Stragglers of the Herd Get Eaten:
Security Concerns for GSM Mobile Banking Applications

Michael Paik
New York University
mpaik@cs.nyu.edu

ABSTRACT

The first GSM standard was published in 1989 [10], fully two decades ago. Since then, cryptanalysis has weakened or broken significant parts of the original specification. Yet many of these compromised pieces remain in common use, particularly throughout the developing world.

This state of affairs presents a significant risk given the recent proliferation of high visibility and high value targets within the branchless banking space in the developing world such as M-PESA, GCASH, mChek, and Zap, each of which makes use of SIM Toolkit (STK) security measures, but in an obfuscated manner.

This paper will present an overview of recent developments in GSM security and outline the need for increased cooperation and standardization in the face of rapidly eroding security measures currently in place for 2G GSM.

Categories and Subject Descriptors

E.3 [**Data Encryption**]: [Standards]; K.4.4 [**Computing Milieux**]: Electronic Commerce—*Security*; C.2.1 [**Computer Communication Networks**]: Network Architecture and Design—*Wireless communication*

General Terms

Design, Security, Standardization

Keywords

GSM, USSD, SMS, A3, A8, A5/1, A5/2

1. INTRODUCTION

3G Americas projects that as of September 2009, the number of GSM connections in use will have reached 4 billion [26]. As GSM usage becomes ever more ubiquitous, it also becomes ever more attractive as a data-bearing infrastucture component, particularly in the developing world where other data backhauls are both scarce and costly.

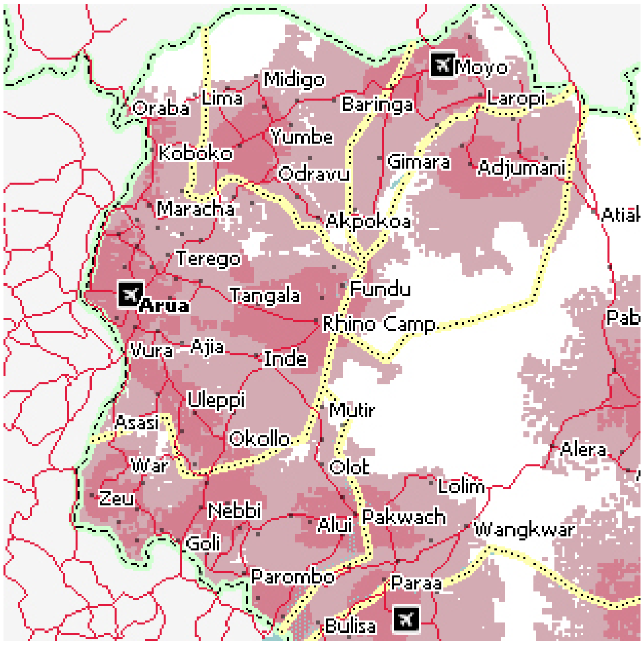

Figure 1: Northwestern Uganda as an example of high rural GSM penetration

Increasingly, value added services are being provided to populations of rural and developing regions using readily available GSM technology and steadily growing penetration of coverage into those regions. Branchless banking in particular is increasingly popular, with solutions like M-PESA [14] from Safaricom Vodafone and Zap [22] from Zain in Kenya, GCASH [9] from Globe Telecom in the Philippines, and mChek [21] in India leading the way forward.

Thus far, security concerns about these banking solutions have been somewhat masked by GSM traffic channel (TCH) encryption, but in recent years, many of the security primitives upon which GSM relies on have been shown to have significant weaknesses opening them to practical attack.

1.1 GSM Security Overview

1.1.1 Authentication

GSM handsets identify themselves to networks using a unique identifier known as an International Mobile Subscriber Identity (IMSI), which is sent in cleartext during the negotiation of a connection. The handsets are subse-

HotMobile 2010 Annapolis, MD

quently authenticated to the network using a cipher family known as A3, and session keys are generated using a cipher family known as A8 [3]. Using a symmetric 128-bit pre-shared secret key known as Ki, these functions identify the handset to the network and create a 64-bit session key known as Kc, respectively, using Ki and a random value supplied per-session by the mobile base station. The reference implementation of these two ciphers provided by the European Telecommunication Standards Institute (ETSI) is called COMP128.

1.1.2 Resource Requests

When a handset wishes to make a call or send a message via the Short Message Service (SMS), it sends a Radio Request (RR) to the base station, which then responds with conditions for the call including the Ciphering Modes (A5/0-3) it supports. The handset subsequently negotiates an encryption standard both the handset and the base station support and agree on the other parameters of the communication session.

