STK IMPLEMENTATION IN SMS BANKING IN M-PESA -KENYA, EXPLOITS AND FEASIBLE SOLUTIONS

Doreen Nyaketcho, Dale Lindskog, Ron Ruhl
Information Systems Security, Concordia University College of Alberta, Edmonton, Canada
dnyaketc@student.concordia.ab.ca, {dale.lindskog, ron.ruhl}@concordia.ab.ca

***Abstract* – STK is used in Kenya to facilitate SMS Banking using primarily GSM phones for transmission of the SMS messages. While providing a valuable banking solution it is not without security risk, some of which has been exploited. This paper will describe the underlying architecture of Kenyan STK based M-Pesa banking, various vulnerabilities will be discussed and methods suggested to overcome them.**

Keywords: STK, SIM Tool Kit, M-Pesa, SMS Banking, GSM.

I. INTRODUCTION

Mobile Banking, also known as m-banking or SMS banking, is a term used to refer to various banking related tasks performed via mobile devices, such as balance checks, account transactions, or payments. Mobile banking today is most often performed via Short Message Service (SMS), a communication medium that enables transfer of data over a network in a 160 character text format. The simplicity of SMS messages means they can be used in all regions of the world and in most mobile phones, including non-smartphones.

Sim Toolkit, also referred to as Sim Application Toolkit (STK/ SAT), is part of the GSM standard that enables the Subscriber Identity Module (SIM) to initiate actions to further exploit SMS by providing value-added services such as mobile banking. SIM Toolkit comprises a set of commands programmed into a SIM that are used to define how the SIM interacts directly and initiates commands independently of the handset and the network.

Global System for Mobile Communications (GSM) is a standard developed by the European Telecommunications Standards Institute (ETSI) to describe protocols for second generation (2G) digital cellular networks used by mobile phones. It is used an open, digital cellular technology used for transmitting mobile voice and data services.

M-Pesa is a mobile banking service developed to allow Kenyans to transfer money via SMS using the Subscriber Identity Module (SIM) card in their cell phone. It does not require users to have a bank account, it provides easy and convenient banking services, and M-Pesa is used by over 50% of Kenya`s adult population, including those without bank accounts [1]. It functions as an electronic wallet that holds up to a maximum of 100,000 Kenyan shillings (approximately $1,200 USD), from which users can buy digital funds from an M-Pesa agent and transfer the funds via SMS to other mobile phone users, who in turn redeem it for conventional cash from any agent [2].

This paper reviews possible exploits to the system and explores mitigation strategies to minimize the implications of those exploits, so as to improve this GSM SMS banking system. This paper also explains how SIM Tool Kit (STK) technology facilitates SMS banking, and suggests ways to better implement supporting technologies like GSM, STK and SMS, so as to improve M-PESA SMS banking security. Feasible solutions to the security vulnerabilities in a GSM and STK reliant M-Pesa SMS banking system are suggested, taking into consideration the current technology and phones used, and the infrastructure in Kenya. Although focused on Kenya, these suggestions will be applicable to other third world countries using similar banking systems and having a similar infrastructure.

II. M-Pesa

SMS banking in Kenya is implemented by Safaricom, a provider of about 80% of cell phones in use in the country. M-Pesa relies on sending SMS store-and-forward messages to parties of a transaction, using GSM as the transmission medium. Commands and functionality for this are provided by a custom STK application placed onto the phone by the service provider, Safaricom.

To enable M-Pesa, a customer must obtain GSM cell service from Safaricom. During the activation of the cell phone SIM card, Safaricom places a permanent secret key (Ki) on the SIM card (a standard process for all providers of GSM SIM cards). This is used to encrypt the communication from the Mobile Station (MS) cell phone to the provider. Safaricom also uses STK to place a custom Safaricom software application on the phone, which can be used to carry out M-Pesa transactions, and is secured by a four digit PIN. After activation the subscriber can use any web banking application to transfer money to Safaricom, and use the resultant e-money to pay for goods and services from merchants accepting M-Pesa. For those without a bank account, cash can be given to Safaricom at an agent at point of sale, and this can similarly be added as e-money to the customer account with Safaricom.

M-Pesa relies on the security of GSM to encrypt SMS messages. After a GSM phone is turned on, it authenticates to the network and a key for encryption (Kc) is initialized, using the Ki secret (known to both the MS and the provider) and a random value chosen by the provider. This Kc and the GSM frame number provides a key stream to encrypt the GSM frames which carry the digital GSM SMS messages. To create the key stream, the Kc and GSM frame are put through a one way function to create the key stream required for each sequential GSM frame. Calculations for the Kc and calculation of an authentication response are completed by the algorithms A3 and A8 and the encryption of frames with the key stream is completed by the A5 algorithm, which has several levels of encryption (all variations of Comp128) [20].

