Master Thesis Project Plan

Mobile Banking in Developing Countries
Secure Framework for Delivery of SMS-banking Services.

Author:

Abunyang Emmanuel
Student Number: s0535249

Supervisor:

Prof. Dr. Bart Jacobs

May 2007

1. Introduction

This project proposal plan is in fulfillment of the requirement of a Masters Thesis project in the Security theme, Computing Science at the University of Nijmegen. It gives an overview of the research project and discusses the project overview, problem definition, research methods and the research schedule.

1.1 Project Overview

The way we live today is so much influenced by computing technologies. Computers control the economy, transportation, banking and many other functions. This development has made information attractive to criminals because of the economic value of such information. The advent of the Internet and wireless communication is believed to particularly have opened an entire new area of crime. The European cyber crime treaty has drawn a criminal policy aimed at protecting society against cyber crime by deterring and prosecuting actions directed against the confidentiality, integrity and availability of computer systems, communication networks and computer data [1]. This indicates the extent to which authorities are getting prepared to fight cyber crime in society.

Internet and mobile technologies are increasingly being adopted and utilized in the banking industry; this has reshaped the consumption of financial services [2]. In this research we analyze the security of electronic banking services with an emphasis on mobile commerce transactions with a focus on mobile banking using mobile devices specifically cell phones. Electronic banking is considered a way of delivering banking services through the internet to the consumer at a reduced cost to the banking industry and improved convenience to the customer [4]. However there exists a low internet connectivity in the developing countries given the costs of connection especially in rural areas and yet banking services need to be brought closer to the population to enhance development [16]. A viable solution here is mobile banking. Here we are interested in what the implications are in the terms of security and also in the economic viability of these technologies in developing countries.

Mobile commerce shall be defined as commercial transaction activities carried out via communication networks that interface wireless or mobile devices. A mobile device is a device used to connect to a mobile service for example cell phones and Personal Digital Assistants (PDA). The high diffusion rate of mobile phones coupled with the stability of mobile communication technologies have greatly contributed to the enhancement of mobile banking solutions in the provision of financial services in the world [5]. Mobile banking is considered as a service that enables users to receive information regarding the status of their accounts, to transfer among bank accounts, to facilitate stock trading and direct payment confirmation using mobile devices.

A number of enabling technologies are being used in the delivery of mobile service applications. They include Interactive Voice Response (IVR), Short Messaging Service

(SMS), Wireless Access Protocol (WAP) and stand alone Mobile Application Clients (MAC).
It is worth noting that a mobile user device in itself may not be able to keep data secure, because it can be stolen or lost. So the question arises, to what extend therefore should these devices be trusted? The goal of this research project will be to analyze these enabling technologies and applications that enhance mobile device trustworthiness in order to investigate the security limitations and challenges and to propose possible solutions to mitigate them. The analysis will be carried out using security attack trees. Attack trees provide a formal methodological way of describing security of systems. We will specifically look at the SMS enabling technology because it's the most cost effective service suitable for a developing country. However it has a number of security limitations for example when authorizing a bill payment the format is Account Number, PIN and amount [6]. Because these messages are not encrypted, prone to human error and normally telecommunication companies keep a copy of these messages in their servers they are quite an easy target for criminals. The intention of this research will be to propose and implement some measure that can be used to offset these limitations given the computing restrictions of the ordinary cell phone which are predominantly used in the developing countries.

1.2 The solution

The solution to offset the above mentioned limitations is to use SMS for encrypted and signed messages. This solution will specifically apply to Global system for Mobile Communications (GSM) networks to enable consumers securely transmit banking information. SMS was specifically intended for sending non sensitive information in a GSM network therefore in its implementation security considerations in terms of confidentiality, integrity, non-repudiation and authentication were not catered for [7]. In general end to end security measures are not implemented.

