SMS BASED M-COMMERCE: MEETING APPLICATION AND SECURITY REQUIREMENTS

Anurana Saluja
CISSP, CISM, ISSMP, ISO 27001 Auditor
Head Operations,
NSS MSC Sdn Bhd
E-21-7, Plaza Mont Kiara
Kuala Lumpur
anurana.saluja@mynetsec.com

ABSTRACT

This paper outlines the potential of SMS Based financial information and transaction services which can help users in account access, payments and in making time and location independent transactions.

So far, existing m-commerce initiatives have focused on GPRS or SIM based approaches which have their specific limitations. After highlighting comparative strengths of SMS based m-commerce solutions vis a vis GPRS and SIM Based solutions the vulnerabilities of SMS technology are brought out in detail.

Having outlined the security and application requirements for an m-commerce solution this paper details how Secure SMS based notification and transaction system meets these requirements.

KEYWORDS

m-commerce, mobile payments, SMS, GPRS, m-banking, payment systems

1. INTRODUCTION

Financial services were expected as one of the key commercial drivers for the mobile commerce market (Durlacher Research 1999, Roland Berger 2000, Frost & Sullivan 2002). As we know today, the market development of mobile financial services including mobile banking and m-commerce has not lived up to these expectations. Financial institutions should base any decision to implement m-banking products and m-Commerce services on a thorough analysis of the costs and benefits associated with such action.

Some of the reasons institutions offer m-Commerce include –

- Lower operating costs,
- Greater geographic diversification,
- Improved or sustained competitive position,
- Increased customer demand for services, and
- New revenue opportunities.

Mobile (wireless) commerce would be enabled when the customer is able to access the financial institution's networks through a cellular phone or personal digital assistant (or similar device) via wireless networks provided by telecommunications companies. Wireless services can extend the reach and enhance the convenience of an institution's banking products and services, provided the risks associated with the delivery channel can be managed/mitigated.

In this paper we focus on how application and security requirements can be met for m-Commerce. Therefore, we analyze a promising application domain (SMS based Mobile Commerce) which can provide added value for customers and address the shortcomings of currently used security mechanisms. While

most efforts till date on mobile banking and commerce have chosen to create a web counterpart on the mobile phones, our proposed application domain is not based on or a counterpart of traditional online services. This domain focuses on a SMS based application scenario which provides some key value adds to the users as well as financial institutions.

Unlike Mobile Commerce initiatives using GPRS, the potential resulting from an integration of mobile notification and transaction services make SMS based m-commerce more interactive and thus more likely to succeed. However SMS has traditionally not been considered as a robust and secure enough technology for use for business or financial purposes. This paper looks at the SMS security and performance vulnerabilities. In doing so we derive the security and application requirements for mobile commerce applications. Finally a SMS based secure architecture for Mobile Commerce Applications which meets thee security and application requirements defined in earlier sections is proposed.

2. M-COMMERCE

Using mobile commerce services enables users to be informed instantly about relevant financial information without having to access other media like online services, news papers, manuals or visiting a branch. Solely increasing the level of information by mobile notification services will not lead to widespread adoption of mobile commerce. Furthermore, users must be empowered to perform necessary transactions in time or they will not be able to take advantage of the better information situation. Consequently, a stringent service integration of mobile notification and transaction services is required which can not be fulfilled by existing concepts using GPRS and or other means. This paper analyzes general security and application requirements for the proposed notification and transaction services to be able to derive an alternative approach in order to bring these security requirements in line with the application requirements (stringent integration of notification and transaction services).

In order to evaluate the requirements and feature sets for m-Commerce the mobile banking model is considered as an example for this paper. The following type of services could be made available through Mobile banking based on secure SMS notifications and transactions –

Push – This is a purely one-way interaction and helps the bank to inform customers about various transactions related to his /her account. The alerts that can be sent include but are not limited to Credit/Debit information, Salary credit information, Bounced cheque alert, Balance below alert etc.

Push-pull – This requires two-way interaction. Bank-customers, usually from the retail segment, can send requests for the services listed in succeeding paragraphs. This is based on a pre-decided menu and they would receive information on queries like Balance enquiry, Last three transactions, Cheque status enquiry etc.

