Threats and Countermeasures in GSM Networks

Valer BOCAN
Department of Computer Science and Engineering, Politehnica University of Timişoara, Romania
Alcatel Romania, IT S&D Department
E-mail: vbocan@dataman.ro

Vladimir CREŢU
Department of Computer Science and Engineering, Politehnica University of Timişoara, Romania
E-mail: vladimir.cretu@cs.upt.ro

***Abstract*–Mobile networks not only provide great benefits to their users but they also introduce inherent security issues. With respect to security, the emerging risks of denial of service (DOS) attacks will evolve into a critical danger as the availability of mobile networks becomes more and more important for the modern information society. This paper outlines a critical flaw in GSM networks which opens the avenue for distributed denial of service attacks. We propose a way to mitigate the attacks by adding minimal authentication to the GSM channel assignment protocol.**

***Keywords*–security, denial of service, attack, wireless networks, GSM, GPRS, 2G, DREAD**

I. INTRODUCTION

Wireless telephony exceeds land telephony in terms of number of subscriptions in most of the European and Asian countries and the new generation of GPRS and 3G devices truly enable mobile Internet access. Widespread acceptance of 802.11 and Bluetooth enable seamless integration of laptop, PDA and cell phone platforms with support for powerful new mobile applications. The immense benefits of ubiquitous networking do come with a unique set of risks.

Wireless technology is extremely complex. Unfortunately, radio engineers are almost never security experts and the general tendency is to consider that security will be added later, if required. This is a very unhealthy way of thinking since security must be "blended" together with the radio technology. Another major mistake that is often done is to consider that security procedures are sophisticated enough as to deter attacks of any kind. This is wrong. An attacker may never attempt to attack a strong cryptographic system instead will choose the weakest link in the communication chain. That link is the radio domain.

This judgment has already resulted in some careless implementations, such as the IEEE 802.11b/g WEP and Bluetooth [1]. These systems had no initial security analysis, with the assumption that commercial security mechanisms may simply be added at a later stage.

This paper is structured as follows: Section 2 describes security issues in wireless networks, section 3 outlines the current security mechanisms in GSM networks (authentication, encryption, key lengths), section 4 describes and ranks according to severity the threats on GSM networks, section 5 gives a detailed anatomy of a denial of service attack on a GSM network and shows the attacker profile and attack economics, section 6 describes authors' proposed DOS mitigation technique and outlines the deployment issues associated with it. Finally, section 7 summarizes the subject of the paper and the main contributions.

II. SECURITY IN WIRELESS NETWORKS

Security in wireless networks is an important issue since users are likely to put personal, important or mission-critical data over an infrastructure that is not truly secure. The security weaknesses stem from both using multiple incompatible security schemes and design flaws in security protocols, which is inherent. The greatest danger is that the user may perceive the entire structure as secure and may mistakenly trust it to convey confidential information. The wireless environment poses many security issues, such as confidentiality, authentication, integrity, authorization, non-repudiation and accessibility. Other issues may include convenience, speed, ease-of-use and standardization [2]. Therefore, the security strategy must be devised and implemented with respect to the type of data being transported and the estimated loss in case of eavesdropping or tampering with the data. We have to also consider the fact that many security issues arise due to poor implementation, feature interactions, unplanned growth and new flaws created due to prior attacks (Figure 1). Taking denial of service attacks as a reference, although this type of attack does not directly corrupt the data, here's no reason not to believe that another kind of subversive action is in preparation or in progress [3].

Based on "Mitigating Denial of Service Threats in GSM Networks", by Valer BOCAN and Vladimir CREŢU which appeared in the Proceedings of the First International Conference on Availability, Reliability and Security (ARES) Wien, Austria, April 2006.