In our prototype implementation the goal will be to write a MIDlet that secures the value of information that is being transmitted in line with the elements of security that constitute secure communication [3].These are; ensuring data integrity to ascertain that message contents are not altered. This will be achieved using a message digest which constitutes the hashed value of the message contents. In order to ensure data confidentiality we shall use symmetric encryption. Symmetric encryption will be preferred here compared to asymmetric encryption given that the later involves complex mathematical algorithm which require bigger memory. This cannot be handled by the mobile devices given their low volatile memory capabilities. Authentication requires parties to be able identify themselves this will be achieved by validating the stored PIN numbers. To guard against non-repudiation that is, the sender should not be able deny having sent a message. A one time password for encryption will be used.

A secure SMS banking application will be considered to comprise of three components namely the mobile application (MIDlet), bank server and the backend database. This is illustrated in the figure below.

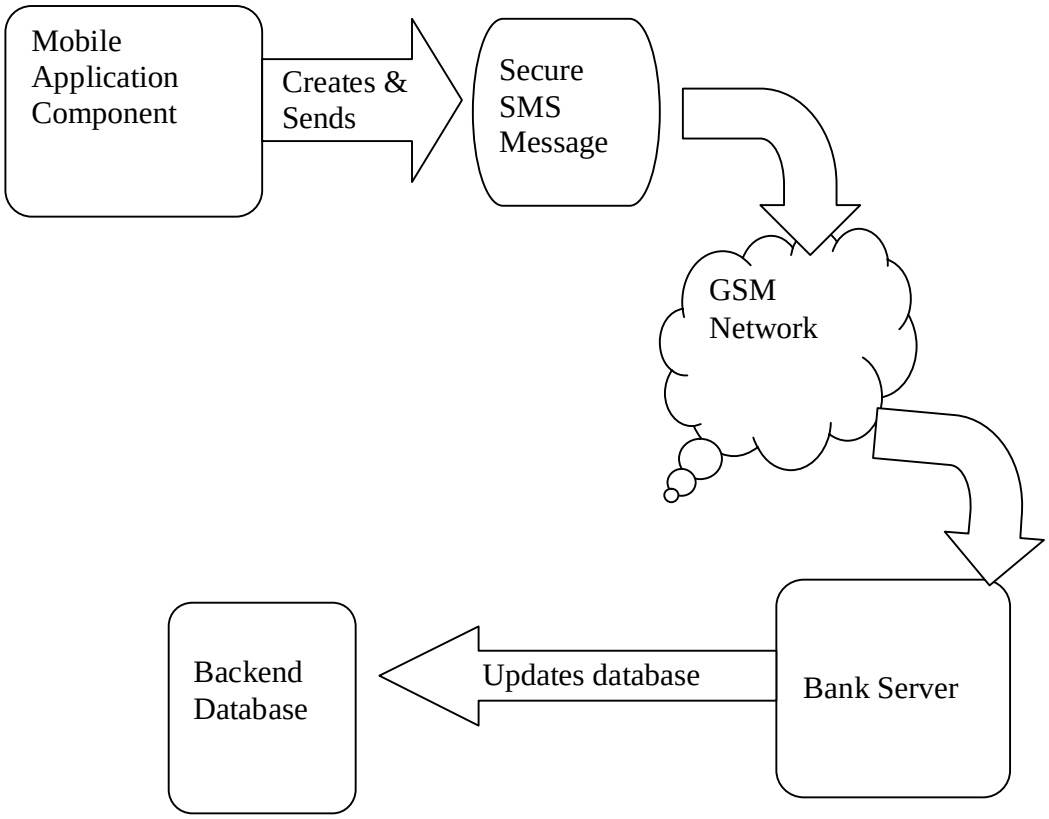

Figure 1. Overview of the Solution

1.2.1 Mobile Application Component

The main focus of the project is writing a MIDlet for the mobile application component. This component will reside on the mobile device it captures all the security information from the user. This information comprises of the users banking details and will be used in generating the secure SMS message that is sent to the server.

Message digest will be used to ensure integrity of the message. To ensure confidentiality a symmetric encryption algorithm using a one time pass word entered by the user will be used. This pass word will only be known by the server and the user. On completing processing the secure message it will be sent to the server through the GSM network.

