Title: Cell phone cloning: A perspective on GSM security

Authors:

1. Ramesh Singh, Senior Technical Director, National Informatics Center, New Delhi, India (www.home.nic.in)

2. Preeti Bhargava, undergraduate student, Delhi College of Engineering, New Delhi, India (www.dce.edu)

3. Samta Kain, undergraduate student, Delhi College of Engineering, New Delhi, India (www.dce.edu)

Mr. Steve Andrews almost got a heart attack after seeing his monthly mobile bill for $8000. He contacted his cell phone provider to let them know that somebody else is also using his cellphone without his knowledge but they weren't interested in helping him and asked him to pay.

Are your mobile phone bills unexpectedly high like that of Mr. Andrews? Then there is a chance that you might be a victim of "mobile cloning". It is also known as cell phone piracy and has been taking place throughout the world since decades.

1. What is Cell Phone Cloning?

Cell phone cloning or mobile cloning is copying the identity of one mobile telephone to another mobile telephone. Usually this is done for the purpose of making fraudulent telephone calls. The bill for the calls goes to the legitimate subscriber.

2. How is a phone cloned?

The **"**cloning**"** occurs when the account number of a victim telephone user is stolen and reprogrammed into another cellular telephone. Every cell phone is supposed to have a unique factory-set Electronic Serial Number (ESN) and Mobile Identification Number (MIN). A cloned cell phone is one that has been reprogrammed to transmit the ESN and MIN belonging to another (legitimate) cell phone. Unscrupulous people can obtain valid ESN/MIN combinations by illegally monitoring the radio wave transmissions from the cell phones of legitimate subscribers. After cloning, both the legitimate and the fraudulent cell phones have the same ESN/MIN combination and cellular systems cannot distinguish the cloned cell phone from the legitimate one. The legitimate phone user then gets billed for the cloned phone's calls.

Cellular thieves can capture ESN/MINs using devices such as cell phone ESN reader or digital data interpreters (DDI). An ESN reader is a cellular telephone receiver designed to monitor the control channel. The ESN reader captures the pair as it is being broadcast from a cellular telephone to a cell site and stores the information into its memory. What makes this possible is the fact that each time your cellular telephone is turned on or used; it transmits the pair to the local cellular site and establishes a talk channel. It also transmits the pair when it is relocated from one cell site to another. DDIs are devices specially manufactured to intercept ESN/MINs. By simply sitting near busy roads where the volume of cellular traffic is high, cellular thieves monitoring the radio wave transmissions from the cell phones of legitimate subscribers can capture ESN/MIN pair. Numbers can be recorded by hand, one-by-one, or stored in the box and later downloaded to a computer. ESN/MIN readers can also be used from inside an offender's home, office, or hotel room, increasing the difficulty of detection.

Softwares are available to clone even CDMA and GSM phones. CDMA uses spread spectrum techniques for transmitting voice or data over the air. Rather than dividing the radio frequency spectrum into separate user channels by frequency slices or time slots, spread spectrum technology separates users by assigning them digital codes within the same broad spectrum. GSM is a digital mobile telephone system that is widely used in Europe and other parts of the world. GSM uses a variation of TDMA and is the most widely used of the three digital wireless telephone technologies. GSM digitizes and compresses data, then sends it down a channel with two other streams of user data, each in its own time slot. The ubiquity of the GSM standard makes international roaming very common between mobile phone operators, enabling subscribers to use their phones in many parts of the world.

However, one of the greatest threats to GSM is due to the flaws in the encryption and authentication algorithms used, which can be then exploited.

3. Global Service for Mobile communications (GSM)

GSM is a cellular network, which means that mobile phones connect to it by searching for cells in the immediate vicinity. GSM networks operate in four different frequency ranges. Most GSM networks operate in the 900 MHz or 1800 MHz bands. There are four different cell sizes in a GSM network - macro, micro, pico and umbrella cells. The coverage area of each cell varies according to the implementation environment. Macro cells can be regarded as cells where the base station antenna is installed on a mast or a building above average roof top level. Micro cells are cells whose antenna height is under average roof top level; they are typically used in urban areas. Picocells are small cells whose diameter is a few dozen meters; they are mainly used indoors. On the other hand, umbrella cells are used to cover shadowed regions of smaller cells and fill in gaps in coverage between those cells. Cell radius varies depending on antenna height, antenna gain and propagation conditions from a couple of hundred meters to several tens of kilometers.