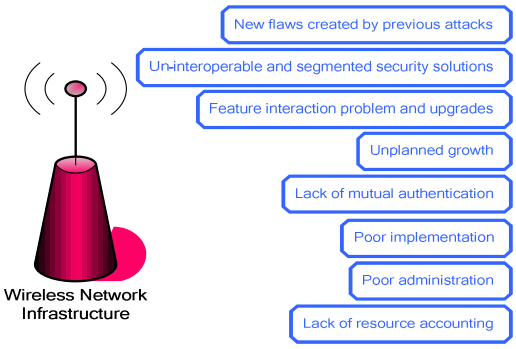

Figure 1. Security issues in wireless networks

To be truly effective, the security strategy must be applied end-to-end, i.e. from source to destination regardless of path. For example, WAP provides security using WTSL (Wireless Transport Security Layer), but this is not necessarily end-to-end security since encryption takes place only between the mobile device and the WAP gateway [5].

III. Security Mechanisms in GSM Networks

Security and confidentiality in GSM were some of the reasons for which it was considered superior to other mobile communication systems and the tremendous success has inspired other systems such as Code Division Multiple Access (CDMA), Personal Handy Phone System (PHS), and Digital Enhanced Cordless Telecommunications (DECT). Another great enhancement over traditional mobile systems was the introduction of the SIM (Subscriber Identifier Module) card which clearly separated the mobile device from the subscriber. The SIM card contains the *International Mobile Subscriber Identity* (IMSI) and a *Subscriber Identification Key* (K_i), both used to authenticate the client against the GSM network. GSM security relies on three algorithms: A3 and A8 for authentication and A5 for encryption.

With more than 1 billion users worldwide, GSM is a potential target for several kinds of attacks. The easiest to mount are the low tech attacks, such as call forwarding to premium numbers (depending on the network operator), bogus registration details, roaming fraud and terminal theft. Fraud management systems monitor a variety of indicators, such as multiple calls at the same time, large variations in revenue paid to other parties, large variations in duration of calls (very short or very long), changes in customer usage (indicating that a mobile has been stolen or is being abused) and closely monitoring customer during a probationary period [13].

The GSM system has several security-related issues:

- Communication and signaling traffic are not protected when connected to fix networks, therefore the GSM network is only as secure as the fixed network to which it connects.
- GSM infrastructure does not address active attacks, such as identity cashing, camping on a false BTS, eavesdropping, etc.
- Lawful interception was considered as an after-thought.
- Cryptographic and authentication mechanisms are very difficult to upgrade.
- Lack of user visibility of security mechanisms (the user is not aware how secure his data really is).

There are five acknowledged attacker capabilities that influence the security in GSM networks (Table 1). The first capability is the easiest to achieve. Subsequent capabilities imply more investment from the attacker and we assume that an intruder having a certain capability also has all lower ranked capabilities [13].

Table 1. Attacker capabilities

Difficulty ↓	
	Eavesdropping The capability of an intruder to intercept traffic and signaling information associated to other users. The required equipment is a modified mobile phone.
	Impersonation of a user This is the capability of sending rogue data and/or signaling messages to the network with the intent of making them appear from another user. This again only requires a modified mobile phone.
	Impersonation of the network This is the capability of sending rogue data and/or signaling messages to another user with the intent of making them appear from a genuine network. This requires a modified BTS.
	MITM – Man-In-The-Middle This is the capability of an attacker to put itself between the network and the legitimate user in order to eavesdrop, modify, delete, re-order, re-play and spoof signaling data between the two parties. This requires a modified BTS in conjunction with a modified mobile phone.
	Network Authentication Compromise The intruder possesses a compromised authentication vector (challenge-response pairs, cipher keys, integrity keys, etc.)

Eavesdropping and user impersonation were two issues known at the time 2G security was developed. 3G security however aimed at protecting against all issues.

A. Authentication

Client authentication is performed by a simple challenge-response algorithm as shown in Figure 2. The GSM Authentication Center (AuC) generates a random 128-bit number and sends it to the mobile station via radio link. This number and the subscriber key (K_i) are fed to the A3 algorithm which produces a signed response (SRES) which is in turn sent back to the AuC. Meanwhile, AuC has already computed its own SRES based on the same inputs and it is now capable of deciding whether the mobile station is who it says it is. There are several issues with this design. The A3 (authentication) and A8 (key generation) algorithms are operator specific and they are best kept secrets. This is obscurity rather than security. It is well known the fact that a secret authentication or encryption algorithm may be vulnerable since it does not benefit from the experience of the cryptanalytic community who may try to uncover flaws and errors in design.

