Security of mobile banking
Project proposal

Prepared by Kelvin Chikomo and Ming Ki Chong
Supervisor: Alapan Arnab, Andrew Hutchison

Data Network Architecture Group
Department of Computer Science
University of Cape Town
Rondebosch 7701

Email: {aarnab, hutch, kchikomo, mchong} @cs.uct.ac.za
1. Project description

In the past decade, the number of online banking users has increased rapidly. This has led to developers investigating on more convenient methods for bank customers to perform financial transactions. This has in turn resulted in the introduction of mobile banking. Mobile banking is a new convenient scheme for customers to perform banking transactions across nations without location boundary. The usages of mobile banking are predicted to increase as the number of cellular phone users are increasing and mobile usage are foreseen to revolutionize payment banking for industries world wide [1].

The security architecture for cellular network is not entirely secure. As described in [2], GSM (Global System for Mobile communication) network infrastructure was proven to be insecure and many possible attacks have been discovered and protection discretions were not considered, therefore sending protective banking information across open mobile phone network is insecure.

In this project, we propose to investigate on the security issues within mobile banking through cellular phone network (GSM). The goal is to build portable device applications that ensure users can securely send their banking information via the mobile network.

Our objective for this project is to investigate security issues in each level of the mobile network architecture. At each level we intend on investigating how messages and signals are sent across from user’s cellular phone to mobile network (the overall security architecture of mobile network, message encryptions) to bank server. We will inspect the flaws of securities within cellular networks, the current international standards and practices for mobile banking and we will examine some existing security protocols for mobile transactions. Details will be discussed in section 3.2.

We will investigate the current security within SMS banking and GPRS banking. For each solution, we will focus on its economical advantages and disadvantages, its end-to-end security and its cost factor.

Secure protocol applications using SMS/GPRS will be developed to simulate protected mobile banking procedures.

2. Related Work

The initial idea of mobile transactions is to provide a convenient and cost effective way for customers to pay and perform banking transactions. Mobile banking (m-banking) service is a modified version of internet banking using cellular technology and the GSM network as a medium to transfer request over wireless network.

2.1 Transaction Architecture

The mobile transaction architecture consists of three main components i.e. the user, the device and the mobile transaction provider, [1]. The user is the client who is requesting for the service, the device is the mobile device which connects the client and the service provider through the wireless network, and the mobile transaction provider could be a cellular operator, a bank or a combination of both [1]. Figure 1 below outlines the summarization of modular architecture of cellular phone transactions.
For a transaction to be secure, it consists of the following three independent modular processes:

- **Identification**, the user sends his/her unique identification information to the server via a cellular device network for verification. Identification component can consist of user’s password or bio-metrics information.

- **Authentication**, the service provider should authenticate the transaction from users via an identification process or cryptographic mechanism.

- **Secure Performance**, the transaction is performed on the service provider side. The service provider has the responsibility to ensure the requested transaction is performed under a secure environment and ensure a safe protocol for payment transfer.

2.2 Existing SMS banking services

In 2005, South African First National Bank launched a new service for their customers to perform banking transaction across any location in South Africa. Customers use mobile phones to send banking requests via SMS (short message service) technology to the banking server. FNB mobile banking allows customers to purchase cellular phone airtime, check account balance, get bank statements, transfer money to other accounts and etc. This service is initiated by the customer providing a banking instruction by sending the keyword to a specific number and followed by the customer dialing a specific string attached with a PIN (Personal Identification Number, selected during registration process) code to identify the cellular phone user. Once the PIN is authenticated for the phone number, the bank will reply with the request output for the customer, for full instructions, refer to [3]. This is a convenient method for customers to do banking, as the user does not require traveling to a physical location to interact with a bank teller and this service provides twenty-four hours real time services [4].

2.3 Existing GPRS mobile banking solutions

GPRS based mobile banking is fairly new in South Africa, with most leading banks offering the service. According to Paul Vecchiatto and Tracy burrows of ITalk Investec private bank and Absa, they are offering mobile banking over GPRS. [8] Standard bank has a similar offering; they provide cell phone internet banking over GPRS and EDGE technology and their cell phone banking options use HTTPS SSL 128-bit encryption.

FNB launched a WAP (mobile Internet) banking offered a few years ago, but result it had very few FNB customers use such service, for this reason the CEO of FNB Mobile and Transact Services claims that the bank is focusing more on making cell phone banking available to all its customers, on any phone, on any network using their current menu and SMS cell phone banking offering. [8]
Investec mobile

“Regarded as one of the most innovative banks in the world, Investec Private Bank, a division of international specialist banking group Investec plc (INP, INL), is now introducing a capability that will enable clients to manage their finances anywhere, anytime, from a secure platform.”[7]

Investec private bank introduced mobile banking in March 2006; its mobile banking service is based on its web banking service. Investecmobile uses GPRS, Edge, and 3G technology. Investecmobile boasts of its multilayered security approach and its application to cellular phone technology. It also boasts of its detective and preventative security measures that they have implemented so as to achieve a secure channel between the mobile station and the bank.