1.1.3 Traffic Encryption

The traffic between the mobile equipment (ME) and the base station is encrypted by a family of ciphers known as A5. A5 has four incarnations: A5/0 is a dummy cipher which sends data in the clear, A5/1 is the standard security implementation used in Europe and North America, A5/2 is a weaker cipher that the GSM alliance provided to "unstable" states, and A5/3 is a newer, stronger cipher used to secure 3G services under UMTS.

1.1.4 Cell Selection

2G GSM uses a protocol known as C1 to select mobile cells to associate with, alongside C2, which handles reselection [2, 4]. These protocols pick cells primarily based on signal strength and carrier. The carriers of GSM cells are identified by Mobile Country Code (MCC) and Mobile Network Code (MNC), which are sent over the air in cleartext.

1.2 GSM Security Erosion

Over the course of time, security of several of the fundamental components in GSM's initial 2G implementation have been shown to have significant weaknesses. Wagner and Goldberg showed in 1998 [41] that COMP128 had critical flaws, including a key deliberately weakened from 64 to 54 bits. This weaker key allowed the practical cloning of SIMs by exposing their secret Ki among other attacks. Cloning initially required physical access to the SIM but subsequently was performed over the air without such access [40]. Subsequent reimplementations of COMP128, known as COMP128-2 and COMP128-3 appear to have greater security, but their details remain unpublished so no academic cryptanalysis not based on reverse-engineering has taken place.

A5/2, used in many places throughout Asia, Africa, and South America, was shown in 1999, again by Wagner and Goldberg [30], to have serious cryptographic flaws, enabling realtime traffic interception, which has been academically explored in several publications [27, 29].

Finally, A5/1, used in the 'developed' world, has had several significant attacks upon it [28], though in practice it appears that at present only a very well-funded attacker (governments, law enforcement) could decrypt traffic.

Compounding these issues are regulatory decisions on the parts of several governments in mandating the use of weaker encryption standards, either through inertia in not changing existing infrastructure build in the shadow of the Cold War, or in order to allow for interception of call traffic. For instance, recent surveys [7] show that GSM voice and data traffic on all Indian carriers is sent in the clear, without any encryption at all. Surprisingly, even French carrier SFR sends SMS in cleartext.

1.3 Better-Equipped Attackers

In the past few years, hardware has become readily available for users to create their own small GSM cells [11], allowing individuals to potentially masquerade as mobile carriers at very low cost. Moreover, open-source hardware and software projects allow users to accomplish similar results using very low-cost hardware. In particular, Ettus Research's Universal Software Radio Peripheral (USRP) [8] and OpenBTS [19, 20] grant most of this functionality for less than $1000.

We address some concerns that arise from these facts in the following section.

2. STATE OF PLAY

In the past decade, great strides have been made in the use of mobile technologies to provide services to the poor and disenfranchised in the developing world, with applications ranging from health [13] to politics [31] to commerce [6]. However, the application with the most impact by far has been branchless banking, with GCASH of the Philippines and M-PESA of Kenya as standard-bearers.

2.1 Big Targets

M-PESA transacts an estimated $2 million per day among its 7 million users, as of August 2009 [15], with an aggregate circulation of more than $1.7 billion since its commercial launch in March 2007. While this level of activity cannot be called the norm, it is not out of line with other significant players in the field, including e.g. mChek in India, which claims 25 million users [16]. GCASH, operated by Globe Telecom in the Philippines, operates on another scale altogether, with $100 million transacted through the system daily [36].

These organizations have varying implementations, but most have factors in common. These include the use of SIM Toolkit [5] (STK, an ETSI standard, for secure storage and implementation of cryptographic protocols) and transmission over the air via SMS or the Unstructured Supplementary Service Data (USSD) channel. Additionally, none of these organizations appears to be recognized as a bank by the relevant jurisdiction, limiting governmental guarantees against theft and fraud.

M-PESA, developed by Sagentia at the behest of Vodafone and Safaricom [38], uses USSD as a transport layer, upon which an ostensibly secure protocol is built using STK. Details about the security of the protocol are unknown, as are details of what precisely is carried over the air.

mChek, developed in-house, claims "128-bit, 3DES, end-to-end encryption." However, 3DES takes 56, 112, or 168-bit keys, with no option to trim or augment keys, rendering this statement highly suspect. mChek does, however, add an Interactive Voice Response (IVR) callback feature to each transaction which calls the handset a transaction ostensibly originates from to confirm the transaction details using touch tones and automated menus.