Since M-Pesa SMS banking in Kenya relies heavily on GSM encryption, weaknesses here affect the entire M-Pesa system. Implementing weak encryption with Comp128 V1 leaves the encryption channel open to compromise and can even leave the GSM phone itself open to cloning, as stated by several authors [e.g. 20,25]. In any case, since the first step in cloning is to retrieve the Ki, this means that the underlying encryption is open to compromise whenever Comp128 V1 is used. In retrieving the Ki an attacker is able to use a false base station attack because in the default GSM configuration the network is not authenticated as it is, for example, with Extensible Authentication Protocol – SIM (EAP-SIM).

By default, SMS messages are sent in the clear as they leave the application and then encrypted from the MS to Safaricom by GSM using the key stream described above. They are then decrypted and stored (as plaintext) until they can be delivered to the default target. When delivered, the SMS message is encrypted and sent to the target MS using the target MS's encryption key. Once received the target MS or agent acts on the SMS message [7].

M-Pesa SMS banking has utilized an STK application to extend SIM functionality to support additional services on the existing infrastructure [5]. Delivery of mobile banking services has employed a number of additional enabling technologies, such as Interactive Voice Response (IVR), standalone Mobile Application Clients (MAC) and Short Messaging Service (SMS) as bearer mediums applicable to the Kenyan banking system. Below each of these technologies are introduced in the context of their role in supporting the M-Pesa SMS banking system.

A. Interactive Voice Communication (IVR) In Kenya

Kenyan based banks like *I & M Bank* and *Barclays* utilize interactive voice response, a service that requires clients to call a pre-specified IVR number in order to access banking services. They will usually be greeted by a stored electronic message followed by a menu of different options. This service utilizes a text to speech program and is expensive compared to SMS, since it involves making voice calls [4].

B. Kenyan Standalone Mobile Application Clients (MAC)

Standalone mobile application clients are used and are appropriate for complex banking transactions like trading in securities. They are customized according to the user interface complexity and supported by the phone.

Mobile application clients are downloaded onto the mobile device, and thus require the device to support development environments such as Java Platform Micro Edition or J2ME [8].

The main shortcoming with standalone mobile application clients is that the application needs to be

customized to each mobile phone on which it is to be run, and thus development of mobile application client based systems are costly [4].

C. Short Messaging Service (SMS) In Kenya

SMS is a service that utilizes the text messaging standard and has been used to support mobile application based M-Pesa SMS banking, providing a mechanism for transmitting short messages to and from wireless devices. Clients request information by sending an SMS containing a service command to a pre-specified number.

The bank subsequently responds with a reply containing the specific requested information. SMS services are hosted on an SMS gateway that connects to Safaricom SMS Centre [4]. This process is explained below.

III. SMS TRANSMISSION OVER SAFARICOM NETWORK

GSM networks are used to transmit SMS from one device to another. GSM is a system that offers users the ability to be mobile. This system consists of a Mobile Station (MS) or base phone that has a SIM-enabled card, Transceiver Station (BTS), Base Station Controller (BSC), Mobile Switching Centre (MSC), and Home and Visitor Location Registers (HLR and VLR) [2].

A mobile Station initiates a communication signal and sends it to the Base Transceiver which receives and transmits radio signals to and from the MS, translates the signal into digital format and then transfers them to the Base Station Controller [2], including initial authentication as discussed earlier.

The BSC then forwards the received signals to the Mobile Switching Centre, and the MSC interrogates the Home and Visitor Location Registers, a database that retains information about location of the destination MS.

In the event that the received signal is an SMS message, it is routed to Safaricom's Short Message Service Centre (SMSC) [2]. This message is known as an SMS SUBMIT [10]. This SMS information is encrypted by the GSM network during transmission from the MS to the SMSC and then decrypted when stored in the SMSC. Thus, SMS security in part depends directly on the strength of GSM encryption, when using default settings.

A Short Message Service Centre (SMSC), owned and run by a Safaricom, is responsible for the routing and delivery of SMS. When a SMS message is delivered to Safaricom's SMSC, a store-and-forward message mechanism is implemented whereby the message is temporarily stored, and then forwarded to the recipient's phone when the recipient device is available [2]. This message is referred to as an SMS DELIVER [10]. While at rest in the SMSC the SMS message is, by default, in a decrypted state.

