Analysis of Security Risks in Mobile Payments
A Case Study Using DNAT

By
Jing Ba

Department of Computer and Systems Sciences
Degree project 30 HE credits
Degree subject (Computer and Systems Sciences)
Degree project at the master level
Spring term 2012
Supervisor: Louise Yngström
Reviewer: Stewart Kowalski
Acknowledgment

During the thesis project I really want to express my utmost gratitude to my supervisor Prof. Louise Yngström for her patient guidance and help. And for my studies in Department of Computer and System Science, she also provided support as much as possible.

To my dear family, Huang, Y.L. and Wang, H.X., thank you for your love and encouragement through these years, I can’t finish the study without you.

And to my dear friends, you are with me all the time and always make me better when I am in troubles, thank you all.
Abstract

Technology development always makes the life easier and faster thus it also impacts the way we do business in our lives. As the widespread usage of mobile devices in recent years mobile technology has created an environment in which people around the world are getting closer. Recently the popularity of personal mobile devices like Ipad and Iphone leads to the appearance of opportunities to improve payments more fast and efficient. And for the past years various services and applications for mobile payment have been developed by the companies which are eager for the leader positions in the new market. With the development of mobile payment and the important relationship between payment and our lives, a lot of security risks associated with this field should be extensively studied. This thesis aims to analyze the security risks related to the mobile payment.

This thesis uses an explorative method to research the stakeholders, critical assets and vulnerabilities within mobile payment by utilizing case studies of Square and Google Wallet. The information gathered from the case studies and security analysis is further analyzed by the dynamic network analysis tool (ORA) in order to discover the security risks.

The results of this thesis indicate that accounts and business data are the most critical assets in mobile payment because accounts are the foundation to perform payment transactions. Further, the mobile payment service provider, merchant and consumer are the stakeholders affected most by the security risks. And this thesis concludes that all the stakeholders should be aware of the security risks within the mobile payment environment, and further if service and device providers want to keep continuous business they should make more effort to cooperate with each other to protect the users against these risks.

Key words: Mobile Payment, Square, Google Wallet, DNAT, Security Risks
List of Figures

Figure 1-Thesis Structure.................................................................4
Figure 2-Value Chain of Mobile Payment Model [Smart Card Alliance 2008]........15
Figure 3-Systemic-Holistic Model [Yngström 2007]........................................20
Figure 4-Meta-Network for Mobile Payment System of Square.........................36
Figure 5-Agent and Resource Network..................................................37
Figure 6-Event-Resource Network..........................................................37
Figure 7-Agent-Resource-Event Network....................................................38
Figure 8-Capacity of Risks and Assets......................................................38
Figure 9-Capacity of Risks and Stakeholders...............................................39
Figure 10-Centrality of Risks and Assets...................................................39
Figure 11-Centrality of Risks and Stakeholders............................................40
List of Tables

Table 1-Pros and Cons for each Operator-Centric Model Stakeholder.....................10
[Smart Card Alliance 2008]
Table 2-Pros and Cons for each Bank-Centric Model Stakeholder........................11
[Smart Card Alliance 2008]
Table 3-Pros and Cons for each Peer-to-Peer Model Stakeholder.........................12
[Smart Card Alliance 2008]
Table 4-Pros and Cons for each Collaboration Model Stakeholder.........................13
[Smart Card Alliance 2008]
Table 5-Risk Level of Properties .........................................................................28
Table 6-Security Analysis of Accounts as Assets in Square....................................29
Table 7-Security Analysis of Accounts as Assets in Google Wallet........................29
Table 8-Security Analysis of Hardware Device as Asset in Square ......................30
Table 9-Security Analysis of Hardware Device as Asset in Google Wallet .............30
Table 10-Security Analysis of Business Data as Asset in Square .........................31
Table 11-Security Analysis of Business Data as Asset in Google Wallet...............32
Table 12-Security Analysis of Threats and Vulnerabilities in Mobile Payment....33
Table 13-Meta-Matrix showing relationships within nodes entities......................34
[Krackhardt and Kathleen Carley 1998]
Table 14-Elements and Relationships comprising Organizations [CASOS website]..35
# Table of Content

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>List of Figures</td>
<td>iii</td>
</tr>
<tr>
<td>List of Tables</td>
<td>iv</td>
</tr>
<tr>
<td>Chapter 1</td>
<td>1</td>
</tr>
<tr>
<td>Introduction</td>
<td>1</td>
</tr>
<tr>
<td>Background</td>
<td>1</td>
</tr>
<tr>
<td>Research Problem</td>
<td>1</td>
</tr>
<tr>
<td>Research Questions</td>
<td>2</td>
</tr>
<tr>
<td>Research Methodology</td>
<td>2</td>
</tr>
<tr>
<td>Alternative Research Method</td>
<td>3</td>
</tr>
<tr>
<td>Thesis Structure</td>
<td>4</td>
</tr>
<tr>
<td>Chapter 2</td>
<td>6</td>
</tr>
<tr>
<td>Mobile Payment</td>
<td>6</td>
</tr>
<tr>
<td>History of Mobile Payment</td>
<td>6</td>
</tr>
<tr>
<td>Relevant Research</td>
<td>6</td>
</tr>
<tr>
<td>Business Models in Mobile Payment</td>
<td>9</td>
</tr>
<tr>
<td>Payment Methods</td>
<td>13</td>
</tr>
<tr>
<td>Chapter 3</td>
<td>15</td>
</tr>
<tr>
<td>Case Study</td>
<td>15</td>
</tr>
<tr>
<td>Value Chain</td>
<td>15</td>
</tr>
<tr>
<td>Stakeholders</td>
<td>16</td>
</tr>
<tr>
<td>An overview of Square</td>
<td>18</td>
</tr>
<tr>
<td>A holistic analysis of Square</td>
<td>20</td>
</tr>
<tr>
<td>An overview of Google Wallet</td>
<td>22</td>
</tr>
<tr>
<td>A holistic analysis of Google Wallet</td>
<td>22</td>
</tr>
<tr>
<td>Chapter 4</td>
<td>25</td>
</tr>
<tr>
<td>Security Analysis</td>
<td>25</td>
</tr>
<tr>
<td>Background</td>
<td>25</td>
</tr>
<tr>
<td>Security Properties</td>
<td>26</td>
</tr>
<tr>
<td>Assets Analysis</td>
<td>27</td>
</tr>
<tr>
<td>Threats and Vulnerabilities</td>
<td>32</td>
</tr>
<tr>
<td>Chapter 5</td>
<td>34</td>
</tr>
<tr>
<td>Analysis through DNAT</td>
<td>34</td>
</tr>
<tr>
<td>Background of DNAT</td>
<td>34</td>
</tr>
<tr>
<td>Implementation</td>
<td>35</td>
</tr>
<tr>
<td>Results and Discussion</td>
<td>36</td>
</tr>
<tr>
<td>Chapter 6</td>
<td>41</td>
</tr>
<tr>
<td>Conclusion</td>
<td>41</td>
</tr>
<tr>
<td>Conclusions</td>
<td>41</td>
</tr>
<tr>
<td>Limitation and Further Work</td>
<td>42</td>
</tr>
<tr>
<td>References</td>
<td>43</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>50</td>
</tr>
</tbody>
</table>
Chapter 1

Introduction

Background

As an indispensable part of commerce environment, payment with paper currency and in face-to-face way has existed for centuries. With the rapid development of technology, payment has been persistently changing from traditional methods to the ones more fast and convenient. For the past decades, along with the popularization of the internet, the E-commerce has emerged and fitted in many fields around us. Therefore internet has made it possible to revolutionize the way we do payment.

The mobile payment refers to payment services operated under financial regulation and performed from or via a mobile device [Wikipedia]. Internet environment and mobile devices make merchants and customers around the world connected. With the information technology, the mobile payment can simplify payment procedure tremendously. Users of mobile payment can get rid of the limitation from real currency and geography.

Recently mobile payment has sharply risen with the issue of the Google Wallet. The value of mobile transaction is expected to reach more than $600 billion by 2013 and Asia, Western Europe and North America will be responsible for most of all mobile payment transactions [Wikipedia].

Therefore, a variety of security risks will emerge in mobile payment because of the huge potential market. Since transactions and currencies are stored and transmitted in the mobile and internet environment, security of mobile payment has been the pivotal factor in it.

Research Problem

Mobile payment no longer is a new field for the international business. In recent years, it has absorbed enormous attention to be a furious and attractive battlefield for the companies interested in it. The Square, founded at the beginning of 2010, had gained a million users at the end of last year. Meanwhile, the PayPal starts testing their mobile payment business in two companies in Stockholm. Issue of the Google Wallet in 2011 has rapidly accelerated the development of mobile payment. And the new
company Isis, founded by Verizon, AT&T and T-Mobile, also invaded mobile payment field with the cooperation with Visa, MasterCard, American Express and Discover. Not only these companies, but also countries all over the world have started to run the mobile business. Japan and South Korea implemented mobile payment platform around 2005 and 2004. Last year, the size of mobile payment in China was more than 10 billion dollars [EnfoDesk 2012].

