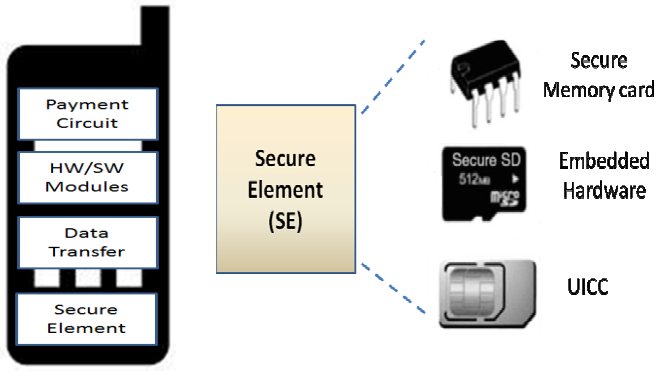

Fig. 3: (a) Modules of a Mobile Payment system; (b) Alternative implementations of the Secure Element.

The Secure Element (Fig. 3 (b)) is a platform in which to store, customize and manage customer's confidential data. Therefore, it is a crucial system component due to the extreme importance of information stored inside it such as, e.g., the login credentials, credit card numbers, and the transactions identification number. The SE is tamper-resistant and is based on a combination of sub-modules: Integrated Circuit IC on SIM UICC (Universal Integrated Circuit Card) or micro SD card, Operating System (OS) and an application able to store and manage data of users, transactions, and operations.
Additional hardware components useful to manage payments are a voice synthesizer and recognizer, biometric devices and sensors, while other software components are built in dedicated applications and widgets. Finally, the payment circuit software modules are in charge of connecting with financial institutes to accomplish bank transfers, as well as transactions with credit/debit cards.

2.2 Classification

Two main criteria adopted to classify Mobile Payment systems are based on:

a) *offline and online payments*: this classification is related to the possible involvement of one mobile network operator (MNO);
b) *remote or proximity payments*: this classification is related to the distance of the mobile terminal enabled for the payment.

a) Off line and on line payments

In off-line payments the transaction between customer and merchant is direct, so data exchange exclusively takes place between their respective devices. Thus it is unnecessary to involve third-party entity, and management of security and encryption procedures are more simple. However, this method requires that the buyer's device contains an electronic wallet which needs to be charged in advance before executing any transaction.
A proper protocol for off-line transactions involves the use of "digital vouchers" and strong cryptographic methods. The protocol establishes the rules for the secure exchange of information between the two devices involved in the payment.
On the contrary, on-line payments need the involvement of other entities such as the MNO and the companies that first authorize the transaction of money and then check the status of the whole payment procedure. With respect to off-line payments, in an on-line payment the user does not need a pre-charged credit stored into the phone, since she/he can directly access own bank account via web and can use the phone as if it were a credit card.

b) *Remote or proximity mobile payments*

Remote Mobile Payments (RMPs) include those made via a mobile device when the distance between seller and buyer devices has no influence on the transaction. As a consequence, for such payments the MNO provides a data connection via web browser or SMS. A practical example of RMP is one user purchasing an app for the smartphone.
Proximity Mobile Payments (PMPs) include payments that ask for the buyer and the seller to be physically close. Proximity connections are based on protocols, such as RFID, NFC or high frequency sound waves.

3. Mobile Payment procedure

The classification of mobile payment systems introduced above is useful to define several phases of a payment procedure and the involved entities.
In case of mobile remote payment the main phases are (Fig. 4):

- The customer ("payer") uses own mobile device to send a payment request to a Payment Service Provider (PSP) over a wireless network. This request includes the details of the merchant ("payee") and the amount to be paid.
- The PSP verifies the customer's credentials and the payee's identity (basically it checks whether the customer and the payee registered for the m-payment service).
- Optionally, the PSP might ask the customer for some more details (like a password) for authentication purposes.
- Once the customer's credentials have been assessed, the PSP requests the payee for confirmation by forwarding the payment details.
- The payee then sends a confirmation message to the PSP.
- After successful confirmation, the PSP performs backend processing to update the accounts of the payer and the payee.
- It sends a payment receipt to the payer. It might also optionally send a "Transaction completed" message to the payee.