List of the possible services could include but not be limited to -

Inquiries

Balance Inquiries:

- Daily Balance
- All Debit Balances
- Debit Balance Over <X> Amount
- Debit Balance Below <X> Amount
- Credit Balance Only
- Credit Balance Over <X> Amount
- Credit Balance Below <X> Amount

Transaction Inquiries:

- All Transactions
- All Debit Transactions
- Debit Transactions Over <X> Amount

- Debit Transactions Below <X> Amount
- All Credit Transactions
- Credit Transactions Over <X> Amount
- Credit Transactions Below <X> Amount

Other Inquiries:
- Inward Remittances
- Salary Credit
- Other Bank's Cheque Cleared
- Other Bank's Cheque Returned
- Your Cheque Cleared
- Your Cheque Returned

Where <x> Amount refers to any amount specified by the account owner.

Transactions

Funds Transfer
- Between own accounts
- From own account to third party account (intra bank)
- From own account to third party account (inter bank)
- From / To Credit Card

Payments
- Utility Bills
- Loan Repayment
- Insurance Premiums

Payment Options
- Pay through credit card
- Pay through debit card
- Wire from account

Purchase
- In house products & services
- Third party products & services

3. COMPARISON BETWEEN GPRS AND SMS BASED M-COMMERCE

Wireless encryption that occurs as part of the data transmission process is based upon the device's operating system. A key risk-management control point in wireless banking occurs at the wireless gateway-server where a transaction is converted from a wireless standard to a secure socket layer (SSL) encryption standard and vice versa. Wireless network security reviews should focus on how institutions establish, maintain, and test the security of systems throughout the transmission process, from the wireless device to the institutions' systems and back again. For example, a known wireless security vulnerability exists when the Wireless Application Protocol (WAP) transmission encryption process is used. WAP transmissions deliver content to the wireless gateway server where the data is decrypted from WAP encryption and re-encrypted for Internet delivery. This is often called the **"gap-in-WAP"** (e.g., wireless transport layer security (TLS) to Internet-based TLS). This brief instant of decryption increases risk and becomes an important control point, as the transaction may be viewable in plain text (unless encryption also occurred in the application layer). The WAP Forum, a group that oversees WAP protocols and standards, is discussing ways to reduce or eliminate the gaping - WAP security risk.

Security Issues

	WAP/GPRS	**SMS BASED** Technology
Phishing	Vulnerable	Not applicable. Digitally Signed and Encrypted Message Delivery
Identity Theft	Vulnerable	Not applicable. Digitally Signed and Encrypted Message Delivery
Gap in WAP	Applicable	End to end security
Browser Vulnerabilities	Vulnerable	Sandboxed Application
Mutual Authentication	Not available	Two way security implementation. Server and sender are both verified to each other

Table 1: Comparison between GPRS and SMS Based m-Commerce: Security Issues

Comparison - Technology Maturity

	WAP/GPRS	**SMS BASED** Technology
Subscription	Need to subscribe	Default capability
Penetration	Operator and Phone Dependent. Friendly only to PDA and Blackberry users.	High application and service penetration. J2Me based application. Supports over 200 phone models
High Reliability	Connection Quality Varies	Highly reliable. Close to 100% reliability in domestic networks
Cost Effective		Cheap to use
World Wide Availability	Not introduced in certain regions	Provided by all telecom providers worldwide
Roaming	May become unusable while roaming	Default roaming capability

Table 2: Comparison between GPRS and SMS Based m-Commerce: Technology Maturity

Comparison - Technology Capability

	WAP/GPRS	**SMS BASED** Technology
Push/Pull Architecture	Pull Only	Push/Pull Capability
Audio Visual Information	Supported	Text Based Information Only

Table 3: Comparison between GPRS and SMS Based m-Commerce: Technology Capability

*Pull only implies that the connection always has to be initiated by the user. There is no mechanism in WAP/GPRS based applications to push data to the user's handsets. However SMS-SMS BASED , ***allows organizations providing critical information to send the data directly to their subscribers****, without the need for an explicit request.*

Comparison – Convenience

	WAP/GPRS	**SMS BASED** Technology
User Interface	High latency for information intensive pages.	Intuitive UI. Instant loading of predefined application menus
Encoding Schemes	Superfluous for text-only information.	Efficient solution for secure text based information transfer

Table 4: Comparison between GPRS and SMS Based m-Commerce: User Convenience

Automation/Payment Mechanism

	WAP/GPRS	**SMS BASED** Technology
Integration	Redesign of all web pages for mobile screens	SMS BASED Enterprise Plus, integrates easily with existing backend via standard protocols like HTTPS, SMTP; will need integration work /APIs to connect to bank's online workflows