With the competitions from various corporations, a variety of applications and services have been developed. The increasing popularity of mobile payment leads to security risks in implementing these mobile transactions. We should study these risks and decrease their impacts which can influence the users’ acceptance extent. This thesis intends to research the security risks related to the mobile payment and the impact of them.

Research Questions

According to the research problem described above, there are some questions need to be handled in this thesis. First of all, “which stakeholders are involved in the mobile payment?” should be researched. By identifying the relevant stakeholders we could excavate the assets which are critical to the stakeholders and the payment environment.

After the stakeholders, we need to analyze “what assets should be protected for the mobile payment?” These assets will be connected with the stakeholders and help us to study the potential security risks and threats.

As the previous questions are settled, “what are the security risks and threats in the mobile payment?” need to be explored. These identified security risks and threats will impact the important assets mentioned before.

Finally, “which stakeholders and assets are most important, and which risk impacts the most?” will be researched. The last question will help us reduce the risks and influences brought by them in order to make the mobile payment more secure and reliable.

Research Methodology

Mobile payment has been carried out around 10 years ago and is developing fast recently. As security stands in the center of business, researches about security issues in mobile payment are important to explore and understand the mobile payment environment. Before the research of this thesis starts a literature study will be constructed in order to explore what work has been carried out about the security research. The literature study can provide an overview of mobile payment and help us
select the risks and threats analyzed in this thesis. And from the literature study, appropriate case studies in these researches can be discovered and particular data can be collected for this thesis. The literatures reviewed in this thesis are searched from IEEE Xplore, library database of KTH and other research organizations.

As the mobile payment is prevailing around the world recently and little research related to particular mobile payment system has been constructed, an explorative research approach is used in this thesis. [Mack et al. 2002] indicated that qualitative research methods have advantages for exploratory research such as qualitative methods can use open-ended questions rather than simply “yes” or “no” in quantitative methods. And in the comparison of two research methods, one of the analytical objective of the qualitative method is to describe and explain relationships. In this thesis relationships within threats, assets and stakeholders will be analyzed, therefore, a qualitative method is selected to construct the research.

After the literature study case studies of particular mobile payment systems will be analyzed in this thesis to solve the research questions. In the case studies, systemic approach and security models will be utilized to understand the mobile payment environment and discover the risks and threats related to the payment environment.

With the information we collect from the case studies, the data used to answer the research questions are analyzed by using Dynamic Network Analysis Tool in order to figure out the relationships within the components such as assets, stakeholders, risks and threats.

**Alternative Research Method**

In addition to the case studies and dynamic network analysis tool used in this thesis, a wealth of other research methods can be utilized to build the research. One common method is quantitative method like constructing a survey towards users and other participants in mobile payment. This method could collect direct response from the users and developers. However it is very difficult to get affluent data because these new mobile payment systems are issued in the last several years, and this new payment method has not been accepted by customers completely. Thus it is difficult to collect enough survey data to analyze. Furthermore not all the users are aware of the threats and risks in the mobile payment environment, therefore the results indicated by the surveys can’t be reliable enough.

And in many security researches some analysts would use practical methods to explore the security issues of a system. It requires the researcher to understand the operation and technologies of the whole system. And it also requires special skills such as decryption and eavesdropping. Meanwhile the legal issues should be considered for this method as well.
Compared with all the options discussed above case studies of Square and Google Wallet and dynamic network analysis tool are chosen to perform this research. Case study can provide a holistic view of particular mobile payment system to help us understand the environment. And the dynamic network analysis can give the visualization of the relationships within the systems. Thus it is determined to use this approach for this thesis.

**Thesis Structure**

In the first part of this thesis, we will give an overview of the mobile payment. Chapter 1 will describe the brief background and the research problem and questions this thesis focuses on. Chapter 2 is constructed to provide an extended background of mobile payment. Different kinds of mobile payment services will be presented in this chapter.

In the second part, case studies are built to classify the relevant stakeholders, critical assets and risks. We choose two different mobile payment platforms, the Google Wallet and Square, to implement the qualitative research. Chapter 3 analyzes the two platforms holistically and identifies the stakeholders involved. Chapter 4 provides the exploration of the critical assets, risks and threats by using security analysis.

In the last part, Dynamic Network Analysis Tool will be used to construct the risks analysis. Chapter 5 will give the analysis processes, the results from the analysis and
related discussion. Finally, chapter 6 will present the conclusion, limitation and further work.
Chapter 2

Mobile Payment

History of Mobile Payment

Mobile payment is based on mobile commerce which is said to start in 1997. Coco Cola vending machines were enabled with smart phones by SMS (Short Messaging Service) text message in Helsinki, Finland. In 1999 two national commercial platforms for mobile commerce, Smart Money and i-Mode, were launched in Philippines and Japan. Later in 2000, mobile parking system was set up in Norway while the mobile purchases of airline tickets were offered in Japan [Wikipedia]. In the same year, banking services based on mobile phones started in China.

With the rapid development and popularity of PDAs (Personal Digital Assistant) and smart phones, it provided an opportunity and environment to create a revolutionary payment method. In 2008, UCL Computer Science demonstrated the service applications on mobile devices. The company Square which focuses on mobile payment was founded in 2010 and recently Google issued the Google Wallet to compete in this battle.

Nowadays, technologies in mobile payment have developed from SMS message to WEB, USSD (Unstructured Supplementary Service Data) and NFC (Near Field Communication) etc. Attracted by the market of more than 600 billion dollars, smart phone manufacturers, banking institutions and network operators all start to play important roles in this business field.

Relevant Research

In order to identify and analyze the stakeholders, critical assets and threats in mobile payment, a literature review is constructed to understand the existing background of mobile payment. It shows related pieces of research that have been done to describe what problems the mobile payment is facing and how it operates generally.

General Research

[Chen and Adams 2004] researched different kinds of short-range wireless technologies used in mobile payment field: RFID (Radio Frequency Identification Device), Bluetooth and Near Field Communication. [Lawrence and Zmijewska 2006]
built a qualitative survey to study how the stakeholders affect the development of mobile payment. [Cai et al 2011] explored mobile payment based on 3G network through an integrated mobile phone payment system, and he also indicated what roles the different participants (bank industry, mobile network operators and platform providers) would play in mobile payment and how the relations between them would be. [Schierz, Schilke and Wirtz 2010] discussed the acceptance of mobile payment services with an empirical analysis. [Meiton and Lagström 2011] have explored contactless mobile payments in the European market.

In the following part, the studies according to particular aspects (technologies, security and consumer adoption) in mobile payment will be mentioned.

### Technologies

Mobile payment is based on various information technologies during its development. [Dahlberg et al. 2008] analyzed potential networking technologies including Infrared, Bluetooth, Near Field Communication and the 2nd and 3rd generation mobile networks. [Cai et al 2011] explored different mobile payment solutions and had a study about integrated mobile payment system through 3 aspects (payment channel, payment carrier and security authentication). [Ondrus and Pigneur 2007] build an assessment for future payment systems based on Near Filed Communication. They demonstrated that NFC performs much better than other existing mobile phone technologies. [Yen and Lancaster 2008] studied Bluetooth and WiMax (Worldwide Interoperability for Microwave Access) in the mobile commerce in the future. [Rusu and Man 2007] have analyzed the RFID technology applications in mobile payment.

### Security

Security is always regarded as a vital part affecting different parties in business transactions. Not only is security the foundation of mobile payment operation, but also a crucial factor of users’ adoption. In terms of security in mobile commerce environment, many studies have explored security threats and technologies used to deal with them. [Agarwal, Khapra, Menezes and Uchat 2007] studied security issues in mobile payment systems. They have researched various technologies and standards for mobile payment systems like GSM, CDMA, SAT and SATSA in J2ME. They also explored vulnerabilities by categorizing them into standard (GSM), platform (J2ME) and technology (Bluetooth). Finally they described attacks from mobile malware and spyware.

[Hassinen, Hyppönen and Haataja 2006] described the implementation of an open, PKI-based mobile payment system. [Kadhiwal and Zulfiqar 2007] analyzed different mobile payment security measures and standards. Transmission security mechanisms like SSL, KSSL and WTLS were also explored in their report. [Leung, Sheng and
Cruickshank 2007] explored security threats and security requirements from different perspectives, they also studied the integration of IPSec/AAA and Hierarchical Mobile IPv6, in which IPSec may be used for security of data transmitted in the network and AAA may be used for authentication of mobile node which is used to access the network.

**Consumer Adoption**

In the mobile environment, consumer adoption of mobile applications and service is largely decided by the trust extent. [Kim et al 2009] showed that “both technical protections and security statements are significant factors for improving consumers’ perceived security. Consumers’ perceived security is positively related to consumers’ perceived trust.”[P. 8]

[Mallat 2007] built a qualitative study to research consumer adoption of mobile payments. The factors affecting adoption were described in this report as relative advantage, compatibility, complexity, costs, the trust and perceived security risks. And the dynamical change of these effects was also described in the research. A familiar research written by [Boyd 2011] indicated observability is also a factor driving the adoption of mobile payment. [Lu et al 2011] explored the affects coming from trust and customer’s perceptions to the use of mobile payment and described the interaction between the internet payment environment and mobile payment environment. [Schierz, Schilke and Wirtz 2010] found that perceived compatibility has the greatest affect on the intention to use mobile payment services.

