Mobile Banking Security

A security model

Imran Ashraf MSc – imran.ashraf@gmail.com
Post Graduate IT Audit – Vrije Universiteit, Amsterdam
Student number 2043068
Thesis number 1073
The Hague, The Netherlands – April 2012

University supervisor
Dr. R.P.M. Mattheijse RE
Vrije Universiteit

Company supervisor
Drs. E.J.M. Ridderbeekx RE CISA
ABN AMRO Bank N.V.
Acknowledgements

Firstly I would like to thank René Matthijse and Ed Ridderbeekx for their supervision and guidance, starting from the definition phase up to the final stages of this research.

Secondly I would like to thank all the people who provided me with feedback when I first drafted my research proposal and the people who were kind enough to contribute to this research: Martijn Bot, Jean Paul van Deursem, Hans Koster, Taeke Kooiker, Hans Lameijer, Ad de Visser and Nikki Webster.

Lastly I would like to thank my family. My mother who has endured much hardship to provide me with the opportunities that have allowed me to stand where I am today. My little brother who always puts a smile on my face with his crazy ideas. And my fiancée, my research is done, but you are the one who completes me.

Imran Ashraf

The Hague, April 2012

Illustration on the front page by Melanie Colosimo and is available through Creative Commons license ((by-nc-nd 3.0)).
Abstract

When dealing with security aspects for mobile banking in the context of mobile devices and applications, a few common themes emerge. If these themes are not addressed properly, through security controls and measures, the underlying threats could compromise the confidentiality, integrity and availability of mobile security assets. Mobile security assets that need protection are mobile devices, the mobile application and private information. Eight threats were identified in this research. These threats can be categorized in the following manner: users, devices, applications and data, and governance. Based on this categorization and interviews with professionals in the field of banking and IT security, the Mobile Banking Security Model was created which can be used to define security controls and measures, perform risk assessments for mobile banking in the context of mobile devices and mobile applications or in preparation of audit fieldwork.

Keywords:
Mobile, banking, security, device, app, application
# Table of contents

Acknowledgements .......................................................................................................................... 3
Abstract ............................................................................................................................................ 5

Chapter 1: Introduction ..................................................................................................................... 11
  1.1 Rationale for research ................................................................................................................ 12
  1.2 Scope, research objectives and questions .................................................................................. 12
  1.3 Research methodology .............................................................................................................. 14
  1.4 The structure of the thesis ......................................................................................................... 14

Chapter 2: The current state of mobile banking .............................................................................. 15
  2.1 Chapter outline .......................................................................................................................... 15
  2.2 Mobile banking ........................................................................................................................ 15
    2.2.1 Definition of mobile banking ............................................................................................... 16
    2.2.2 Advantages of mobile banking for the customer ................................................................. 16
    2.2.3 Advantages of mobile banking for the financial institution ............................................. 17
    2.2.4 The current state of mobile banking in the Netherlands .................................................... 17
  2.3 Future direction of mobile banking ........................................................................................... 23
  2.4 Chapter summary ...................................................................................................................... 25

Chapter 3: Security challenges for mobile banking ........................................................................... 27
  3.1 Chapter outline .......................................................................................................................... 28
  3.2 Security assets .......................................................................................................................... 28
    3.2.1 Mobile device as a security asset ........................................................................................ 29
    3.2.2 Mobile application as a security asset ................................................................................. 29
    3.2.3 Information as a security asset ............................................................................................ 29
  3.3 Security objectives .................................................................................................................... 29
    3.3.1 Confidentiality .................................................................................................................... 30
    3.3.2 Integrity ............................................................................................................................... 31
    3.3.3 Availability .......................................................................................................................... 31
  3.4 Threats ....................................................................................................................................... 32
    3.4.1 Lack of user awareness ....................................................................................................... 33
3.4.2 Malware .................................................................................................................. 34
3.4.3 Eavesdropping ....................................................................................................... 36
3.4.4 Denial of Service ................................................................................................. 36
3.4.5 Unauthorized access ............................................................................................ 37
3.4.6 Device or application malfunction ....................................................................... 38
3.4.7 Loss, theft and improper disposal of devices ....................................................... 39
3.4.8 Platform Alteration .............................................................................................. 39
3.5 Chapter summary ...................................................................................................... 40

Chapter 4: Security model for mobile banking .............................................................. 41
4.1 Chapter outline .......................................................................................................... 41
4.2 Categorization of identified risks ............................................................................. 41
4.3 Security assets per categorized threat ..................................................................... 43
  4.3.1 Users .................................................................................................................... 45
  4.3.2 Devices ............................................................................................................... 45
  4.3.3 Applications and data ........................................................................................ 45
  4.3.4 Governance ....................................................................................................... 46
4.4 Chapter summary ...................................................................................................... 46

Chapter 5: Case analysis of security model and controls .............................................. 47
5.1 Chapter outline .......................................................................................................... 47
5.2 Types of controls ....................................................................................................... 47
  5.2.1 Preventive controls ............................................................................................ 47
  5.2.2 Detective controls .............................................................................................. 48
  5.2.3 Corrective controls ............................................................................................ 48
5.3 Control measures for the mobile banking security model ....................................... 48
5.4 Chapter summary ...................................................................................................... 50

Chapter 6: Synthesis of findings and conclusions .......................................................... 51
6.1 Chapter outline .......................................................................................................... 51
6.2 Synthesis of findings ............................................................................................... 51
  6.2.1 Clear roles and responsibilities of internal and external stakeholders .. 51
  6.2.2 Customer awareness is important .................................................................... 52
6.2.3 Quality of own product should be above any doubt........................................53
6.2.4 Investing more in detective controls.............................................................53
6.2.5 Support processes should be in place...........................................................53
6.3 Recommendations for further research.........................................................54
6.4 Chapter conclusion .......................................................................................54

Chapter 7: Concluding the research ....................................................................55

References ...........................................................................................................57
Appendix .............................................................................................................61
Chapter 1: Introduction

*"I saw a bank that said "24 Hour Banking", but I don't have that much time."*  
-- Steven Wright (American comedian)

‘Information. Anywhere, any time, on any device.’ That was the mantra proclaimed during the dot-com era. Even though “any device” also included mobile devices, the technology was not mature enough to offer the same kind of experience as personal computers. Mobile devices lacked the processing power and had slow data connections to perform smooth operations.

Today we see a resurging mobile revolution. This revolution rides on devices that feature powerful processors, increased storage, fast data connections, greater user experience and a myriad of applications. The promises made at the turn of the century are finally coming true.

One of those promises was banking using a mobile device. Not only does it give the customer the convenience of banking anywhere and anytime, it also gives the financial service provider another channel to serve the customer, in addition to local branches, the telephone and the internet.

Offering internet banking on a mobile device introduces its own unique challenges that have to be dealt with, for example security issues which could undermine the trust customers have in their bank. Trust is one of the fundamental cornerstones of banking. Without it, it would be hard for banks to stay in business. However, the customer also expects traditional banking services on mobile devices. Furthermore, with the increased sales of mobile devices, transaction volumes originating from mobile devices will keep on increasing. Mobile devices are a development a bank cannot ignore if it does not want to be left behind by its competitors.
1.1 Rationale for research

What is so interesting about mobile devices, on which mobile banking services are offered, is that it is a new field. However, the process of shifting from platform to platform, which is taking place, is not new. Payment solutions used to run on exclusively on mainframes in large data centres. Later there was a shift to a client server model, where one had to install software on a local PC to send payments to the bank. Then Internet Banking was introduced, using a web browser one could login to a secure site to send and receive payments. Now we see yet another platform, the mobile platform. There are multiple vendors with each their own platform (e.g. iOS, Android, BlackBerry) and each has its strengths and weaknesses. These strengths and weaknesses may influence how the customer perceives mobile banking services, which in turn influences the adaptation of the service offered.

Mobile devices have been researched before. However, the focus has been on the usage of mobile devices within a corporate environment. Controlling the mobile device, the applications that run on the device and the data it contains in terms of confidentiality, integrity and availability, has been of upmost importance. An example of this is the widespread usage of Blackberry devices, since these can be configured and locked to a high degree. Other manufacturers also offer device management tool kits. When a bank offers financial services to the customer, through a customer owned mobile device, much of that control is lost.

1.2 Scope, research objectives and questions

In the context of our research, the term “mobile devices” refers to smart phones (e.g. BlackBerry, iPhone), personal digital assistants (PDAs) (e.g., iPod) and tablet devices (e.g. iPad) that enable access to the Internet and to services offered through the Internet using an application installed on that mobile device. Our definition of mobile devices does not include laptops/notebook personal computers.
Furthermore our research focuses on the consumer usage of a banking application ("app\(^1\)) installed on customer owned mobile devices. The security of the network (e.g. the GSM network) or services running on the side of the bank (e.g. bank-end services for payment processing) are not in scope of this research. The type of applications in scope are mobile banking applications, which will be defined further in chapter 2. Furthermore our research is geographically limited to apps offered by financial institutions in the Netherlands. This however does not mean that the conclusions are not applicable to other countries.