Table 5: Comparison between GPRS and SMS Based m-Commerce: Payment Mechanism

4. COMPARISON BETWEEN SIM CARD BASED AND SMS BASED M-COMMERCE

Memory capacities for conventional SIM cards range from 8k (now obsolete) to 256k (just released). Most of the SIM cards in the market today are either 32k or 64k capacity cards. Given the memory limitations of these devices, it is not possible to host a security application in totality on a SIM card. A typical cryptographic application with a user interface would easily take up as much as a 100kb on the host device, making deployment on a SIM card impossible. In addition, there is little processing ability on a smart card for tedious cryptographic operations. Therefore, the likely approach of integrating security onto a SIM card would involve just copying of the cryptographic keys onto the card.

This approach has various limitations from a deployment, maintenance, and security perspective. In order, for the telecom company to implant cryptographic keys on the SIM a new workflow would need to be implemented for their SIM card generation process. In addition, a recall exercise would have to be initiated in order to provide existing customers the benefits of this new SIM card.

Since it is not possible for a full fledged security application to be loaded onto a SIM (due to memory and processor limitations), it would be necessary to provide the user with an application that allows him to use these cryptographic keys. This application would have to be stored on the phone and would access the SIM for the cryptographic keys. Therefore, in essence, all the SIM provides the user with is a location to store cryptographic keys and is thus not a complete security solution.

Storage of the keys on the SIM is also a serious security flaw. This is because, if the cryptographic keys are being accessed by an application loaded onto the phone, then the entire security of the solution is subverted, as a third party application is able to extract secure data. In addition, key generation and induction at a third party site (telecom) may violate the trust of the end user"

Compared directly against Secure SMS based banking application, a SIM card based solution is likely to lose out on – User experience, Security, Ease of implementation by the telecoms, Features, and Efficiency. The USP of such a solution would just be easy migration, when a user switches phones. However, even then all the user would have would be the keys and would still need to reinstall all the applications that utilize these keys.

Also a solution that only works with SIM-cards have not entered the market yet. Consequently one could argue that mobile operators will not have any interest in providing more expensive SIM-cards equipped with a cryptographic coprocessor.

5. STUDY OF SMS: POTENTIAL AND ARCHITECTURE

This section offers a detailed description of the underlying wireless, SMS specifications and the innate and potential security and vulnerability. It describes in brief SMS Based Mobile technology and its specifications. SMS Based Mobile technology is based on mobile applications using cryptography technology. SMS BASED Technology helps make SMS messages trustable.

SMS Usage - The mobile phone is already an integral part of the lives of more than 1.8 billion people worldwide. Mobile usage is increasing in volume as well as diversity. More than 80 % of mobile users do not leave home without their phones. Businesses are increasingly turning to the mobile phone to "get the message across" to employees anywhere anytime. The desire to communicate more easily and have timely access to information is universal. The mobile phone is today being adopted and adapted in innovative ways to enhance business productivity. The Short Message Service (SMS) facility plays a leading role in this adoption.

Ubiquity - SMS enjoys enormous popularity as an economical and convenient mode of exchanging information. It not only saves time and cost but in many situations is also found to be more convenient than making a phone call. SMS has changed our working habits and social lives in many ways. SMS has simplified exchange of important short messages and also led to creation of services that are fun to use. People can easily share a private moment with their friends, family and work in other geographical locations in a cost effective and instant manner. SMS is further being used in business: for instance simplifying grocery shopping, providing alerts for best buys, bank alerts or such monitored events. Besides that it is being used these days in getting daily news, stock-market information, sports scores, quotes, travel and weather news. Many value added services (VAS) such as contest voting, songs request, ring-tone or service initiation are also being done using SMS. The list of services being facilitated through SMS is growing every day.

SMS Security Loopholes Preclude Business Transactions - It is known today that SMS travels as plain text and privacy of the contents of SMS cannot be guaranteed, not only over the air, but also when such messages are stored on the handset. Informed individuals have grown more and more skeptical of using SMS for sensitive and personal message exchanges. With growing awareness of such security loopholes in SMS, many value-adding business services are not being rolled out or are being deferred for end-users until appropriate security assurance is available.

SMS services currently provided by vendors, banks or other business houses are mostly passive in nature. The SMS, with its underlying gaps in security and vulnerabilities, is not accepted for active business transactions. The demand for active SMS based services can only be satisfied when a solution that addresses end-to-end security issues of SMS technology is available, where primary security parameters of authentication, confidentiality and non-repudiation are satisfied.