GCASH, an older system, is accompanied by what appears at first glance to be a less robust security suite. Registration is accomplished via vanilla SMS containing the string **reg** plus a PIN number, the user's mother's maiden name, the user's first and last names, and the user's address to a specific number (2882) with the relevant information populated. Cash can be transferred in a similar way, by sending the string **amount** plus the aforementioned PIN number to the same number as the registration step, but with the ten digit mobile phone number of the recipient appended.

More recently, GCASH has also implemented an STK-based system containing the above functionality, but the original system is still in common use and it is unclear what the adoption rate of the newer system is.

Endemic to this class of application is obfuscation of security details, either through limiting claims to very broad statements or through appeal to industry standards (e.g. ISO 27001 [34] and PCI DSS [24]) which have no requirement of actual analysis of protocols, particularly when no clear best practice exists.

2.2 Little Targets

Myriad smaller scale offerings of similar services exist around the globe, backed by central banks, NGOs, and corporations alike. These, however, tend to have a significantly weaker security profile than the larger entities.

Representative examples include two bank-led efforts in El Salvador: Movibanca [17], based in Guatemala with backing from HSBC, Banco Internacional, Banco Reformador, Citibank, and G&T Continental, and BAC Movil [1], run by Banco de America Central. A 2008 study by USAID [32] notes that messages between the handsets and the base stations in both cases are sent in cleartext via SMS, protected only by whatever encryption the mobile carrier chooses to use.

2.3 Attackers

For the sake of my analysis, I will only consider attackers with a reasonable (i.e. sub-governmental) amount of resources to bring to bear on the problem. The canonical example of this might be organized crime rings or companies engaging in industrial espionage.

2.3.1 Replay

Most of the SMS-based services (GCASH, Movibanca, BAC Movil) are vulnerable to simple interception and replay. These messages are protected only by A5, and in the developing world, the dummy A5/0 and weak A5/2 algorithms are far more commonplace than the somewhat stronger A5/1. This means an attacker with commodity hardware such as a USRP and appropriate scanning software could capture messages travelling in either direction. Additionally, even when encryption is used for the traffic channel of GSM, SMS is sent in the clear by default [35], meaning additional configuration is necessary to ensure that these messages are protected at all. Finally, 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.

In addition to the above concerns, as SMS is neither guaranteed reliable nor in-order, it's possible that transactions will never reach, will reach out of order, or be sent multiple times under the assumption that a message was lost and then execute multiple times.

USSD based solutions are more resistant to replay, as USSD is a session-based protocol, making it simpler to identify irregular transaction flows than with a sessionless protocol like SMS.

2.3.2 Spoofing

As mentioned earlier, SIM cards have been cloned in the wild, and although updated algorithms have been circulated to GSM providers, it is unclear whether these updated versions are currently in use. This is particularly true in regimes which may wish a blanket regulation to prevent strong encryption. For instance, India's IT Act of 2000 mandates that no encryption be used anywhere in India [25], though it makes no attempt to define what encryption is or at what layer of service this law may apply. As a result, no Indian GSM carrier uses traffic encryption.

In any milieu in which SIM cloning is practicable, spoofing is a real and present danger, particularly for SMS-based systems which do not have a robust authentication protocol above and beyond piggybacking on the GSM layer's authentication. USSD-based applications are also vulnerable to this if they choose not to provide additional authentication via STK's cryptographic APIs or implement the related protocols poorly.

Even in cases where an additional authentication factor is required, e.g. a PIN number or other secret information, the factor becomes moot if the traffic can be intercepted and decoded, even if this decoding does not occur in realtime.

2.3.3 Denial of Service

Denial of Service for GSM is trivially simple to implement with very inexpensive hardware. A USRP can be configured with the same MNC and MCC as a valid carrier, e.g. 02 and 639 respectively for Safaricom in Kenya, and given sufficiently strong signal output, can cause any phones nearby to associate to it rather than to Safaricom, leading to a loss in service. This is a particular issue for USSD-based solutions which do not recover cleanly from interrupted transactions if a mobile reassociates to the false base station in the middle of an ongoing transaction.