2.4 Researched SMS communication protocol

A Security Mechanism for Secure SMS Communication by Ratshinanga of University of Pretoria [5] has indicated that the GSM network does not provide important security facilities such as authentication, end-to-end security, non-repudiation and anonymity. In the GSM network, mobile SMS text content is sent over in clear text format or in a breakable encrypted format [2], which consequently makes sensitive text messages sent across the cellular network insecure. This vulnerability enables an attacker with the right equipment to eavesdrop on the information being sent, therefore a better SMS communication protocol is needed to transmit text data between server and client.

Ratshinanga [5], have suggested establishing an encrypted protocol connection using public keys and session keys between clients to server. The client initiates the connection by sending its username and a salt number\(^1\) encrypted using the server's public key to the server. When the server receives the client message it is decrypted using the server's private key. The server retrieves the salt number and username from the received message, and retrieves the relative user PIN from the database; the server can calculate a session key for the client by using hash functions. Once the session key is calculated, the server replies and establishes connection with client. The client can calculate the session key in parallel, once the client receives a reply from server, a secure connection is established.

The session key is generated individually by hashing the username, salt number and the shared PIN number. Attackers cannot generate a session key without knowing the PIN for the specified username. The salt value provides a more secure session key generation as the salt number is 128 bits long [5], it increases difficulty for attacker to break the session key. To prevent replays, a SQ (sequence number) is used. This number is incremented by one each time when the message reaches the destination. The client or the server can check if SQ is incremented by one, if not the received information can be discarded; as it indicates it is out of sequence.

This protocol generates a secure communication channel between client and server via SMS. It ensures confidentiality and integrity of SMS communication [5], in contrast the encryption and keys generation causes the protocol to operate very slowly causing inefficiency.

2.5 Upcoming Service Provider: Fundamo

Fundamo is a company which provides mobile applications and business solutions for corporations that intend on offering mobile transaction services. Fundamo builds applications for banks, mobile shopping and mobile payment.

\(^1\) Salt is an initialization vector of a block cipher. Often specifically salt is an initialization vector used to obscure a pass phrase. http://en.wikipedia.org/wiki/Salt_(cryptography)
In August 2005, Standard Bank and Fundamo agreed on a joint venture with MTN to introduce a new banking service that allows customers to access their accounts via their cellular hand sets [6]. This service offers SMS alert, Person-to-Person alert payment, fund transfer, bill payment and etc. Fundamo uses a three layers security to achieve protection against fraud. It requires the user’s SIM (Subscriber Identity Module) in the user’s mobile phone, a PIN (selected by user) and the user's voice print [6]. The transaction is tied to these three security means. The customer’s request is only granted when the user is authenticated. The three layers of security provide a unique protection mechanism, the SIM card provides as a physical security key, the PIN as a password security and the voice print verification act as bio-metric security.

3. Outcomes

3.1 System

3.1.1 Software
The outcome of the project in the software section will comprises of three main parts i.e.
- A subset of banking services,
- A secure GPRS banking protocol
- A secure SMS banking protocol

Subset of banking services
The subset of banking services will encompass some of the banking services that exist in current architectures like SMS banking or ATM banking. Some of these banking services include balance enquiries and money transfers between two different accounts. The final implementation of the banking services will follow the architecture illustrated in figure 2 below. Instead of updating proper bank servers we will implement a simulated banking server which we can test on. We intend on implementing the banking services to communicate with both GPRS and SMS connections.

![Figure 2. Illustration of Mobile banking architecture](image-url)
Secure GPRS banking protocol
Figure 3 below illustrates a basic banking GPRS protocol. Our secure banking protocol will build on this protocol.

Secure SMS banking protocol
Figure 4 above shows the overview layers of mobile banking using SMS as communication protocol
- **Banking Application** is the application layer that the users’ interface interacts with to the bank server.
- **Secure SMS protocol** layer provides a secure communication channel using SMS messages to transfer communication data.
- **Mobile phone interface** is the cell phone specification that is specified by the mobile phone manufacturer.
- **Short Message Transport Protocol** layer is specified by the GSM network, this layer transmits SMS messages across the mobile network using SM-RP (Short Message Rely Protocol) and SM-CP (Short Message Control Protocol).
- **GSM network** is the mobile phone service provider network.
- **Banking server** is the bank server which authenticates users, accepts user’s banking transactions and replies users with performed transaction status.