An SMS message may pass through a number of SMSCs or SMS gateways, which act as bridges between two or more SMSCs running different SMSC protocols, before reaching the recipient's device. If the intended SMS recipient is not online, the SMSC will keep the stored SMS message for a "validity period", normally 24 hours, before deleting it from storage [2].

SMS is a vital feature of the M-Pesa banking system, allowing the transfer of funds between various entities. The M-Pesa banking system is described below.

IV. M-PESA IMPLEMENTATION IN KENYA

M-Pesa's implementation was based on consideration of various factors, such as available communication channels, popular phone types, economic climate in Kenya, and target population. The limited number of smartphones in Kenya limited M-Pesa communication channel options to SMS, as it offered the best compromise between usability, security and cost. At the application layer, and with usability in mind, a menu-driven access SIM toolkit is standard software on all SIM cards.

Safaricom is a well-established network provider with hundreds of airtime dealer outlets across the country, including in rural communities. Forming a partnership with Safaricom, M-Pesa was able to provide this service to the large population. [7].

In practice, M-Pesa money transfer between entities involves 4 steps: registration, cash-in, transfer and cash out.

To use this service, individuals must register or open an account at any M-Pesa agent kiosk, by showing an

identity card (they pay no registration fees). Their information is sent to a server that creates an account and mobile wallet, and a confirmation SMS is then sent to the customer [7].

Once customers have an M-Pesa account, they can use their phones to transfer funds to both M-Pesa users and others, pay bills, and purchase mobile airtime credit, all for a small, flat, per transaction fee.

The customer uses the STK menu which prompts for a PIN in order to transfer e-value to the recipient's mobile wallet. After successful authentication, a GSM encrypted SMS is sent from the sender to the mobile server, with details relevant for the transfer to the recipient. The mobile server verifies the availability of funds, debits the senders account and credits the recipient's account. Finally, a GSM encrypted confirmation text is sent to both the sender and recipient. The transfer of funds between two entities consists of the following series of steps:

STEP 1: M-Pesa agents act as an intermediary between the bank and its customers. Agent *A* deposits money into an M-Pesa bank account to buy e-money float, which is transferred to his phone.

STEP 2: Consumer *C* pays for a specific amount of physical money to purchase e-value from agent *A*, and with his special SIM, *A* transfers e-value to C's account. An SMS is sent from the *A*'s mobile, requesting a transfer between the two accounts. *C* can then go ahead and transfer funds or make a purchase.

STEP 3: *C* then transfers e-money to customer *D*, by sending an SMS that specifies the amount to be paid out.

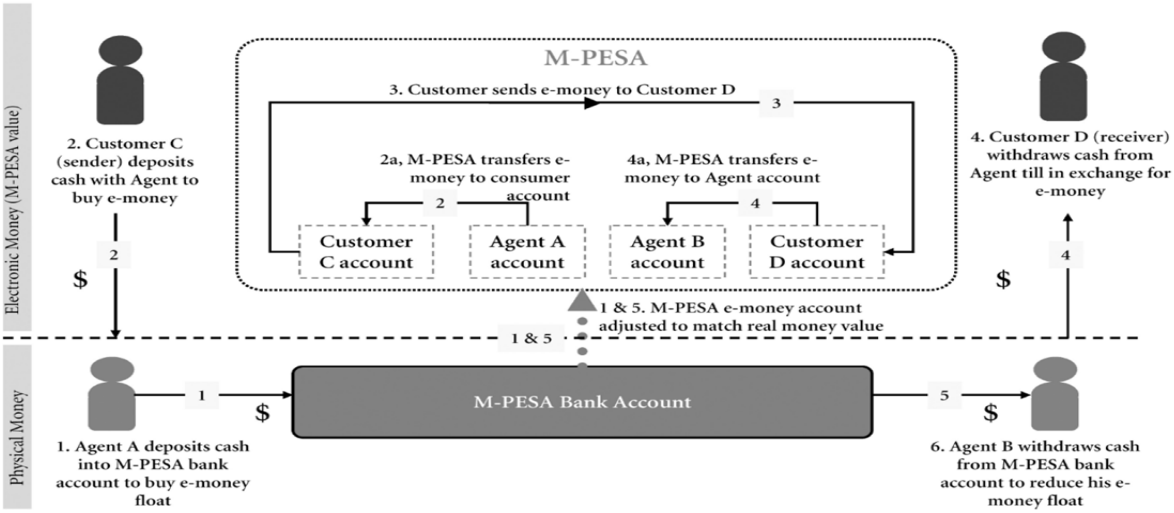
STEP 4: *D*, with this SMS, goes ahead to retrieve physical money from Agent *B*, by showing the SMS received on his phone, plus a piece of identification.