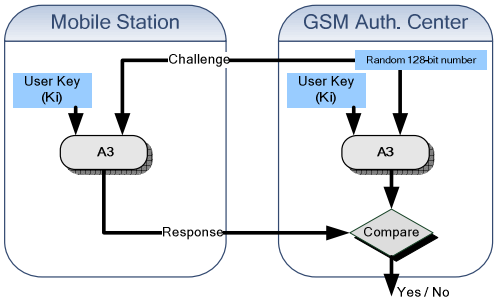

Figure 2. Authentication in GSM networks

In the software world, when a program claims to employ a new secure algorithm that is several times as fast as DES or AES, chances are that the algorithm is nothing more than a series of XORs. The requirement to run on a smart card (such as the SIM) has a severe impact on the practical implementation. Thus, 3rd Generation Partnership suggests default implementations for A3 and A8 as a simple series of XOR operations, fact which demonstrates our point [9]. Surprisingly, the fact the SRES in only 32 bit long has little impact on the security in the case of a birthday attack since this quantity is used in conjunction with the random key from the AuC and the number of successful eavesdrops is thus 1.84 x 10^{19} ($2^{128/2}$) rather than 65536 ($2^{32/2}$). For more information on birthday attacks see [10].

B. Encryption

Unlike A3 and A8, the GSM standard specifies the A5 algorithm, used for encrypting the speech, data and signaling information over the radio link. The information is encoded two frames at a time (2 x 114 bits), one for uplink and the other one for downlink. In the initial design (called A5/1), the session key K is mixed with the frame counter to initialize a set of 3 registers that will produce the 228 bit output by XORing the LFSR with the plaintext.

A partial source code implementation of the GSM A5 algorithm was leaked to the Internet in June 1994. Rumors go that this implementation was an early design and bears little resemblance to the A5 algorithm currently deployed. Nevertheless, insight into the underlying design theory can be gained by analyzing the available information. The details of this implementation, as well as some documented facts about A5, are summarized below [12]:

- A5 is a stream cipher consisting of three clock-controlled LFSRs of degree 19, 22 and 23.
- The clock control is a threshold function of the middle bits of each of the three shift registers.
- The sum of the degrees of the three shift registers is 64.
- The 22-bit TDMA frame number is fed into the shift registers.
- Two 114-bit key streams are produced for each TDMA frame, which are XOR-ed with uplink and downlink traffic channels.
- It is rumored that the A5 algorithm has an "effective" key length of 40 bits.

A disagreement between cellular telephone manufacturers and the British government centering on export permits for the encryption technology in GSM was settled by a compromise in 1993. Western European nations and a few other specialized markets such as Hong Kong would be allowed to have the GSM encryption technology, in particular the A5/1 algorithm. A weaker version of the algorithm (A5/2) was approved for export to most other countries, including Central and Eastern European nations [11]. This is mainly a political issue which involves privacy rights of the individual, the ability of law enforcement agencies to conduct surveillance and the business interests of corporations manufacturing cellular hardware for export.

The simple design of A5/1 eventually proved insecure and it was broken around April 1998 by Ian Goldberg and David Wagner who also succeeded to break the A5/2 algorithm in as few as 5 clock cycles. This is very uncomfortable for anyone who uses the GSM infrastructure for private communication.

For domestic uses, the GSM security proves far better than the analog cellular systems. The use of authentication, encryption and temporary identification numbers ensures the privacy and anonymity of users as well as preventing fraudulent use. Even GSM systems with the A5/2 encryption algorithm or with no encryption are inherently more secure than analog systems.

C. Key Length

When designing or deploying cryptographic algorithms, the natural question that comes is how long should the key be? Unfortunately there is no single answer to this question as there are several variables, such as the value of the protected data, secrecy time and an approximate estimation of the attacker resources. The world renowned cryptologist Bruce Schneier emphasizes the close relationship between the value of the data and the effort to encrypt it. For instance, a customer list may be worth $1000. Financial data for an acrimonious divorce case might be worth $10,000. Advertising and marketing data for a large corporation might be worth $1,000,000 and the master keys for a digital cash system might be worth billions of dollars [4, 14]. Similarly, there is also a relationship between the secrecy time and the effort to encrypt the data. In the world of commodity trading, secrets only need to be kept for minutes. In the newspaper business, today's secrets are tomorrow's headlines and the U.S. Census data are required by law to remain secret for 100 years. Table 2 (cited from Ref. [14]) shows the security requirements for different kinds of information.