A number of active SMS services can be brought to users at a personal level and to government and corporate users at a business level:

- Banking: Check balances, transfer funds between accounts, pay bills using credit cards. VAS are valuable not only for the subscriber but also for financial institutions offering this service.
- Customer service: charge a customer's credit card right at the table, at any time, instead of going to a fixed POS terminal located by the register.
- Track the location of a moving asset. Interchange small amounts of information in an inexpensive manner, such as the longitude and latitude, current time, and perhaps parameters like temperature or humidity.

- Home security, vehicle security – Alerts and notifications.

SMS Architecture - Short messages are delivered in GSM signaling channels between the MS* and the BSS. The messages flow as normal calls, but they are routed from the MSC to a short message service center (SMSC). The SMSC stores the message until it can be delivered to the recipient(s) or until the message's validity time has elapsed. The recipient can be a normal MS user or a SMS gateway. The gateways are servers that are connected to one or more SMSCs to provide SMS applications for the MS users. These applications include ring tone and icon delivery, entertainment, bank services, and many other beneficial services.

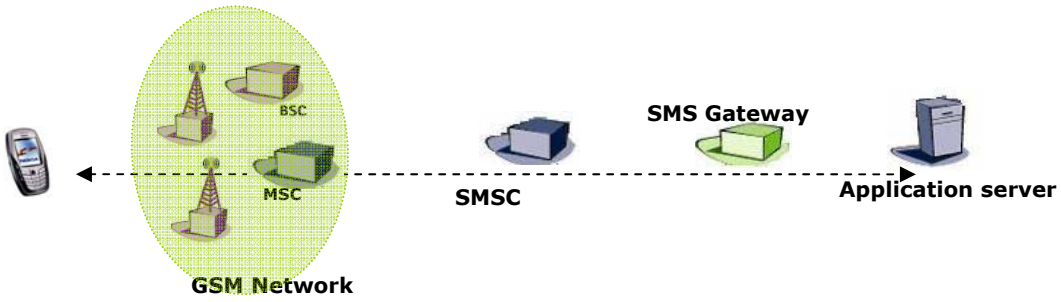

Figure 1: A diagrammatic representation of the SMS Network components

6. SMS: SECURITY ISSUES AND VULNERAILITIES

Two important aspects for any entity using consumer technologies such as SMS for business purposes:

- SMS is not a secure environment.
- Security breaches often occur more easily by concentrating on people rather than technology.

The contents of SMS messages are visible to the network operator's systems and personnel. Therefore, SMS is not an appropriate technology for secure communications. Most users do not realize how easy it is to intercept messages. It would likely be a relatively complex to hack into a telecom provider's systems to obtain the content of SMS messages, but finding staff privileged to look at SMS messages and persuading them to reveal the contents is much easier. Gartner Research has already expressed reservations about security in U.K. trials of SMS voting in local elections held in May 2002. Enterprises, including governments, can not use SMS in its present state for any confidential communication. Enterprises seeking secure communication channels to mobile employees should consider encrypted end-to-end solutions on devices having additional security features.

The underlying specifications and technology for SMS transmission leave many security gaps. These gaps make SMS vulnerable to –

Snooping - On device, at the store and forward network elements

SMS Interception - Over the air, in wired network

Spoofing - Using commercial tools, own SMS gateway

Modification - Using conventional hacking techniques

Attacks on GSM, the SMS Carrier Technology -
Often the weakest link in security is the mobile phone itself. Even leaving the mobile phone unattended inadvertently could expose your private and confidential messages to snooping. For instance, a sneak

preview of the messages and contacts on a colleague's handset left on desk during a coffee break! A stolen SIM not protected by a security PIN code may reveal all messages and contacts that were stored in the SIM memory.

Attacks on the A5 Algorithm -
There are several ways to eavesdrop on a call, although it is not so easy to eavesdrop on real time calls. There are different attacks against the A5/1 algorithm, which is the algorithm used to cryptographically protect voice, data (SMS) and signaling. A5/2 also exists, and it is even weaker than A5/1. The attacks include a brute force attack, which is quite time consuming and thus cannot be used in real time. Another attack is called divide and conquer. Although more efficient, this attack is also not fast enough to be implemented in real time. A third attack is called biased birthday attack, which can be implemented in seconds with a PC, although 2 or more minutes of GSM voice/data (SMS) stream must be recorded first. A random sub graph attack can be done in 4 minutes with a PC, and it only needs about 2 seconds of GSM voice stream recorded. The A5/1 algorithm can even be reversed and a secret session key can be recovered. All the previously described attacks compromise the actual A5/1 algorithm.