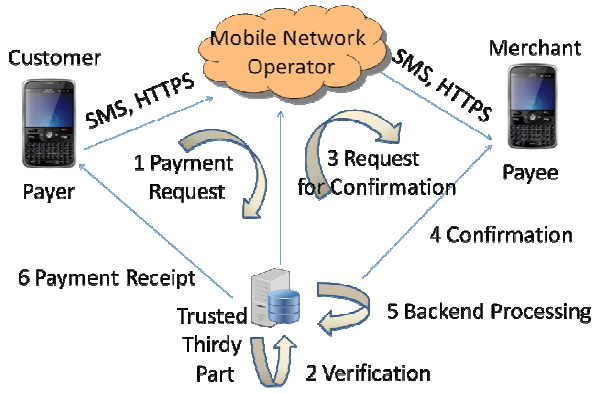

Fig. 4: Remote Mobile Payment Phases.

In remote m-payments, the customer first sends the payment request to the PSP over a wireless network by using a remote wireless technology. The PSP then forwards this request to the payee. However, in proximity m-payments, the customer directly sends the payment request to the payee typically using a short-range wireless technology. The payee then forwards this payment request to the PSP over a wireless network. Figure 5 summarizes the steps in proximity m-payments. [2]

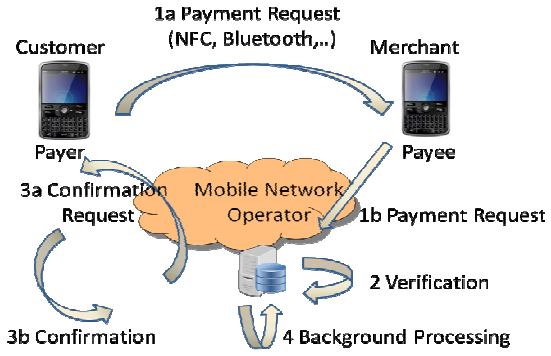

Fig. 5: Mobile Proximity Payment Phases.

4. Security approaches in Mobile Payment

4.1 Main characteristics

In a general payment system security aspects are very crucial to be managed. They are often related to technical procedures and management necessary to ensure the following properties:

• *Data confidentiality:* in an electronic transaction, only legitimate involved entities must be able to understand the content of the messages exchanged among the parties. The confidentiality in a payment system must be ensured in order to prevent decryption actions made by unauthorized users. This property is provided through encryption and decryption operations performed by mobile terminals.

• *Authentication*: should be implemented before the actual transaction begins. This feature consists of the mutual identity confirmation of identity of two legitimate entities involved in the payment process. In this way, it is possible avoiding a third party to make an entity substitution. Usually, this is achieved by using authentication protocols.

• *Authorization:* After the authentication phase, the phase of authorization allows the parties to make only operations allowed to them.

• *Data Integrity:* this feature ensures that the information contained in the messages and exchanged among the parties is not altered as a result of an error or malicious action. This can help to prevent an intrusion in message reception by the user. Data integrity is achieved by signing digitally transmitted data.

• *Non-repudiation:* After user sending or receiving a message, the entity which performed any of these actions should not be able to deny it. Also this property is achieved by means of the digital signature.

• *Availability:* this feature enables users to use the payment system in mobility, as determined by service subscription, avoiding any attacks aimed at making the system not working. The use of firewalls and security protocols suitable for this purpose makes this property feasible.

4.2 Layered approach

A layered approach to security management in m-payment is useful to define different layers and sections associated to different types of vulnerability (Fig. 6). [4, 9]

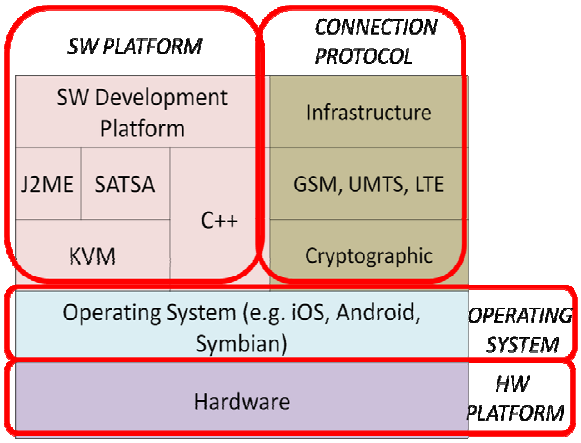

Fig. 6: Layered approach to security in m-payment systems.

Four main sections can be considered:

- Software Platform
- Connection Protocol
- Operating System
- Hardware Platform.