1.2.2 Bank Server

This component will be responsible for receiving and decoding the secure SMS message. The server will check to ascertain that the message is suitable for a secure SMS protocol. It will then proceed to check for the account identifier from the message and find out if the identifier exists in the server database. After the above check the server decrypts the message using the one time password. The pass word will be discarded when the decryption is successful.
To ascertain message integrity the server will calculate the message digest from the decrypted message using the same algorithm used by the mobile application. It then

compares the two digests for message integrity .When this checks are found to be positive by the server it proceeds to retrieve the PIN (account holders password) from the message and compares it to the account holders PIN from the servers database. The transaction will finally be performed when all the security checks have passed.

1.2.3 Back end Database.

The backend database will serve as a store for the users banking and security details. The communication between the bank server and the backend database will be independent from the one between the mobile device and the bank server. In this research we shall specifically concentrate on the security of communication between the bank server and the mobile application.

1.3 GSM Architecture.

The Global System for Mobile Communication network is the data transmission media in the SMS protocol and the flaws in its architecture have lead to the security shortfalls in SMS-banking system. It is therefore important to provide an overview of its architecture. The GSM technical specification [7] elaborates the architecture of the GSM system. The figure 2 below shows the structure of the GSM architecture.

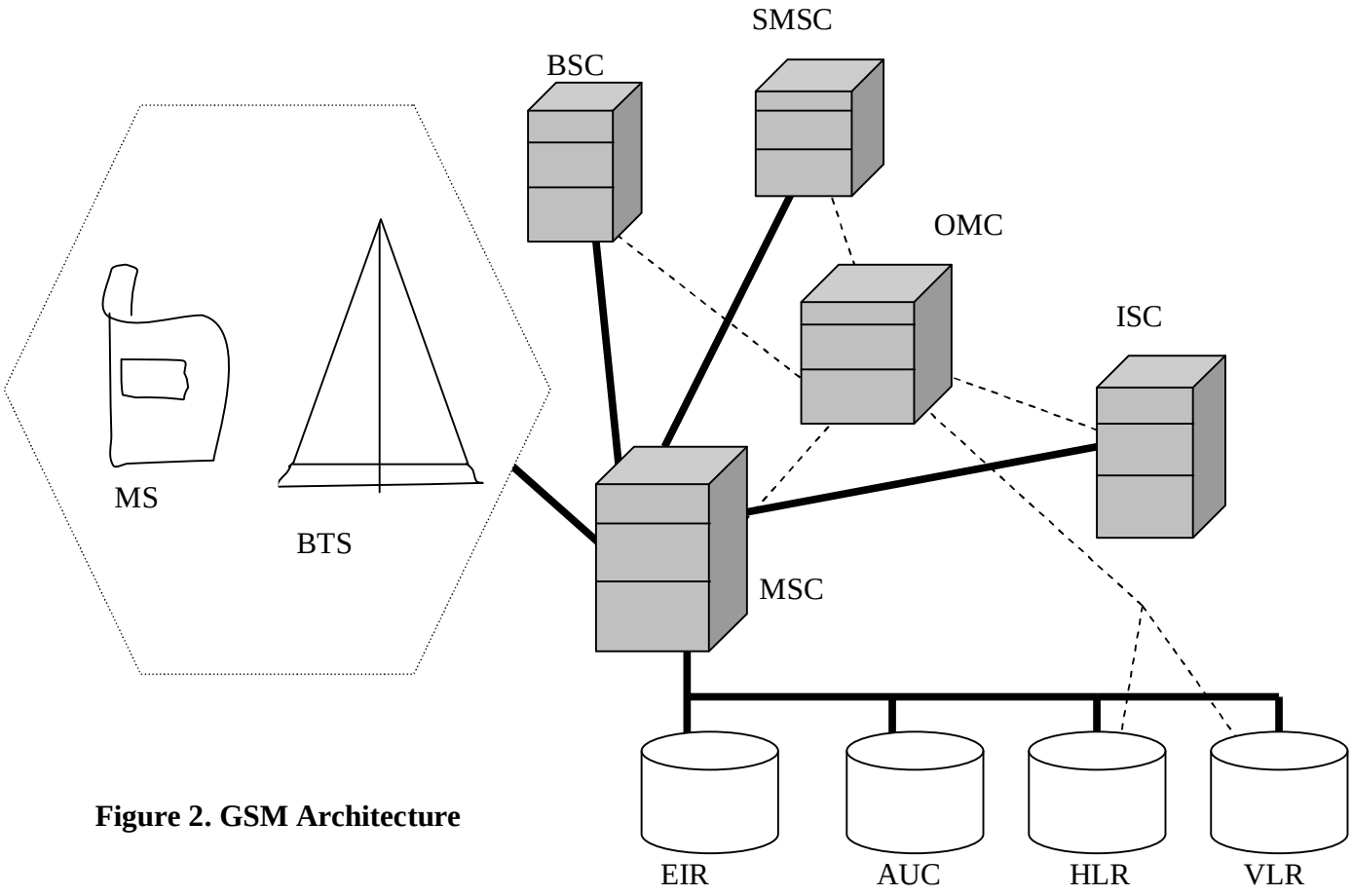

Figure 2. GSM Architecture

Key:

MS - Mobile station
BTS - Base Transceiver Switch
BSC - Base Station Controller
MSC- Mobile Switch Centre
ISC - International Switching Centre
VLR- Visitor Location Registry
EIR- Equipment Identity Register
AUC- Authentication centre
HLR- Home Location Registry
SMSC-Short Message Service Centre.
OMC- Operation Management Centre

This section briefly describes the functionality of the various components illustrated in figure 2.The GSM comprises of various components in the figure the solid lines show communication between core components. The dotted lines show the internal connection for communication used during maintenance. In a typical communication operation the Mobile Station (MS) which is in effect a cellular handset initiates the communication. The communication signals are transmitted from the MS and received by the Base Transceiver Station (BTS). The function of the BTS is to receive and transmit radio