Limitations in GSM Security -
There are other ways of eavesdropping on GSM calls. The calls are only encrypted and decrypted between the BTS and the MS, leaving the rest of the network quite unprotected. If an intruder obtains access to the SS7 network, which is used in the GSM operator's network, all the call and signaling traffic is completely unprotected. An attacker might also get access to the HLR, which is normally better protected, but is an attractive target for an intruder, since it contains all the subscriber information. Another possibility of eavesdropping GSM calls is to find out the secret key of a subscriber, on which the whole GSM security system is based. This key can be recovered many ways. One can use a SIM card reader and a PC to send a huge amount of challenges to the SIM card of the victim. The SIM card generates responses to all of the challenges. When enough challenges are received, the key can be deduced, and the whole subscriber account is compromised. The same attack may be possible even over the air. A third possibility would be to make requests to the AC and constructing the key from the responses of the AC. The above limitations of GSM security could lead to of compromise of the carrier technology thereby also leaving SMS vulnerable to snooping and interception.

Theft of Mobile Phones-
One problem characteristic of mobile networks is that mobile devices are easy to steal. Mobile phones are commonly stolen and sold to third parties or used until the customer account is switched off by the operator. The current approach to prevent stealing GSM phones is the use of EIR, the equipment identity register. When a mobile phone registers itself to a GSM network, it sends a special identity number of the phone device, International Mobile Equipment Identifier (IMEI), to the GSM network. This identity number is then checked against the EIR, which is a database including black, grey and white lists. Black lists include identity numbers of stolen or faulty equipment. If the identity number is on the black list, the device is not provided access to the GSM network. Grey lists include identity numbers of devices that must be tracked. White lists include ranges of identity numbers, which are granted access to the network, and they are not suspected of anything. As mentioned earlier, EIR is an optional part of the GSM standard. While it would be a powerful method to make stealing less useful, it is not used by many operators, since it is optional. In addition to stealing mobile phones for unauthorized calls, modern mobile devices may attract thieves for snooping confidential content. Since some of the devices are more than just phones today, the phone owners may store important or sensitive information into their mobile devices' memories. Also, a mobile device may be used as a means of payment. These extra threats showcase the urgent need for protection against theft.

Attacks on SMS -
The connection between the SMSC and the SMS gateway is not part of the GSM standard. There are many different protocols available for use between the SMSC and the gateway. These protocols are built on familiar protocols, such as TCP/IP and X.25. Also, the connections are not part of the GSM network, but part of the operator's or content provider's network or, even worse, the Internet. The connections are very loosely protected. It should be obvious that the connection is an easy target for a cracker, since the content is delivered in plain text and binary fields. Although the gateways are authenticated, in many protocols this

is done using plain text header fields containing a login name and password. Using the originator IP address is not really a superior way of authenticating, since it is very simple to do a man-in-the-middle attack against TCP/IP and intercept the communication.

Naturally one can spoof short messages as well as traditional calls exploiting the same GSM vulnerabilities described above but there is an easier way of spoofing short messages: It is a straight consequence of the weak protection of SMSC-gateway connections. Using a normal network listener one can record the login and password fields of a message passed from a SMS gateway to a SMSC. This seems very simple but isn't actually the case, since operators normally run both the gateway and the SMSC behind a firewall. But this is not a rule and not the case every time either. This way an intruder can set up his own fake gateway that pretends to be the real gateway. This fake gateway can then send all kinds of malicious short messages to the MS users through the SMSC. Also, in many SMSC protocols the original sender of the message is identified in a specific field of the short message. Using the spoofing technique described above and giving a false MSISDN in that field may cause the message to appear as one coming from another mobile phone. That depends on the SMSC implementation, because the SMSC may be smart enough to check the sender field and ban the message, since it comes from a gateway, not from a mobile phone. One possibility is to spoof the other way around, since the SMSC is not authenticated. This client authentication provides an attacker a chance to make a SMSC simulator pretend to be the real SMSC. This way the gateway can be fooled and, for instance, a bank application using the gateway could easily be made to send account information to outsiders. It could even be used to make unauthorized bank transactions.