**Ethical Issues**

Regarding the lack of regulation about mobile transaction, there are a lot of ethical issues mobile payment have to face. [Gunner 2011] indicated that customer service is the largest ethical issue to mobile-commerce. Besides customer service, pornography, transaction security breaches and unsolicited e-mail are also the ethical issues related to mobile-commerce. [Gatto and Thoren-Peden 2012] have described legal issues about mobile payment such as intellectual property, privacy and virtual currency. In their research they provided examples of Apple and Starbucks. In the research by [Perlman 2010], it was said that very little article is about regulatory guidelines, but there are some laws in different countries described in this research like the “New e-money paper Nov 09” in South Africa and the “New m-banking rules Dec 09” in India. Furthermore [Metaggart 2011] had a report discussing some legal questions regarding service providers in mobile payment.
Business Models in Mobile Payment

In this part success factors of mobile payment are described. And a variety of business models in mobile payment are discussed in this section. Exploring the business models can provide a good understanding for participants and operations in mobile payment.

[Hort et al 2002] examined critical success factors of mobile payment. The main results of this work indicated in the abstract:

First the consumer perception of the payment instrument was regarded as the key success factor. Users are the foundation of mobile business as essential participants in trading. The mobile payment can maximize the benefits and effectiveness when users can understand what advantages the mobile payment could provide and then they can learn to use the payment services easily. So the ease of learning to use is known as a key factor for adoption of mobile payment.

Another key element is that the merchants have to accept the payment method while they have to bear the costs and higher risk than consumers. Mobile payment is supposed to provide a brand new payment solution which is simpler and instant. According to sensitivity of information trading in mobile environment, security risk has been the most important issue worried by both merchant and consumer. As consumer is the stakeholder who provides only the personal information and money, the merchant certainly will face the costs from infrastructures like POS (Point of Sale).

Further, technology has catalysis for achieving or improving certain critical success factors. Technology makes mobile payment possible and decides how the mobile payment system operates. Ease of use and security are implemented with technologies utilized in mobile payment.

According to the multiple stakeholders in mobile payment market, various potential business models have been designed to operate mobile payment systems. Stakeholders play different roles related to their responsibilities in mobile transactions. [Smart Card Alliance 2008] described four potential business models through interviews with mobile operators, merchants, financial institutions and trusted service providers. In the following section these models are discussed to show how mobile payment operates.

Operator-Centric Model
In this model, the mobile operators independently develop and deploy mobile payment applications to customers’ NFC-enabled mobile devices. The customers may pay for the service and transactions through prepayment or added charges to their
existing wireless bills. For the merchants operators may provide wireless POS systems or payment applications on merchants’ NFC mobile devices. As the operators ultimately have control of infrastructure and associated revenues, they also need to face corresponding risks. Although all the stakeholders can benefit from growth of revenue, customer increment and marketing delivery, they still have kinds of challenges to overcome. The table followed described the pros and cons for stakeholders in this model.

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bank</td>
<td>• None</td>
<td>• Disintermediation from mobile payments value chain</td>
</tr>
<tr>
<td>Mobile Operator</td>
<td>• Control over majority of the revenue stream</td>
<td>• Assumption of risk of additional customer credit</td>
</tr>
<tr>
<td></td>
<td>• Leverage of existing infrastructure to bill customers to</td>
<td>• Assumption of cost of theft and fraud</td>
</tr>
<tr>
<td></td>
<td>pay merchants</td>
<td>• Potential for low merchant acceptance of new payment approach and reluctance to adopt new POS mechanism</td>
</tr>
<tr>
<td></td>
<td>• Customer loyalty</td>
<td>• Management of integration with multiple issuers</td>
</tr>
<tr>
<td></td>
<td>• Reduced customer turnover</td>
<td></td>
</tr>
<tr>
<td>Merchant</td>
<td>• Reduced cash-handling costs, including theft, shrinkage and cash deposit charges</td>
<td>• Fee for low value payments</td>
</tr>
<tr>
<td></td>
<td>• Increased efficiency, throughput, and convenience</td>
<td>• Reimbursement dependent on operator’s payment cycle (delay in payment)</td>
</tr>
<tr>
<td></td>
<td>• Reduced counterfeit exposure</td>
<td>• Exposure to mobile operator with limited payments processing experience</td>
</tr>
<tr>
<td></td>
<td>• Potential for increased impulse spending</td>
<td>• Investment required for new payment mechanism</td>
</tr>
<tr>
<td>Customer</td>
<td>• Customer convenience</td>
<td>• Billing complexity</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Security risk</td>
</tr>
</tbody>
</table>

Table 1-Pros and Cons for each Operator-Centric Model Stakeholder
[Smart Card Alliance 2008]

Bank-Centric Model
The bank-centric model is an extension of the model used for credit cards in the mobile environment. The NFC-enabled phones are regarded as existing credit cards. In a similar situation, customers’ banks directly provide the customers fully-featured NFC phones or only add appropriate payment applications into the existing NFC phones. Meanwhile the merchants’ banks provide suitable device as the POS, in this model banks need to develop new technology for the implementation but also get client loyalty and transaction-based fees in return for the investment. And for the mobile operators, they could charge at the banks’ applications which are on the mobile operators’ chips to implement the transactions. The following table shows the pros and cons for the stakeholders in this model.
### Table 2 - Pros and Cons for each Bank-Centric Model Stakeholder [Smart Card Alliance 2008]

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
</table>
| Bank            | - Revenue stream capture for micro-payments  
                  - Reduced cash/check handling  
                  - Potential to include value-added advertising to retailers for a fee  
                  - Potential for new customer acquisition (including unbanked)  
                  - Enhanced security features  
                  - Increased value of customer relationships and retention | - Limited experience in application distribution or phone accessories  
                  - Added cost of installation and maintenance of mobile applications for multiple operators, each with unique platforms  
                  - Potential for paying “rental” fees to operators. Operators can block usage.  
                  - Competing from factor to cards |
| Mobile Operator | - Possible increase in data transaction volumes and revenues  
                  - Potential incentive fees for introducing new customers | - Operators bypassed in mobile payments value chain |
| Merchant        | - Reduced cash-handling costs, including theft, shrinkage and cash deposit charges  
                  - Increased cashier efficiency and throughput and shorter queues  
                  - Reduced counterfeit exposure  
                  - Increased impulse spending  
                  - Faster payment directly into merchant’s account | - Commissions/transaction fees for low-value transactions  
                  - Merchant resistance to increasing card-based transactions due to interchange |
| Customer        | - Speed and convenience  
                  - Less disruptive -- provides access to transaction history for low-value purchases  
                  - Alternative to costly “white-label” ATM fees. | - Limited to specific bank offering a service – may not be permitted to add other applications |

Peer-to-Peer Model
In this potential model, payments are processed without existing wire transmission and bank card networks. The peer-to-peer service provider can take advantage of existing online applications to complete transactions without POS infrastructure required. Peer-to-peer service providers can earn revenue by licensing fees of applications and software but the mobile operators and banks fail to share a large benefit with service providers. Lack of customer base and payment performance infrastructure will impede the development of this brand-new model. The next table indicates the pros and cons for the stakeholders.
Collaboration Model

The collaboration model is regarded as the most feasible by these participants in this interview because it makes stakeholders focus on their own core competencies. Both financial institutions and mobile operators predict the prevailing of this model. The collaboration involves banks, mobile operators and other stakeholders, including a potential trusted third-party manager responsible for the management of mobile payment applications. In operation of this model, standards for applications may be negotiated and set by the industry associations and NFC-enabled mobile devices and POS devices are required. Potential revenue which is expected to be shared among mobile operators, financial institutions and third-party trusted service managers may include transaction fees, marketing fees and application fees. As discussed above, a table involving pros and cons for stakeholders in this model is presented.