Going back to the GSM system, if we overlook the proven security flaws in the A5 design and consider the key length as the only security factor, it is interesting to see how long it would take to decrypt a message with a given key length, assuming a cracking machine capable of 1 million encryptions per second [12]. The time required to break a 128 key is extremely large. For comparison, the age of the universe is believed to be 1.6 *

10^{10} years. Assuming that the effective key length of the A5 algorithm is 40 bits, it currently provides adequate protection for information with a short lifetime; however it shouldn't be used to transfer confidential information with a lifetime longer than approximately two weeks.

Table 2. Security requirements for different information

Type of traffic	Lifetime	Key Length
Tactical military information	Minutes / hours	56-64 bits
Product announcements, interest rates	Days / weeks	64 bits
Business plans	Years	64 bits
Trade secrets (e.g. recipe for Coca-Cola)	Decades	112 bits
H-bomb secrets	> 40 years	128 bits
Identities of spies	> 50 years	128 bits
Personal affairs	> 50 years	128 bits
Diplomatic embarrassments	> 65 years	At least 128 bits
U.S. Census Data	100 years	At least 128 bits

IV. THREATS ON GSM NETWORKS

In order to successfully understand the threats on communication system, we need a way to rank and categorize them. In this paper we will use a threat ranking methodology named DREAD.

A. The DREAD Threat Ranking

Howard and LeBlanc introduced a risk assessment methodology called DREAD [17]. This alarmist, but appropriate, name is an acronym from the following terms:

- **Damage potential**

How great can the damage be? Measure the extent of actual damage possible with the threat. Typically, the worst score is 10, representing a threat that allows the attacker to circumvent all security restrictions and do virtually anything.

- **Reproducibility**

How easy is it to get a potential attack to work? Measures how easy it is to get a threat to become an exploit. High reproducibility is important for most attackers to benefit.

- **Exploitability**

How much effort and expertise is required to mount an attack? For example, if a novice programmer with a home PC can mount the attack, that would score a big fat 10, but a national government needing to invest $100,000,000 to mount an attack is probably 1. Also consider what degree of authentication and authorization is required to attack the system. For example, if an anonymous remote user can attack the system, it ranks 10, while a local user exploit requiring strong credentials has a much lower exploitability.

- **Affected users**

If the threat were exploited and became an attack, how many users would be affected? This measures roughly what percentage of users would be impacted by an attack: 91–100 percent (10) on down to 0–10 percent (1). We need to think about market size and absolute numbers of users, not just percentages. One percent of 100 million users is still a lot of affected people!

- **Discoverability**

This is probably the hardest metric to determine and we always assume that a threat will be taken advantage of, so we label each threat with a 10.

Each item is evaluated on a scale from 1 to 10, according to the consequences it has on the system.

In the following paragraphs we apply the DREAD threat ranking methodology to some known GSM security flaws in order to determine which one of them should be addressed first in the event of an infrastructure upgrade. Some of the following security flaws are mentioned in [13].

B. Denial of Service Attacks

The GSM radio interface is vulnerable to denial of service attacks as scarce resources such as signaling channels are blindly granted to anyone who requests them. Flooding the signaling channels with rogue or legitimate requests essentially means that the traffic channel is paralyzed. The flood on the signaling channel may be caused by a misbehaving mobile station [16] or by genuine requests [15]. The next section contains an extensive description of denial of service attacks.

$Risk_{DREAD} = (5 + 10 + 7 + 9 + 10) / 5 = 8.2$

C. De-registration Spoofing

An attacker may spoof a de-registration request (IMSI detach) to the network. This means that the user is detached from the visited location area and is thus inaccessible to network paging requests. The net result is that all mobile terminated services will fail.