4. Architecture of GSM Network

A GSM network is composed of several functional entities and can be divided into three broad parts. The Mobile Station is carried by the subscriber; the Base Station Subsystem controls the radio link with the Mobile Station. The Network Subsystem, the main part of which is the Mobile services Switching Center, performs the switching of calls between the mobile and other fixed or mobile network users, as well as management of mobile services, such as authentication. The Mobile Station and the Base Station Subsystem communicate across the Um interface, also known as the air interface or radio link. The Base Station Subsystem communicates with the Mobile service Switching Center across the A interface.

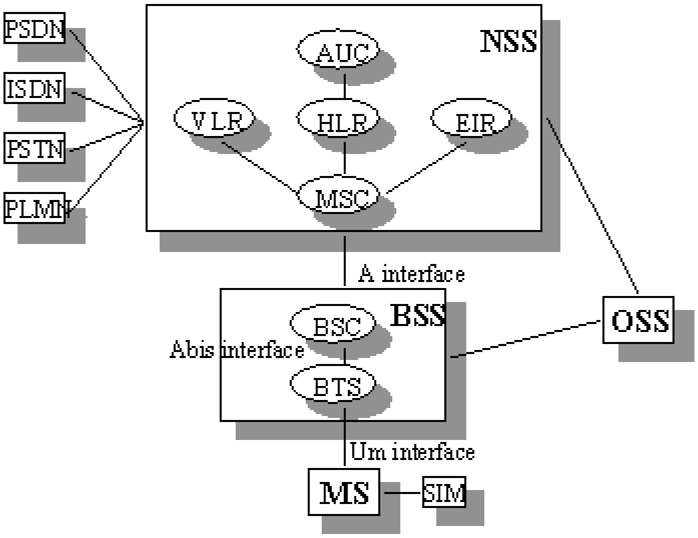

Figure [1] Architecture of a GSM network [15]

4.1 Mobile Station

The mobile station (MS) consists of the physical equipment, such as the radio transceiver, display and digital signal processors, and a smart card called the Subscriber Identity Module (SIM). The SIM provides personal mobility, so that the user can have access to all subscribed services irrespective of both the location of the terminal and the use of a specific terminal. By inserting the SIM card into another GSM cellular phone, the user is able to receive calls at that phone, make calls from that phone, or receive other subscribed services.

The mobile equipment is uniquely identified by the International Mobile Equipment Identity (IMEI). The SIM card contains the International Mobile Subscriber Identity (IMSI), identifying the subscriber, a secret key for authentication, and other user information. The IMEI and the IMSI are independent, thereby providing personal mobility. The SIM card may be protected against unauthorized use by a password or personal identity number.

4.2 Base Station Subsystem

The Base Station Subsystem is composed of two parts, the Base Transceiver Station (BTS) and the Base Station Controller (BSC). These communicate across the specified Abis interface, allowing (as in the rest of the system) operation between components made by different suppliers.

The Base Transceiver Station houses the radio transceivers that define a cell and handles the radiolink protocols with the Mobile Station. The Base Station Controller manages the radio resources for one or more BTSs. The BSC is the connection between the mobile and the Mobile service Switching Center (MSC). The BSC also translates the 13 kbps voice channel used over the radio link to the standard 64 kbps channel used by the Public Switched Telephone Network (PSTN) or Integrated Services Digital Network (ISDN).

4.3 Network Subsystem

The central component of the Network Subsystem is the Mobile services Switching Center (MSC). It acts like a normal switching node of the PSTN or ISDN, and in addition provides all the functionality needed to handle a mobile subscriber, such as registration, authentication, location updating, handovers, and call routing to a roaming subscriber. These services are provided in conjunction with several functional entities, which together form the Network Subsystem.

The Home Location Register (HLR) and Visitor Location Register (VLR), together with the MSC, provide the callrouting and (possibly international) roaming capabilities of GSM. The HLR contains all the administrative information of each subscriber registered in the corresponding GSM network, along with the current location of the mobile. The current location of the mobile is in the form of a Mobile Station Roaming Number (MSRN) which is a regular ISDN number used to route a call to the MSC where the mobile is currently located. There is logically one HLR per GSM network, although it may be implemented as a distributed database.