signals to and from the MS. It is also responsible for translating the radio signals into digital format and transferring them to the Base Station Controller (BTS). The BSC forwards the received signals to the Mobile Switching Centre (MSC). The MSC interrogates the Home and Visitor Location Registers (HLR and VLR) this databases keep information about location of the destination MS. In the event that the received signal is an SMS message then it is routed to the Short Massage Service Centre (SMSC) for delivery to the required destination. The SMSC keeps a copy of the sent SMS in its database after it has been sent. In case of an international connection the signal is routed through the International Switching Centre. In order to facilitate equipment verification and user authentication the Equipment Identity Register and Authentications Register database are used. The operation and management centre controls maintenance operations.

1.4 System Development.

The solution will comprise of developing a MIDlet using the Java™ technology. The Java ™ technology is a suitable development environment because presently many mobile phones in the market come with a standard built in Java ™ Virtual Machine (JVM). The Java™ technology also has many libraries to assist in the mobile application development. The java platform that is going to be used is the Micro Edition (J2ME) it is specifically designed for consumer devices with limited memory, display capabilities and resources [8]. Within this platform there are two configurations that is the Connected device Configuration (CDC) and the Connected Limited device configuration (CLDC). The implementation will be using the (CLDC) configuration because the defined characteristics of the cellular handset fall under this category. The CLDC defines a specification for a JVM and a set of java classes (libraries). The minimum software and hardware requirements for CLDC are [8];

- 128 kilobytes of memory for running the JVM and CLDC libraries.
- 32 kilobytes of volatile memory for runtime memory allocation.
- The host Operating system capable of launching and selecting applications.

- And it should also have the ability to remove java applications from the device.

The majority of mobile handsets do have this minimum requirement which makes CDLC configuration a suitable tool for the development of the suggested solution.

1.5 SMS Secure Message Protocol.

1.5.1 Message Structure.

In order to be able to explain the SMS secure protocol it's important to specify the message format. The format of an SMS message packet provides for four bytes to specify meta data and the size of the payload. The maximum length of the payload is 160 characters at 8-bits per character adopted from (Clements 2003) [9]. The message structure is shown in figure 1. Below.

