SECURITY ISSUES FACED BY MOBILE CASH TRANSFER APPLICATIONS IN KENYA ON GSM AND 3G NETWORKS

G. W. Chemwa
Institute of Computer Science and Information Technology, Jomo Kenyatta University of Agriculture and Technology, Nairobi, Kenya
E-mail: chemwex@icsit.jkuat.ac.ke

Abstract
This paper postulates that since mobile cash transfer and banking applications security architectures were developed in obscurity, they could easily be cracked when they lose their obscurity. The paper investigates the security loopholes present on 3G networks and their likely impact on the security of cash transfer and banking applications. The study also looks at the security of the applications themselves and how biometric authentication can be used to improve security through multimodal authentication.

Key words: Mobile banking, 3G, mobile applications, security, convergence, mobile cash transfer

1.0 Introduction

The remarkable growth in access to mobile telephony in developing markets has created the possibility of delivering new financial services by leveraging secure, low-cost mobile networks and platforms (Hughes, 2007). Kenya now has four mobile cash transfer services in the form of Safaricom's M-PESA, Zain's Zap, Yu's Yu Cash and Orange's Orange Money. These services have a subscriber base of over fifteen million (15M) and transact over four hundred billion Kenya shillings a year (CBK, 2009). Most of these systems are text based and access is controlled using a four digit password only. The introduction of mobile banking services like M-Kesho by Equity bank, KCBConnect by Kenya Commercial Bank (KCB) and Pesa Pap by Family Bank has introduced new security challenges at the various inter-network points of convergence, more specifically vulnerabilities in the Switching System 7 (SS7) protocol used for GSM networks. Already, a security firm in the United States of America discovered gaping security loopholes in mobile banking applications which could allow a person to acquire the user name, password and account details from iPhone and Android phone memories (Spencer, 2010). In a developing country like Kenya, the mobile user for the foreseeable future will find utility in standard (basic) handsets. Feature phones and Smartphone's are still a shilling too expensive. Standard handsets do not have facilities to secure or encrypt data before sending it to server based applications at the mobile financial services providers (mFSP) or the ability to run programs (Trust, 2008). This paper will analyze the security vulnerabilities of 3G networks, explore the security of applications architectures and conclude by looking at various biometric authentication vectors and how they can enhance mobile applications security.

2.0 Materials and Methods

This paper was compiled on the basis of: personal knowledge and experiences of the author; published reports from various sources listed in the references; interviews with staff in leading mobile cash transfer and banking providers; interviews with customer outlet agents for mobile cash transfer; interviews with users chosen at random in both urban and rural Kenya.

3.0 Results

The mobile handset consists of various stand alone or client applications whose general architecture is as depicted in Figure 1. The picture shows that security cuts across the application architecture.

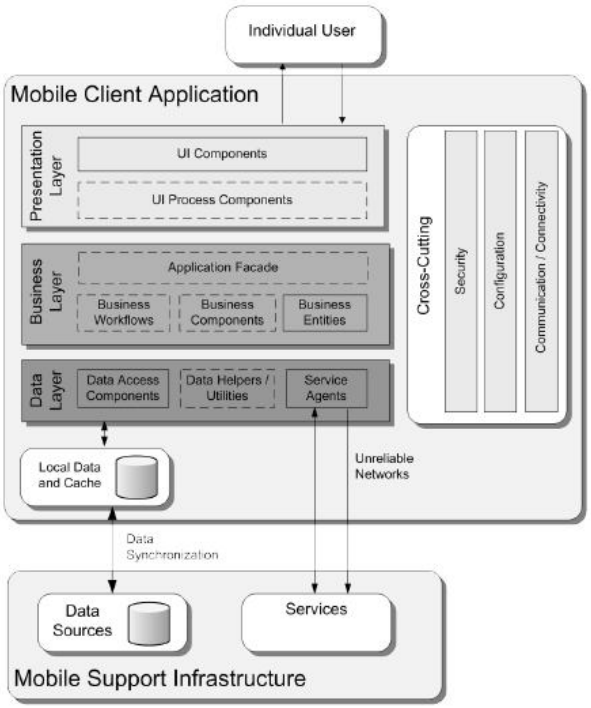

Figure 1: The mobile phone application architecture ©Microsoft Patterns & Practices 2008