The Visitor Location Register contains selected administrative information from the HLR, necessary for call control and provision of the subscribed services, for each mobile currently located in the geographical area controlled by the VLR. The other two registers are used for authentication and security purposes. The Equipment Identity Register (EIR) is a database that contains a list of all valid mobile equipment on the network, where each mobile station is identified by its International Mobile Equipment Identity (IMEI). Some implementations of EIRs list the IMEIs of banned Mobile Stations; some list the IMEIs of permitted terminals; and some list all terminals. There are three responses to an IMEI query:

- Whitelisted – The MS is permitted to connect to the network.
- Greylisted – The MS can connect to the network, but there may be problems with this equipment. Either way, it should be investigated.
- Blacklisted – The MS is not permitted to connect to the network.

An IMEI is marked as invalid if it has been reported stolen or is not type approved. The Authentication Center (AC or AuC) is a protected database that stores a copy of the secret key stored in each subscriber's SIM card, which is used for authentication and ciphering of the radio channel.

4.4 Mobile Subscriber Roaming

When a mobile subscriber roams into a new location area (new VLR), the VLR automatically determines that it must update the HLR with the new location information, which it does using an SS7 Location Update Request Message. (Signaling System #7 (SS7) is a telecommunications protocol suite used by the telephone companies for interoffice signaling). The Location Update Message is routed to the HLR through the SS7 network, based on the global title translation of the IMSI that is stored within the Signaling Connection Control Part (SCCP) Called Party Address portion of the message. (Signaling Connection Control Part is a routing protocol in SS7). The HLR responds with a message that informs the VLR whether the subscriber should be provided service in the new location.

4.5 Mobile Subscriber ISDN Number (MSISDN) Call Routing

When a user dials a GSM mobile subscriber's MSISDN, the PSTN routes the call to the Home MSC based on the dialed telephone number. The MSC must then query the HLR based on the MSISDN, to attain routing information required to route the call to the subscribers' current location.

The MSC stores global title translation tables that are used to determine the HLR associated with the MSISDN. When only one HLR exists, the translation tables are trivial. When more than one HLR is used however, the translations become extremely challenging, with one translation record per subscriber. Having determined the appropriate HLR address, the MSC sends a Routing Information Request to it.

When the HLR receives the Routing Information Request, it maps the MSISDN to the IMSI, and ascertains the subscribers' profile including the current VLR at which the subscriber is registered. The HLR then queries the VLR for a Mobile Station Roaming Number (MSRN). The MSRN is essentially an ISDN telephone number at which the mobile subscriber can currently be reached. The MSRN is a temporary number that is valid only for the duration of a single call.

The HLR generates a response message, which includes the MSRN, and sends it back across the SS7 network to the MSC. Finally, the MSC attempts to complete the call using the MSRN provided.

5. Cryptography Fundamentals

Cryptography is the study of message secrecy. Cryptography includes encryption, the process of converting ordinary information (plaintext) into coded text (i.e. ciphertext). Cryptanalysis includes Decryption, which is the reverse of encryption, and involves converting ciphertext to plaintext. Cryptology includes both cryptography (art of devising ciphers) and cryptanalysis (art of breaking ciphers). A cipher (or cypher) is a pair of algorithms which perform this encryption and the reversing decryption. The detailed operation of a cipher is controlled both by the algorithm and, in each instance, by a key. A key is a piece of information that controls the operation of a cryptography algorithm. In encryption, a key specifies the particular transformation of plaintext into ciphertext, or vice versa during decryption.

Public key cryptography, also known as asymmetric cryptography, is a form of cryptography in which a user has a pair of cryptographic keys - a public key and a private key. The private key is kept secret, while the public key may be widely distributed. The keys are related mathematically, but the private key cannot be practically derived from the public key. A message encrypted with the public key can only be decrypted with the corresponding private key. The method works like this : A person, say A, wanting to communicately secretly with another person, say B, uses B’s public key as the encryption key to encrypt a message and sends it to B. B can then decrypt the message using his/her private key as the decryption key. No one else can read the encrypted message because the encryption system is assumed strong and because it is difficult to derive the private decryption key from the public encryption key.

CRAM (challenge-response authentication mechanism) is a scheme for authenticating network users that is used as part of the Web's Hypertext Transfer Protocol (HTTP). Using the CRAM, the server (or, alternatively, a proxy server or gateway) issues a challenge to a user in the form of a "401 unauthorized" request for a password. The password is a string of characters known only to the user and the server. When the server receives the user response, it checks to be sure the password is correct. If so, the user is authenticated. If not, or if for any other reason the network does not want to accept the password, a "403 forbidden" message is issued, and access to the site is denied.