Table 3-Pros and Cons for each Peer-to-Peer Model Stakeholder [Smart Card Alliance 2008]

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bank</td>
<td>• Revenue stream capture from processing fees</td>
<td>• Potential disintermediation if the service provider utilizes another bank as the payment processor</td>
</tr>
<tr>
<td></td>
<td>• Access to broader set of customers from peer-to-peer provider</td>
<td>• Lack of visibility to customer’s transactions</td>
</tr>
<tr>
<td></td>
<td>• Potential to form partnerships</td>
<td>• Certification of device security</td>
</tr>
<tr>
<td>Mobile Operator</td>
<td>• Possible increase in data transaction volumes</td>
<td>• Disintermediation from mobile payments value chain</td>
</tr>
<tr>
<td></td>
<td>• Potential to partner with peer-to-peer provider</td>
<td>• Customer service issues: customers may call with peer-to-peer issues or inquiries</td>
</tr>
<tr>
<td>Peer-to-Peer Service Provider</td>
<td>• Revenue capture from transaction fees and potential commissions</td>
<td>• Significant entry costs to gain wide acceptance by merchants and customers</td>
</tr>
<tr>
<td></td>
<td>• Marketing revenues</td>
<td>• Assumption of risk for theft/fraud</td>
</tr>
<tr>
<td></td>
<td>• Cross-sell opportunities for other offerings or products</td>
<td>• Need for new competency for marketing/loyalty</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Low usage to date</td>
</tr>
<tr>
<td>Merchant</td>
<td>• Reduced cost of cash handling and increased processing speed</td>
<td>• Commissions to peer-to-peer service provider for low value purchases</td>
</tr>
<tr>
<td></td>
<td>• Potential for increased transactions</td>
<td>• New service provider with limited equity in reputation</td>
</tr>
<tr>
<td></td>
<td>• Faster payments</td>
<td>• Risk of loss in case of dispute or fraud</td>
</tr>
<tr>
<td></td>
<td>• Access to loyalty programs</td>
<td></td>
</tr>
<tr>
<td>Customer</td>
<td>• Potential for less expensive remittance/payment option</td>
<td>• Need to transfer funds to peer-to-peer provider (tying up funds)</td>
</tr>
<tr>
<td></td>
<td>• Inexpensive or free</td>
<td>• Need to manage new bill</td>
</tr>
<tr>
<td></td>
<td>• Remote option</td>
<td>• Potential fees charged by the service provider</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Difficulty of managing disputes</td>
</tr>
</tbody>
</table>
Table 4-Pros and Cons for each Collaboration Model Stakeholder [Smart Card Alliance 2008]

### Payment Methods

As mobile payment is being the next battlefield where the stakeholders compete, a variety of mobile payment operation methods are developed. [Fairweather 2011] described four existing methods in mobile payment:

**Smart phone as credit card machine**
In this method smart phone is a POS to handle transactions. The devices and applications used to gain information of credit card are attached with smart phones.

**Smart phone as swipe card**
With the NFC technology and related applications embedded in smart phones, telephones can be used for payment instead of cash and credit cards. Similar with the first method, POS device is required in merchants to implement acceptance of transaction information.

**SIM and/or USSD based mobile money transfers**
This method uses SIM toolkit or USSD technology to complete payment.
Voucher-based systems
In this method consumers can transact with merchants even without a bank account or a credit card. From some special retailers consumers can purchase voucher which is represented by digital numbers in mobile phones to pay for their shopping.
Chapter 3

Case Study

In this chapter of the thesis, the holistic analysis of two existing mobile payment systems is constructed. Before the case studies, value chain of mobile payment and stakeholders involved in it will be described. The two mobile payment systems used for analysis are SQUARE and GOOGLE WALLET. According to the holistic analysis relevant risks and vulnerabilities will be explored, as well as the improvement that has been done to handle these threats.

The case study in this part will be used in the following security analysis. Information and data gathered in this chapter are regarded as the basis of the analysis constructed by dynamic network analysis tools.

Value Chain

[Smart Card Alliance 2008] explored value chains in terms of the four business models which are described in chapter 2. According to the roles and responsibilities of various stakeholders, each stakeholder contributes in different processes of value chain in different models. The following figure shows the main processes composing the mobile payment value chain.

![Figure 2-Value Chain of Mobile Payment Model](Image)

Through this value chain mobile payment environment involves all stakeholders according to their roles and behaviors. In this thesis, Square and Google appear as service providers in the payment environment. Service providers deploy mobile payment applications to consumers’ mobile devices and POS terminals to merchants. And the applications and terminals are provided as portals for customers to order and purchase products. Contactless (Google Wallet) or peer-to-peer (Square) technologies are used to perform the payment process. Secure payment requests will be sent to service providers and payment will be transferred to merchants’ accounts after successful identification. For account management, consumers and merchants establish user accounts with service providers (Square) or funds are transferred to merchants’ bank accounts directly (Google Wallet), therefore financial institutions are involved in the account management. For the market development the service providers would establish cooperation with retailers to provide value-added service.
Stakeholders

In this section, we define the participants involved in the operation of mobile payment. Understanding of key stakeholders in the transaction environment can help us explore critical assets and security risks related to the stakeholders. In the identification of the stakeholders, how they take their responsibilities and contribute to the mobile payment operation will be discussed.

As described above, a wide range of stakeholders with various motivations are involved to create effective and competitive mobile payment services. [Smart Card Alliance 2008] defined stakeholders in different business models of mobile payment. These are “banks”, “mobile operators”, “merchants”, “customers”, “peer-to-peer service provider” and “trusted service managers”. The definition of stakeholders in mobile payment is also done by [Mobey Forum 2012] which defines stakeholders in mobile wallet as “any organization or individual that provides, provisions or uses mobile wallets and their associated content and ecosystem.” The key groups of stakeholders in mobile wallets include “mobile wallet providers”, “mobile wallet users”, “mobile wallet content providers” and “payment service providers”. [European Payments Council 2012] discussed stakeholders in two kinds of mobile payment ecosystems, mobile contactless payment and mobile remote payment. In its report the most salient stakeholder in the mobile contactless payment ecosystem is the secure element issuer who is a trusted third party responsible for the issuance and maintenance of a secure element. And in the mobile remote payment ecosystem the mobile network operator is responsible for securely routing data, operating mobile network, issuing and recycling mobile phone number meanwhile the trusted service manager is a trusted third party acting on behalf of secure element issuers and/or application issuers.

In this thesis stakeholders of mobile payment are identified as “merchants”, “customers”, “mobile network operators”, “payment service providers”, “device manufacturers” and “financial institutions”. First of all, the customers, as the foundation, are end users of mobile payment. They use mobile network, employ applications and make transactions with owned mobile phones to generate value for other stakeholders in the ecosystem. Since the value is generated through the performed payment transactions, the mobile phones used to complete payment processes, personal and account information and their money stored and transferred in mobile payment system are the most valuable assets to customers.

As the other role in the service-use side, similar analysis can also be applied to merchants. Merchants can use point-of-sale to provide faster and easier checkout service to customers like they operate with credit and debit cards system. In addition to the checkout, merchants can make real-time interaction like offering discount and marketing information to customers through the mobile payment system. With the
increment in revenue and customer loyalty, merchants can benefit from the mobile payment. Further the low cost and security technology would enhance merchants’ acceptance of mobile payment services. According to the role played by merchants in mobile payment context, their merchandises, business accounts and benefits gotten from transactions are the most important assets to them. And the merchants also value their customer loyalty since it is the source of revenue.

On the other side, the service-providing stakeholders are comprised of mobile network operators, device manufacturers, payment service providers and financial institutions. [Varian and Shapiro 1999] constructed the fundamental principles of microeconomic analysis and identified seven key assets for the service providers. We list the seven assets below:

- Control over an installed and loyal customer base of users
- Intellectual property rights and the ability to enforce them
- An ability to innovate
- A first mover advantage
- Manufacturing abilities
- Strength in complementary products or services
- Brand name and reputation

The role and responsibility of mobile network operators have changed continuously in recent years. Now they are not only managing mobile network infrastructure, but also providing value-added services to users. In mobile payment mobile network operators are key contributors because they are controlling the basic communication network and have the largest amount of customers. And operators can stand on a significant position because through the SIM card and collaboration with phone manufacturers they can put the required applications in customers’ mobile phones. According to the essential role of mobile network operators in the mobile payment, the revenue can come from communication service and transaction fees. In addition to that, operators even can develop their own payment systems or applications embedded in mobile phones. As the discussion above, mobile network operators will value the control over the communication network infrastructure and the customer base of users.

Device manufacturers produce the devices used for operation of mobile payment. Compared to the mobile network operators, the manufacturers are controlling hardware devices to ensure the payment applications can be integrated with their products to provide comfortable user experience. Furthermore for the payment industry, manufacturers also need to ensure the security elements are successfully resided on their mobile devices. Their revenue comes from the sales of hardware devices and the collaboration with other stakeholders in providing service. Based on contribution of manufacturers in the ecosystem, they are more concerned with the availability and capability of mobile devices, as well as the branding for excellent sales.
The service providers mainly include operation system providers, payment application providers and value-added service providers. Operation system providers like Apple and Google develop and maintain the environment in which the payment applications are running. They need to keep updating the systems to ensure the security. Meanwhile the application providers act as trusted third-party developers to provide reliable applications performing mobile transactions. And value-added service providers offer advertisements, discounts and customer records to users in order to create remarkable customer experience. As the transactions are enforced with these applications, the assets that affect the security and usability of applications and operation environment will be critical for the service providers. According to the seven key assets researched by [Varian and Shapiro 1999], strength in complementary products or services and intellectual property rights are also significant.