Eavesdropping and Modifying can be implemented just as in the case of normal GSM phone calls. The SS7 network and the A5 algorithms are vulnerable, as was mentioned earlier. It may be easier to eavesdrop on messages passing to and from the SMS gateway, if the connection between the SMS gateway and the SMSC is not protected. A normal network listener is enough to gain access to information. At this point it is also possible to alter the message content; if possible checksums and field lengths are taken into account. Another part of the SMS application that is not always protected is the connection between the SMS gateway and the application server. It is easy to eavesdrop this connection also. It is thus possible to change sums or account numbers in a bank transaction and alter stock information broadcasted to stock service subscribers etc.

Example: SMS Spoofing in a Cellular provider's Infrastructure

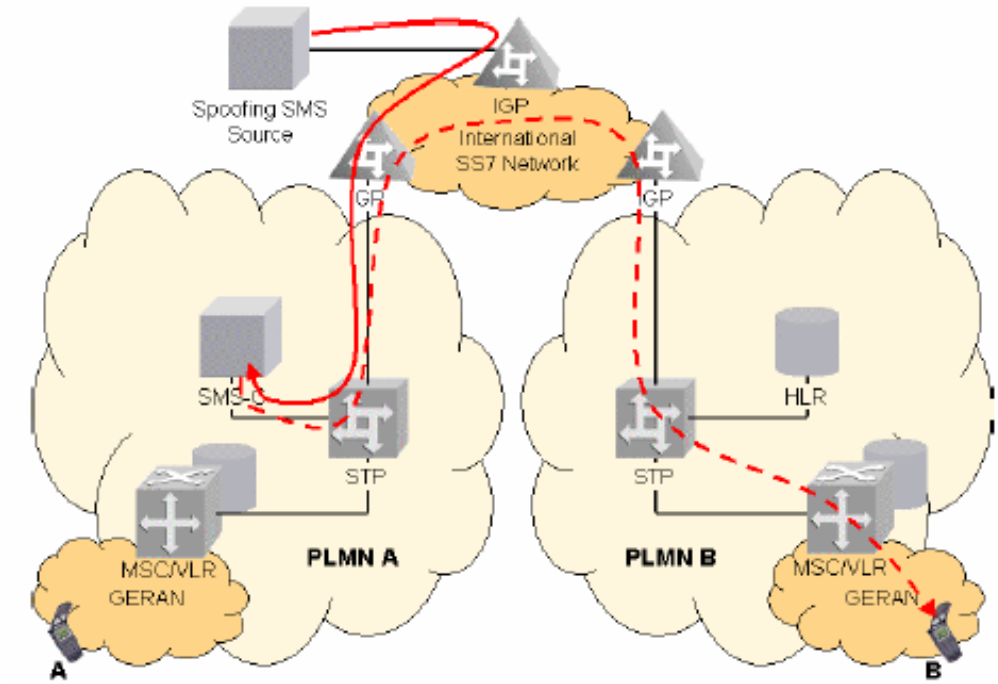

Figure 2. SMS Architecture depicting spoofing in a Cellular provider's Infrastructure

- The SMS sent to the SMS-C has a manipulated originating MSISDN A number.
- One example is shown in the figure, where the "SMS Spoofing Source" simulates a roaming end-user from PLMN A, sending an SMS to a foreign end-user in PLMN B.
- The "Spoofing SMS Source" is a specific system with an SS7 application. It uses real or false MSISDN A numbers, originating VLR and / or SCCP addresses.