3.1.2 Key features
Some of the noteworthy features in our mobile banking solution will include:
- Session handling
- Key management
- Encryption algorithms
- End-to-end architecture
- GPRS solution should be accessible through a number of transaction channels, i.e. it should be accessible through EDGE, 3G, and 3.5 G technology
- Any security implementations on the Bank server should have a plug-in option into existing bank servers.
3.2 Questions to tackle
This project intends on covering two main topics of investigation

We plan on investigating the different security protocols on offer by the various solutions and their underlying technologies, from the research we are determined to produce a thorough paper on these security protocols and their underlying security detailing their strengths and weaknesses.

We intend on analyzing and exploring the transactions at every link from the cell phone to the bank server and back. Our research will comprise of analysis of the encryption algorithms used, density (number of users) of base towers and a risk analysis of the security vs. reward at each stage. We also intend on investigating the international practices and how they relate to the South African context.

A huge section of our research will involve investigating the possible alternatives to SMS banking, and how security objectives such as confidentiality, integrity can be achieved using these alternatives.

3.3 Expected impact of your project
From the project we expect to produce a complete secure protocol for mobile banking which will cater for all network security requirements i.e. authentication, non repudiation, authorization, availability, integrity, confidentiality, and access control. Depending on the insecurity of existing protocol, we expect to produce attacks that can unravel flaws in existing mobile banking protocols.

3.4 Key success factors
Success of our project depends on the following major factors:
- Level of completion of our mobile banking protocol
- Extensity of our research paper.

4. Schedule

4.1 Timeline
Appendix A has a detailed Gantt chart with the start date, end date and duration for each task.

4.2 Resources required
- GSM modem
- GPRS, EDGE and Java enabled phones.
- Java Platform, Micro Edition (J2ME).
- Collaboration with banks with existing solutions like FNB and Standard bank.
4.3 Milestones and deliverables

<table>
<thead>
<tr>
<th>ID</th>
<th>Task Name</th>
<th>Finish</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Background Research</td>
<td>July 16</td>
</tr>
<tr>
<td>2</td>
<td>Research paper complete</td>
<td>July 16</td>
</tr>
<tr>
<td>3</td>
<td>Build Architecture models</td>
<td>July 21</td>
</tr>
<tr>
<td>4</td>
<td>Bank server design</td>
<td>July 28</td>
</tr>
<tr>
<td>5</td>
<td>GPRS/SMS phone applications design</td>
<td>August 4</td>
</tr>
<tr>
<td>6</td>
<td>Report: Definition, theory and Chapter on design</td>
<td>August 11</td>
</tr>
<tr>
<td>7</td>
<td>Project presentation</td>
<td>August 15</td>
</tr>
<tr>
<td>8</td>
<td>Bank server development</td>
<td>September 21</td>
</tr>
<tr>
<td>9</td>
<td>GPRS/SMS phone applications development</td>
<td>October 4</td>
</tr>
<tr>
<td>10</td>
<td>Bank server testing</td>
<td>October 11</td>
</tr>
<tr>
<td>11</td>
<td>GPRS/SMS phone application testing</td>
<td>October 18</td>
</tr>
<tr>
<td>12</td>
<td>Implementation running</td>
<td>October 19</td>
</tr>
<tr>
<td>13</td>
<td>Web page design</td>
<td>October 21</td>
</tr>
<tr>
<td>14</td>
<td>Report: Chapters on implementation and Testing</td>
<td>October 23</td>
</tr>
<tr>
<td>15</td>
<td>Web page development</td>
<td>November 5</td>
</tr>
<tr>
<td>16</td>
<td>First draft of report</td>
<td>October 27</td>
</tr>
<tr>
<td>17</td>
<td>Due: Final report</td>
<td>November 3</td>
</tr>
<tr>
<td>18</td>
<td>Poster design and development</td>
<td>November 10</td>
</tr>
<tr>
<td>19</td>
<td>Due: poster, webpage, research paper</td>
<td>November 10</td>
</tr>
<tr>
<td>20</td>
<td>Project demonstrations to supervisors and second readers</td>
<td>November 17</td>
</tr>
<tr>
<td>21</td>
<td>Final project presentations</td>
<td>November 24</td>
</tr>
</tbody>
</table>

Figure 5: Milestones and deliverables

4.4 Work Allocation

Kelvin Chikomo
- Research on current security with GPRS connections
- Design mobile banking solution using GPRS
- Implement mobile banking solution using GPRS
- Implement user interface to interact with mobile bank server through GPRS
- Design and implement GPRS banking server
- Thorough testing on GPRS mobile banking server with GPRS application
- Produce comprehensive report on all the research performed.