![Services at bank side, The internet, Mobile banking app on device]

Main research question:

*What are the security aspects of mobile banking and what controls can be applied to address those aspects?*

In order to answer the main research question the following three sub questions need to be answered:

1. What is the current state of mobile banking?
2. What are the security challenges when dealing with mobile banking on mobile devices?
3. What are the controls and measures that can be applied to address the security challenges for mobile banking?

\(^1\) The term app is an abbreviation of application. In this research both terms are used interchangeably.
1.3 Research methodology

This research starts with a solid theoretical basis into mobile banking, mobile device and application security. From this theoretical basis an overview of threats to mobile banking applications will be given. Interviews with professionals in banking and IT security will be conducted to define controls and measures for mobile banking. This will culminate in a synthesis between theory and practice that will complete the security model for mobile banking.

1.4 The structure of the thesis

This thesis is divided into three parts. The first part outlines the theoretical background of the subject. Part two focuses on an analysis of the theoretical background from an IT security perspective. Lastly in the third part a case study will be performed and the conclusion will be presented where the main research question will be answered.

In chapter 2 a short overview will be given of the current mobile banking landscape and the devices used to access mobile banking services. After the introduction to the object of study, the security challenges on the main mobile platforms offered today to the customer will be examined in chapter 3.

In chapter 4 the outcomes from chapter 3 will be categorized into a security model for mobile banking in the context of mobile banking and applications. Controls and measures in order to minimize the risk of the threat will be based on expert interviews. The results from those interviews will be covered in chapter 5.

Our research will conclude with a synthesis of the outcomes from the previous chapters in chapter 6. Recommendations for further research will be given. In chapter 7 the sub questions and main research question of chapter 1 will be revisited.
Chapter 2: The current state of mobile banking

The number of mobile devices in use continue to rise. For example, with around 6 billion mobile phones currently in use (GSM Association 2011) it is hard to argue with the success of mobile devices. With a rapid adoption rate over the years, mobile phones have become a natural extension of the people who use them in a wide range of activities. Not only did mobile phones change the way people communicate with each other, but they also changed the way information is processed and how business is conducted.

Before the security aspects of mobile banking can be discussed, an overview of the current landscape is in order. This will be done in this chapter. By the end of this chapter we should have a good understanding of the current state of mobile banking.

2.1 Chapter outline

In this chapter one of new uses of mobile devices will be examined, namely banking. First mobile banking will be defined. Then an overview of the current mobile banking landscape in the Netherlands will be given and the current mobile banking offers in the Netherlands. Lastly the future direction of mobile banking will be discussed.

2.2 Mobile banking

Accessing banking services on a mobile device give customers a high degree of freedom. Not only does it put them in charge, it also enables them to do their banking independently of their location and time. In traditional banking, a customer needs to be present at one of the branches of a bank and has to take into account the opening hours the bank has established. In the 1990s banking for customers using modems (e.g. Telebankieren) was introduced in the Netherlands and it allowed customers to do their banking from home using a personal computer. Customers were put in charge of their own banking activities. Mobile banking gives the customer another degree of freedom, namely geographical independence.
2.2.1 Definition of mobile banking

We see that banks have seized the widespread use of mobile devices as an opportunity to connect with their customers. Several types of products can be offered, for example a way to transfer funds using a mobile device, or as a virtual wallet. A clear distinction can be made between mobile payment and mobile banking. X. Hu et al. (2008) define mobile payment and banking as ‘using mobile phones to pay for services (bus, train, movies, entertainments), goods (retails stores, coffee shops, restaurants, vending machines, online stores), bills (electric, gas, credit cards, phone), and transfer funds (bank to mobile, bank to bank, mobile to mobile)’.

It is important to note the difference between mobile payment and mobile banking. In the context of transferring funds, mobile banking is a subset of electronic banking (Barati & Mohammadi 2009) and mobile banking (in a broader sense) can be defined as ‘that type of execution of financial services in the course of which [...] the customer uses mobile communication techniques in conjunction with mobile devices’ (Pousttchi & Schurig 2004). There are several types of mobile banking. For completeness, these different types are described in paragraph 2.2.4. The type of mobile banking which will be examined for this research will be described there.

Mobile payments on the other hand, are a way to pay for a product or service in a retail environment using a mobile device, whereas mobile banking is based on the banks own systems and infrastructure (Mallat 2006). An example of a mobile payment is the usage of a mobile phone that contains a small chip where the mobile phone has to be held in front of a terminal. A wireless connection is then set up to initiate the transaction. An example of mobile banking is accessing the internet banking site of a bank using the phone’s web browser or a dedicated application installed on the mobile phone.

2.2.2 Advantages of mobile banking for the customer

Mobile banking has several benefits for the customer. It enables customers to perform their banking activities anywhere, any time and at a lower cost (Esmaili et al. 2011; Suoranta 2003). As stated previously, they do not have to travel to a branch anymore. Furthermore it gives the customer access to the information relevant to
them, be it a request for the current account balance or an overview of recent transactions. Traditionally one would have to call or visit the bank to find the latest account balance, or the status of a transaction. Finally, it puts customers in the driver’s seat of their own banking; they can initiate transfers or buy and sell stock orders.

2.2.3 Advantages of mobile banking for the financial institution
Mobile banking increases the advantages which electronic banking offers to the bank. Processing an electronic transfer is less costly than a traditional transfer. Burgelman and Bamford (Rao, Louis Minakakis 1999) indicate that a ‘trip by a customer to a retail bank location costs the bank approximately $5 per transaction, a phone call costs $1 per transaction, while an online transaction costs a mere 10 [dollar] cents.’. This is caused by the fact that no personnel are needed to perform the actions and in the long run fewer branches are needed to facilitate the customer. Mallat et al. (2004) describe mobile banking services as modified version of existing banking services. Mobile banking uses the current electronic banking environment, which enables optimal usage of the existing IT infrastructure. Lastly, the usage of mobile banking appeals to a brand new demographic, which have grown up with such devices. If a bank does not offer services which appeal to this demographic, it will seek a competitor who does.

2.2.4 The current state of mobile banking in the Netherlands
In order to give an overview of the current state of mobile banking in the Netherlands, the mobile banking offers of the large banks in the Netherlands will be examined. For this, the “system bank” definition will be used. A system bank is a bank that is crucial to the financial system of the Netherlands. In November 2011 the Ministry of Finance and DNB qualified four banks in the Netherlands as system banks (ANP 2011):

- ING Bank;
- RaboBank;
- ABN Amro Bank;
- SNS Bank.
For these four banks, three types of financial services were found, which fit the definition used for mobile banking:

- Mobile website banking
- SMS-banking
- Mobile banking client on mobile phone

Results of the mobile banking inventory process can be found in tables 1 to 6. Results exclude marketing oriented services (e.g. RaboBank offers the Rabo Hockey app, since it sponsors the national hockey team)

<table>
<thead>
<tr>
<th>Mobile website</th>
<th>Balance enquiry</th>
<th>Transactions</th>
<th>Transaction history</th>
</tr>
</thead>
<tbody>
<tr>
<td>RaboBank</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
<tr>
<td>ING Bank</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>ABN Amro Bank</td>
<td>-²</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>SNS bank</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
</tr>
</tbody>
</table>

Table 1: Mobile banking through mobile website

<table>
<thead>
<tr>
<th>SMS Banking</th>
<th>Alerts</th>
<th>Balance enquiry</th>
<th>Transactions</th>
</tr>
</thead>
<tbody>
<tr>
<td>RaboBank</td>
<td>yes</td>
<td>yes</td>
<td>yes³</td>
</tr>
<tr>
<td>ING Bank</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>ABN Amro Bank</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>SNS bank</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
</tr>
</tbody>
</table>

Table 2: Mobile banking through SMS

² Closed per 01-09-2009 due to low usage (ABN Amro Bank N.V. 2009)
³ Using 3rd party mimitix
<table>
<thead>
<tr>
<th>Rabobank</th>
<th>Client application: RaboBankieren App</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>iPhone</td>
</tr>
<tr>
<td>Balance Enquiry</td>
<td>yes</td>
</tr>
<tr>
<td>Transactions</td>
<td>yes</td>
</tr>
<tr>
<td>Transaction history</td>
<td>yes</td>
</tr>
</tbody>
</table>

Table 3: Rabobank Mobile Banking through client application

<table>
<thead>
<tr>
<th>ING Bank</th>
<th>Client application: ING Bankieren</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>iPhone</td>
</tr>
<tr>
<td>Balance Enquiry</td>
<td>yes</td>
</tr>
<tr>
<td>Transactions</td>
<td>yes</td>
</tr>
<tr>
<td>Transaction history</td>
<td>yes</td>
</tr>
</tbody>
</table>

Table 4: ING Bank Mobile Banking through client application

<table>
<thead>
<tr>
<th>ABN Amro Bank</th>
<th>Client application: Mobiel Bankieren</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>iPhone</td>
</tr>
<tr>
<td>Balance Enquiry</td>
<td>yes</td>
</tr>
<tr>
<td>Transactions</td>
<td>yes</td>
</tr>
<tr>
<td>Transaction history</td>
<td>yes</td>
</tr>
</tbody>
</table>

Table 5: ABN Amro Bank Mobile Banking through client application

<table>
<thead>
<tr>
<th>SNS Bank</th>
<th>Client application: SNS Saldo</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>iPhone</td>
</tr>
<tr>
<td>Balance Enquiry</td>
<td>yes</td>
</tr>
<tr>
<td>Transactions</td>
<td>no</td>
</tr>
<tr>
<td>Transaction history</td>
<td>yes</td>
</tr>
</tbody>
</table>

Table 6: SNS Bank Mobile banking through client application

The three types of mobile banking services offered by banks in the Netherlands will be further described in the next paragraphs.