6. Cryptography in GSM

The encryption mechanisms used in GSM utilize algorithms (A), keys (K), random number challenges (RAND) and signed responses (SRES).

The GSM mobile phone cryptography techniques are employed in phones to protect the privacy of their cellular voice and data communication. When a customer wishes to establish communication over their cellular phone, they are first authenticated by a challenged-response digital signature scheme, for billing purposes etc. After the customer has been authenticated, they can then transfer information encrypted using a key based stream-cipher algorithm known as A5.
Suppose a GSM customer wants to place a secure call on his GSM phone. Inside his phone is a Subscriber Identity Module, also known as a SIM card. The SIM card contains a private key Ki that uniquely identifies the customer’s phone. The key is also stored in a private database in a GSM base station. Also stored on customer's SIM card is a one-way hash function known as A3. When the customer's phone establishes a connection to the GSM network, the phone receives a 128 bit random number RAND from a base station. The customer's phone then computes a signed response SRES = A3 (RAND, Ki) and sends it back to the base station. Mean while the base station makes the same computation and compares it to the SRES sent by the customer's phone. If the numbers match then customer is authenticated and may continue otherwise customer receives an authentication failure and the connection is dropped.

After the customer is authenticated, his phone gets a 64 bit cipher text key Kc that is computed using another one-way key based hash function called A8 with the same RAND used in authentication, i.e. Kc = A8(RAND, Ki). Then Kc is fed into the A5 algorithm stored on the customer’s phone and all the data transfer from then on is encrypted using the A5 algorithm. Mean while the base station performs the same computations and uses the key Kc with the A5 algorithm to decrypt the data sent by the customer. Note that in both the authentication and in the data transfer, neither of the keys is transmitted over the network since the base station has the information necessary to produce both of the keys.

6.1 A3, the MS Authentication Algorithm

The authentication algorithm used in GSM security model is A3. Its function is to generate the SRES response to the MSC's random challenge, RAND, which the MSC has received from the HLR. The A3 algorithm generates a 32 bit output known as the SRES response after it gets the RAND from the MSC and the secret key Ki from the SIM as input. Both the RAND and the Ki secret are 128 bits long.

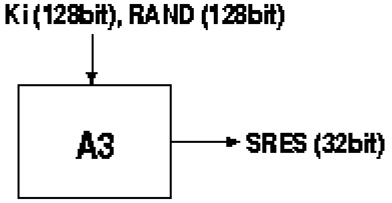

Figure [2] Signed response (SRES) calculation

Nearly every GSM operator in the world uses an algorithm called COMP128 for both A3 and A8 algorithms. COMP128 is the reference algorithm for the tasks pointed out by the GSM Consortium. The COMP128 takes the RAND and the Ki as input, but it generates 128 bits of output, instead of the 32-bit SRES. The first 32 bits of the 128 bits form the SRES response.

6.2 A8, the Voice-Privacy Key Generation Algorithm

The key generation algorithm used in GSM security model is the A8 algorithm. The A8 generates the session key, Kc, from the random challenge, RAND, received from the MSC and from the secret key Ki. The A8 algorithm generates a 64-bit output from two 128 bits input. This output is the 64-bit session key Kc. This is the same Kc which the BTS receives from the MSC. HLR is able to generate the Kc, because the HLR knows both the RAND (the HLR generated it) and the secret key Ki, which it holds for all the GSM subscribers of this network operator. One session key, Kc, is used until the MSC decides to authenticate the MS again. This might take days.

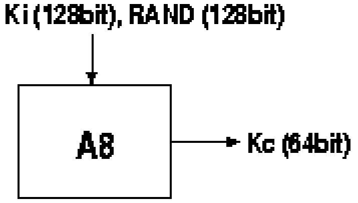

Figure [3] Session key (Kc) calculation

Both the A3 and A8 algorithms are stored in the SIM in order to prevent people from tampering with them. This means that the operator can decide, which algorithms to use independently from hardware manufacturers and other network operators.