The software platform section may include different modules, like J2ME, KVM (K Virtual Machine),[1] SASTA[2] and C++. The connection protocol section includes modules related to network infrastructure and cryptography. The operating system section is related to the Operating System installed in the mobile terminal and, finally, the hardware platform section includes hardware components of the mobile terminal. To

[1] Java virtual machine suitable for mobile phone.

[2] Security and Trust Services API for J2ME.

ensure the security of the m-payment system as a whole it is necessary that every section in the m-payment system is made robust to malicious attacks.

5. Vulnerabilities

A layered approach to security management in mobile payment systems can provide a full taxonomy of vulnerabilities and attacks, as shown in Fig. 7. [10]
In particular, several types of attacks can be considered for each layer. Different layers or categories can be affected by the same vulnerabilities.

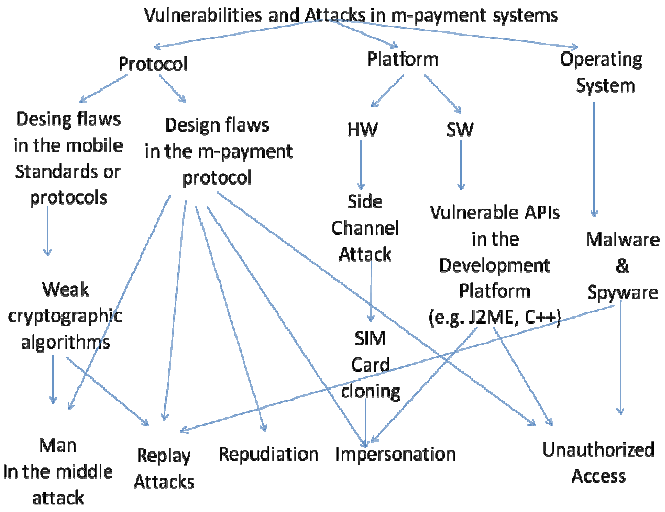

Fig. 7: Taxonomy of vulnerabilities in m-payment systems.

5.1 Connection Protocol

As mentioned before, a radio transmission medium (such as NFC) addresses issues of communication interception.
Possible attacks that can be executed against the NFC systems, including those for mobile payments, are listed below. For each of them appropriate countermeasures are achieved.
• *Eavesdropping:* interception of transmitted radio signals made by a possible attacker. To do this, the attacker must possess the necessary equipment to receive the signal and also specific knowledge to extract and interpret the data contained in the received signal.
• *Data Corruption:* in this case the goal of the attacker is not only a simple interception of transmitted data, but also alteration of the transmission. In the simplest case, the attacker simply wants to disturb the communication, so that the receiver is not able to understand the data sent from the other device. This type of attack can be implemented by transmitting on the same frequencies used by the original data. This is possible if attacker has a good knowledge of the protocols, modulation and encoding used by the system under attack. This attack is not very complicated to implement, but only allows the attacker to disrupt communication.
• *Data Modification:* in this case the attacker intends to receive valid data to the receiving device, but manipulated. This attack is therefore different from the simple data corruption. The feasibility of this attack depends heavily on the transmission parameters such as the modulation index. The use of encryption techniques makes it very difficult this type of attack.
• *Data Insertion:* In this type of attack, the attacker inserts the message within the data exchanged between the two communicating devices. This type of attack is possible if the device that responds to a message takes a very long time to respond. The attacker can then send their data before the receiver legitimate. The attack will be successful only if the data entered can be transmitted before the original device to begin responding. In fact, if both streams of data overlap, there will be a corruption of the data.
• *Man in the Middle:* In this case the two parties that want to communicate with each other are deceived by a third party, which causes them to enter without their knowledge in a three-way conversation. To prevent this, it may be useful to use a communication in which a device works in active mode and the other in passive mode. So RF field is continuously generated by one of the two parts.
Due to its nature, NFC systems are inherently protected from attack by the Man-in-the-Middle and it is easier to establish a secure communication channel.

5.2 Platform

J2ME is one of the most popular Software Platform, but it can be affected by several type of attacks. An important example is malicious java Applications (MIDlets) installed on customer's mobile terminal and able to send SMS to Payment Gateway and then to initiate a transaction without his approval or to access the data stored by another MIDlet using some lower level APIs.
Hardware Platform can be affected by side channel attack, based on information intercepted by attacker using a physical cryptosystem. SIM card cloning is the most negative result.