The last but not least, the financial institutions are playing leader roles in mobile payment. Financial institutions provide customers’ financial services and customers choose financial institutions based on security and customer trust. As financial institutions have responsibility to manage customers’ financial accounts and have already established payment cards system, it would be a good way for them to increase customers and reputation by participating in secure mobile payment services and having harmonious cooperation with other stakeholders. Like mobile network operators are the manager of the environment where the transactions are processed in, the financial institutions have the capital stored in accounts and are handling the money transfer in payments, so they can get the opportunities to stand on the irreplaceable position. [Fiserv 2011] published a report about mobile payment from financial institutions point of view which indicated that the most important valuable assets for financial institutions is customer trust. Basically, the security of accounts and transmission is what the financial institutions actually concern.

**An overview of Square**

As mobile phones have been items which are brought with people every day, it has created so many opportunities to simplify our lives. While more and more social applications and entertainment applications are coming up in mobile environment, the appearance of payment service based on mobile device will bring us a revolution. Square is a company which was founded by co-founder of Twitter Jack Dorsey in 2009. It provides mobile payment service on mobile phones. Recently Square announced 2 million users have joined the payment platform and the trading volume has been over 6 billion dollars. After financing 250 million dollars, the valuation of this company has risen to around 4 billion dollars.

Processes of payment on Square are implemented with a white cube which is used as a credit card reader. Customers only need to swipe cards through the white cube attached with the merchants’ mobile devices to complete transactions. For the security of payment, Square also provides photo identification and transaction notification
service for customers. Now Square offers the cube device for free and takes revenues through transaction fees which are lower than the charge of general credit cards.

In addition to the simplified mobile payment service, Square has also developed application called “Card Case”. This application is regarded as payment service without cash, credit card and receipt. First users store their credit card information in the “card case”. Then customers can find the merchants supplying Square around them through the search service called “start a tab” in the “card case”, browse and purchase the merchandises they are interested in. Customers provide their names at checkout and merchants will search and check user information to complete the payment. In the new version of the application, favorite merchants’ information can be opened automatically when customers stay around the merchants without entering the stores.

Furthermore, according to the service offered by Square, many related value-added services can be brought up. Merchants can record and analyze their transaction information through the functions in the applications to understand what their customers like. And the service based on geography such as Google Map will be developed.
A holistic analysis of Square

In this part a holistic analysis of Square is constructed with the Systemic-Holistic Model [Yngström 2007]. Architecture, technical and non-technical aspects will be explored in order to have a better understanding of the environment the Square is operating in. Through this analysis the security-related risks and vulnerabilities can be identified clearly.

![Figure 3-Systemic-Holistic Model](image)

**Architecture**

In Square’s payment architecture all the payments are processed through the applications developed by Square and the applications are embedded in customers’ mobile phones. In common cases transaction data is switched and stored in Square’s databases, as well as the accounts information. But in the “card case” service the customers’ accounts information is also connected to their mobile phones. In this kind of architecture the third-party service provider is the only bridge between customers and merchants. The servers of Square have to face plenty security risks because of the stored sensitive data. Hackers can have unauthorized access to the servers to modify accounts and payment data and make the payment system out of services. Once the servers are compromised, a disaster to all users will occur.

Transactions information is transferred through mobile network to complete the payment. The threats aiming at channel security are also worried by customers and service providers. Intercept and modification to the transaction information in the network will cause security threats to the payment system.
Technical aspects

When customers swipe cards at checkout the white cube device can read credit card information and transform it to audio signal which is transferred to mobile phones through headset interfaces. The applications installed in mobile phones will code the signal and send the transaction data to Square servers through mobile network. During the processes, transmission in mobile network is known as one phase where security risks and threats will occur. Besides this, the signal transformation and signal coding are also potential risks in the payment processes. Hackers can use malwares and modify the Square application to steal credit card information. Generally payment is completed without a password, and the payment confirmation is based on customer signature. In order to provide security, Square has encrypted credit card information and transaction information before they are transmitted between white cubes and mobile phones, and also before the transmission in the mobile network.

Square also provides the payment service on android platform which is known as an open source environment. In this environment value-added services can be developed by users in order to share marketing information. But this will give hackers chances to destroy the payment application through learning the programming and creating applications with malware and vulnerabilities.

Non-technical aspects

For the non-technical aspects, Square provides tips to users about how to set their account passwords. And it is notified that employees in Square will not ask sensitive information about users.

According to the “card case” service, account information is linked with the mobile phones. If mobile devices are lost, someone else may use the account illegally to enforce payment. To prevent from embezzlement Square has the user-photo identification mechanism to enhance payment security.

As Square allows merchants to send marketing information and advertisements to customers, it may cause the occurrence of phishing scams and spam to steal customers’ account information.
**An overview of Google Wallet**

Google Wallet is an android mobile application providing mobile payment service. This application is embedded in mobile phones which support NFC technology to turn the mobile phones into virtual wallets. It stores the information of users’ credit cards, prepaid cards or gift cards in the phones and offer fast and convenient payment process at checkout. Google Wallet was launched in 2011 and in the first year, the devices supporting this service have expanded from only Nexus S 4G to many other mobile phones such as LG Viper. All these mobile phones are attached with NFC chips. Google has collaboration with MasterCard on the financial side, so the users can complete payment through the PayPass terminals at stores in United States. The users who have no CitiBank MasterCard need to recharge their Google Wallet accounts with prepayment [Google Wallet 2011].

As described above, this application stores information of users’ credit cards in mobile phones. These phones embedded with NFC chips communicate with PayPass terminals by tapping. Transaction data and card information will be transmitted to the terminals, as well as the marketing information like discounts or advertisements can also be sent to users’ mobile phones through the terminals. In order to provide the secure payment service the Google Wallet makes customers confirm payment by inputting their PIN codes.

After one year’s operation, Google Wallet is prevailing to provide not only quick and simple payment but consumption incentive and development of communication technology. But the popularization of Google Wallet still needs a variety of improvements like more mobile devices supporting the mobile payment service, collaboration with other financial institutions and security technologies.

**A holistic analysis of Google Wallet**

**Architecture**

As Google Wallet is a NFC-based mobile payment service, the POS devices which are used to receive the customers’ account information are needed at stores to perform the payment. Customers’ account data including credit card number, holder name and expire date are stored in their mobile phones. According to the sensitivity of the information, it turns mobile phones into potential targets to the people who want to steal this information with unauthorized access. Hackers can attack the payment applications or use other malwares to intercept users’ account data. Like the discussion in Square’s case, Google Wallet is also an application based on Android operation system which is an open source platform. This open environment is also a potential threat for the payment system.
Technical aspects

Google Wallet system processes payment with NFC technology which is under a two-way, short-distance and low-power communication protocol between two devices. Because NFC is a wireless communication between two devices, attackers can use devices with antenna to receive the transmitted data. In addition to the eavesdropping, attacker can also modify the transmitted data by transmitting valid frequencies of data spectrum at a certain time which can be calculated [Haselsteiner and Breitfuß 2006].

In the mobile devices supporting Google Wallet, NFC chips are embedded in the phones to complete data transmission by sending information of credit cards to the POS terminals. As payment application can read credit card data stored in the phones for payment, there is potential threat that other applications can also read the sensitive data. Furthermore since the NFC technology is a two-way communication and Google Wallet allows merchants to provide marketing information to customers, it gives hackers opportunities to use malwares or phishing mails to embezzle users’ account data. In order to provide security against this threat, Google fixes an encryption chip called “secure element” to control the access to data stored in mobile phones. All the communication between the applications and stored data is processed through this encryption chip [Google Wallet 2011].

Although Google Wallet is protected by secure element and other security mechanisms, there are still several security vulnerabilities threatening the system. A report by ViaForensics pointed out that data stored in various SQLite databases in unencrypted form includes holder name, the last four digits of credit card, card limit, expiration date, transaction dates and locations [ViaForensics 2011]. First researchers found that attackers can get the PIN codes with root or privileged control of the devices. This is because the PIN codes are stored in the application instead of the secure element [Rubin 2012]. Then another blog announced that the prepaid cards in the mobile phones can be used by others through cleaning the data for the Google Wallet application and resetting the new PIN codes [Fannin 2012].

Non-technical aspects

For the usage aspect of application, Google Wallet also has security mechanisms to protect sensitive data. When customers process payment, they need to input the PIN code to unlock the payment application and this procedure will be required to do again if the application has not been used for 30 minutes, and after five unsuccessful attempts to input the PIN code the Wallet application will be completely locked. According to the vulnerabilities described above by [Rubin 2012], Google suggests customers not to acquire the root privilege of the devices.

Besides the protection by PIN code, the NFC chips will be closed when the screens of
mobile phones are locked, which means no data can be transmitted if customers are only walking around a NFC reader.
Chapter 4

Security Analysis

Background

As we mentioned in chapter 3, the trades and communication within mobile payment environment create a large amount of data and information which is critical to users and developers. The vulnerabilities and threats targeting these data and information could result in losses to all the stakeholders involved in the mobile payment system.