6.3 Description of A5/1 Algorithm

A GSM conversation is sent as a sequence of frames every 4.6 millisecond. Each frame consists of 114 bits representing the communication from A to B, and 114 bits representing the communication from B to A. Each conversation can be encrypted by a new session key K. For each frame, K is mixed with a publicly known frame counter Fn, and the result serves as the initial state of a generator which produces 228 pseudo random bits. These bits are XORed (Exclusive ORed) by the two parties with the 114+114 bits of the plaintext to produce the 114+114 bits of the cipher text.

Algorithm A5/1 comprises of R1, R2 and R3, the three linear shift registers (LFSR) of lengths 19, 22 and 23 bits respectively with the rightmost bit labeled as bit zero. The taps of R1 are at bit positions 13, 16, 17, 18; the taps of R2 are at bit positions 20, 21; and the taps of R3 are at bit positions 7, 20, 21, 22 (see Figure 1). The taps of a register are XORed together whenever a register is clocked with the result being stored in the rightmost bit of the left shifted register. At each clock cycle, the majority function of the clocking taps (bit 8 for R1, bit 10 for R2 and bit 10 for R3) is calculated and if the clocking tap of a register is in agreement with the majority bit, then the register is clocked.

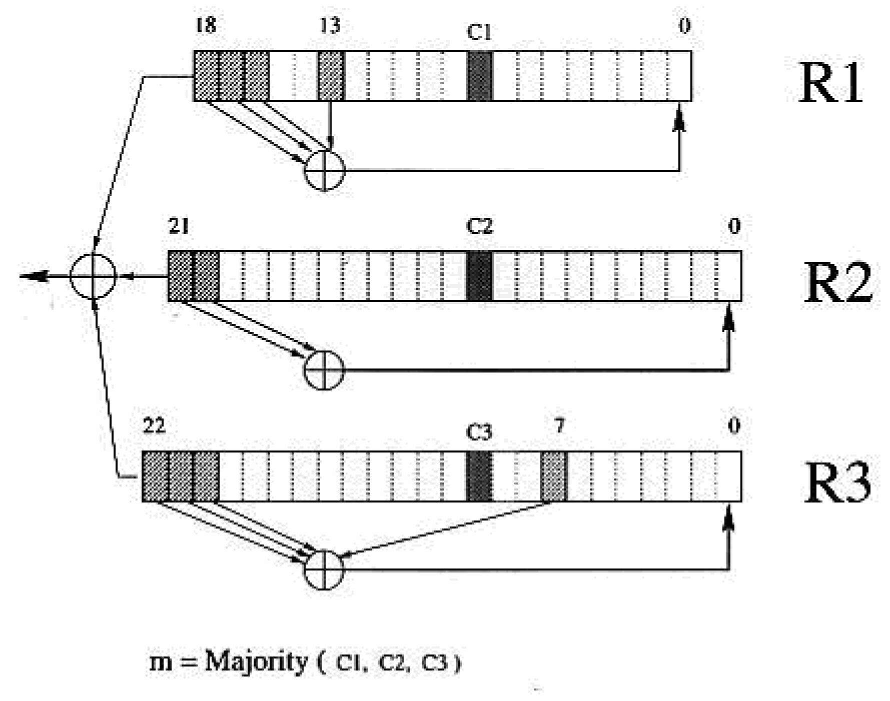

Figure [4] the A5/1 Stream Cipher

To generate the pseudo random bits from the session key *K* and the frame counter F_n, initially R1, R2 and R3 are zeroed and then clocked for 64 clock cycles. Each bit of K (from LSB to MSB) is XORed in parallel into the LSBs of the three registers. The initial state of the frame is obtained when the three registers are again clocked for another 22 cycles, ignoring the stop/go control. Each bit of the Fn (LSB to MSB) is then XORed in parallel into the LSBs of the three registers. - The three registers are clocked for 100 additional clock cycles with the stop/go clock control but without producing any outputs. In order to produce the 228 output bits, R1, R2 and R3 are again clocked for 228 cycles with the stop/go control. At each clock cycle, one output bit is produced as the XOR of the MSBs of the three registers.

7. Breaking the algorithms

7.1 Breaking the A3 and A8 algorithms

Most GSM providers use a version of COMP128 for both the A3 authentication algorithm and the A8 key generation algorithm.

Ian Goldberg and David Wagner of the University of California at Berkeley demonstrated [4],[5] that all A8 implementations they looked at, including the few that did not use COMP128, were deliberately weakened. By sending large number of challenges to the authorization module, they were able to deduce the Ki within several hours. They also discovered that Kc uses only 54 bits of the 64 bits. The remaining 10 bits are replaced by zeros, which makes the cipher key purposefully weaker.