STEP 5: *B* then returns to the bank to withdraw physical money from his M-Pesa bank account, which in turn will reduce his e-money float.

This process is somewhat similar to walking into a point of sale merchant, paying for a purchase with a debit card, and during this process having an additional amount added over the purchase price and receiving this extra as cash back. In this case, these point of sale stores function as a third party bank (agent) or an intermediary between the bank and the customer, allowing the customer to obtain cash from the point of sale and have that debited against their bank account (rather than going to the bank or using an ATM machine).

Below is a diagram describing the transfer of M-Pesa funds between customers and agent

Figure I: MPESA MOBILE MONEY TRANSFER PROCESS



Reprinted from Nick Hughes and Susie Lonie, M-PESA: Mobile Money for the "Unbanked" Turning Cellphones into 24-Hour Tellers in Kenya, 2007

This diagram depicts the process through which funds are exchanged within the M-Pesa banking system, as explained earlier. The next section provides a brief description of the M-Pesa application layer support framework, SIM toolkit, used by M-Pesa agents and clients to further enhance SMS.

V. SAT/ S@T/STK (SIM TOOLKIT) IN M-PESA

The SIM Toolkit (STK) framework is defined by European Telecommunications Standards Institute (ETSI) TS 101.476 V8.5.0 (2002-09) and requires a GSM Java Card runtime environment. To extend SIM functionality to support additional services on the existing infrastructure and to exploit SMS further, the SIM Application Toolkit Specification, often called the "SIM Toolkit" (STK), was developed. STK applications in M-Pesa were implemented as text-based, menu driven interfaces from which a user highlights a command in the menu provided on the screen of the user's device [6]. The SIM also initiates commands independently of the handset and the network [12].

Using a standard STK platform, Safaricom adds their own applications to mobile handsets [5]. STK applications are downloaded over the air (OTA) and stored in the SIM card. Encryption for this OTA process can use the default DES (Data Encryption Standard) or 3DES as defined by ETSI TS 102 225. When DES is used, it is open to brute force attacks which can use Rainbow Tables to dramatically accelerate success [11, 19]. Safaricom keeps total control of the applications, and determines when they are to be updated, downloaded and removed, all of which is achieved OTA; Safaricom is responsible for OTA security.

VI. M-PESA BANKING SYSTEM WEAKNESSES

Safaricom's custom-made SIM Tool Kit (STK) has been used to provide end to end security, but despite all efforts, there have still been security breaches of M-Pesa SMS banking.

Not much is known publicly about M-Pesa's security implementation but, recent attacks on the system reveal that it does not guarantee end-to-end security to customers [10]. M-Pesa turns to STK to provide end-to-end security but, despite existence of security mechanisms that provide authentication, message integrity, replay detection and sequence integrity, proof of receipt and proof of execution, and message confidentiality, this application depends on transmission mechanisms such as SMS and GSM, which are known to have weak security systems if using default settings [11]. When using OTA encryption with DES rather than 3DES the system is further weakened [19]. Furthermore, STK does not protect against denial of service attacks; nor does it provide non-repudiation [23].

SMS does not have any built-in procedure to authenticate the text and offer security for the text transmitted as data. When a signature is applied to an SMS, the message exceeds 160 characters, and SMS reassembly is a critical part of the process, where a single dropped message means that the whole is lost. This has to be taken into consideration when designing applications with the SIM Toolkit, and on the receiver side [13].

An additional concern with the default M-Pesa SMS banking system is that the authentication key used for the signature of the transaction is generated by and known to the telephone operator (based on the Ki in the phone which was distributed to the SIM by Safaricom). This means that the financial institution cannot guarantee payment to the retailer, since the signature may be reproduced by a third party, should that third party gain access to the Ki[14]. Furthermore, M-Pesa uses the subscriber identity module (SIM) for the purposes of authentication, making Ki security a key area of concern. It gives the network operator on whose behalf the SIM has been issued complete control over all subscription and security issues. [4]

SIM toolkit is dependent on other devices, such as the mobile phone, and thus is affected by any malware they contain. Therefore, SIM toolkit cannot be relied upon to provide 100% secure services to the M-Pesa banking system, unless Ki remains secure both from logical and physical attack.