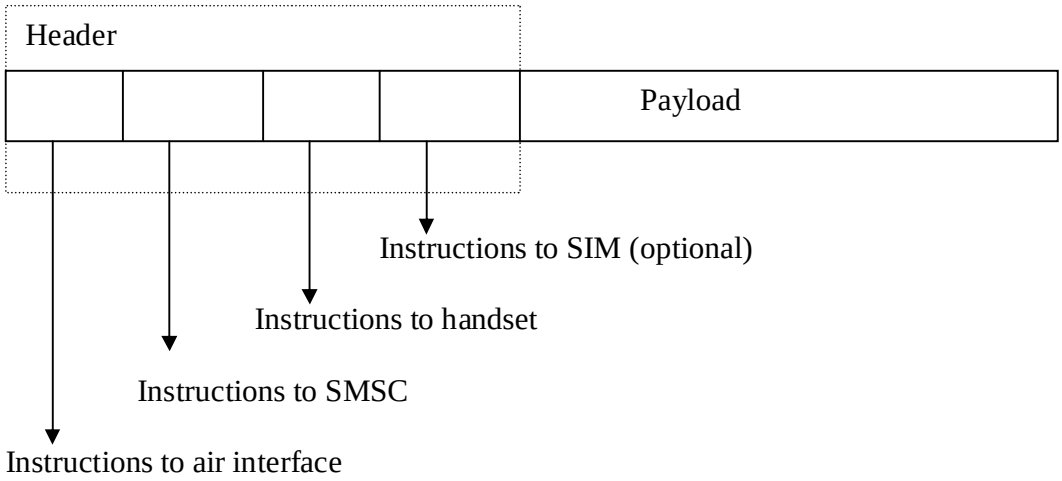

Figure 1. SMS message structure.

Using the above structure we derive the following secure SMS message structure. The secured message comprises of multiple fields for various security checks required by the protocol. The message structure will have a generic format as follows.

<Version><AccID><Seq>< Secure Message>

- In order to ensure the bank server does not receive messages that are not intended for it a *version* number is used with a specified bytes pattern.
- The *AccID* comprises the account identifier of the user.
- The *seq* will specify a sequence number of the one time password.

The secure message field includes the following subfield formats.
<Encrypted Text Length><Encrypted Banking Details><Digest length><Digest>

- The Encrypted text length gives fixed maximal length with padding of the ciphered message.
- Digest length also gives the number of next bytes that comprise the message digest.

- The Digest is for the server to check for message integrity. In the protocol the digest will comprise the following fields *Version, AccID, Seq, Time Stamp, PIN, Type of Transaction* and *Transaction payload*

Further the Encrypted banking details field will comprise of the following subfields
<PIN><Type of Transaction><Transaction Payload><Encryption Payload>

- In order for the server to authenticate the user the *PIN* comprising of the users predefined password is used.
- In this protocol we specify two transaction types though more types could be added. The transaction types are check balance and transfer among accounts. The *Type of Transaction* field is used by the server application to identify the type of transaction to be performed.
- The Transaction Payload depends on type of transaction and comprises of extra data used for the transaction. For the case of the money transfer and check balance they will have the following fields respectively.
  <Destination Account><Amount><Random Bytes>
  <Random bytes>(No transaction payload required)

1.5.2 Review of Possible Handshake Protocols.

Ratshinanga et al [10] suggested a handshake protocol that uses the public and session symmetric key and authentication cryptography strategy. The following denotations are used in the explanation of the protocol.

BS: - Denotes the Bank Server.
MC: - Denotes the banks Mobile Client.
BPK_{pub}:-Denotes the public key of the bank server.
BPK_{pri}:-Denotes the private key of the bank server.
R_{MC}:-Denotes the random challenge response generated by the mobile client.
R_{BS}:-Denotes the random challenge response generated by the bank server.
SK:-Denotes the symmetric session key shared by the bank server and mobile client.
SQ: -Denotes the sequence number (nonce) generated by the mobile client starting at 1 on commencement of the protocol..
Slt:-Denotes a salt value generated by MC its used by bank server and the mobile client to generate the session key (SK).
||:- Symbolises concatenation.