---

4 No official native client. Unofficial client uses the mobile website functionality
**Mobile website banking**

Like previously stated, mobile banking services are mostly iterations of existing services that use the bank's current systems and infrastructure (Mallat 2006). Given the fact that internet banking infrastructure is already in place and reusing existing components is a cost-effective way to build new systems, mobile website banking is a natural next iteration of internet banking.

For mobile banking, we agreed to use the following definition: ‘that type of execution of financial services in the course of which [...] the customer uses mobile communication techniques in conjunction with mobile devices’ (Pousttchi & Schurig 2004). In the context of internet banking, mobile website banking falls within that definition. The internet banking website accessed is a mobile website through a mobile device. A mobile website is a website optimized for viewing on a mobile device (e.g., adjusted screen size, small downloads).

As stated previously, at the moment only Rabobank and SNS Bank offer mobile website banking services. Both require authentication in the form of a separate device. For Rabobank, the Random Reader is used only for registering for the first time and, depending on the transaction, during transfers, and for SNS Bank, the Digipas is always used for logging in and for transfers. The Random Reader and Digipas are devices which are used to generate responses to a challenge received from the bank in order to authenticate the customer.

**SMS-banking**

SMS is the abbreviation for Short Message Service and ‘allows users to send and receive text messages on a mobile phone’ (GSM World n.d.). An SMS can be up to 160 characters long and is independent from the mobile carrier, i.e., a user can send a message to someone who is using another mobile phone carrier (e.g., Vodafone to T-Mobile and vice versa).

The simplest service a bank can offer via SMS to its customers is information about their current account balance (Mallat et al. 2004; Pousttchi & Schurig 2004). The customer sends an SMS with a command to the bank and the bank replies back.
(Pousttchi & Schurig 2004). With functionality like number recognition (also known as ‘caller id’), the bank is able to recognize customers by their mobile phone number. For this to work, it is important that customers have identified themselves earlier using other means, for example via the traditional internet banking environment or via a letter which contains activation codes.

When looking at the SMS-banking landscape in the Netherlands, two types of SMS-banking can be identified:
1. Informational
2. Transaction initiating

Informational SMS-banking entails text messages received from the bank regarding the current status of the account or a certain transaction. For example the current account balance, or when a certain amount is subtracted from the account. All the banks in the list provide such services.

Transaction initiating SMS-banking is offered only by Rabobank through a third party called Minitix. When signing up for this service, a virtual wallet is created. This wallet can contain up to 150 euro. To send money to someone else, an SMS must be sent to a phone number. The SMS must contain the amount and the mobile phone number of the receiving party.

**Mobile banking client on mobile phone**

Mobile phones also have the functionality to execute applications installed on them. These applications can be programmed directly into the phone operating system (for example games or a built-in web browser) or by introducing an extra ‘execution layer’ on top of the OS layer, for example a virtual machine. The widest spread virtual machine on mobile phones is Java ME (Java Micro Edition) which is installed on over 3 billion phones (Oracle n.d.). With the increasing processing power of mobile phones, a more fluent end user experience could be delivered to customers. It was however the introduction of the iPhone in 2007 and the App Store in 2008 (Apple Inc. 2007; Apple Inc. 2008), which launched a new era of client applications on mobile phones.
The App Store is a mechanism to distribute applications to iOS enabled devices (iPhone, iPod Touch and iPad). There are several advantages to opening an App Store\(^5\). The advantage for the customer is that it gives the customer a wide variety of applications that can be downloaded, thereby creating added value for the customer from the mobile device. For the App Store owner the advantage is that it creates an extra revenue stream, Apple for example earns 30\% of the list price of an application. The second advantage for the App Store owner is that it creates a vendor lock in. Apple mobile applications only run on iOS devices, so when customers have bought many applications and music, it is more likely that they will protect that investment by buying another iOS device when it is time to replace the old one.

Subsequently in 2007 Google launched its mobile operating system called Android, which it acquired in 2005 (Google Inc. 2007). In 2009 Google introduced the Android Market (Android Developers Blog 2009), which is similar to Apples App Store. Soon other manufacturers followed, like BlackBerry and Microsoft.

The first mobile applications to appear from banks were applications to inform customers on existing distribution channels, for example the location of ATMs and branches. Soon applications started to appear in the App Stores with which the current account balance could be checked. In some cases these are based on existing infrastructures, for example the infrastructure set up for SMS-banking. Later banking applications followed with which transactions could be initiated. First they were available only on the iPhone, later other platforms followed. When we take the previous definitions we gave for mobile banking we can define mobile banking with a client as carrying out banking transactions over the internet using a dedicated client application on a mobile device.

\(^5\) Even though Apple Inc. claims to have a trademark on the term App Store, we will generally refer to the term App Store for non-Apple App Stores as well.
Overall the following lifecycle of an application and its stakeholders can be identified:

For the remainder of this research the focus will be on mobile banking in the context of mobile device and mobile applications.

### 2.3 Future direction of mobile banking

Mobile banking is here to stay. It provides the customers with the convenience to bank when and where they want. According to a survey held by McKinsey amongst European bankers a majority of bankers indicated that they saw great promise in mobile technology through benefits offered to the customer (Lien et al. 2011). Furthermore, mobile devices are a technology that has the potential to change the face of retail banking. In the same McKinsey survey, a majority of respondents also acknowledged that they are not investing enough to take advantage of the opportunities the mobile platform offers.
We expect to see a shift from OS-specific apps to browser-based apps. At the moment applications are developed and launched, targeted at the various operating systems (e.g. iOS, Android). Developing and maintaining mobile applications targeted at different platforms is costly (Schievink 2010). Hence, the platform of choice would be the web and the application offered would be a web application. For example, because of the costs of developing and maintaining different apps, the NOS (Dutch National Broadcasting Corporation) is shifting to browser based apps. All the major mobile devices have a browser, which supports HTML 5. HTML 5 enables developers to develop a web-application with the look, feel and performance of a native application running on the mobile device. This has several advantages:

- Bringing down the cost of development: separate development teams are no longer needed. For example, the programming language for the iPhone is Objective-C, for Android it is Java, and for Windows it is .Net
- Make continuous and instant improvement to the web application. By using a web application the App Store is bypassed. This increases the time to market. The Financial Times created an HTML 5 application and decommissioned its native iOS app. It did so because it did not want to pay a 30% commission on subscription sales. Most important for the Financial Times was that it could not obtain the subscribers’ data, when selling through the Apple App Store.

At the same time we do not expect that banks will opt for a web only application for several reasons:

- The App Store is an additional marketing and survey instrument. Users are able to rate applications and leave reviews in the App Store. Good ratings can be used as social proof by the bank in order to convince other people to use the mobile banking application. Reviews are a good way to study the reception of the app by the public and come up with ideas for new functionality.
- Some functionality requires access to the mobile device functions. For example, several apps exist which allow the scanning of an “acceptgiro”, which can immediately be inserted into the transaction screen.
Taking the above into consideration we expect that the next mobile banking app will be a skeleton client that facilitates access to mobile device functions and also locally caches items like images. At the same the skeleton client is a browser which accesses the mobile banking website on the web.

### 2.4 Chapter summary

The goal of this chapter was to develop a good understanding of the current mobile banking landscape. First mobile banking in the context of this research was defined. After the definition an overview was given of mobile banking solutions in use by the four largest banks in the Netherlands. Three types of mobile banking can be distinguished:

1. Mobile banking through a mobile website
2. Mobile banking through SMS
3. Mobile banking using a dedicated application installed on the mobile device

The last type, a dedicated application (app) installed on the mobile device, is what is in scope of this research. The chapter was concluded with expectations of the direction mobile banking of the third type will take in the future. In the next chapter the focus will be on the security challenges associated with mobile apps.
Chapter 3: Security challenges for mobile banking

2012 is the year that mobile devices will be put to the test. Both McAfee and Kaspersky expect a large increase in the number of malware attacks on mobile devices because of the increasing number of devices and applications installed on it. The mobile operating systems will be thoroughly examined for flaws to exploit (GTISC 2011; Kempenaar 2012).