Therefore the structure comprising the payment system has to keep the issues related to confidentiality, integrity and availability secure. In mobile payment content, many vulnerabilities and threats in payment system are similar to those in computer system such as viruses attached in emails or other applications to steal critical data about users’ accounts and trade information.

[Kadhiwal and Zulfikar 2007] described essential properties of mobile payment system in mobile payment security analysis and these properties are similar to the security aspects included in computer system: confidentiality, authentication, integrity, authorization, availability and non-repudiation.

As architectures analyzed in chapter 3, a secure element is required to enhance the security of mobile payment. [European Payments Council 2010] mentioned that “In other words, the experience in card payments has shown that no other technology or business process is as efficient and cost effective as the chip in mitigating risk of fraud.”[P. 11]

In addition to the technical aspects in security issues within mobile payment content, another aspect involved in mobile transaction is the trust. In some conditions, merchants or payment service providers may utilize the vulnerabilities to violate the transactions or steal confidential information of customers.

The trust that customers and merchants have in payment is one of the critical factors in mobile payments. Many other aspects including the security of payment transactions and the relationship between customers and payment service providers are also important to keep this trust [European Payments Council 2012].

Thus a security architecture which covers all security aspects in process level, application level and implementation level should be constructed for the mobile
payments ecosystem [European Payments Council 2012].

Security Properties

According to the description above and the knowledge about the security in information system, the security issues related to these properties will be discussed in this part.

Confidentiality

In the mobile payment environment, critical information should be concealed in order to protect the whole mobile payment system. The information includes user accounts data and transaction data. Even the social information stored in the mobile device is also worth the protection.

In the instance about Google Wallet, the information about user accounts is stored in the users’ mobile phones. It is possible to reveal and steal this account-related information because some data about holder name of credit card and expiration date is stored in unencrypted form in the database [ViaForensics 2011]. And the hackers may eavesdrop on the transaction data transmitted in mobile environment in order to modify it to make profit.

According to risks towards the critical information the devices providing Google Wallet service are embedded with secure elements which are used to control the communication between the applications and stored data [Google Wallet 2011].

Integrity

The integrity is an essential factor in the mobile payment to keep the transaction secure. It protects the payments from fake information which is a main reason of losses in E-business. The users of mobile payment service may face the fake or duplicated transaction information and even worse the payment application has been modified or corrupted. It is also important for merchants to ensure that they are doing business with legal owners of the transaction accounts.

Availability

All the transactions in mobile payment rely upon the availability of the mobile payment system. Unavailable systems or services would result in huge economic losses because the users are not able to manage their accounts and perform transactions. As in traditional network environment, DDoS (Distributed Denial of
Service) attacks are also a main threat to the availability of the mobile payment system.

No-repudiation

In the mobile payment content, not all the transactions are performed face to face. Like the “card case” service from the Square instance, the payment application could make it possible for consumers to purchase the goods when they are near the merchants without having to go into the stores. Therefore the no-repudiation will ensure that the users can’t deny the transactions that they have performed.

Access Control

The user accounts are the basis of the mobile transactions. Thus the access control of user accounts is critical to the security of the mobile payment system. Unauthenticated access and use of the user accounts will corrupt the foundation of payment systems. In order to keep the accounts secure, Google Wallet requires users to input PIN code to access accounts and to finish transactions. Meanwhile Square provides photo identification service.

Assets Analysis

As the stakeholders discussed in Chapter 3, related critical assets are identified according to the different roles of stakeholders. The extent in which these assets impact stakeholders determines the risk level of the security properties analyzed in the previous section. The method used is to construct a scenario based analysis of the assets concerned by different stakeholders such as Google Wallet and Square. For each asset a table showed below is used to indicate the risk level of security properties to different stakeholders. After the assets, analysis of vulnerabilities and threats will use the same method as well. The value of risk level is measured according to the extent in which the security properties are related to stakeholders and the extent in which economic interests of stakeholders are affected by destroyed security properties.
Accounts

The accounts composing of user name and password are regarded as the foundation of the mobile payment system. In addition to the credentials log-in information, the accounts also include the transaction history and the balance status. Even more, as the accounts are linked to the users’ credit cards to perform the payments, they have been virtual wallets controlling most of the users’ finance. If the accounts are compromised by hackers with malicious code, not only the log-in information but also the credit cards will be stolen.

In terms of stakeholders, security of accounts is important to all of them, but the extent to which it is critical differs within these stakeholders. Both in Google Wallet and Square instances, consumers perform and manage their payments with their accounts. So if the accounts are stolen by others, the consumers will lose their money stored in accounts and the linked credit cards. And for merchants, accounts don’t impact the merchants in the Google Wallet because the merchants don’t need to have accounts to accept payments. This is different to the merchants in Square where the risk is higher than that in Google Wallet. In Square the merchants need accounts to accept credit cards to finish payment, and they also link their own credit cards like their customers when they apply for this payment service. For the mobile network operators and device manufacturer they are not directly impacted by the account issues. For the payment service providers, as their revenue comes from the fee on service, the loss of accounts will not lead to profit loss. But finally they will suffer the loss of reputation and customers. For the financial institutions, as the accounts are linked to the credit cards, if the customer accounts are compromised, the credit cards linked with these accounts are all impacted. But the profit of financial institutions is from the transaction fees, therefore the financial institutions are not affected deeply by risks of user accounts.
<table>
<thead>
<tr>
<th>Security Properties</th>
<th>Merchant</th>
<th>Customer</th>
<th>Mobile Network Operator</th>
<th>Payment Service Provider</th>
<th>Device Manufacturer</th>
<th>Financial Institution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>H</td>
<td>H</td>
<td>L</td>
<td>M</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td>Integrity</td>
<td>H</td>
<td>H</td>
<td>L</td>
<td>M</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td>Availability</td>
<td>H</td>
<td>H</td>
<td>L</td>
<td>H</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td>Non-repudiation</td>
<td>H</td>
<td>H</td>
<td>L</td>
<td>M</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td>Access Control</td>
<td>H</td>
<td>H</td>
<td>L</td>
<td>M</td>
<td>L</td>
<td>L</td>
</tr>
</tbody>
</table>

Risk Level: High (H), Middle (M) and Low (L)

Table 6-Security Analysis of Accounts as Assets in Square

<table>
<thead>
<tr>
<th>Security Properties</th>
<th>Merchant</th>
<th>Customer</th>
<th>Mobile Network Operator</th>
<th>Payment Service Provider</th>
<th>Device Manufacturer</th>
<th>Financial Institution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality</td>
<td>L</td>
<td>H</td>
<td>L</td>
<td>M</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td>Integrity</td>
<td>L</td>
<td>H</td>
<td>L</td>
<td>M</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td>Availability</td>
<td>L</td>
<td>H</td>
<td>L</td>
<td>H</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td>Non-repudiation</td>
<td>L</td>
<td>H</td>
<td>L</td>
<td>M</td>
<td>L</td>
<td>L</td>
</tr>
<tr>
<td>Access Control</td>
<td>L</td>
<td>H</td>
<td>L</td>
<td>M</td>
<td>L</td>
<td>L</td>
</tr>
</tbody>
</table>

Risk Level: High (H), Middle (M) and Low (L)

Table 7-Security Analysis of Accounts as Assets in Google Wallet

**Hardware Device**

In terms of mobile payment, the mobile devices like mobile phones are the basic equipments for the operation. For the merchants in Google Wallet and Square, they all need mobile devices as POS to accept payments. If the mobile devices are stolen or compromised by hackers, information stored and transmitted in the devices such as user accounts and transaction data may be revealed and violated. This will cause huge damage to the users. Since the customers in Google Wallet and those who are using “Pay with Square” APP in Square need to use their mobile devices to perform their payments, the loss and corruption of mobile devices are equivalent to the loss of their real wallets, and also their credit cards.

For the payment service providers, they pre-embed the payment applications in
mobile devices, all the service they provide is enforced through mobile devices. Thus the theft and invasion of mobile devices will be a disaster to the trust and availability of mobile payment. For the device manufacturers, in the Square case, the service provider is also the device provider, so they have to face the high security risks of both software and hardware. If the encryption of the data in the device (card reader) can’t keep transactions secure, all the service will fail. And in Google Wallet instance, device manufacturers provide devices supporting NFC technology, and they need to ensure that the data can be transmitted securely and accept accurately. If it is easy to eavesdrop on and modify the data, the manufacturers have to suffer the loss of reputation and economy.