The handshake protocol is defined as follows;

M1: C → S: E_{BPKpub}[AccID|| Slt || SQ || R_{MC}]

M2: S → C: E_{SK}[R_{MC}|| R_{BS}|| SQ] where $SQ_n > (SQ_{n-1} + 1)$

M3: C → S: E_{SK}[R_{MC} || R_{MC} || SQ] where $SQ_n > (SQ_{n-1} + 1)$

In order to initiate the connection the mobile client sends its username and a salt number[1] to the bank server. The sent message is encrypted using the bank server public key. The bank server decrypts the message using its private key upon reception and retrieves the salt number and account number from the message. The bank server thereafter retrieves the users PIN from its database. This data is then used to generate the session key and a secure connection is established. The session key is generated individually by hashing the account identity, salt number and the shared PIN. The sequence number is used to guard against replay attacks. The sequence number is incremented each time a message reaches its destination. A message is discarded if the sequence is not followed. The purpose of the random challenge is to assure the freshness of authentication [12]. The R_{MC} is random challenge used to ensure that a client is not able to perform an attack on the protocol by replaying previously used messages of a legitimate protocol.

Lam et al (2003) [13] also present a light weight security protocol for mobile commerce platforms discussed below. In the discussion the following denotations are used.

- S:-denotes the server side of the security protocol;
- C:-denotes the client side of the security protocol;
- $EK_{S:}$ - denotes the public key of S. We assume that the public key of S is made known to C prior to the execution of the protocol;
- DK_S :-denotes the private key of S;
- PIN: - is the password of user C which is known only to C and is verifiable by S. The password typically has a length of eight to sixteen printable characters;
- Ra: - is a nonce identifier (a random number) generated by S;
- (Rb1 and Rb2):- are nonce identifiers (random numbers) generated by C;
- SN: - is a sequence number generated by S for this protocol run;
- SK: - is the symmetric session key shared by S and C for protecting transaction messages in the session;

The protocol commences when a mobile client wishing to perform a commercial transaction sends an authentication request to a server. The following protocol between the server and the mobile client is then carried out to establish a shared secret key that is used for the subsequent secure communication for the session.

M1 C → S: I am C
M2. S → C: Ra
M3. C → S: $EK_S[Ra, R_{b1}, PIN], EK_S[Ra, R_{b2}, SK]$
M4. S → C: $E_{SK}[SN, R_{b2}]$
The description of the protocol is as follows.
In message (M1) the server sends a random challenge Ra as an assurance for protocol freshness to the client.

Message (M2) the client returns a two message response. The first contains the secret password (PIN) known only to the client and server. The PIN allows the server

[1] Salt number is a-bit random string used to obscure a password. It makes dictionary attacks on passwords less effective [11].

authenticate the client by verifying the correctness of the password. The secrecy of the PIN is enforced by encrypting the message using the public key of the server EKs. The server checks the value of Ra to ensure that the message is not a replay of some previous protocol message. Since Ra is sent in clear form a nonce identifier R_{b1} is included to prevent brute force attack on the message to retrieve the PIN. In the second part the session key (SK) is generated by the client C. The nonce identifier R_{b2} is included to allow the client to confirm that the server knows SK because DKs is only available to the server.

In message (M3) by encrypting the nonce identifier Rb2 with SK, the server proves to the client it knows the shared key. The communication is thereafter proceeds using the shared key SK.

In both protocols presented above its quite clear the cost implications of the communication is a big concern. This is because the key exchange involves use of three messages per transaction implying a huge cost to the customer. The protocols do not use the concept of the time stamp to ensure the protocol freshness because not all mobile phones will have their clocks coinciding with that on the server. However for some less sensitive transaction like checking a balance we shall use the timestamp approach.

Considering the above issues we derive separate protocols for the check balance and money transfer transactions given the fact that each has a different level of security sensitivity.

1.5.3 Check balance

Since this transaction has less security sensitivity we propose sending a single message to the server. The message is encrypted using the public key of the server and comprises of the following.

M1: C → S: E_{BPKpub} [AccID || Timestamp || Slt || PIN]

M2: S → C: E_{AccP} [<balance>] or [<Error message>] in plain text

1.5.4 Money Transfer.

In this protocol we propose use of a random password generator that will create a list of passwords and corresponding sequence numbers written to a file. This list will be known only to the user and the bank.