Josyula R. Rao, Pankaj Rohatgi and Helmut Scherzer of IBM and Stephane Tinguely of the Swiss Federal Institute of Technology showed a method[6] by which COMP128 can be broken in less than a minute.

The COMP128-2 and COMP128-3 algorithms have been developed to address the security issues of COMP128-1. COMP128-2 and COMP128-3 are secret algorithms which have not been subject to cryptanalysis. COMP128-3 overcomes the loophole where 10 bits of the Session Key (Kc) were set to zero.

GSM network operators are slowly migrating from COMP128 (also known as COMP128-1) to COMP28-2 or COMP128-3. Because the A3 and A8 algorithms are stored in the Subscriber Identity Module, this requires changing the GSM subscribers SIM cards.

7.2 Breaking the A5 algorithm

Alex Biryukov, Adi Shamir and David Wagner showed [7] that they can find the A5/1 key in less than a second on a single PC with 128 MB RAM and two 73 GB hard disks, by analyzing the output of the A5/1 algorithm in the first two minutes of the conversation.

Ian Goldberg and David Wagner of the University of California at Berkeley published [8] an analysis of the weaker A5/2 algorithm showing a work factor of 2^16, or approximately 10 milliseconds.

Elad Barkhan, Eli Biham and Nathan Keller of Technion, the Israel Institute of Technology, have shown [9] a ciphertext-only attack against A5/2 that requires only a few dozen milliseconds of encrypted off-the-air traffic. They also described new attacks against A5/1 and A5/3.

These attacks on the algorithms make the SIMs susceptible to cloning.[17]

8. The Future – 3RD Generation Partnership Project(3GPP)

The 3G radio access link security was built on the security of GSM. 3G security tries to correct the problems with GSM by addressing security weaknesses and by adding new features. The 3G security has the following security features: mutual authentication and key agreement between MS and network, encryption of user traffic and signaling data over the air interface, and integrity protection of signaling data over the air interface.

The encryption of the user traffic and the signaling data over the air interface is performed through an algorithm called KASUMI, which has an open design process, taking a longer cipher key length (128-bit) derived during authentication. The encryption terminates at the RNC, a 3G entity similar to the BSC. The links BS-RNC that may be over microwave are thus ciphered. KASUMI is also used for the integrity protection of commands (critical signaling) between MS and RNC.

9. Conclusion

Although the GSM network was designed to be a secure mobile system and it did provide strong subscriber authentication and over-the-air transmission encryption, it is now vulnerable to some attacks targeted at different parts of an operator's network. The main reason is that some of the algorithms and specifications were leaked out, analyzed and some critical flaws were found (see section 7). However, the security can be improved by adopting new measures (see section 8).

10. References:

[1]. http://www.gsm-security.net/
[2]. http://www.crypto.com/papers/others/a5.ps
[3]. http://jya.com/crack-a5.htm
[4]. www.isaac.cs.berkeley.edu/isaac/mobicom.pdf
[5]. www.it.kth.se/courses/2G1723/lectures/encryption.pdf
[6]. http://www.research.ibm.com/intsec/gsm.ps
[7]. http://www.cs.berkeley.edu/~daw/papers/a51-fse00.ps
[8]. http://cryptome.org/a51-bsw.htm
[9]. http://www.gsm-security.net/papers/a3a8.shtml
[10]. http://www.gsm-security.net/papers/a51.shtml
[11]. http://en.wikipedia.org/wiki/Public-key_cryptography
[12]. http://en.wikipedia.org/wiki/Encryption
[13]. http://en.wikipedia.org/wiki/Cryptography
[14]. http://rf-web.tamu.edu/security/secguide/V2comint/Cellular.htm
[15]. http://www.cs.ucl.ac.uk/staff/t.pagtzis/wireless/gsm/arch.html
[16]. http://whatis.techtarget.com/
[17]. http://www.cellular.co.za/gsm_sims_hacked.htm
[18] http://www.3gpp.org/TB/Other/algorithms.htm
[19]. B. Schneier. *Applied Cryptography: Protocols, Algorithms and Source Code in C*. John Wiley and Sons, Inc., New York, NY, USA, second edition, 1996.