Example: SMS Spam in a Cellular provider's Infrastructure

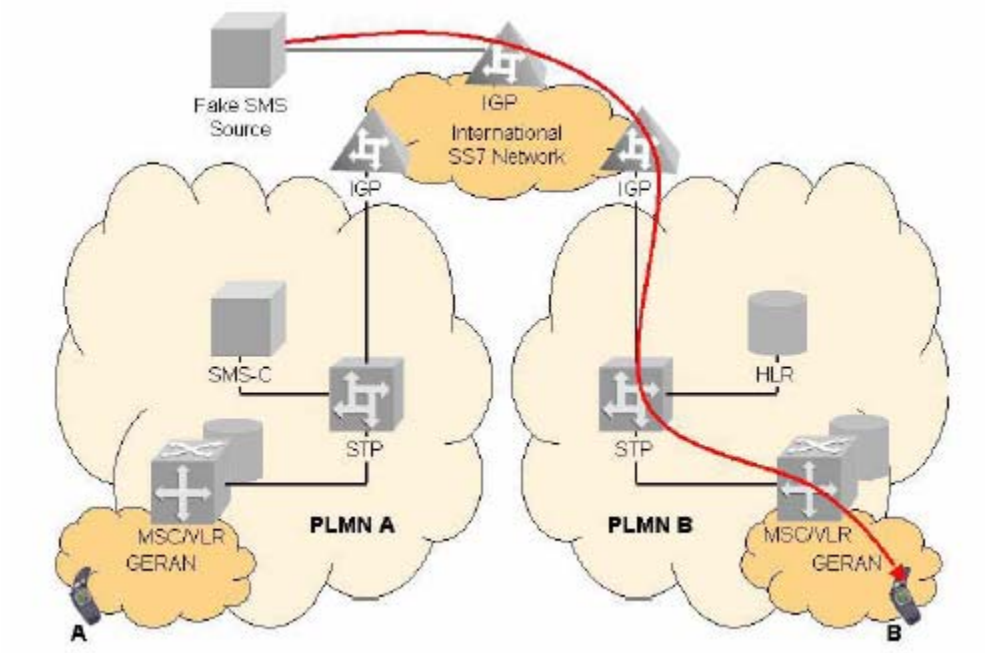

Figure 3. SMS Spam in a Cellular provider's Infrastructure

- The Faked SMSes have manipulated MAP addresses. The source address of the SMS pretends that these are sent from another network (in Figure, from PLMN A).
- To do so, it has to know the end-users' IMSI, otherwise an HLR interaction has to take place. In this case the Fake SMS Source has to use his own real SCCP and MAP SMS-C address.
- If the VLR is unknown, the source has to send the SMS to every VLR in the network, which together with the false IMSI addresses can generate a heavy load in the network equal to SMS Flooding.

7. M-COMMERCE: SECURITY AND APPLICATION REQUIREMENTS

It is essential for the users that the whole process, starting with the notification and leading to a possible transaction, is as little time consuming and as much convenient as possible. This would enable the user to spend most of the available time for the decision making. Therefore, another application requirement would be.

Requirement I: The complete process of notification and transaction services has to be as little time consuming and as much convenient as possible.

Since investors use a great variety of different mobile devices the service provider should have an interest to design the service as compatible as possible to most devices. Therefore, another application requirement would be.

Requirement II: The notification and transaction services should be useable with (almost) any mobile phone on the market.

Because of the short time span in which the user has to react to the information available / notification it is not possible to cross check the received information. Therefore, the notification service has to provide a way to ensure the integrity and authenticity of the notifications. Otherwise, a potential attacker could alter notification messages or create false notification messages that could lead to false decisions by the user. It is also important that the notification does not get lost or delayed (availability is the corresponding property). Obviously, the notification service on its own cannot guarantee fulfillment of any of these requirements (e.g. when communications are interrupted or tampered within parts of the network outside of its control), but it is important that the user knows about the state of the message he gets.

Requirement III: The notification service has to provide means to ensure that violations of the integrity or authenticity of the notification message can be detected by the receiver and to ensure that the message reaches the user in time.

The linked transaction services should also provide integrity and accountability of the process. In addition, the communication between the user and the financial institution should be confidential.
Consequently, another security requirement for the transaction service would be.

Requirement IV: The transaction service should provide availability, integrity, accountability and confidentiality.

8. SMS BASED M-COMMERCE: MEETING SECURITY & APPLICATION REQUIREMENTS

The infrastructure proposed is based on the assumption that the user is using a smart phone equipped with an application that is capable of encrypting the data, using a hashing algorithm and creating digital signatures. The technology for doing all these exists but has largely been using SIM cards focused on channels other than SMS and has not gained much market penetration so far. NSS Research & Development Labs has developed such an application that is capable of creating digital signatures (DSA) on SMS, SHA-1 hashing algorithm for integrity and also provides AES encryption. Using such an application the user can register his public key at the Financial Institution's server and can obtain a copy of the public key of the notification / transaction service provider.

Our goal is to achieve as many of the application and security requirements defined in section 5 as possible. Therefore, we propose an implementation using a J2ME based software application which also ensures compatibility to almost all mobile phones.