M1: C → S: E_{sk}[AccID || Destination AccId || Transfer amount ||SQ||PIN]

M2: S → C: E_{AccP} [<confirmation>] or [<Error message>] in plaintext**.**

Where E_{AccP} denotes encryption using concatenation of the user account identification and PIN. The reply message will automatically launch the mobile application requesting the user to input his/her account identification and PIN in order to access the message.

1.5.5 Protocol Sequence.

We consider the protocol sequence in two parts. In the first scenario the mobile application generates the message and sends it to the server. The second scenario

involves the security checks and message reception. The parts are elaborated in the following sections.

1.5.5.1 Secure Message Generation and Transmission.

Security information from the user is captured through the mobile application resident on the cellular phone. The information includes the account identification number, user PIN (personal identification number), sequence number or random salt number and one time pass word from the user. This information is used to generate the secure SMS message that is sent to the server.

In order to ensure message integrity on the receiving side message digest is used. The contents for the digest are as discussed in the preceding section 1.1 of message structure. To maintain message integrity of the message at least some of the content used in calculating its integrity needs to be encrypted. This is to ensure that on event of message interception an attacker cannot generate another digest. The integrity validation check will fail if the original message is altered.

Further more in order for the server to be able to identify the account holder's identity some identification details need not to be encrypted. The choice is dependent on the developer. Symmetric encryption algorithm is employed using one time pass word known to the user and server. The password is used to generate the key for encryption. On completion of the security processing of the contents the SMS message is sent to the server through the GSM network.

1.5.5.2 Secure SMS Message Reception and Decoding.

The server upon receiving the message through the GSM network decodes it according to the message structure described in section 1.5.1. The version bit pattern is checked and if found to be correct the message is considered suitable for the SMS secure protocol.

The server proceeds to read and check the account identification to find out if it exists in its data base. On event that the above checks are satisfactory the server retrieves the one time password from the data base. The password serves as a decryption key to decode the encrypted message.

When the decryption of the message is successfully accomplished the one time password is discarded and the server sequence counter incremented. The sever reads the secured contents necessary to calculate the message digest. The server uses the same algorithm used by the mobile application to calculate the digest. The two digests are thereafter compared for message integrity by the server. The server also retrieves the account holder PIN from its database and compares it to that on the message. The requested transaction is performed if all the above security checks are satisfactory.

1.6 Scope.

The research will mainly look at the security implications in terms of privacy and data protection from the perspective of cyber crime with possibility of suggesting and implementing a prototype MIDlet for delivery of SMS-banking services using cell phones in context of a developing country.

2. Problem Statement

In mobile banking data is electronically transmitted over wireless communication channels and the internet. These processes raise issues of how users are authenticated, how integrity of data is maintained and importantly the confidentiality of this data. Considering the low extent of development of ICT in developing countries when compared to the developed countries e-banking has not really been able to diffuse into society given the low rate of internet access [15]. However the advent of mobile telephony has seen the widespread adoption of cell phone usage this makes mobile banking in the developing countries a very attractive service for the banking industry for example in Uganda mobile cellular subscribers have increased from 3000 in 1996 to over 2.3 million in December 2006 [16].

2.1 Research questions

Main question

What are the security considerations and challenges for a secure SMS mobile banking service framework and how can the risks be managed?

Sub-questions:

1. What are the observed requirements, limitations and challengers of the current mobile banking applications in the context of the developing countries?
2. What are the current GSM security implementations?
3. What are the security concerns on the current mobile SMS protocol?
4. What security measures are currently deployed to offset these security shortfalls?
5. How can a secure SMS banking model be implemented?

3. Research Approach and Method

3.1 Objectives.

It is important that the research project be of high quality and be finished in time with a result of a thesis report detailing the problem and various methods used.

3.2 Method

The research will involve the study of necessary literature to answer questions 1 to 4 of the problem definition. The information is available in existing scientific journals. The following journals give significant amount of literature regarding this topic.

Communications of the ACM
Information system Frontiers
Mobile Networks and Applications
Computers and Security
Personal and Ubiquitous Computing
International Conference on Mobile Business - IEEE

There are book series available regarding the subject of mobile banking this include;
International Federation for information Processing (IFIP) series
Lecture Notes in Computer Science-Springer
E-Business management- Springer

The above literature resource will serve as an information base for this research. However other relevant information sources will be consulted as the research progresses taking into account that this area of research is still in its infant stage.