5.3 Operating System

Operating System layer is essentially sensible to attacks conducted by mobile malware and spyware**.** [3]
The most popular malware are worms, viruses and trojans, but the last ones now are especially dominant. In fact trojans do not need any propagation vector and can attract user because of their masquerading as utility programs or popular games.
Trojans are usually combined with spyware able to detect and collect any kind of information related to phone calls (e.g. PbStealer), web surfing, HTTP connections, or m-payment details like digital receipt, user credentials or SMS (e.g., Flexispy).

6. Techniques for ensuring security guarantees

There are different techniques to guarantee security in m-payment systems. Classical methods are end-to-end encryption and tokenization. [10]

With *end-to-end encryption*, the card account number and magnetic stripe data are captured and encrypted at the first point of entry (i.e., magnetic-stripe reader head or smart-card reader contacts), in a tamper evident security module (e.g Secure Element) or in an independent software crypto module. Triple DES (or AES) is used as the cryptographic standard for securing the confidentiality and integrity of sensitive data and PIN security, coupled with dynamic key management.

With *tokenization* an encrypted or random value, called token, replaces the card number (PAN) or the magnetic stripe track data in an electronic transaction. The token then becomes the reference number representing the card number, so all tokens can be referenced back to the original card number. Tokenization is usually deployed using Format Preserving Encryption (FPE). FPE preserves the length and formatting characteristics of the token in alignment with the data element associated with storage of the card data, thereby overlaying it with the encrypted token data.

In the last years enhanced authentication techniques have been developed in order to prevent fraudulent attacks. Ultimately the best solutions will use multi-factor authentication and dynamic authentication, providing the most protection from unauthorized individuals compromising the payment transaction.

Multi-factor authentication is related to options like something a customer has (such as a card), something he knows (such as a PIN), and something he is (such as a fingerprint). [6,7]

Authentication solutions can be either static or dynamic, although the latter is significantly more secure. With static authentication the same credential data is used for validation, whereas dynamic authentication uses different credential data for each authorization, and the credential used is typically specific to the transaction being performed. [2]

The following innovative technologies for security guaranteeing are available in the market today.

- *Security tokens* (e.g., one-time password tokens; USB tokens, display cards, or software-based tokens) generate a one-time password in a token device (like a mobile phone) and use an algorithm that only the authenticator knows. Security tokens that use hardware encryption devices (such as card readers) leverage a familiar form factor, and offer the most robust encryption, but adoption and fulfillment (i.e., getting handheld devices in the hands of consumers) remain a challenge. Software tokens are easier to work with and interface to, but they are less secure because they are prone to malware such as key loggers. [2]
- *Knowledge-based authentication* is typically performed using a password and challenge responses, and site key. In recent years, this authentication method has become more prevalent in online banking programs, but there are some shortcomings. First, knowledge-based authentication often is implemented as single factor, e.g., something you know. Adoption can be difficult as some consumers have problems remembering the answers to the challenge questions. And, with so many online accounts using challenge questions for authentication, the answers to these questions are now becoming overused thereby diluting their inherent secrecy. Also it has been demonstrated that consumers may be redirected to a fraudulent site that may not contain the picture image or site key. Not realizing they have been spoofed, unsuspecting consumers enter user names and passwords anyway, defeating the security.
- *EMV/Chip cards* have only gained traction in the U.S. in closed-loop environments. Chip cards using PINs provide a high level of security by combining secure cryptograms with dynamic transaction data, each time creating a unique and therefore highly secure authorization value. Keys need to be systemically generated and managed in a chip card program. Recently there have been reported incidences of hacked chip cards, which suggests that increasing level of cryptographic security may be needed for the next generation of chip cards.
We are beginning to see the deployment of contactless cards in public transit and merchant locations with low dollar average ticket size. Contactless cards use a radio frequency identification (RFID) chip or NFC (Near Field Communication) and some use dynamic CVV (Card Verification Value) cycling.
- *Magnetic Stripe Unique Profiling offers* a highly reliable method of card authentication. This dynamic card authentication technology is based on the unique physical properties of the magnetic stripe that appear naturally on each magnetic stripe card as a byproduct of the manufacturing process. It provides validation that the card itself is genuine and that its encoded data has not been altered.
This solution can be implemented at low price point compared to other authentication solutions in the market. Since existing magnetic stripe cards contain this unique authentication technology in their inherent state, there is no need to reissue cards to consumers. However the cards must be registered. The card reader technology tied to this solution is now sufficiently advanced to encrypt the magnetic stripe card data at the reader head, providing added security. Retailers can readily upgrade their POS technology as part of the routine device upgrade/replacement cycle.
- Among the dynamic authentication solutions available in the market, magnetic stripe unique profiling best leverages the existing payment infrastructure and minimizes cost expenditures to the retailer. The solution does require a working agreement between merchants, acquirer processors, and cards issuers before the benefits are realized, and this has lagged in the market place.
- *Out-of-band authentication* uses a secondary channel and different medium to communicate to the user. Out-of-band techniques (delivered via email or SMS text message to the mobile phone) have emerged to track near real-time monitoring of card misuse. This method of authentication has been quite popular in online and mobile banking programs,

but is still in the nascent stages of development and can be cumbersome for the consumer and more time consuming at POS. [2]