A. Weaknesses Applicable To M-Pesa Agents and Customers

SMS Denial of Service: SMS passes through encrypted GSM channels, through to the base station, and terminates at the mobile network operator, where it is typically stored unencrypted, which means that

the chain of encrypted communication between the customer and the bank is broken [16].

Flooding or Denial of service (DOS) attacks are possible by sending repeated messages to a target mobile phone, making the victim's mobile phone inaccessible. “Studies also show that weaknesses in the SMS protocol could be exploited to launch a Denial of service attack on a cellular phone network. For example, it was found that sending 165 text messages a second was enough to disrupt all the cell phones in Manhattan” [2].

Brute Force Attack: Despite security features of STK, usage of the mobile client's PIN code, usually a 4 digit-number, can be guessed and entered into stolen or lost mobile phones, and can undermine the security provided by encryption algorithms or large keys [17]. In a survey by Symantec, it was noted that one in three phones have been lost or stolen [24].

SMS Spoofing: As mentioned earlier, SIM cards have been cloned using both physical and OTA methods. Although updated algorithms have been circulated to GSM providers, it is unclear whether these updated versions are currently in use. In a setting in which SIM cloning and spoofing is a real and present danger, SMS-based systems and USSD-based applications are vulnerable if they choose not to provide additional authentication via STK's cryptography, or if they implement related protocols poorly. Even in cases where additional authentication is provided, security is debatable when the traffic can be intercepted and decoded. In one attack, a malicious customer, with the help of a remote conspirator spoofing SMSs on behalf of the bank, was able to convince an unsuspecting agent to yield cash even without the bank having recorded a cash transfer. The attack exploited the simple fact that the system does not enable clients to authenticate bank originating SMSs, thus making them susceptible to easy spoofing attacks [10].

Since encryption is not applied to short message transmission by default, messages can be intercepted and snooped during transmission. In addition, SMS messages are stored as plain text by the SMSC before they are successfully delivered to the intended recipient. These messages might be viewed or amended by users in the SMSC who have access to the messaging system [2].

Even when encryption is used for the traffic channel of GSM, SMS is sent in the clear by default. SMS originating address (OA) fields are spoofable, meaning that a handset other than the sending entity can pass off an SMS as having originated from another number [1, 4].

B. Weaknesses Applicable To STK

SIM Toolkit has been compromised through proactive commands, command header packets and phone types used. STK proactive commands provide a mechanism through which the SIM initiates actions to be taken by the ME. We begin our discussion of these weaknesses by briefly listing a number of commands relevant to our discussion, together with a brief description:

Display text command: This displays text on screen (no more than 160 characters). A high priority replaces anything else on the screen.

Provide local information command: Requests the MS to pass local information to the SIM: the mobile country and network codes of the network on which the user is registered.

Call Control: When this service is activated by the SIM, all dialled digit strings and supplementary service control strings are first passed to the SIM before the MS sets up the call or supplementary service operation.

STK Denial of Service: Using the SIM Toolkit DISPLAY TEXT command, with the "high priority" and the "wait for user" bits set, can cause messages to fill the screen, and the user must explicitly dismiss them. Repeatedly doing this will cause messages to block the screen and result in a denial of service. The user dismisses the message by pressing the "back" or "OK" button, or some other facility on the phone, which prompts the phone to send a TERMINAL RESPONSE command back to the SIM card. An alternative SIM toolkit stack could re-send the same DISPLAY TEXT command in response to the TERMINAL RESPONSE, causing an infinite loop and thus a denial of service [21].

STK command header packets are octets within a secured packet transmitted by the sending entity to the receiving entity, containing a secured application

message. Below are brief definitions of several aspects of STK relevant to this discussion [10]:

Ciphering Key Identifier (KIc) - Key and algorithm identifier for ciphering

Key Identifier (KID) - Key and algorithm identifier for Redundancy Check (RC) /Cryptographic Checksum (CC) /Digital Signature (DS)

Toolkit Application Reference (TAR) - This is part of the header that identifies and triggers the OTA feature, which is an application on the SIM

Security Parameter Indicator (SPI) - This defines the security level applied to the input and output message

When a SIM card has data download via SMS Point-to-Point allocated and active, the ME passes the message transparently to the SIM using the SMS-Point to Point download command. An alert of the short message waiting will not be displayed on the ME screen. Furthermore, when the proof of receipt in the second octet of the security parameter indicator is set to be sent via SMS DELIVER-REPORT or SMS-SUBMIT, a weakness is created through SIM Toolkit command header packets.