What brought mobile devices to the point that they have become targets? A few years ago nobody had heard of malware for mobile devices. The sudden rise has several reasons. One is the increasing homogeneity of mobile devices in terms of the operating systems running on them. In the past, when mobile platform uniformity used to be a challenge because of the large variety of devices (Schwiderski-Grosche & Knospe 2002; Jürjens et al. 2008), it would not have been feasible to launch large-scale attacks. Now we see that there is a move towards homogeneity revolving around a few core operating systems for mobile devices (Windows Mobile, Android and iOS). The second reason is the increased use of these devices. Mobile devices, like phones, have become a natural extension of their users. They are using it for reading emails, doing their banking, sharing files and music, staying in touch with their loved ones and ordering things online. It has become the gateway to the world for most people as it is available 24/7 due to “always-on” fast internet access. The change of user behaviour in combination with the increasing homogeneity, makes targeting the devices and their users increasingly more attractive to cyber criminals (GTISC 2010).

Even though mobile devices rival personal computers in processing power and memory, they still have several constraints (e.g. battery limitation, small screens) that means traditional security measures are difficult to implement (e.g. antivirus, firewall).
In this chapter the security challenges for mobile banking in the context of mobile devices and applications will be examined. This in turn will answer sub question 2 and will be a good basis to build the security model for mobile banking in the next chapter.

### 3.1 Chapter outline

In this chapter the threats to mobile devices and applications in a mobile banking context will be examined. First the security assets that need protection will be defined in the context of mobile devices and applications. Then the security objectives that are applicable to the security assets will be defined. Finally the threats that could compromise those security objectives will be examined. At the end of the chapter a summary of our findings will be given.

### 3.2 Security assets

Before we can go into the specific threats applicable to mobile banking, we need to define the assets that need protection. A mobile banking application runs on a mobile device and contains information that is displayed on the screen.

Jeon et al. (2011) identify three assets for mobile devices:

- Device;
- Application;
- Private information.

In the context of this research, these assets will be applied to the consumer side of mobile banking. The bank side (e.g. bank servers) and the network assets (e.g. telecom provider) are not the scope of this research.

An asset can be defined as a target of attack.
3.2.1 Mobile device as a security asset
Firstly the mobile device itself is an asset. It is the platform on which mobile applications run. The mobile device contains the peripherals to communicate with the outside world, for example for making calls and surfing the internet. Without it the user is no longer able to perform actions on the device. For example when customers lose their phone, they can no longer use it. A lost phone can also be misused by someone who finds it, for example by making expensive phone calls.

3.2.2 Mobile application as a security asset
Secondly there is the application that runs on the device that can be seen as an asset. Applications are used to perform certain operations where information is received, transformed and displayed to the user. A mobile banking application could have the following functionality: it receives the current account balance, converts it to a currency format and the euro amount is displayed on the screen of the device. The mobile application is responsible for access to the information it contains and for performing certain operations. An example in case of mobile banking; before sensitive account information can be accessed a pin-code has to be entered in on the screen.

3.2.3 Information as a security asset
Private information includes all data stored in the mobile device and transmitted to the device. An example of private information is the call history or address book. The information is handled by applications. Since the information is handled by application, the security of applications should be good in order to protect the information. In case of mobile banking applications we can state that banking information that is contained in the application or received by the application can be considered as private information. An example of this could be a recent transaction or a cached pin-code so that the customer does not have to input it repeatedly.

3.3 Security objectives
Now that we have established the assets which need protection, we can identify what the threats are for mobile devices and applications in a mobile banking context. The next step is to describe the security objectives for the assets that need protection. A mobile device can be seen as a miniaturized computer and partly deals
with the same issues as conventional computer security in terms of confidentiality, integrity and availability (Jeon et al. 2011; Schmidt 2011). In addition to these security objectives additional security objectives can be defined. Both Kadijiwal & Zulfiquar (2007) and Bangdao et al. (2010) indicate authentication, authorization and non-repudiation as additional security objectives for the mobile platform. Subramanian (2011) uses the term accountability instead of non-repudiation. For the additional security objectives it can be argued that these are a refinement of confidentiality, integrity and availability.

In the next paragraphs the security objectives that we listed in this paragraph will be defined. Instead of giving our own definition for each security objective, definitions from the following institutions will be used:

- NIST - National Institute of Standards and Technology (Stoneburner et al. 2002)
- ISACA - Information Systems Audit And Control Association (ISACA 2012)
- ISO - International Standards Organization

The security objectives will be examined in the context of the security assets as described in paragraph 3.2. A summary of key elements of the security objectives can be found in Table 1. In the remainder of the paragraph the security objectives will be described using definitions taken from NIST, ISACA and ISO.

<table>
<thead>
<tr>
<th>Confidentiality</th>
<th>System and data confidentiality refers to the protection of sensitive or private information from unauthorized disclosure or intelligible interception.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integrity</td>
<td>System and data integrity refers to safeguarding the accuracy, completeness, validity of information and processing methods.</td>
</tr>
<tr>
<td>Availability</td>
<td>Ensuring that information and vital services are available to the business processes when required to its end users.</td>
</tr>
</tbody>
</table>

Table 1: Summary of security objectives according to ISACA, NIST and ISO.

3.3.1 Confidentiality

According to ISACA (2012) confidentiality refers to the protection of sensitive or private information from unauthorized disclosure. The definition given by ISACA revolves around the protection of private information, which is one of the security
assets defined in paragraph 3.2. NIST (Stoneburner et al. 2002) makes a distinction between system and data confidentiality. Data confidentiality also refers to security asset private information. In the case of mobile applications, the private information is handled by the application. The application itself runs on top of the operating system on the mobile device. Since the application is the entry point to private information and the mobile device is the entry point to the application and private information, the confidentiality of the system should also be taken care of. ISO 27002:2005 introduces another important aspect of confidentiality that applies to mobile banking applications, namely protecting information from intelligible interception (Paans 2010). Some of the information required by the mobile banking device resides on the servers of the financial institution. The transfer of that information from the bank systems to the mobile device should also be addressed.

3.3.2 Integrity
ISACA (2012) refers to integrity as the accuracy, completeness and validity of information. The information which is referred to is the previously mentioned private information which needs protection. In the case of mobile banking, adequate measures should be taken to protect the information (confidentiality) but also to ensure that the information used is the data as intended. For example, when a customer makes a payment to another account, it should not be possible to manipulate the transaction. Furthermore when a manipulation does take place, measures should be in place that detect the manipulation (e.g. by the means of analysing logs). NIST (Stoneburner et al. 2002) again makes a further refinement between system and data integrity. The concept of data integrity has just been discussed. System integrity refers to the mobile application and the mobile device. When a virus infects a mobile device, no certainty can be given regarding the integrity of the mobile device and the mobile application anymore. ISO 27002:2005 calls this the integrity of the processing methods (Paans 2010). When the integrity of the processing methods is no longer guaranteed, in turn the integrity of the private information is also no longer certain.

3.3.3 Availability
ISACA (2012) defines availability as information that is accessible when required by the business process now and in the future. When we take into consideration the
security assets, just like the other security objectives, availability can be applied to all three assets. Availability of the device, the application and the private information should be assured. For example, a faulty device causing the battery to drain affects availability. Another example is the loss of access to information needed, for example a current account balance. This can be caused by the private information not being available (data corruption), the application not being available (error in application) or the device not being available (device stolen). The definition provided by NIST (Stoneburner et al. 2002) goes further than the definition provided by ISACA. While the definition given by ISACA focuses on the business process, NIST makes the link between the goals of the organization and its end users. NIST states that unavailability of a system to its end users could hamper the organization's mission. In the case of mobile banking the end user of the mobile banking application is the customer. ISO 27002:2005 is along the same lines as the definition given by ISACA, with the addition that availability also applies to the services providing the information (Paans 2010).

### 3.4 Threats

In contrast to traditional mobile phones, mobile devices are much more like computers. Just as on personal computers there are many different attack gateways. Attackers can take advantage of weaknesses in applications such as email clients, browsers and the operating system (GTISC 2010).

Before we can go into detail of the threats that exist for the mobile platform we need to distinguish vulnerabilities from threats. A vulnerability is defined as a weakness in the design, implementation, operation or internal control of a process that could expose the system to adverse threats from threat events (ISACA 2012). A threat is defined as anything (e.g., object, substance, human) that is capable of acting against an asset in a manner that can result in harm (Jeon et al. 2011).

According to current literature (which will be detailed in the next paragraphs), the security objectives described in paragraph 3.3 can be harmed by the following threats:
• Lack of user awareness
• Malware
• Eavesdropping
• Denial of Service
• Unauthorized access
• Device or application malfunction
• Loss, theft and improper disposal of devices
• Platform Alteration

Broadly two types of threats can be defined. Threats caused by:
• Attackers (external factors)
• User unawareness or intention (internal factor).

In the next paragraphs threats to mobile banking in the context of mobile devices and applications will be described.

3.4.1 Lack of user awareness
Most users see their mobile device as phones instead of mini computers, furthermore they see their phone as a protected device (GTISC 2010). This view also affects the way people handle their phones, the applications they use on their phones and messages they encounter on their phones.