- *IP Geolocation* leverages mobile phone technology by comparing the user's current location (identified by satellite) to that previously registered by the user. Two factor authentication is supported, e.g., the consumer's cell phone and physical location. Viable hybrid solutions are also emerging in the market place. One-time passwords that are delivered through an out-of-band channel provide the benefits of both two-channel and two-factor authentication. All of these authentication methods require some type of registration process and/or issuance process. Even though the card issuer stands to benefit, the cost burden lies with the retailer.

Innovative techniques of *Dynamic Transaction Authentication* are based on dynamic authentication of all elements of the transaction including the user, user's card, the data on the user's card, the terminal or device, the network switches and host computers of the data recipients and the transaction details. This approach ensures that the transaction is secure not only from the first point of entry at the terminal and across the payment infrastructure, but also makes certain that the card itself and the data on the card are not altered.

The need for dynamic transaction authentication has arisen because end-to-end encryption alone cannot protect retailers from breaches due to skimming or sniffing. Dynamic transaction authentication provides retailers with a multi-layered solution for securing each element of the payment transaction. It leverages a combination of strong encryption, secure tokenization, counterfeit detection, tamper recognition, data relevance and integrity, and dynamic digital transaction signatures - which together validate and protect the entire transaction and each of its components.

7. Conclusions

A comprehensive analysis of Mobile Payment systems and procedures is strictly related to security issues to be managed and to coordination of several market stakeholders. Due to relevance of money transfers, security aspects become very important for a technological and commercial success.

Users have to change their traditional approach to payments: they can purchase a good sending digital information, which is invisible, and not using usual paper, which is visible and therefore apt to immediate control.

The success of e-payment and m-payment methods is mainly linked to their secure use, to the awareness of the end user who must have a strong perception of security in the entire m-payment market.

From a technological point of view, high levels of security can be achieved by a combination of end-to-end encryption, tokenization and dynamic transaction authentication.

In particular a strong expansion of end-to-end encryption in all the life-cycle of m-payment transaction is needed, together with a large diffusion of tokenization technique (not only limited to smaller merchants and small amounts) and usage of dynamic authentication in all sections of a transaction. Finally, these techniques must be easy to use for the end user.

In this paper we dealt with crucial role of security factors to be managed in entire transmission chain of a mobile payment system. A combination of different techniques for ensuring security guarantees must be applied not only data transfer section (in order to intercept a transaction) but also to other technological sections: Operation System, Software Platform and Hardware Platform.

References

[1] "Mobile Payment Acceptance Security of Guidelines, ver 1.0" PCI Security Standards (PCI-SS),

[2] "Security of Proximity Mobile Payment", Smart Card Alliance, 2009.
Allan, Ant. "Q&A: Phone-Based Authentication Methods", Gartner, June 24, 2010

[3] Basso, Monica and Gammage, Brian. "Smartpone Virtualization: Making Mobile Applications More Trustable", Gartner, April 21, 2011

[4] Litan, Avivah. "Best Practices in Mobile User Authentication and Layered Fraud Prevention", Gartner, August 11, 2011

[5] "8th Annual Card Issuers' Safety Scorecard: Proliferation of Alerts Lead to Quicker Detection Time and Lower Fraud Costs" Javelin Strategy & Research, June 2012

[6] "Consumer and Mobile Financial Services", Board of Governors of the Federal Reserve System, March 2012

[7] "Recommendations for the Security of Internet Payments", European Central Bank, April 2012

[8] "Consumer and Mobile Financial Services", Board of Governors of the Federal Reserve System, March 2012

[9] WHITE PAPER ON SECURITY ENHANCEMENTS, Avenue B, 2010

[10] "Security Issues in Mobile Payment Systems", Shivani Agarwal1, Mitesh Khapra1, Bernard Menezes1 and Nirav Uchat, IIT Bombay, India