In addition, given that some networks, particularly in the developing world, have suboptimal architectures or aging equipment, the amount of traffic necessary to cause significant DoS is lower than it could be. Significantly, anecdotal accounts indicate that M-PESA in particular was, as of August, already operating with a four-day lead time to process incoming messages and forward acknowledgments to recipients [18], indicating that it is already somewhat inundated with requests.

A USRP can also conceivably be configured to masquerade as a mobile handset or GSM modem and clog the channel with radio resource requests and other control requests on the GSM control channels (FACCH, SACCH, SDCCH) with different IMSI's and prevent other handsets from transmitting, particularly at higher power levels.

A denial of service attack which can cause a phone to deactivate itself is also possible with a USRP by sending a signal to IMSIs which connect to it to disable themselves. Remediation requires a hard reboot of the handset at best and unlocking by the manufacturer at worst.

Finally, a simple jammer can be used to selectively jam GSM frequencies. Such a device can be made for less than $100 depending on output wattage.

2.3.4 *Man in the Middle*

Man in the Middle attacks are potentially the most hazardous, and the barriers to entry for this have recently decreased significantly with the advent of OpenBTS and the USRP device.

As mentioned in the previous section, USRPs can be configured to transmit an arbitrary MNC and MCC, and spoof a valid carrier. It can also use a high-power transmitter to force the C1 cell-selection algorithm to prefer it over the genuine base station, particularly where coverage is sparse, such as the very rural or developing areas in which these mobile banking applications operate. As the base station is responsible for dictating the level of encryption it supports, it can negotiate any associating handset down to A5/0. While handsets are mandated by relevant GSM standards to have the ability to indicate to the user what encryption mode is being used, the behavior is set by a bit on the SIM, which in turn is set by the carrier. In most cases, this bit is deactivated and the user has no idea when his calls are being sent in the clear.

3G/UMTS adds an additional hurdle insofar as it authenticates the network to the phone in addition to authenticating the phone to the network; therefore the phone can have confidence that the network is not masquerading. However, since UMTS and GSM operate on different frequencies, it is straightforward to jam those frequencies UMTS operates on and force the handsets back to GSM mode.

Once a handset is associated with a false base station, any number of steps can be taken to attack the system. Given sophisticated enough software and a spoofed SIM, the USRP can listen to traffic sent in the clear and send it to the base station, altering the traffic inline if it is sent without encryption in addition to that used by GSM. In addition, as of the currently deployed Java Card 2.2.2 specification [12], SIM Toolkit applications do not appear to have any way to determine the GSM ciphering mode that is active during communications with the base station. Having a false base station also reduces barriers to some of the attacks listed above.

3. A CONCRETE EXAMPLE

Given the above attack vectors, several strategies seem immediately apparent to attack, for instance, GCASH. GCASH is the largest system carrying the most funds. Using any phone with a field testing mode, e.g. any Nokia S60 phone, one can ascertain the level of encryption used for SMS. If it is A5/0 decryption is trivial. If A5/2, slightly more difficult but still theoretically achievable in realtime using only ciphertext. If A5/1, offline decryption may prove necessary. However, using a USRP, the handset can be negotiated down to A5/0, and as the handset has no concrete indication that the connection is unencrypted, the user is easily fooled into providing his PIN via an SMS. Given SMS's unauthenticated OA, an attacker can rig a handset with the legitimate user's IMSI and send a transaction using the captured IMSI and PIN of an arbitrary amount to an arbitrary number, and can repeat this as many times as he is able to capture a unique IMSI's transaction.

4. REMEDIATION

All of the attack vectors mentioned above can be prevented or mitigated with adaptations of standard techniques used in wired network protocols. The SIM Toolkit, when installed on an appropriate SIM device such as units supporting cryptographic hardware from Gemalto, Giesecke & Devrient, and Oberthur, provides rich cryptographic primitives including AES and 3DES.

However, the inchoate state of applications built in SIM Toolkit coupled with the secrecy involved in developing the security standards associated with 2G GSM lend to the lack of a consistent, open standard which can be used by interested parties without having to reinvent the security wheel.

Consistent use of 3DES with three separate keys, ensuring keys are never sent over the air even in ostensibly encrypted form, compression or obfuscation to alleviate known-plaintext attacks, intelligent use of unique transaction identifiers, and other simple strategies which are commonplace in the ecommerce realm on the wired internet would go a long way toward preventing a catastrophic attack on systems which are clearly carrying more and more funds as time goes on.