People can be tricked or manipulated to divulge private information (for example their PIN-codes) or perform certain actions (for example send money to a fraudster). This is called social engineering. Social engineering is known to be used to spread malware or to stage phishing attacks (Subramanian 2011). An attacker can create a fake application which a user then installs and uses with the idea that it is a legitimate application.

Even though the creator claimed no malicious intent, the iPhone application “Blauwe Leenw” is a good example. A user of the ING mobile banking app for the iPhone created his own version called “Blauwe Leenw”. After submitting the app to the App Store other users could download it. To use the app, users had to enter the
username and password which they used for ING Internet Banking. Due to the security implications, ING had the app removed by Apple (Schop 2011). One can argue that users are likely to be tricked into downloading this app because of the association made with ING.

![Screenshot of the iPhone app Blauwe Leen](image)

Figure 1: Screenshot of the iPhone app Blauwe Leen

Questions can also be raised on the application submission process to App Store owners regarding the screening procedure for submitted apps.

Lack of user awareness could compromise the confidentiality of private information. Like the example given before, because of lack of user awareness the customer can be tricked into revealing information that could lead to the customer losing money.

### 3.4.2 Malware

Malware or malicious software can find its way to the mobile device of a customer. Malware is software that can compromise the security objectives we defined. In turn when these are compromised the malware can harm a mobile device or cause damage to the owner without the owner's consent (Subramanian 2011). Examples of malware are viruses, worms, spyware, Trojan Horses, etc. These can be installed via various means. User unawareness is one of them (see paragraph 3.4.1) for example by disguising malware as a game (Radack 2009).
A mobile device has many interfaces. For example it can connect to the internet via 3G or Wi-Fi, it can be used to place calls and send/receive text-messages, and it could have a slot for memory expansion. These are all interfaces that can be exploited by malware. Other infection vectors are email (for example through SPAM mail), SMS, MMS (Jeon et al. 2011) or Bluetooth, internet connectivity, memory cards or connection with another device (Subramanian 2011).

Malware can enter the mobile device and pose a threat to the device and its applications through one of those interfaces; via internet downloads, messaging services, Bluetooth communications, which lead to attacks (Hollestelle 2011; Jeon et al. 2011). Examples of malware are intercepting SMS messages which contain TAN (Transaction Authentication Numbers) codes, which are used to authenticate internet banking transactions (Subramanian 2011); hijack the mobile device and ask ransom money in order to make the device work again (Wokke 2009); or sending the contents of the address book to a remote server in China through a wallpaper app (Bahr 2011).

Malware tends to attack flaws in the underlying operating system of the mobile device. Mobile devices do not commonly receive patches and updates (GTISC 2011).
Reasons could be the sheer file size of an update; the manufacturer is not willing to provide device updates; or the user just does not know or care.

Malware can compromise the confidentiality, integrity and availability of all three security assets defined in paragraph 3.2. In the context of mobile banking this could mean that transactions might be intercepted or even initiated without the customer ever knowing.

3.4.3 Eavesdropping

A mobile device communicates over a wireless network, typically via Wi-Fi or 3G data connection. The confidentiality and integrity of the communication can be compromised by the means of eavesdropping, man in the middle attack or by spoofing (Hollestelle 2011) since the communication goes over the air (Schwiderski-Grosche & Knospe 2002).

Eavesdropping is unauthorized capturing of information (e.g. capturing usernames and passwords), thereby compromising the confidentiality (Schmidt 2011). When information is manipulated it also compromises the integrity of the data.

Eavesdropping can compromise the confidentiality and integrity of private information.

3.4.4 Denial of Service

A denial of service attack is an attack that floods a device so that all the resources are consumed so that normal operation is no longer possible. A denial of service attack can be raised against a mobile device which can cause the battery to drain or consume its limited resources, for example its CPU, memory, available port numbers or bandwidth (Subramanian 2011). An example of a denial of service attack is the flooding of the IP-address of the device with a large number of connection requests which the device cannot handle in a timely fashion.

A denial of service attack could compromise the availability of a mobile device. Customers are then unable to do banking on their mobile device.
3.4.5 Unauthorized access

Unauthorized access to the mobile device or its applications can be obtained by bypassing the authentication credentials. For example, a passcode of four digits can be set on the iPhone, however emergency calls (to 112 or 911) should be possible. Early versions of iOS (version 2.0) had a flaw in the emergency call screen that made it possible to access the recent call list. Since the recent call list is part of the phone application, phone calls could be placed by accessing the phone dial pad through the recent call part.

![Bypassing the emergency call screen](image)

Figure 3: Bypassing the emergency call screen

Guessing the passcode is also a possibility. All modern mobile devices have touch screens which are easily smudged. These smudges could be used to decipher passwords in order to gain access. The researchers took photos of the smudge trails left on the screen and adjusted the contrast, and were able to find the unlock pattern (Aviv et al. 2010).
Unauthorized access could compromise the confidentiality of the private information. An attacker could gain access to the mobile banking application and perform certain transactions.

### 3.4.6 Device or application malfunction

According to Jeon et al. (2011) there are two types of malfunctions. Malfunction caused by the user by mistake or wrong configuration and malfunction of the application due to incompatibility between the application and platform.

Malfunction by user error is covered under paragraph 3.4.1 Lack of user awareness.

Malfunction of the applications can be due to several causes. Agarwal et al. (2007) names flaws in the application itself, flaws in the API’s (application programming interface) of the development platforms and flaws in the protocols used (e.g. weak cryptographic implementation).

An example of flaws within the application is the mobile banking application of the United Services Automobile Association (USAA). Its mobile banking application saved the following pieces of information in device memory: usernames; passwords; security question answers; pages; images; account balances and routing number (Bahr 2011; Ante 2010).
Malfunction on mobile device and application level could compromise the confidentiality and integrity of the private information.

### 3.4.7 Loss, theft and improper disposal of devices

Its small form factor and high value make mobile devices highly attractive for theft (Subramanian 2011). When a mobile device is lost or stolen, information on the mobile device can be exposed (Jeon et al. 2011). The amount of information exposed can be huge despite the small form factor of a mobile phone (Schwiderski-Grosche & Knospe 2002; Subramanian 2011). Theft is not the only way that information could be disclosed. Information disclosure is also possible when a customer disposes of the device in a not secure manner (Hollestelle 2011), for example by selling the mobile device without properly wiping its contents.

When losing a mobile phone, the confidentiality of the private information on the device could be compromised. With physical access to the device it is much easier to obtain the private information stored on the device or remotely accessing information to which the device has access (Radack 2009). Furthermore since the device is no longer in possession of the user, the availability of the device and thus the application in order to gain access to the private information is no longer available.

### 3.4.8 Platform Alteration

Some users intentionally alter the platform by rooting (Android) or jailbreaking (iOS) a device (Jeon et al. 2011). Rooting a mobile device gives the user much more possibilities than originally intended by the manufacturer or that can be offered by the applications. It removes the security precautions implemented by the manufacturer and gives greater control to the user. However, this is not without risk. When security precautions are removed, malware can take advantage of the lack of controls.

Altering the platform could compromise the confidentiality and integrity of the device, the application and the private information contained on the device. A mobile device where the platform has been altered is much more susceptible to attacks by malware since a security layer has been removed.
3.5 Chapter summary

The focus of this chapter was to determine what the security challenges are for mobile banking. Based on literature research eight security threats emerged which could compromise the confidentiality, integrity and availability of the mobile security assets. The mobile security assets that need protection are the mobile device, the mobile application and the private information.

With these items in mind, there is a solid basis for building the mobile banking security model in the next chapter.
Chapter 4: Security model for mobile banking

In the previous chapter eight security threats were defined based on literature research. These threats could harm the confidentiality, integrity and availability of the security assets for mobile banking. In this chapter, these will be encompassed in a security model for mobile banking in the context of mobile devices and applications. This security model will be the first step in answering sub question 3. In the next chapter the security model will be completed with the addition of control measures.

4.1 Chapter outline

In this chapter the identified threats from chapter 3 will be expanded further in the context of mobile banking. First a categorization of the identified risk will be given. Then, an overview of the security objective per asset for each threat will be given. This chapter will conclude with describing the groups in which the threats are categorized. In the next chapter, the security model will be developed further with specific controls and measures for mobile threats based on expert interviews.

4.2 Categorization of identified risks

In the previous chapter, threats for mobile banking applications were discussed. The threats discussed were:

- Lack of user awareness
- Malware
- Eavesdropping
- Denial of Service
- Unauthorized access
- Device or application malfunction
- Loss, theft and improper disposal of devices
- Platform Alteration

The above threats harm the security objectives for the security assets we defined for mobile banking applications. The security assets we defined for mobile devices are:
The security objectives defined for the security assets are:

- Confidentiality;
- Integrity;
- Availability.

Mobile applications and device security and assurance frameworks are available, however those focus largely on the usage of a mobile device within a corporate environment.