All the Kenyan mobile network operators (MNO's) are struggling to move from second generation (2G) to third generation (3G) platforms. Safaricom was the first to launch the 3G platform while the other networks have moved from 2G to 2.5G and 2.75G. This paper therefore focuses on the security issues on 3G networks, since this framework tries to address loopholes that existed on earlier networks. Table 1.0 shows the evolution of mobile networks, technologies and applications.

Table 1: Evolution of mobile networks, technologies and applications

	Year	*Voice*	*Sms*	*Analog*	*Video*	*Digital*	*Gprs*	*Edge*	*Hspda & Wimax*	*Web*	*Basic . / Advanced. Multimedia*	*Apps*	*Speeds*
1G	1980 – 90s	•		•								None	low
2G	1990s	•	•			•				•		Thin clients, Voicemail, push-to-talk, conference call, caller ID, voicemail,email,web	20Kbps
2.5G	2000 To Date	•	•			•	•	•		•	•	Rich clients, Faxing, browsers, basic multi-media, mapping, light games	90Kbps
3G	Present	•	•		•	•	•	•	•	•	••	Video on demand, video-conferencing, VoiP, music, TV, satellite radio, stand alone Apps, advanced games	2+ Mbps
4G	Future	•	•		•	•	•	•	•	•	••	Complete rich apps	1 Gbps

Mobile cash transfer and banking applications in Kenya such as M-Pesa, Zap and Yu Cash are thin clients based on short message service (SMS) and unstructured supplementary service data (USSD) technologies. In order for an intruder to perform an attack, they must be able to eavesdrop, impersonate the user or network, assume the man-in-the-middle position or compromise authentication vectors (3G TR 33.900, 2000). Table 2 lists the various security vulnerabilities of 3G networks, and indicates those that are yet to find solutions.

Table 2: Various security vulnerabilities

Vulnerability	*Description*	*Solved?*
1.0 Denial of Service	Attacks included deregistration spoofing, location update spoofing Camping on false BS or BS/MS	Yes No
2.0 Identity Catching	Attacks include passive identity catching, active identity catching	Yes
3.0 Network Impersonation	Attacks include encryption suppression between target user and intruder or network Impersonation of network forcing use of compromised cipher key	Yes Yes
4.0 Eavesdropping	Eavesdrop on user by suppressing encryption btw. user & network Eavesdrop on user by suppressing encryption btw. user & intruder Eavesdrop on user by forcing use of compromised cipher key	Yes Yes Yes
5.0 User Impersonation	Through use of compromised authentication vector Through use of compromised authentication response Hijacking outgoing calls with encryption disabled Hijacking outgoing calls with encryption enabled Hijacking incoming calls with encryption disabled Hijacking incoming calls with encryption enabled	Yes Yes Partly Yes Partly Yes

The findings elucidated in Table 2 means that simple access authentication at the application's interface is not enough to guarantee the safety of mobile cash and banking applications. Security should be viewed in a multilayered and multimodal manner as a function of many features some of which include the following: the need to enforce security at every layers of the communication protocol stack; handset/SIM/Smartcard security; internetwork security; intra-network security; application platform security and human administration/agent security.

GSM Layer 1 is normally understood to mean the control software which controls the radio and baseband hardware-the physical layer. Layer 1 multiplex the physical access to the radio channel and provides a number of logical channels which can be used for signalling. Layer 2 is responsible for establishing a data link on these logical channels to allow reliable transmission of Layer 3 signalling messages. Layer 3 is subdivided into a number of separate tasks including the radio resources manager, the mobility manager, and the connection manager.