The creation of an RFC-style standard with specific description of a secure protocol layer and the necessary primitives, akin to the TLS specifications is a desirable course of action in order to ensure the security of these transactions.

5. CALL TO ACTION

I posit that while 2G GSM standards are aging and Europe and the rest of the developed world are moving forward with 3G and beyond, the need for improved security for the 2G GSM system has never been more pressing. With millions of dollars in flux at any given time and the heterogeneous quality of security, branchless banking solutions in rural and developing nations in particular are becoming a more attractive target over time. In addition, as most of these funds are held in small quantities by people who otherwise have little or no access to banks, any victims of theft or fraud in the context of these systems would have little recourse to legal assistance. Finally, and perhaps most importantly, the first high-profile break of such a system has a high likelihood of souring both world and local opinion on the efficacy and security of such systems. In particular, that they are more secure than the 'mud banks' - buried caches of money - that many unbanked users would turn to otherwise, would come into question.

I propose the development of a clear and open reference standard for secure communications methodology which is agnostic to encryption in the carrier channel. This standard should be established by both relevant players in the field (Safaricom Vodafone, Zain, and others) as well as security researchers to provide a reliable, clear best practices framework rather than relying on bespoke protocol implementations from each entity and security through obscurity. It is my position that such a protocol standard will increase the proliferation of these services as well as both their real and perceived security. It will furthermore allow firms to focus on service delivery rather than details of assembling security primitives into a working protocol.

6. CONCLUSION

In this paper I have presented an overview of the status quo of 2G GSM security, with particular focus in the developing world. In particular, I have outlined challenges faced by the nascent mobile branchless banking industry and have put forward the need to establish a standard application-level protocol layer for secure communications using SIM Toolkit analogous to TLS to allow providers of value-added services to safely abstract security considerations away from their applications.

7. ADDENDUM, JANUARY 2010

In the time since this paper was initially submitted for publication, additional cracks have appeared in the security foundation upon which the GSM system is built. Karsten Nohl, chief research scientist at a California security consultancy called H4RDW4RE, has built on attack concepts initially introduced by David Hulton and "Steve" of The Hacker's Choice (THC) [33] and created an A5/1 session key rainbow table which theoretically allows a fully passive attack capable of intercepting A5/1 traffic without need to force handsets to associate with false terminals [39]. Such an attack would be effectively undetectable and could harvest vast amounts of information from A5/1-encrypted SMS and USSD channels in preparation for a concerted strike on one of the aforementioned microfinance targets.

In addition, Adi Shamir, Orr Dunkelman, and Nathan Keller have published a related-key attack on A5/3 [23] which is the most sophisticated of the A5 family, used in 3G/UMTS networks. While this is mostly an academic attack as it requires known plaintext and several related keys (which should be difficult to obtain in practice unless the implementation is flawed), the fact that it requires "4 related keys, 2^{56} data, 2^{30} bytes of memory, and 2^{32} time" as opposed to the 2^{128} brute-force time requirement of the best known attack on its progenitor MISTY [37] raises questions about the longevity of this cryptosystem.

8. ACKNOWLEDGMENTS

I would like to thank Aditya Dhananjay, Faiz Kazi, and Ashlesh Sharma as well as various colleagues for input and feedback in the course of preparing this paper.

I would also like to thank various personal friends and members of the microfinance community for describing the problem addressed by the proposed solution herein.

9. REFERENCES

[1] BAC Movil. https://www.bac.net/regional/esp/banco/bacmovil.html.

[2] *ETSI I-ETS 300 034-1 ed.1 (1993-10), European digital cellular telecommunications system (Phase 1);Radio subsystem link control (GSM 05.08)* . ETSI, October 1993.

[3] *ETSI ETS 300 534 ed.1 (1994-09), European digital cellular telecommunications system (Phase 2); Security related network functions (GSM 03.20).* ETSI, September 1994.

[4] *ETSI ETS 300 535 ed.1 (1995-02), European digital cellular telecommunications system (Phase 2);Functions related to Mobile Station (MS) in idle mode (GSM 03.22).* ETSI, Februrary 1995.

[5] *ETSI GTS GSM 11.14 V5.9.0 (1998-11), Digital cellular telecommunications system (Phase 2+) (GSM);Specification of the SIM application toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface (GSM 11.14 version 5.9.0 Release 1996).* ETSI, November 1998.

[6] CellBazaar: Market In Your Pocket. http://www.cellbazaar.com/web/, 2009.