To answer questions 5 and 6 will involve analysis of the data obtained from answering questions 1-4 and banking industry in Uganda will be used as a case study in the context of developing countries.

3.3 Contact.

In order to enable an interactive working relation with the supervisor it's desirable to hold contact meeting on a bi-weekly basis or on event of specific questions. This will be fixed with collaboration with the supervisor. It is also proposed that to enable frequent contact to enhance work quality e-mail communication will be used whenever need arises.

4. Research Schedule

This plan is not rigid it may be adjusted as the research progresses.

Task	**Activity**	**Time period**	**Deliverable**
Project proposal preparation and plan	Establishing research problem, research questions, comprehensive work plan and study java	15/02/07- 15/04/07	Project proposal.
Work on Abstract	Writing Extended abstract.	15/04/07-20/04/07	Abstract

Literature review and searching of necessary information	Review literature on Mobile – banking, Study java programming and mobile information data programming using J2ME technology.	21/04/07-30/04/07	Introduction Chapter 1 and Thesis content layout.
Holiday for Supervisor		1/05/07-7/05/07	
Analysis and development of secure framework	Come up with effective solution in m-banking according to defined domain. Parallel task Thesis layout content development.	1/05/07-15/07/07	Prototype implementation. Thesis updated layout.
Report compilation	Develop comprehensive Thesis Report.	16/07/07-6/08/07	Draft Thesis Report.
Holiday for Supervisor		21/07/07-5/08/07	
Thesis presentation	Preparation of final thesis report and presentation.	6/08/07-24/08/07	Final Thesis Report & Presentation Date to be determined (20-24/08/07)

5. References

[1] http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

[2] Tommi Laukkanen (2005), Comparing Consumer Value Creation in Internet and Mobile Banking *Proceedings of the International Conference on Mobile Business* pg 655-658.

[3] William Stallings (2003), *Network Security Essentials*, Pearson Education, Inc. Upper Saddle river, New Jersey USA.

[4] Key Pousttchi and Martin Schurig (2004), Assessment of Today's Mobile Banking Applications from the View of Customer Requirements, *Proceedings of the 37th Hawaii International Conference on System Sciences*, pp 1-10.

[5] Niina Mallat, Matti Rossi, and Virpi Kristiina Tuunainen (2004), *Mobile Banking Services Communications of the ACM*, 47, 5 pp 42-46

[6] http://www.c-sam.com/

[7] GSM technical specification (1997), Digital cellular telecommunications system (Phase 2+); General description of a GSM Public Land Mobile Network (PLMN), http://www.etsi.org.

[8] John W. Muchow (2002), Core J2ME Technology & MIDP, The Sun Microsystems Press-Java Series, California USA.

[9] Clements.T. (2003). SMS–Short but Sweet. Sun Microsystems: http://developers.sun.com/techtopics/mobility/midp/articles/sms/

[10] Hulisani Ratshinanga, Johnny lo and Judith bishop (2004), A Security Mechanism for Secure SMS Communication, Proceedings of SAICSIT 1 – 6.

[11]Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone (2001), Handbook of Applied Cryptography, CRC press, USA.

[12] Lam, K.Y and Golmann, D. (1992), Freshness assurance of authentication protocols. Proceedings of the second European Symposium on Research in Computer Science, Toulouse, France, LNCS 648.

[13] Lam, K.Y, Cung, S., Gu, M., and Sun, J. (2003). Lightweight Security for Mobile Commerce Transactions. *Computer Communications* 26, 2052 -2060.

[14]Jonathan Knudsen (2002), MIDP Application Security : design Concerns and Cryptography, Sun Developer network ; http://developers.sun.com/techtopics

[15] Banji Oyelaran-Oyeyinka and Catherine Nyaki Adeya (2004),Internet Access in Africa: Empirical Evidence from Kenya and Nigeria *Telematics and Informatics*, 21, 1 , pp 67-81

[16] http://www.ucc.co.ug/marketInfo/marketstatistics.php