When proof of receipt is set to SMS-SUBMIT, the phone will try to send back a reply to the originated sender, in this case Safaricom, and when set to DELIVER REPORT, the phone will report to the network the status of the message. Since no valid entries are set for the KIc, KID, TAR, the result of the STK command will be an error report causing the SMSC to resend the message, putting on hold until the initial message expires any other future messages that are supposed to be delivered. A SIM Toolkit error message is sent to the operator's message centre, and this is interpreted as a message delivery failure. Operators usually attempt to resend the undelivered message, creating an error loop that prevents the delivery of legitimate SMS messages to a user's handset until a bogus SIM Toolkit message times out, typically after 24 hours or so. Because of this, sending a series of bogus SIM Toolkit messages is a method of executing a SMS Denial of service attack [10].

Disclose Private Information: Cell information for a device connected to the network can be requested and translated to a geographical location, with freely available tools, through the use of SIM Toolkit. The ability to send text messages could allow an attacker to track the location of a victim. The PROVIDE LOCAL INFORMATION command causes the MS to respond with the connected network and cell ID, forming a unique identifier for a certain cell in the network. This information is sent to the attacker using the SEND SHORT MESSAGE command, enabling an attacker can see the victim's location within a few kilometers accuracy, or less in populated areas. When combined with the “location changed” event, an attacker can increase this accuracy and closely follow the victim [21].

Man-In-The-Middle on calls: A SIM card can control all outgoing calls made by the victims’ MS, block or redirect calls to an eavesdropping telephone number that transparently forwards the calls using the SIM Toolkit call control service [21].

Forwarding authentication codes: SIM Toolkit application might be able to receive and check incoming SMS messages, forward them silently to an eavesdropping number, depending on the phone type. When a victim uses SMS messages to authenticate, for example to do a bank transaction, these can be caught and forwarded, facilitating identity fraud [21].

With all these vulnerabilities, and associated possible exploits, there is a need for more security measures in the M-Pesa banking sector.

VII. MITIGATION STRATEGIES

The mitigation strategies suggested in this section are based on the M-Pesa implementation of GSM, SMS and STK by Safaricom in Kenya. The market for cell phones in Kenya is also taken into account as Kenya is ranked 152th out of 177 countries on the 2006 Human Development Index and is among the world’s 30 poorest countries, and thus many cell phone users in Kenya have cell phones which predate smartphones used in most developed countries.

SMS ENCRYPTION: SMS message encryption is one of the strategies that would mitigate weaknesses such as man in the middle and SMS spoofing. Both private and public key methods could be used.

SMS Public Key Encryption

Table I below shows different SMS encryption algorithms and respective encryption and decryption time, in milliseconds. Each SMS costs Ksh1.00 for Safaricom to Safaricom SMS and Ksh2.00 for Safaricom to other local networks. Bearing cost in mind, the most optimal public key encryption algorithm in this case would be RSA, considering time in milliseconds to encrypt and decrypt an SMS.

Table I- Public Key SMS Encryption

Algorithm	Key Size	Cipher Bit	Number Of SMS	Time in Milliseconds	
				Encryption	Decryption
Rsa	256	614	1	37	37
Elgamal	256	1222	2	7098	37
Elliptic	256	789	1	8242	3932
Rsa	512	1230	2	258	259
Elgamal	512	1230	2	29388	194
Elliptic	512	1635	2	57236	27034

Reprinted from M.Agoyi and A.Seral, Sms Security: An Asymmetric Encryption Approach [18].

Each phone would need a private key. To encrypt and decrypt the SMS using asymmetric algorithms such as RSA, the public key of the other party must be known so as to encrypt and decrypt the SMS. Key distribution of the public keys is vital and could impose an additional cost of an extra SMS message to the subscriber. In this case each MS would have to send their public key to the other party which would then be used in combination with the respective private keys to encrypt and decrypt the SMS messages.

Public key distribution would need to be completed OTA or as a part of the STK message itself. Since Safaricom controls the security of the STK, this could be achieved by issuing and installing private keys into phones and distributing certificates for the public key signed by Safaricom. This could deploy as a PKI linking the certificate to a CA, as well as a token based public keys signed within the Safaricom network [22].

A. *Symmetric Key Encryption*

Symmetric algorithms could also be used for encryption and decryption. The key used for this could be distributed to the STK using OTA and thus would also rely on the security of the OTA maintained by the provider.

An assumption here is that the environment (the phone operating system) in which STK operates is secure. Any recommendation for use of weak encryption algorithms such as DES would leave STK messages open to vulnerabilities in the OTA process.