[7] DeCryption. https://svn.berlin.ccc.de/projects/airprobe/wiki/DeCryption, 2009.

[8] Ettus Research, LLC. http://www.ettus.com/, 2009.

[9] Globe - GCASH. http://site.globe.com.ph/web/gcash?sid=1milwr3hbfhum1255917099422, 2009.

[10] History - GSM World. http://www.gsmworld.com/about-us/history.htm, 2009.

[11] ip.access. http://www.ipaccess.com/, 2009.

[12] Java Card Platform Specification 2.2.2. http://java.sun.com/javacard/specs.html, 2009.

[13] JavaRosa. http://code.javarosa.org/, 2009.

[14] M-PESA. http://www.safaricom.co.ke/index.php?id=745, 2009.

[15] M-pesa: Connecting urban and rural communities. http://www.cgap.org/p/site/c/template.rc/1.26.11223/. August 2009.

[16] mChek. http://main.mchek.com/pdf/mchek-brochure.pdf, 2009.

[17] Movibanca. http://www.movibanca.com, 2009.

[18] Mpesa Overload? Technically impossible unless... http://www.kachwanya.com/?p=516, August 2009.

[19] OpenBTS. http://www.kestrelsp.com/OpenBTS.html, 2009.

[20] The OpenBTS Project. http://openbts.sourceforge.net/, 2009.

[21] Welcome to mChek. http://main.mchek.com/, 2009.

[22] Zain Kenya - Zap. http://www.ke.zain.com/en/zap/index.html, 2009.

[23] Another Week, Another GSM Cipher Bites the Dust. http://www.emergentchaos.com/archives/2010/01/another_week_another_gsm.html, 2010.

[24] P. D. 1.2.1. *Payment Card Industry (PCI) Data Security Standard - Requirements and Security Assessment Procedures.* Payment Cards Industry Security Standards Council, July 2009.

[25] N. Ahmad. Restrictions on cryptography in india - a case studyof encryption and privacy. *Computer Law & Security Review*, 25(2):173 – 180, 2009.

[26] G. Americas. Gsm technologies to reach 4 billion mobile connections worldwide. http://www.3gamericas.org/index.cfm?fuseaction=pressreleasedisplay&pressreleaseid=2451, August 2009.

[27] E. Barkan, E. Biham, and N. Keller. Instant ciphertext-only cryptanalysis of gsm. pages 600–616. Springer-Verlag, 2003.

[28] A. Biryukov, A. Shamir, and D. Wagner. Real Time Cryptanalysis of A5/1 on a PC. In *Fast Software Encryption Workshop 2000*, New York, NY, 2000.

[29] A. Bogdanov, T. Eisenbarth, and A. Rupp. A Hardware-Assisted Realtime Attack on A5/2 Without Precomputations. In *Proceedings of the 9th International Workshop on Cryptographic Hardware*

and Embedded Systems, pages 394–412, Vienna, Austria, 2007.

[30] I. Goldberg and G. L. Wagner, D. The Real-Time Cryptanalysis of A5/2. Rump Session of Crypto 1999. Talk., 2009.

[31] L. Grossman. Iran Protests: Twitter, the Medium of the Movement. *Time Magazine*, June 2009.

[32] E. Hamilton and R. Tapia. Mobile Phone Banking Feasability Assessment in El Salvador. microREPORT #146. White paper., September 2008.

[33] D. Hulton and Steve. Cracking GSM. Talk, Black Hat 2008, August 2008.

[34] ISO 27001:2005. *ISO/IEC 27001:2005 - Information technology – Security techniques – Information security management systems – Requirements.* ISO, Geneva, Switzerland, October 2005.

[35] S. Lord. Trouble at the Telco: When GSM Goes Bad. *Network Security*, 2003(1):10–12, January 2003.

[36] B. Lorica. Mobiles and Money in the Developing World. *Release 2.0*, April 2009.

[37] M. Matsui. New Block Encryption Algorithm MISTY. *Lecture Notes in Computer Science*, (1267), 1997.

[38] O. Morawczynski. What you don't know about M-PESA. `http://technology.cgap.org/2009/07/14/what-you-dont-know-about-m-pesa/`. July 2009.

[39] K. Nohl. GSM: SRSLY? Talk, 26th Chaos Communications Congress, December 2009.

[40] B. Potter. Gsm security. *Network Security*, 2004(5):4 – 5, 2004.

[41] D. Wagner and I. Goldberg. GSM Cloning. `http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html`, April 1998.