Square

<table>
<thead>
<tr>
<th>Security Properties</th>
<th>Stakeholders</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Merchant</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>H</td>
</tr>
<tr>
<td>Integrity</td>
<td>H</td>
</tr>
<tr>
<td>Availability</td>
<td>H</td>
</tr>
<tr>
<td>Non-repudiation</td>
<td>H</td>
</tr>
<tr>
<td>Access Control</td>
<td>H</td>
</tr>
</tbody>
</table>

Risk Level: High (H), Middle (M) and Low (L)

Table 8-Security Analysis of Hardware Device as Asset in Square

Google Wallet

<table>
<thead>
<tr>
<th>Security Properties</th>
<th>Stakeholders</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Merchant</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>H</td>
</tr>
<tr>
<td>Integrity</td>
<td>H</td>
</tr>
<tr>
<td>Availability</td>
<td>H</td>
</tr>
<tr>
<td>Non-repudiation</td>
<td>H</td>
</tr>
<tr>
<td>Access Control</td>
<td>H</td>
</tr>
</tbody>
</table>

Risk Level: High (H), Middle (M) and Low (L)

Table 9-Security Analysis of Hardware Device as Asset in Google Wallet
Business Data

In mobile payment environment security issues are related to all the business data transmitted in the network or stored in the mobile devices. For the merchants in both Square and Google Wallet they will provide business information about their products. For example, if merchants’ discount information transmitting to customers is modified, duplicated or intercepted, the business will be impacted deeply. And in Square since the transaction data is transformed into audio signal during the transmission, it is possible for hackers to eavesdrop on the data and even modify it. Meanwhile, customers will receive the receipt after they finish payments. If the receipt is lost during the transmission, customers will pay for the trades again. And the information involved in the receipt like the credit card numbers or names of holders are also sensitive information. For all stakeholders, mobile network operator is responsible for the network security. The mobile payment can’t be operated successfully without the secure transmission of business data in mobile network. If it is easy to eavesdrop on, intercept and modify the business data, not only the operation and reputation of network operator, but also the whole mobile payment context will collapse.

<table>
<thead>
<tr>
<th>Security Properties</th>
<th>Stakeholders</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Merchant</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>H</td>
</tr>
<tr>
<td>Integrity</td>
<td>H</td>
</tr>
<tr>
<td>Availability</td>
<td>H</td>
</tr>
<tr>
<td>Non-repudiation</td>
<td>H</td>
</tr>
<tr>
<td>Access Control</td>
<td>H</td>
</tr>
</tbody>
</table>

Risk Level: High (H), Middle (M) and Low (L)

Table 10-Security Analysis of Business Data as Asset in Square
Google Wallet

<table>
<thead>
<tr>
<th>Security Properties</th>
<th>Stakeholders</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Merchant</td>
</tr>
<tr>
<td>Confidentiality</td>
<td>H</td>
</tr>
<tr>
<td>Integrity</td>
<td>H</td>
</tr>
<tr>
<td>Availability</td>
<td>H</td>
</tr>
<tr>
<td>Non-repudiation</td>
<td>H</td>
</tr>
<tr>
<td>Access Control</td>
<td>H</td>
</tr>
</tbody>
</table>

Risk Level: High (H), Middle (M) and Low (L)

Table 11-Security Analysis of Business Data as Asset in Google Wallet

**Threats and Vulnerabilities**

According to the stakeholders and critical assets discussed above, here the potential threats and attacks are described.

[Holland 2011] constructed a survey on the threats in mobile payment. In network threat participants considered, Wi-Fi has the highest risk to the mobile payment. And in media threat participants considered, SMS, E-mail, Browser and Applications are ranked from high to very high risk, with SMS considered as the highest one. For the attack part, participants ranked social engineering attack and malware attack as the most dangerous attacks that hackers could employ to destroy the mobile payment system. And from the user’s point of view, the education of consumers is also a high risk concerned by the participants. Obviously this can be a threat in case of consumers use guessable or default PINs or passwords [Pihlajamäki 2004].

**Attack Scenarios**

Social engineering attack is the way that hackers use to gain the trust of consumers in order to capture critical information like user name, password and credit card number. Attackers impersonated as officers use fake call, message and e-mail which is the most popular way in virtual world to ask for user’s password and other important information. In Square instance, once the credentials are provided to the hackers, they will take control of user’s account and process their transactions. And if they get the credit card information, they may forge the card to perform payment in merchants like the real user. In addition to the fake email, the applications in App store are also a good way to process phishing. In 2011 some Android applications which purported to be mobile apps for legitimate financial institutions were found to be faked, and they captured bank credentials from the consumers [Holland 2011]. Apart from bank apps,
this situation can happen to Square app as well. But it is lower risk to Google Wallet as the applications are pre-embedded in the mobile phones.

Malware is another way to attack the mobile payment system. Malware like viruses and Trojans are always embedded in some third party applications. Once user runs these applications the malware can be enforced automatically to steal the confidential data and send it to hackers or perform attacks like DDoS to the payment system. For example, the malware can start a huge number of transaction requests at the same time to make the system unavailable.

As transaction data is transmitted through the mobile network, the mobile environment has been risk to the information transmitted in it. Electrical disturbance and electrical interruption can make the system out of service in order to result in loss of sales. And eavesdropping will release sensitive information through the network and meanwhile the business can be modified by hackers as their purposes [Ivarsson 2008].

In addition to the threats from hackers and users, the weakness of mobile payment system and application is also very risky. In the case of Square, hackers can develop a fake application installed in their mobile devices and skim the consumer’s credit card information using the dongle from Square [VeriFone 2011]. For Google Wallet, [ViaForensics 2011 ] has analyzed the security vulnerabilities in Google Wallet. They found that the name on the credit card, the expiration date, last 4 card digits and email account are all recoverable. And when transactions are deleted or Google Wallet is reset, the data can be recoverable as well. After the ViaForensics, a security firm Zvelo had another analysis to realize that Google Wallet’s app database storing PIN code can be hacked and they even created an application running on Android to reveal the PIN code [Rubin 2012].

<table>
<thead>
<tr>
<th>Threats and Vulnerabilities</th>
<th>Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Account</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>H</td>
</tr>
<tr>
<td>Malware</td>
<td>H</td>
</tr>
<tr>
<td>Network Threats</td>
<td>M</td>
</tr>
<tr>
<td>App Weakness</td>
<td>H</td>
</tr>
</tbody>
</table>

Risk Level: High (H), Middle (M) and Low (L)

Table 12-Security Analysis of Threats and Vulnerabilities in Mobile Payment

33
Chapter 5

Analysis through DNAT

Background of DNAT

As the traditional social network analysis can’t adapt to the dynamic nature of organizational forms adequately, Kathleen Carley, Jeffery Johnson and other analysts developed the dynamic network analysis which considers the factors leading to temporal changes in network structure and performance of organization. For the complex systems, dynamic network analysis provides visualization of the system networks. It is a good way to understand the entities involved in the network and the relationships within them. As the mobile payment system is a complex network with multi-stakeholders, multi-assets and threats, dynamic network analysis can help us understand the risks and impacts in the mobile payment environment.

One of the three key advances that extend social network analysis to the dynamic analysis and multi-color networks is the Meta-Matrix [Carley 2000]. It is an approach providing representational framework and a family of methods for the analysis of organizational data. The following table illustrates the meta-matrix with entities and inter-linked networks.

<table>
<thead>
<tr>
<th>People</th>
<th>Knowledge/Resources</th>
<th>Events/Tasks</th>
<th>Organizations</th>
</tr>
</thead>
<tbody>
<tr>
<td>People</td>
<td>Social network</td>
<td>Knowledge network</td>
<td>Attendance network</td>
</tr>
<tr>
<td>Knowledge/Resources</td>
<td>Information network</td>
<td>Needs network</td>
<td>Temporal ordering</td>
</tr>
<tr>
<td>Events/Tasks</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organizations</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 13-Meta-Matrix showing relationships within nodes entities [Carley 2000]
Under this matrix, organization is considered as being comprised of a set of elements which are presenting below:

<table>
<thead>
<tr>
<th>Personnel</th>
<th>Individual agents within the organization (human or otherwise) which are capable of contributing labor to task performance and which form a locus for knowledge (procedural or declarative), social contacts, task assignments, and/or control of resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Knowledge</td>
<td>Functionally coherent elements of procedural or declarative information (generally pertaining to organizationally relevant task performance) to which agents may have access (often synonymous with human capital)</td>
</tr>
<tr>
<td>Resource</td>
<td>Passive elements of organizational structure which act as inputs to task performance and which may be controlled by agents (often synonymous with physical capital)</td>
</tr>
<tr>
<td>Tasks</td>
<td>Organizational objectives which must be met by a specified agent performance (usually involving resources and/or knowledge)</td>
</tr>
<tr>
<td>Organizations</td>
<td>Organizational entities beyond the entity under immediate study (i.e., other organizations within the environment)</td>
</tr>
</tbody>
</table>

Table 14-Elements and Relationships comprising Organizations [CASOS website]

The more connections a node or link attached in the system the more threats and risks it will suffer because all these relationships rely on them. Some specific measurements such as centrality, network density and hubs can be used to determine risks within the system. And the centrality measures combined with other analyses are the most relevant in risk analysis [Armstrong and McCulloh 2010]. In order to construct the analysis and extract the measurements, the Organizational Risk Analyzer (ORA) is selected in this thesis. It is a dynamic meta-network assessment and analysis tool developed by CASOS at Carnegie Mellon. ORA can identify key players, groups, vulnerabilities and model network changes over time.