For encryption to be a success, phones used must have the processing capability to handle encryption and decryption and receive the appropriate keys securely.

With the above described end to end encryption communication the M-Pesa traffic would be protected as it transits both the GSM operator and service provider network [16].

Above all, users who have GSM phones with M-Pesa SMS banking installed with STK should be diligent with physical possession of the phone to prevent exploits to the physical SIM and related STK software, all of which will compromise the security of their e-money held in M-Pesa. This threat affects all lost or stolen phones as described earlier.

Several mitigation strategies for vulnerabilities within the M-Pesa banking system are depicted in Table II:

Table II- Solutions to vulnerabilities to M-Pesa banking System

	VULNERABILITY	SOLUTION
Phone	**Phone viruses**	Avoid downloading programs that contain malware which might affect the operations of the operating systems of the phone, the STK or might prevent the STK from being a trusted program.
SMS	**Brute force attack**	Enforce the use of longer PIN combinations in STK.
	SMS Spoofing **SMS Denial Of Service attack**	Use of strong cryptographic algorithms for mutual authentication and encryption of SMS. Do not use DES.
GSM	**GSM weaknesses**	Using secure algorithms for GSM A3, A5 and A8 implementations to prevent SIM card cloning attack which reveals Ki. This comes with a cost of modifying the software of the HLR. Consider mutual authentication of SIM card and network (i.e. EAP SIM). The use of both COMP128-2 and COMP128-3 algorithms for GSM A5 encryption prevent SIM card cloning and over-the-air cracking of Ki. Securing the backbone traffic between the networks components can prevent eavesdropping or modification of data when at rest.
STK	**STK Denial of service**	Disable data download via SMS point to point capabilities on the SIM card
	Man in the middle	Encryption of STK messages using strong asymmetric or symmetric algorithms
	Forwarding authentication codes	Disable forwarding capability on STK
	Disclosure of private information	Whitelist numbers allowed to use this command for instance the police and emergency responders

VIII. CONCLUSION

The biggest losses in M-Pesa SMS banking are made by M-Pesa agents in this banking system. This is due to errors when authenticating SMS messages received (i.e., in reading the confirmation SMS message). This risk could be mitigated through proper training or improved training of agents to prevent spoofing of messages (in this manual aspect of SMS banking) since the cost of this error would be born by the agent not the customer.

Although there are many other weaknesses to SMS M-Pesa banking which could be directed at individual customers, the cost of compromising an *individual's* M-Pesa account may not be worthwhile, as one can only reap a maximum of $1,200 USD. Equipment used to launch an attack might well cost more than the attacker would gain. Moreover, many M-Pesa customers in Kenya may keep well less than $1,200 USD in their M-Pesa account.

IX. REFERENCES

[1] Medani, A.; Gani, A.; Zakaria, O.; Zaidan, A.A.; Zaidan, B.B. (2011). *Review of mobile short message service security issues and techniques towards the solution.* (Scientific Research and Essays)[Online], Available: http://www.ittc.ku.edu/~krsna/citing.htm.

[2] The Government of the Hong Kong Special Administrative Region. "Short Message Service Security", [online]. Available: http://www.infosec.gov.hk/english/technical/files/short.pdf. 2008 February.

[3] Security Breach at M-PESA: Telco 2.0 Crash Investigation. [Online]. Available: http://www.telco2.net/blog/2010/02/security_breach_at_mpesa_telco.html

[4] Abunyang, E.; (2007 August). "Mobile Banking in Developing Countries: Secure Framework for Delivery of SMS-banking Services", M.S thesis Radboud university Nijmegen, The Netherlands.[Online]. Available: http://www.cs.ru.nl/iii/onderwijs/afstudereninfo/scripties/2007/EmmanuelAbunyangScriptie.pdf.

[5] David G.W. B. "Mobile Financial Services: The internet isn't the only digital channel to consumers" Available: http://www.arraydev.com/commerce/JIBC/9909-05.htm

[6] Sociedade anonima de servicos e comercio, br.; "*Dynamic Display Generation for Mobile Communication Devices*". US Patent 2006/0041470 A1, Feb. 23, 2006. Available: http://www.google.ca/patents?hl=en&lr=&vid=USPATAPP11942686&id=ntCvAAAAEBAJ&oi=fnd&dq=Sim+toolkit+%28STK%29+implementation+in+sms+banking&printsec=abstract#v=onepage&q&f=false