The Bank's notification server creates a notification SMS (encrypted SMS) and sends it to the Encrypted SMS application running on the mobile device of the user. The SMS is electronically signed with the private key of the Bank. After receiving the signed push notification the application can check the integrity and authenticity of the notification by verifying the signature. If the signature is valid the user can read the message. At the other end, the user may initiate a pull request or a transaction from his / her mobile. The user initiates a transaction through a menu driven interface which collects information, packs it into an SMS, encrypts it and is electronically signed by the application using the digital signature functionality of the application. The transaction server verifies the signature and completes the transaction if the signature is valid. In order to open the application and use this for any kind of action the user has to enter a user defined PIN. In addition the financial institution may add their own m-PIN to the work flow thus adding another layer of security.

As the used SMS service does not provide acknowledgements for delivered messages, availability can not be guaranteed. Therefore, additional steps are necessary to make sure the user receives the needed information in time. If the user does not react at all to an incoming notification (for which it is necessary for the user to react), the notification service can be configured to resend the SMS 2 times after 10 and 20 minutes. Notifying 3 times provides a balance between availability and convenience. Another option is to let the investor configure the number and frequency of notification retransmissions.

9. CONCLUSION

This solution seems to be pretty convenient and very time efficient. Having installed an application and registered it with the financial institution, the user has access to the transaction services after entering the authorization PIN. The transaction process is completed when the transaction is confirmed with a digitally signed message. Therefore, we can state that Requirement I (*as little time consuming and as much convenient as possible)* has been met. Since most current mobile phones support J2ME we can also conclude that Requirement II (*should be useable with (almost) any mobile phone on the market)* has been fulfilled. By checking the validity of the electronically signed notification message the Secure SMS application is able to check the authenticity (only the service provider can make a valid signature) and the integrity of the notification message automatically. Moreover, notifications are resent if the user shows no reaction to critical messages. So it can be concludes that Requirement III (violations of the integrity or authenticity of the notification message can be detected by the receiver and to ensure that the message reaches the user in time) has almost been fulfilled, as delivery can not be guaranteed.

By signing the transaction request the user ensures the integrity of this request. It also guarantees that only the user could have requested this transaction enabling accountability. Confidentiality can be provided by ciphering the data transfer between the user application and the transaction server using AES. So we can state that Requirement IV (*provide availability, integrity, accountability and confidentiality)* has been met.

SMS Based M-Commerce Security Bullets

The proposed SMS based Mobile banking solution employs application level encryption undertaken at the device (point of sale / transaction) thus eliminating the need for protocol driven decryption and encryption (wireless transport layer security (TLS) to Internet-based TLS) steps.

SMS Based Mobile uses strong authentication mechanisms using the time tested public – private key technology and digital signatures.

A “key based” approach to authentication eliminates the need for the bank to issue and send PINs or passwords. It also eliminates the requirement on part of the user to remember bank issued PINs or passwords.

Very strong encryption (256 bit key length) works to provide an appropriate safeguard to meet stringent customer information confidentiality requirements.

Processing the message through an industry standard hashing algorithm provides the message integrity essential for all financial transactions.

Every time the user needs to use the application or any of its features he/ she has to enter the unique password (known only to him / her – not even the bank). This prevents misuse of the application or the handset/PDA.

The SMS based Java application is passed through a series of obfuscating operations using state of the art obfuscation engines. This ensures that the compiled midlet is highly resistant to reverse engineering. In addition, the sandbox architecture of Java ensures that once installed it is not possible to tamper or extract

the midlet from the mobile device. Combined with advanced password implementation techniques and the requirement (optional) for mPIN for mobile financial transactions, the customer can rest assured that the highest levels of security are being used to safeguard and transmit his information; and it is not possible for a malicious entity to subvert the security of the solution.

Strong Activation mechanism - Even though the provisioning mechanism for SMS based Mobile provides great flexibility and convenience for the customer while downloading the application, the activation mechanism that has been implemented ensures that only the original registered telephone number is able to actually use the application. Every SMS BASED mobile generated by SMS BASED Enterprise is bound to a mobile number. This unique provisioning and activation procedure ensures that the application cannot be used by any one other than the intended recipient.

ACKNOWLEDGEMENT

The author would like to thank his company NSS MSC Sdn Bhd for access to technical details about their Secure SMS Based product “XMS Mobile Banking”.

REFERENCES

Muntermann, Jan; Rossnagel, Heiko; Rannenberg, Kai, 2005, *Mobile Brokerage Infrastructures – Capabilities And Security Requirements*

Proprietary Documents from NSS MSC Sdn Bhd – the developers of XMS Mobile Banking Solution