NIST published *Guidelines on Cell Phone and PDA Security* (Jansen & Scarfone 2008) and ISACA (Kelson 2010) published the *Mobile Computing Security Audit/Accurance Program*. In addition the Information Security Forum (ISF) published a report with the title *Consumer device security* (Davis 2011), which is about the increasing usage of consumer devices (e.g. iPhone) in a corporate environment. The ISF identifies four key components regarding device security as shown in Figure 5.

![Figure 5: ISF Framework for securing consumer devices (ISF 2011)](image-url)
As indicated all of the examined frameworks are highly focused on the usage and control of mobile devices in a corporate environment. However the components defined are, to a certain extent, applicable to mobile devices as used by a mobile banking customer. This is because the underlying threats for a corporation are the same as for a consumer (e.g. malware, loss of a device), the impact of course could be different.

### 4.3 Security assets per categorized threat

For the frameworks examined, the ISF framework for securing consumer devices comes closest to the mobile banking customer and the security assets, which were defined earlier. Furthermore, the mobile banking application user plays a vital role. Lastly the organization plays a role in the entire process, since it is a service offered by the bank (applications and data) running on a customer (users) owned device (devices). The organization plays a role in the governance of the whole in order to reduce the threats plaguing the confidentiality, integrity and availability of the device, the application and the private data it contains.

In Table 7 the security threats as defined in paragraph 3.4 have been categorized according to the ISF framework for securing consumer devices. The first column lists the category. The second column lists the threat and the third column lists which security objective is compromised for the security assets defined.

<table>
<thead>
<tr>
<th>Components</th>
<th>Security threats</th>
<th>Security assets compromised</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Lack of user awareness</td>
<td>Confidentiality of private information</td>
</tr>
<tr>
<td></td>
<td>Loss, theft or improper disposal of devices</td>
<td>Confidentiality of private information</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Availability of the device and in turn the application and private information</td>
</tr>
<tr>
<td>Devices</td>
<td>Malware</td>
<td>Confidentiality, integrity and availability of the</td>
</tr>
<tr>
<td>Threat Type</td>
<td>Impact</td>
<td></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Eavesdropping</td>
<td>Confidentiality and integrity of the private information</td>
<td></td>
</tr>
<tr>
<td>Unauthorized access</td>
<td>Confidentiality of the private information</td>
<td></td>
</tr>
<tr>
<td>Device malfunction</td>
<td>Confidentiality, integrity and availability of the device and in turn the application and private information</td>
<td></td>
</tr>
<tr>
<td>Platform alteration</td>
<td>Integrity, confidentiality and availability of the device and in turn the application and private information</td>
<td></td>
</tr>
<tr>
<td>Denial of service</td>
<td>Availability of the device and in turn the application and private information</td>
<td></td>
</tr>
<tr>
<td>Applications and data</td>
<td>Unauthorized access</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Confidentiality of the private information</td>
<td></td>
</tr>
<tr>
<td>Application malfunction</td>
<td>Confidentiality, integrity and availability of the application and in turn the private information</td>
<td></td>
</tr>
<tr>
<td>Governance</td>
<td>Risk of mismanagement of the above threats if not adequately addressed by the organization</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Confidentiality, integrity and availability of the application and in turn the private information</td>
<td></td>
</tr>
</tbody>
</table>

Table 7: Categorization of threats according to the ISF Framework for securing mobile devices
4.3.1 Users

In this paragraph the component users will be discussed. Users are part of the mobile banking process, for example when they initiate a transaction. Users can use the application in ways not intended or be tricked to perform certain actions. In the past and even now people are tricked into being money mules, where they give control of their account in exchange for money. In the meantime their account is used for wiring fraudulent transactions to foreign destinations.

Educating the user on proper usage and on the implications of misuse of mobile banking can prevent lack of user awareness. In the case that the user is actively misusing the application or is tricked into misuse, controls should be in place. In case of lack of user awareness, loss or theft, a user should be able to contact the bank for help. User support should be available to assist the user as a corrective control.

4.3.2 Devices

The device and the operation system running on it are a given. It is the platform on which the mobile banking application runs on. As stated before, devices do not tend to get updated often. Most of the time users have to connect their phone to a computer in order to update it. Even when users do this regularly, there is no guarantee that the manufacturer makes updates available for the device.

Since the device is something the banking institution cannot control, the next logical thing to do is build the necessary security controls in the application. For example as a preventive control, the mobile application could include checks to determine if the mobile device is running on the most recent operating system. A detective control could be an integrity check the application performs on itself, which could be extended with a server side validation. A corrective control could be acting upon detection techniques implemented (e.g. data manipulation or denial of service attacks).

4.3.3 Applications and data

As stated in paragraph 3.2 the application and private information both are security assets. The application is used to gain access to the confidential private information.
In the previous paragraph we concluded that since the device is something the financial institution cannot control, the application is the most logical place for the bank to implement security and detection features.

4.3.4 Governance

In the previous paragraphs a categorization was made of the threats as identified in chapter 3, where the focus of those threats was on the security assets (mobile device, the application and the private information it contains). In this chapter the ISF framework for mobile devices was described which introduced the category Governance. Adequately addressing the mobile device and application risks is the responsibility of the financial institution that offers such a service. Thus the risk that mobile device and application threats are not addressed properly is the responsibility of the bank in question. Furthermore when a new banking channel is introduced, processes need to be adapted and support staff trained. In the next paragraph, controls will be discussed where the identified threats will be addressed.

4.4 Chapter summary

In this chapter the first steps were taken into building the mobile banking security model. After a short summary of the outcomes from the previous chapter, we categorized the security threats using the categories as defined in the ISF framework for securing mobile devices. The following four categories are defined in the ISF framework for mobile devices:

1. Users
2. Devices
3. Applications and data
4. Governance

The categories from the ISF framework are in line with the threats we defined in chapter 3. The ISF framework introduces the category governance which we translated as the risk that the organization does not, or is unable to, control the risks of mobile banking.
Chapter 5: Case analysis of security model and controls

In the previous chapter the threats for mobile banking were categorized in *users, devices, application and data* and *governance*. Categorization creates a level of abstraction, which enables one to view the subject from a specific point of view. The next steps are defining control measures to minimize the risks associated with the threats. This will be done in this chapter and with that sub question 3 will be answered.

5.1 Chapter outline

In this chapter the security model will be expanded with security controls and measures for security threats to mobile banking in the context of mobile devices and mobile applications. The security controls described in this chapter are based on interviews with professionals in the field of banking and IT security. Firstly three types of controls will be discussed which will be applied to the security threats defined. After describing the type of controls, the results from the expert interviews will be given. The chapter will conclude with a chapter summary.

5.2 Types of controls

Controls are measures that can be introduced to remove or to reduce the risk to an acceptable level. The controls chosen for the mobile banking security model are preventive, detective and corrective controls. In the next paragraphs the controls will be described. In paragraph 5.3 these controls will be further defined within the security model for mobile banking.

5.2.1 Preventive controls

Preventive controls can be described as an “Internal control that is used to avoid undesirable events, errors and other occurrences that an enterprise has determined could have a negative material effect on a process or end product.” (ISACA 2012).

In the context of mobile banking this could be as simple as an input control in the mobile application. For instance checking that only numbers are entered.
5.2.2 Detective controls
Detective controls can be described as controls that exist to detect and report when errors, omissions and unauthorized uses or entries occur (ISACA 2012).

Usually a detective control is executed after an action has taken place and often covers a group of transactions. For example when customers make payments with their mobile phone, the transaction is checked for enough balance on their account; is below the daily limit he set; and it is not a fraudulent transaction.

5.2.3 Corrective controls
Corrective controls can be described as controls that are designed to correct errors, omissions and unauthorized uses and intrusions, once they are detected (ISACA 2012).

A corrective control could be that the bank discovers, through transaction analysis, that a transaction is fraudulent. Before the transaction is settled by the payment processor, it is removed from the queue.

5.3 Control measures for the mobile banking security model
In order to come to good control measures a series of interviews were held with professionals in the field of banking and IT security within ABN AMRO Bank. In total 5 persons were interviewed. Two persons from the IT department (internet banking and user security) were interviewed and 3 auditors from the internal audit department of ABN AMRO Bank

The auditors interviewed perform different types of audits, but all hold the chartered EDP-auditor title (RE) and have been involved in the mobile banking project at ABN AMRO Bank in their role as assurance provider. One auditor is a senior auditor and performs IT audits with a mix between system and technical audit. The other two auditors have a senior management role, one as head of technical audit and one as head of business audit retail banking.
All of the above mentioned persons have been involved in the mobile banking project at ABN AMRO Bank. ABN AMRO serves retail, private and commercial banking customers in the Netherlands and across the globe. In the Netherlands, ABN AMRO gives its customers the opportunity to do their banking on a mobile device using an app called “Mobiel Bankieren”. The first version (1.0) that allowed the transfer of funds was released in July 2011 for iOS and Android. In November 2011 a version was released for the Blackberry platform. The current version (2.0) of Mobiel Bankieren for iOS and Android was introduced in January 2012.