[7] Hughes,N.; Lonie,S. (2007). "M-PESA: Mobile Money for the Unbanked Turning Cellphones into 24-Hour Tellers in Kenya".[Online]. Available: http://www.changemakers.com/pt-br/system/files/Innovations%20Article%20on%20M-Pesa_0.pdf
[8] Sharma, A; Subramanian, L; Shasha, D. 2009. "Secure Branchless Banking" [Online]. Available: http://dritte.org/nsdr09/files/nsdr09_camera/s4p4_sharma09nsdr.pdf
[9] Mulliner, C.; Miller, C. "Injecting SMS Messages into Smart Phones for Security Analysis"
[10] Alecu,B. "SMS Fuzzing - SIM Toolkit Attack" [Online] Available: https://www.defcon.org/images/defcon-21/dc-21-presentations/Alecu/DEFCON-21-Bogdan-Alecu-Attacking-SIM-Toolkit-with-SMS-WP.pdf
[11] Afanu Kodjo, E.; Mamattah, R.S. "*Mobile Money Security: A Holistic Approach*", MS in Information Security thesis, Luleå University of Technology 2013.[online]. Available: http://pure.ltu.se/portal/files/44007758/LTU-EX-2013-43949783.pdf
[12]http://www.gemalto.com/techno/catalog.html

[13] Patern, G. "Enhanced SIM (ESIM): a proposal for mobile security",[Online] Available: http://pubs.gpaterno.com//2009/enhanced_sim_proposal_sept_2009.pdf

[14] Tobbin, P. 2011. "*Understanding the mobile money ecosystem: Roles, Structure and Strategies*". In proceeding of the Mobile Business (ICMB), Tenth International Conference. [Online]. Available: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6047069&url=http%3A%2F%2Fieeexplore.ieee.org%2Fstamp%2Fstamp.jsp%3Ftp%3D%26arnumber%3D6047069
[15] Soram, R. "Mobile SMS Banking Security Using Elliptic Curve Cryptosystem" *IJCSNS International Journal of Computer Science and Network Security, VOL.9 No.6, June 2009 30* [Online].Available: https://www.researchgate.net/publication/242521762_Mobile_SMS_Banking_Security_Using_Elliptic_Curve_Cryptosystem
[16] Toorani, M.; Shirazi,A.A.B. "Solutions to the GSM Security Weaknesses" [online], Available: http://arxiv.org/ftp/arxiv/papers/1002/1002.3175.pdf
[17] Prof. Dr. Fariborzi, E.; Eng. Kazemabad,A.H. "The security of information in financial transactions via mobile: algorithms" Available:https://www.academia.edu/6252602/The_Security_of_Information_in_Financial_Transactions_via_Mobile_Algorithms
[18] Agoyi, M.; Seral,A. 2010. "Sms Security: An Asymmetric Encryption Approach" . In proceeding of the 6th International Conference wireless and Mobile Communications (ICWMC), [Online]. Available: http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5628740&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5628740
[19] Attack on OTA illustrated at http://nelenkov.blogspot.ca/2013/09/using-sim-card-as-secure-element.html
[20] Singh, J.;Ruhl, R.; Lindskog.D**. "**GSM OTA SIM Cloning Attack and Cloning Resistance in EAP-SIM and USIM"
[21] Gielen, S. (2012 August) "SIM Toolkit in Practice".[Online]. Available: http://sjorsgielen.nl/simtoolkit-in-practice.pdf
[22] Bakdi,I.; "Towards a Secure and Practical Multifunctional Smart Card". In Proceedings of the *7th IFIP WG 8.8/11.2 international conference on Smart Card Research and Advanced Applications*. Springer-Verlag Berlin, Heidelberg , ISBN: 3-540-33311-8 978-3-540-33311-1 doi>10.1007/11733447_2.[Online]. Available: http://dl.acm.org/citation.cfm?id=2097208
[23] Nambiar, S.; Chang-Tien, Lu.; Liang,L.R. ; "Analysis of Payment Transaction Security in Mobile Commerce" *Proceedings of the 2004 IEEE International Conference on Information Reuse and Integration, 2004*.Available: https://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=1431506&pageNumber%3D136802
[24] Norton Survey Reveals One in Three Experience Cell Phone Loss, Theft, Press Release, (2011,Febuary 8) Available : http://www.symantec.com/about/news/release/article.jsp?prid=20110208_01.
[25] Lord, S. "Trouble at the Telco: When GSM Goes Bad" *Network Security Volume 2003 Issue 1, DOI:10.1016/S1353-4858(03)00111-9* [Online]. Available: https://www.researchgate.net/publication/222006774_Trouble_at_the_Telco_When_GSM_Goes_Bad