Ming Ki Chong
- Research on security using SMS communications
- Design secure SMS protocol
- Implement mobile banking solution using secure SMS protocol
- Implement a mobile phone application that has a user interface and uses the SMS protocol.
- Design and implement SMS banking server
- Thorough testing on SMS mobile banking server with SMS application
- Produce comprehensive report on all research performed

Work to be done by both project members
- Research on current architecture of mobile network i.e. GSM network (mainly focus on security issues and vulnerability of communicating through mobile network)
- Design and build architecture model for mobile banking (secure banking transaction using mobile phones)
- Merge mobile bank server
- Record testing results to illustrate on progress and accuracy of implementation
- Compare results and discuss on efficiency, cost factor, advantages and disadvantages using each solution
- Write research paper to provide summary of project
- Design poster
- Design webpage
- Present final project to supervisors
5. Appendix A

<table>
<thead>
<tr>
<th>ID</th>
<th>Task Name</th>
<th>Duration</th>
<th>Start</th>
<th>Finish</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Background Research</td>
<td>31 days</td>
<td>June 16</td>
<td>July 16</td>
</tr>
<tr>
<td>2</td>
<td>Research paper complete</td>
<td>6 days</td>
<td>July 16</td>
<td>July 16</td>
</tr>
<tr>
<td>3</td>
<td>Build Architecture models</td>
<td>5 days</td>
<td>July 17</td>
<td>July 21</td>
</tr>
<tr>
<td>4</td>
<td>Bank Server design</td>
<td>7 days</td>
<td>July 22</td>
<td>July 28</td>
</tr>
<tr>
<td>5</td>
<td>GPRS/SMS phone application design</td>
<td>7 days</td>
<td>July 26</td>
<td>August 4</td>
</tr>
<tr>
<td>6</td>
<td>Report: Definition, theory and Chapter on design</td>
<td>6 days</td>
<td>August 11</td>
<td>August 11</td>
</tr>
<tr>
<td>7</td>
<td>Project presentation</td>
<td>6 days</td>
<td>August 15</td>
<td>August 15</td>
</tr>
<tr>
<td>8</td>
<td>Bank server development</td>
<td>13 days</td>
<td>September 1</td>
<td>September 2</td>
</tr>
<tr>
<td>9</td>
<td>GPRS/SMS phone application development</td>
<td>13 days</td>
<td>September 22</td>
<td>October 4</td>
</tr>
<tr>
<td>10</td>
<td>Bank Server testing</td>
<td>7 days</td>
<td>October 5</td>
<td>October 11</td>
</tr>
<tr>
<td>11</td>
<td>GPRS/SMS phone application testing</td>
<td>7 days</td>
<td>October 12</td>
<td>October 18</td>
</tr>
<tr>
<td>12</td>
<td>Implementation running</td>
<td>8 days</td>
<td>October 16</td>
<td>October 19</td>
</tr>
<tr>
<td>13</td>
<td>Web page design</td>
<td>2 days</td>
<td>October 21</td>
<td>October 21</td>
</tr>
<tr>
<td>14</td>
<td>Report: Chapters on implementation and testing</td>
<td>0 days</td>
<td>October 25</td>
<td>October 25</td>
</tr>
<tr>
<td>15</td>
<td>Web page development</td>
<td>14 days</td>
<td>October 23</td>
<td>November 7</td>
</tr>
<tr>
<td>16</td>
<td>First draft of report</td>
<td>8 days</td>
<td>October 23</td>
<td>October 27</td>
</tr>
<tr>
<td>17</td>
<td>Due: Final report</td>
<td>8 days</td>
<td>November 1</td>
<td>November 11</td>
</tr>
<tr>
<td>18</td>
<td>Poster design and development</td>
<td>5 days</td>
<td>November 1</td>
<td>November 11</td>
</tr>
<tr>
<td>19</td>
<td>Due: poster, webpage, research paper</td>
<td>6 days</td>
<td>November 11</td>
<td>November 11</td>
</tr>
<tr>
<td>20</td>
<td>Project demonstrations to supervisors</td>
<td>5 days</td>
<td>November 1</td>
<td>November 11</td>
</tr>
<tr>
<td>21</td>
<td>Final project presentations</td>
<td>4 days</td>
<td>November 2</td>
<td>November 24</td>
</tr>
</tbody>
</table>

Project Schedule Date: June 12
6. References


[7] INet-Bridge-*Investec launches mobile banking*. (Website) http://www.mybroadband.co.za

[8] Paul Vecchiatto and Tracy burrows - *Mobile Internet banking spreads in SA*