Mobiel Bankieren 2.0 supports viewing the transaction history list and transfer of funds. It also has a functionality called visual banking. Visual banking allows the customer to add pictures to the accounts. When used for the first time a pin code of 5 numbers (pin5) has to be created. Customers need to identify themselves using
two-factor authentication (a device called the e.dentifier, the customers’ bank card and the pin code of the card). A daily limit must be selected and the maximum selectable daily limit is 750 Euros. For transactions below the limit, the customer uses the pin5. The customer needs to use the e.dentifier to do the transfer if the transferrable amount is above the daily limit and if money is transferred to an unknown recipient. For additional specific functionally of this please refer to the website of the ABN AMRO Bank6.

Due to the size, the results from the interviews held with the experts can be found the appendix. The results are in the form of control measures per security threat. It should be noted that the outcomes should be seen in a general context of mobile banking and not specifically to the way ABN AMRO Bank has implemented mobile banking.

5.4 Chapter summary

In this chapter we completed the security model started in chapter 4. For chapter 4 the focus was on categorizing the security threats found. From these first steps in building the mobile security model we went to completing it with control measures. The results can be found in the appendix. The control measures are derived from interviews with professionals in the field of banking and IT security. These persons were carefully selected to have a good mix between a business and an IT point of view.

This has culminated in the mobile banking security model, where the threats are grouped in the categories users, devices, applications and data and governance. With the complete security model we have answered sub question 3.

6 ABN AMRO Bank Mobile Banking information page: http://www.abnamro.nl/mobielbankieren
Chapter 6: Synthesis of findings and conclusions

In the previous chapter the mobile security model was validated and completed through the addition of security control and measures. These additions were derived from interviews with experts in the field of banking and IT security.

6.1 Chapter outline

In this chapter a synthesis will take place from what has been learned so far. Common themes can be identified from the control measures listed in the security model for mobile banking. These will be discussed in the next paragraph. Based on the research, interesting questions came up, which did not fit the scope of this research, but could be worked out in future research. Possible directions for future research will be given. This chapter will conclude with a chapter summary.

6.2 Synthesis of findings

A number of common themes can be identified from the outcomes of the previous chapter. Some security controls and measures repeatedly appeared across the security threats and the categories (users, devices, application and data and governance) which were defined. Furthermore, some threats led to a discussion on how and who is responsible for addressing it.

The following five overall themes could be identified, these will be discussed further in the next paragraphs:

1. Clear roles and responsibilities of internal and external stakeholders
2. Customer awareness is important
3. Quality of the app should be above any doubt
4. Investing more in detective controls
5. Support processes should be in place

6.2.1 Clear roles and responsibilities of internal and external stakeholders

For mobile banking many parties are involved. In chapter 2 the lifecycle of an app was outlined. There the following parties could be identified: The bank/3rd party developer; app store owner; and the user.
In addition, due to the nature of the service offered (financial service offered through the internet), additional stakeholders can be identified: telecom provider (providing the connection); regulatory bodies (e.g. the Dutch Central Bank); payment processors (Equens); other banks; and law enforcement agencies (e.g. high tech crime unit in case of cybercrime). All these are external stakeholders.

In addition to the external stakeholders there are also internal stakeholders. The business that wants a certain feature for the app; IT that has to supply it; and legal, compliance and audit in their respective roles.

With so many internal and external stakeholders involved, for example, overall councils should be in place to give stakeholders a platform to share ideas, knowledge sharing, decision making, and agreements on common approaches. These platforms should be in place within the organization (for internal stakeholders) and outside the organization (for external stakeholders) Due to the potentially large number of stakeholders it may not be always clear where the responsibilities and accountabilities lie. Should a bank be held accountable when a denial of service attack is performed, or is the telecom provider responsible? Should a bank always compensate customers in case of fraud or should customers be held accountable if they are careless with their mobile device? There is no clear answer as of yet, however this will take more shape once the mobile banking platform will mature.

6.2.2 Customer awareness is important
The lack of customer awareness seems to be the cause, or seems to be facilitating several security threats identified in the previous chapter. What is the cause of lack of user awareness, is it ignorance? Is it stupidity? Or perhaps it is a matter of trust? The common themes within user awareness seem to be to educate customers to prevent certain threats to materialize and taking actions against the customer when certain threats materialize as a corrective action. Awareness campaigns should be targeted on the customers’ internal motivation (e.g. the value of the mobile device, misuse of the phone subscription or understanding that money can be lost). All the experts interviewed agree that above a certain threshold corrective action should be
taken against users, however it is difficult to determine what that threshold is. Also, it is not easy to prove that customers are at fault and when the bank is at fault. These are questions for which there is no answer yet. The direction should be determined by the bank, since it is the bank that provides the service to the customer. However the interests of the various internal and external stakeholders should also be taken into account.

6.2.3 Quality of own product should be above any doubt
As stated in the previous paragraphs, there are many stakeholders who should have their role and responsibility. The telecom provider is responsible for the network connection. The customer owns the device and is primarily responsible for the device and its usage. The only part where the bank has a direct influence, is the app and services it provides. Measures should be taken to achieve a high quality product. A clear internal governance structure is the start, where all the stakeholders are involved in, for example, the initial risk assessment, development, testing, deployment and support. This should be done for the entire chain (e.g. app, services running on bank servers and support processes).

6.2.4 Investing more in detective controls
A mobile device is owned by the customer, the bank cannot lock it down like an enterprise mobile device (for example a blackberry supplied to an employee). When the effectiveness of preventive controls is limited, more should be invested to have stronger detective controls. In essence, one can deem the device as untrusted and the application developed as compromised because of a not trusted device. The actions entered in the mobile app eventually are sent to the bank for processing. That is the level where the transactions are processed, that is the place where it can be verified either by server side set limitations (whitelisting, maximum amounts) or by fraud detection.

6.2.5 Support processes should be in place
Support processes should be in place in case an issue does occur. Not only for the customer side but also on the bank side. For example when logs indicate that one account from another bank is used as a money mule it should be swift in notifying the other bank. The customer should also be able to get the support he needs when
he has an issue with usage of the mobile app. When it is not possible for the customer to use the mobile app, alternatives should be offered (transferring funds through mobile banking is not working, but traditional banking is an alternative). Or when the customer is flagged for a fraudulent transaction because of malware, he should be informed by the bank and helped to safely use the mobile app again.

6.3 Recommendations for further research

The scope of this research has been on the consumer side of mobile banking, specifically mobile banking as an application used on a mobile device. The recommendations below are based on the subjects from the previous paragraphs.

- An analysis of the roles and responsibilities of the stakeholders involved and the role of the auditor in such a complex governance structure.
- Finding the right criteria and balance between prevention through user awareness and corrective action when reaching a certain monetary threshold (e.g. sanctioning, transaction insurance).
- An analysis of secure development on a mobile device. A mobile device is an always on device, assumptions for desktop PC’s that cached passwords are destroyed when the device is turned off cannot be made.
- Services running on the bank side for mobile banking, which was out of scope for this research (e.g. servers running back end services, transaction validation, fraud detection, support processes, etc.)

6.4 Chapter conclusion

In this chapter a synthesis was made based on the previous chapters. A few common themes emerged during interviews with experts in the field of banking and IT security. Some security controls and measures repeatedly appeared across the security threats and the categories (users, devices, application and data and governance) that were defined in the mobile banking security model.

In light of these themes possible directions for future research were given. In the next chapter this research will be concluded by revisiting the main research question.
Chapter 7: Concluding the research

In the first chapter of this research the outlines were defined. First the scope was defined. This research focused on the consumer usage of an application (“app”) installed on customer owned mobile devices. The type of application in scope was mobile banking applications.

Then the main research question was drafted which is:

*What are the security aspects of mobile banking and what controls can be applied to address those aspects?*

In order to answer the main research question, three sub questions were formulated. The first sub question was answered in chapter 2 where the current state of mobile banking was outlined. First an introduction to mobile banking was given, three types of mobile banking were touched upon and the future outlook of mobile banking apps was given.

In chapter 3 the security challenges for mobile banking in the context of mobile devices and mobile applications were discussed. Based on literature research 8 threats emerged which could endanger the *confidentiality, integrity* and *availability* of the *security assets of mobile banking*. Sub question 2 was answered with this chapter.

In chapter 4 the outlines of the mobile banking security model were drafted. Threats were grouped in the following categories: *users, devices, applications and data* and *governance*. Security controls and measures listed in chapter 5 were the result of interviews with professionals in the field of banking and IT security. In these chapters sub question 3 and in part the main research question was answered.

This research was concluded in chapter 6 where common themes derived from the mobile banking security model and the expert interviews were discussed and directions for future research were given.
References

ABN Amro Bank N.V., 2009. ABN AMRO Mobiel. , 24(September). Available at:

ANP, 2011. Overheid wijst systeembanken aan. Nuzakelijk.nl. Available at:


Android Developers Blog, 2009. Android Market update: support for priced applications. Available at:

http://online.wsj.com/article/SB10001424052748703805704575594581203248658.html#printMode.


Apple Inc., 2007. Apple Reinvents the Phone with iPhone. Apple Press Info. Available at:


Mallat, N., 2006. Exploring Consumer Adoption of Mobile Payments - A Qualitative Study. Helsinki Mobility Roundtable, 6(44). Available at: http://sprouts.aisnet.org/6-44.