The modern mobile network puts a lot of emphasis on the mobile handset and SIM card as fortified centers of security. Key security issues here include: the need to closely monitor how stolen or malfunctioning cards are replaced; the importance of controlling what applications are installed on the smartcard to avoid K_i loss and the need for SIM misuse tracking system.

The danger of a mobile user losing a handset to a person who may know the access codes both to the SIM and mobile cash transfer and banking applications cannot be overstated. In most cases this could be a close friend or relative.

The biggest challenge here is at the points of convergence between mobile networks and internet protocol (IP) based networks. The signaling System no. 7 (SS7) which connects this mobile to IP networks deals with security issues such as authentication, location updates and call control. Research shows that messages can be altered, injected or deleted into the SS7 signaling without proper control. This provides challenges where mobile cash transfer applications merge with IP based financial systems run by banks in Kenya. The increasing sophistication of the modern cracker with modern computer based tools and access gateways found on the internet creates real

challenges to the security on mobile financial applications. There needs to be continuous screening of incoming SS7 messages to avoid messages that can create a denial of service (DoS).

The unauthorized access to mobile network assets and interfaces such as the Home Location Register (HLR), Authentication Center (AuC) and the Mobile Switching Center (MS) presents a real vulnerability to mobile cash transfer and banking applications. This is because such an access would expose confidential information. Unauthorized access to HLR can easily lead to activation of subscribers who are invisible to the billing system or cause a denial of service attacks. At this point privileged man-machine (MM) commands can be used to illegally manipulate other HLR's on the network. Secondly, unauthorized access to the AuC will enable an attacker to clone subscribers on the network. Lastly, a successful attack on MSC would result in the loss of confidentiality of user data, unauthorized access to services or denial of service for large numbers of subscribers.

Mobile cash transfer and banking applications can either be complete handset applications, mobile web applications or text based as illustrated in Figure 2.0. Each set of applications provides unique security challenges.

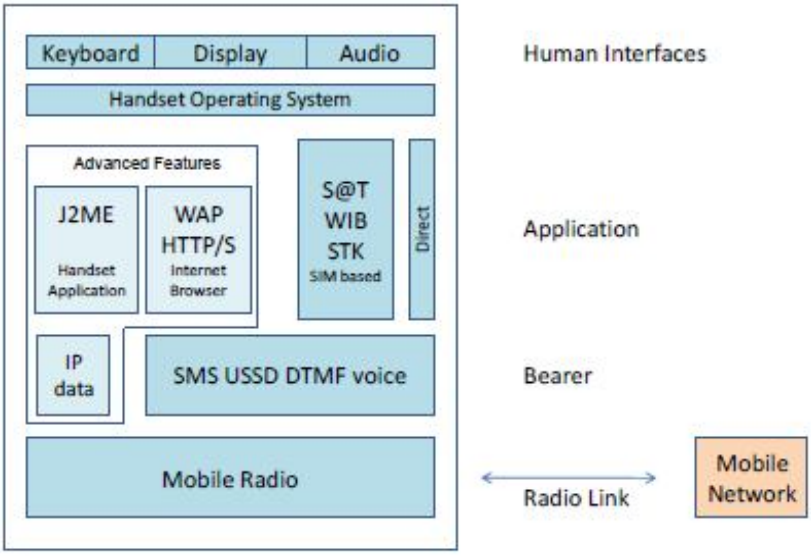

Figure 2: Mobile phone applications ©Bankable Frontier Associates 2008

SMS – Short Message Service USSD – Unstructured Supplementary Service Data J2ME-Java 2 Platform Micro Edition WAP- Wireless Application Protocol HTTP – Hypertext Transfer Protocol HTTPS – Secure HTTP IP – Internet Protocol

Table 3 summarizes the various technology platforms that mobile cash transfer and banking applications can be developed on and the risks associated with each:

Table 3: Technology platforms useful to mobile cash transfer and banking applications

Technology	*Application Scenario*	*Associated Risk*
SMS/USSD/MMS, Voice/IVR	Application runs on generic mobile bearer services	There is no encryption of information so the channel from the mobile to the mobile financial services provider is open to monitoring, replay, modification and impersonation
HTTP/S, WAP	Applications run on mobile browsers provided on the phone. They do not depend on mobile network providers.	These applications run on the mobile web and are accessible through mobile based browsers e.g. Opera Mini. The security of the applications depends on security standards such as secure socket layer (SSL) and browser security
J2ME, SYMBIAN, ANDROID	Applications use advanced services provided on the phone. These are rich clients connected to servers over mobile network. These applications are partly independent.	Mobiles less exposed to the Internet and the threats. SSL can be used. End-to-end security can be enforced.
SIM Toolkit, WIB, S@T and Java Cards	Applications use the secure environment provided by the mobile network operators.	This provides the highest end-to-end security. The application runs securely within the SIM and the encryption keys are kept within the SIM.

Weaknesses in the information security policy that governs access to network elements and information assets by employees, agents or external people can greatly compromise the security of the mobile applications and the supporting information communication and technology (ICT) assets. A granular approach to different user's access to mobile cash transfer and banking applications and other information assets must be implemented. On the other hand, all the paperwork needs to be properly classified to avoid sensitive documents falling into the hands of unintended staff. Physical access control to mobile information assets needs to be carefully thought out to deter both unauthorized insiders and outsiders from accessing them.

3.0 Discussion and Conclusion

The foregoing findings point to weaknesses in the mobile cash transfer and banking applications, mobile networks and administration issues which can impact on the security of cash transactions. The simple password access control on the application interface is not enough to assure security. Also, the vulnerability of the SS7 switching protocol at the points of convergence between mobile networks and IP based networks still leaves a lot to be desired. Although recorded attacks have been accidental, the future security terrain calls for urgent sealing of existing loopholes. Lastly but not least, the false base stations attack has not been dealt conclusively even in 3G networks, and this can be exploited to cut genuine users off from their home network as the attacker tries to acquire confidential information from the user.

In view of these findings, it would be good to develop a multimodal security model especially at the points of user authentication in the applications and networks. Biometric technology comes in handy as a method that can be used together with other authentication vectors to enhance security of applications. Fingerprints and facial features authentication are two methods which are finding quick acceptance on mobile platforms. Facial identification needs to avoid replay attacks based on real life size photographs by analyzing the 3D images of video. The key challenge here is that the volume of code needed to achieve this feat may be too much for the mobile platform.

References

3GPP, (2000). A guide to 3rd generation security p.5-20. 3GPP Project, Antwerp.

Bankable Frontier Associates Trust F. (2008) *Managing the risk of mobile banking technologies p.3-33* Bankable Frontier Associates.

Chikomo, K. et al Security of mobile banking p.3-4 University of Cape Town, Rondebosch.

Guo, Y. and Chaskar, H. (2002) *Class-based quality of service over air interfaces in 4G mobile networks* P. *132-137* IEEE Communication Magazine.

Gritzalis, S. et al Security protocols over open networks and distributed systems: Formal methods for their analysis, design and verification p. 1-5 University of Aegean, Athens.

GSI, (2008). Mobile commerce opportunities and challenges p. 43 Blue Tower, Brussels.

Kim, D. and Hong, K. (2008). Multimodal security authentication using teeth image and voice in mobile environment p.1-4 IEEE,NewYork.

Sarin, A. (2007). The transformational potential of m-transactions p.8-11 Vodafone, UK.

Sieger, H. (2010). User preferences for biometric authentication methods and graded security on mobile phones p. 1-2 Technische Universitãt, Berlin.

Zhu, B. et al (2009). PCM: A privacy-preserving detection mechanism in mobile ad-hoc networks p. 7 Wiley and Sons, USA.