Implementation

To analyze the risks and vulnerabilities with ORA, the objects and related relationships are described according to the set of elements and their inter-linked connections discussed above. For this thesis, the meta-network required for ORA can be constructed by the information provided in the case study and the security analysis. Stakeholders and identified critical assets will be input as nodes in ORA, and the risk degrees analyzed in assets analysis and threats analysis will determine the relationships between different nodes.

The first class of nodes identified as people/personnel is user account in the case study of mobile payment. The cluster of nodes about knowledge is the skills and knowledge
required to use and perform the mobile payment service. The resource nodes are all the critical assets including hardware and software used to perform the payment. Finally the event nodes are potential vulnerabilities and risks within mobile payment system. The node classes created in the analysis are agents, resource, knowledge and events. And the networks illustrating the relationship between two nodes are classified as: agent-agent, agent-resource, agent-knowledge, event-agent and event-resource. The meta-network composing of all the nodes and networks will be inputted in ORA in order to analyze the critical nodes and risks in mobile payment system. Since the merchants in Google Wallet accept the payment without user accounts, Square is selected to perform the DNAT analysis.

**Results and Discussion**

In this section research results are discussed according to the research questions presented in Chapter 1.

The meta-network of Square constructed for the analysis includes four node classes and five networks. As the stakeholder is the participant in the mobile payment, it is analyzed according to the relationships with other node classes and after the stakeholders resource was also analyzed in terms of the threats in the network.

![Figure 4-Meta-Network for Mobile Payment System of Square](image)

Through the visualization of the agent-resource network, we can see that hardware and business data are the most critical assets in the mobile payment. And to the stakeholders in this network, consumers, merchants and service providers are the stakeholders who have the most connections. But in terms of the different weight of the links, consumers and merchants are the most important stakeholders in the mobile
payment environment.

![Figure 5-Agent and Resource Network](image)

From the event-resource network, it is illustrated that user account has the highest risk from the threats. Account is connected with all the threat nodes in event class, and malware, social engineering and app weakness are the main risk to user account. Similarly, business data also has the same three threat connections with the same weight as user account. This can support the situation presented in agent-resource network that business data is key factor for the mobile payment.

![Figure 6-Event-Resource Network](image)

According to the visualization of agent-resource-event network, it is presented that account and business data have the most connections in the network. Consumers and merchants use the accounts to perform the payment and the business data is the content of the transactions. Therefore if threats occur towards these two assets in the network, all the transactions will be impacted and the whole mobile payment system will collapse. And as the central location of the consumers and merchants, it denotes that these two stakeholders are the most critical stakeholders in the network.
In addition to the visualization analysis, diverse measures can be used to analyze the impact from threats to stakeholders and assets. The Capacity of threats illustrates the extent in which the various threats affect the network. In the threat capacity between risks and assets, it presents that malware, network threat and app-weakness are the main threats to the assets with malware is the highest risk. Malware could affect performance of payment through the impact on business data and account. Social engineering only affects the user account. And from the capacity between risks and stakeholders, we can see that malware is also the threat with most connections with stakeholders. Network threat could impact the operation of mobile payment as well, thus it has similar capacity as malware.
The Centrality in Degree of risks and assets measures the higher or lower relevance between the threats and assets. It confirms that user account has the highest risk when threat occurs. Meanwhile, in terms of the same measure of risks and stakeholders, consumers, merchants and service providers run the highest risk if threat happens.
Figure 11-Centrality of Risks and Stakeholders
Chapter 6

Conclusion

Conclusions

According to the results from analysis with ORA, the research questions presented in Chapter 1 can be answered. In chapter 3 and chapter 4 related stakeholders and critical assets were discussed. In chapter 4 we also identified the potential relevant threats in the mobile payment environment. The relationships and impacts within threats, stakeholders and assets are analyzed in this chapter.

In terms of the research questions mentioned in chapter 1, stakeholders living in mobile payment environment are classified as consumers, merchants, payment service providers, network operators, hardware manufacturers and financial institutions. The critical assets related to stakeholders are identified as user account, hardware device and business data. And from the threats and vulnerabilities analysis, malware, network threats, social engineering and app weakness are the main threats to the mobile payment system.

For the whole mobile payment system, consumers and merchants are fundamental participants in the transactions, thus the two stakeholders encounter the biggest risk in mobile payment environment. This result is similar to the description in the report published by [Mobey Forum 2012]. It is mentioned that merchant plays a significant role in success of mobile payment, and their involvement and commitment is vital for the success of mobile wallet. Meanwhile the report said that consumers generate value for all the other stakeholders in the ecosystem. As the service providers have the direct connections with consumers and merchants, they are running the same high risk as these two. To all the stakeholders, hardware and business data are the most critical assets but to consumers and merchants, user account is what they are most concerned about. User account is impacted by various threats deeply, as well as the business data transmitted in the mobile network and stored in mobile devices. Lastly, in the diverse threats, malware is the one which affects most stakeholders and assets. Similar phenomenon is also mentioned in other’s report. PCI Security Standards Council indicated that malware is one of the top security threats to mobile payment.

From the analysis of mobile payment, it’s important that users and developers are aware of threats related to their assets and how to protect their assets. Users of mobile payment should update the security of applications according to the official release and download the payment applications from official websites. And the service
providers need to not only improve the security technology in products, but also provide guide about security for users.

**Limitation and Further Work**

As the dynamic network analysis tool ORA is used to analyze organizational networks or complex systems, much more information can be found out with these dynamic network analysis tools. There are lots of other measures in DNA tools that can be used to indicate more reliable results. Through this method the system analyzed will be understood holistically, therefore this results in some challenges in the exploration. It requires all available situations to be considered for the data collection in order to make the analysis as reliable as possible. As the author of the thesis is using the dynamic network analysis tool for the first time, learning to use the tool efficiently is also a challenge in the research processes. Furthermore, in the part of threats and risks analysis the users’ own behavioral threats are not considered. For example, the lack of education of users can be a risk impacting the security of payment transactions.

According to the background part and the research results in this thesis it is indicated that the mobile payment has been developing rapidly. All the stakeholders in the environment are trying to take advantage of their superiorities in order to get a leader position. As the prevailing of existing cases like Square and Google Wallet the mobile payment has potential of becoming a new economic platform to change people’s lives. Thus research about this field will be more and more thriving. There are still plenty of questions that can be explored in terms of security issues within mobile payment. Many different payment systems based on different payment methods can be analyzed to complement this field. And other research methodologies and risk analysis tools can be used to analyze the security risks and threats.
References


CASOS website, [Online], Available:  

Coleago Consulting (2011) “Who will win the mobile payments standards war?”.  
Published 26th Sep, 2011, [Online], Available:  
http://www.coleago.co.uk/uploads/media/Who_will_win_the_mobile_payments_standards_war.pdf [August 2012]


EnfoDesk (2012) ”Market data of mobile payment in China, 2011”, [Online], Available:  

[Online], Available:  

[Online], Available:  

Fairweather, A. (2011) “Four very different mobile payment services”, [Online], Available:  
http://ventureburn.com/2011/06/4-very-different-mobile-payment-services/ [June 2012]

Fannin, H. (2012), “Second Major security flaw found in Google Wallet”, [Online], Available:  
http://thesmartphonechamp.com/second-major-security-flaw-found-in-google-wallet-rooted-or-not-no-one-is-safe-video/ [June 2012]


Ivarsson, S. (2008) ”Mobile payment with customer controlled connection-Can it be constructed to be safe enough?”, Department of Systems and Software Engineering, School of Engineering, Blekinge Institution of Technology.


Mobey Forum (February 2012) “A series of White Papers on Mobile Wallets Part 2: Control Points in Mobile Wallets”.


Perlman, L. (April 2010) “Regulatory and legal issues in mobile financial services in the developing world”, Macroeconomics of Mobile Money, CITAL.


Secure Mobile Payment Services (SEMOPS), [Online], Available: http://www.semops.com [June 2012]


Abbreviation

AAA: Authentication Authorization Accounting

APP: Application

CASOS: Computational Analysis of Social and Organizational Systems

CDMA: Code Division Multiple Access

DNAT: Dynamic Network Analysis Tools

DDOS: Distributed Denial of Service

GSM: Global System for Mobile Communication

IPSEC: Internet Protocol Security

IPV6: Internet Protocol Version 6

J2ME: JAVA 2 Platform, Micro Edition

KSSL: Kylobyte Secure Sockets Layer

NFC: Near Field Communication

ORA: Organizational Risk Analyzer

PDA: Personal Digital Assistant

PIN: Personal Identification Number

PKI: Public Key Infrastructure

POS: Point of Sales

RFID: Radio Frequency Identification

SAT: Subscriber Identify Module Application Toolkit

SATSA: Security and Trust Services Application Programming Interface
**SIM:** Subscriber Identify Module

**SMS:** Short Message Service

**SSL:** Secure Sockets Layer

**USSD:** Unstructured Supplementary Service Data

**WIMAX:** Worldwide Interoperability for Microwave Access

**WTLS:** Wireless Transport Layer Security

**3G:** 3rd Generation of Mobile Telecommunication Technology