## Appendix

### Users

<table>
<thead>
<tr>
<th>Security threat</th>
<th>Control type</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of user awareness</td>
<td>Preventive</td>
<td>• Public awareness campaign together with the government and other banks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Awareness campaign from the bank and tailor to specific customer groups</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Awareness through deterring examples shown in media, brochures and website of own bank</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Educate customer by showing messages on first time usage of the app and during usage</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Offer security training to users</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Clearly inform customer that there are limits on what the bank is willing to compensate (limited liability from bank, customer is responsible for own behaviour) stated in the terms and conditions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Confront customer with own behaviour</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Introduce “own risk” for the customer</td>
</tr>
<tr>
<td></td>
<td>Detective</td>
<td>• Measure user awareness through customer surveys, panels and individual interviews</td>
</tr>
</tbody>
</table>
| Loss, theft or improper disposal of devices | Preventive | • Only allow authorized access to the mobile device (pin code)  
• Only allow authorized access to the mobile banking application (pin code)  
• Encrypt data on the device  
• Minimize amount of data on the device  
• Offer re-initialization functionality in the app |
| Corrective | • Analyse incidents to shape preventive, detective and corrective measures  
• Measures towards the customer: send information brochure to victims, highlight own responsibility, impose sanctions, charge own risk |
| Corrective | • Record usage statistics and support requests from customer and consult this database at bank side  
• Fraud detection at bank side |
| Corrective | • Offer support processes (self-service or customer support) to block the mobile banking application, contact the customer and remote wipe the private information/app/mobile device  
• When app has not been used for some time, message the customer to authenticate |
| Detective | • Customer finds out self  
• Customer uses phone localization feature  
• Usage detection (e.g. second device activation, period of time not used) at bank side  
• Fraud detection at bank side |
In case of fraud, block the transaction, contact the customer and remote wipe the private information/app/mobile device

Measures towards the customer: send information brochure to victims, highlight own responsibility, impose sanctions, charge own risk

Table 9: Component users: Security threats and solutions

<table>
<thead>
<tr>
<th>Security threat</th>
<th>Control type</th>
<th>Actions</th>
</tr>
</thead>
</table>
| Malware         | Preventive   | • Awareness against installing rogue apps and platform alteration  
                  • Install antivirus software to prevent infection  
                  • Only allow installation of app through closed distribution  
                  • Signing the app with private signature  
                  • Minimize amount of data stored on device  
                  • OS hardening |
| Detective       |              | • Malware detection through antivirus application  
                  • Malware detection in the app  
                  • Include integrity check in mobile banking application  
                  • Have application and bank servers detect current operating system version and inform customer to update to latest version |
<table>
<thead>
<tr>
<th></th>
<th>Corrective</th>
<th></th>
<th>Preventive</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• Usage analysis and fraud detection at bank side</td>
<td></td>
<td>• Awareness to shield the access code on entering it in the application</td>
</tr>
<tr>
<td></td>
<td>• Upon detection force re-initialization of the mobile device and reinstalling the app</td>
<td></td>
<td>• Random number pad on each app start</td>
</tr>
<tr>
<td></td>
<td>• Shutdown app and remotely wipe the private information upon malware detection and inform customer and bank</td>
<td></td>
<td>• White listing of recipients</td>
</tr>
<tr>
<td></td>
<td>• Remove malware from device</td>
<td></td>
<td>• Encrypt the connection end-to-end</td>
</tr>
<tr>
<td></td>
<td>• Upon detection, limit the app functionality or raise security requirements when initiating transaction (e.g. tokens needed)</td>
<td></td>
<td>• Encrypt the user session on application level (user id and pin code)</td>
</tr>
<tr>
<td></td>
<td>• Act upon usage and fraud detection findings (delay or block transactions)</td>
<td></td>
<td>• Force changing of access code application remotely</td>
</tr>
<tr>
<td></td>
<td>• Upon detection, analyse the malware and use weaknesses of malware against themselves</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Trace down malware spreader</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Measures towards the customer: send information brochure to victims, highlight own responsibility, impose sanctions, charge own risk</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>Precaution</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detective</td>
<td>Use one time transaction tokens generated through other channel</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Real time fraud detection on bank side</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Afterwards analysis of logs</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Customer can see fraudulent transaction in own transaction list</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Detect data manipulation on server side (e.g. verifying digital signatures or one time transaction tokens)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Corrective</td>
<td>Offer support processes for customer</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Upon fraud detection, block the transaction, block the application, record in knowledge base, and inform the customer and bank.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unauthorized access</td>
<td>Preventive</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Awareness not to leave phone unattended</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Usage of pin code to access device</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Usage of two factor authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Add biometric authentication</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Detect the verification and identification means on input</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Fraud detection on bank side</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Corrective</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Block the device after a certain number of tries</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Upon fraud detection, block the transaction, block the application, record in knowledge base, and inform the customer and bank.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device malfunction</td>
<td>Preventive</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Customer can use plastic case to protect device</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Platform alteration</td>
<td>Preventive</td>
<td>Detective</td>
<td></td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------</td>
<td>-----------</td>
<td></td>
</tr>
<tr>
<td>Device performs regular self-tests</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rigorous testing of the device in combination with the app</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Perform penetration tests on the mobile device</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Limit amount of data on the device</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Upon device self-check fail inform customer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application detects device malfunction</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disable certain functionality in the app or shutdown app upon detection malfunction</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Offer support processes to help the customer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer should have mobile device repaired</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Awareness towards customers on the risks of platform alteration</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Record in the terms and conditions of usage that no support is given when platform is altered</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inform customer that platform alteration is not supported</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device and OS hardening</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Force certain checks on the service side (force encryption of the connection server side)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Include platform alteration detection in the mobile banking application</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Detect that certain server side required settings are not adhered to</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Fraud detection on bank side

Corrective
- Upon detection, inform the customer and the bank, block the application, remote wipe of the private information
- Upon detection, mark all transactions as high risks, delay transactions, block transactions, increased own risk, insurance fee or customer wholly responsible

Denial of service
Preventive
- None, responsibility of network access is at telecom provider

Detective
- None, responsibility of network access is at telecom provider

Corrective
- Upon detection (through customer support or social media) contact telecom providers and government agencies
- Offer alternative channels to the customer (e.g. phone)

Table 10: Component device: Security threats and solutions

Applications and data

<table>
<thead>
<tr>
<th>Security threat</th>
<th>Control type</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unauthorized access</td>
<td>Preventive</td>
<td>- Application pin code</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Pin code to access app is different from authorizing a payment</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- White listing of account numbers the customer is allowed to transfer funds to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Two factor authentication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Biometric authentication</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Random change of the number pad</td>
</tr>
<tr>
<td>Application malfunction</td>
<td>Preventive</td>
<td>Detective</td>
</tr>
<tr>
<td>-------------------------</td>
<td>------------</td>
<td>-----------</td>
</tr>
<tr>
<td></td>
<td>- Only allow access when there is a valid session, session is only provided after login</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Encrypt the data in the app and the connection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Minimize the amount of data stored</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- First time authentication through other means</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Server side check of the pin code</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Fraud detection on bank side</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Detect simple pin codes (e.g. 12345)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- After number of wrong tries, block app and remote wipe private information</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Upon fraud detection, delay transaction, block transaction, contact customer</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Good vendor selection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Secure development</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- In case of exception, the right action should be performed by the app</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Good test management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Penetration testing of application</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Conduct customer pilots</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- USAGE OF HASH TOTALS TO VALIDATE ELSEWHERE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- For continuity reasons, good knowledge management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Detect malware and platform alteration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Validate hash totals</td>
<td></td>
</tr>
</tbody>
</table>
• App integrity self-check
• Analysis of log data and reporting
• Customers start to complain through customer support or social media
• Incident management
• Detecting version of app used and inform customer and bank

Corrective

• On new app update, force update the new app version
• Inform customer if hash totals cannot be validated, offer direction to reinstall the app
• Good problem and change management with good governance structure
• Repair the malfunction
• Offer alternative to customer

<table>
<thead>
<tr>
<th>Security threat</th>
<th>Control type</th>
<th>Actions</th>
</tr>
</thead>
</table>
| Risk of mismanagement | Preventive | • Define a policy on the development and usage of client facing mobile applications  
• Set up incident response processes and scenarios  
• Identify number and type of logging necessary  
• Decide on level of support in terms of knowledge and support hours  
• Risk management of own processes |
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>
| **Detective** | • Checking the controls: compliance, risk management, auditing processes and IT systems  
• Quality assurance  
• Complaints from customers (through customer support or social media)  
• Monitoring of mobile threats |
| **Corrective** | • Training of IT and helpdesk staff  
• Detection and reporting of risks  
• Good management and reporting information  
• Take actions on governance issues (e.g. reviewing incidents, training of IT and helpdesk staff)  
• Adequately resolving findings from control function |

Table 12: Component *governance*: Security threats and solutions