$Risk_{DREAD} = (3 + 10 + 5 + 1 + 10) / 5 = 5.8$

D. Location Update Spoofing

This attack is similar to the previous one. The attacker spoofs a location update request in a different location area from the one in which the user is roaming. Again, the net result is that all mobile terminated services fail.

$Risk_{DREAD} = (3 + 10 + 5 + 1 + 10) / 5 = 5.8$

E. Camping on a False BTS

The mobile phone can be enticed to camp on a rogue BTS, making it inaccessible to paging signals of the serving network. Alternately, the rogue BTS may act as a relay and let traffic through at will. This attack requires a modified BTS.

$Risk_{DREAD} = (3 + 10 + 4 + 1 + 10) / 5 = 5.6$

F. Passive Identity Caching

Under certain circumstances, the network may request the user to send its identity in plain text. A modified

mobile station can be used to cache the information for other uses.

$Risk_{DREAD} = (2 + 8 + 5 + 1 + 10) / 5 = 5.2$

G. Active Identity Caching

This attack is similar to the previous one, except that the user may be enticed to camp on a false BTS which in turn continuously requests that the mobile identity be sent unencrypted.

$Risk_{DREAD} = (2 + 8 + 4 + 1 + 10) / 5 = 5$

H. Encryption Suppression

As the mobile station has no way of authenticating messages over the radio interfaces, it may be enticed to camp on a false BTS and communicate with the attacker in an unencrypted mode. The attacker can spoof the cipher mode command and it maintains the call for as long as the attack is needed and it remains undetected.

$Risk_{DREAD} = (2 + 10 + 3 + 1 + 10) / 5 = 5.2$

I. Compromised Cipher Key

This is an attack that requires a modified BTS and the possession by the intruder of a *compromised authentication vector* and thus exploits the weakness that the user has no control upon the cipher key. The target user is enticed to camp on the false BTS/MS. When a call is set-up the false BTS/MS forces the use of a compromised cipher key on the mobile user.

$Risk_{DREAD} = (2 + 8 + 3 + 1 + 10) / 5 = 4.8$

J. Eavesdropping on User Data by Suppressing Encryption

This attack that requires a modified BTS/MS and that exploits the weakness that the MS cannot authenticate messages received over the radio interface. The target user is enticed to camp on the false BTS. When the target user or the intruder initiates a call the network does not enable encryption by spoofing the cipher mode command. The attacker however sets up his own connection with the genuine network using his own subscription. The attacker may then subsequently eavesdrop on the transmitted user data.

$Risk_{DREAD} = (2 + 10 + 2 + 1 + 10) / 5 = 5$

K. Suppression of Encryption between Target User and True Network

The target user is enticed to camp on the false BTS/MS. When the target user or the genuine network sets up a connection, the false BTS/MS modifies the ciphering capabilities of the MS to make it appear to the network that a genuine incompatibility exists between the network and the mobile station. The network may then decide to establish an un-enciphered connection. After the decision not to cipher has been taken, the intruder may eavesdrop on the user data.

$Risk_{DREAD} = (2 + 10 + 2 + 1 + 10) / 5 = 5$

L. Eavesdropping on User Data by Forcing the Use of a Compromised Cipher Key

This is an attack that requires a modified BTS/MS and the possession by the intruder of a compromised authentication vector and thus exploits the weakness that the user has no control the cipher key. The target user is enticed to camp on the false BTS/MS. When the target user or the intruder set-up a service, the false BTS/MS forces the use of a compromised cipher key on the mobile user while it builds up a connection with the genuine network using its own subscription.

$Risk_{DREAD} = (2 + 10 + 2 + 1 + 10) / 5 = 5$

M. User impersonation with compromised authentication vector

This attack requires a modified MS and the possession by the intruder of a compromised authentication vector which is intended to be used by the network to authenticate a legitimate user. The intruder uses that data to impersonate the target user towards the network and the other party.

$Risk_{DREAD} = (2 + 10 + 2 + 1 + 10) / 5 = 5$

N. User impersonation through eavesdropped authentication response

The attack requires a modified MS and exploits the weakness that an authentication vector may be used several times. The intruder eavesdrops on the authentication response sent by the user and uses that when the same challenge is sent later on. Subsequently, ciphering has to be avoided by any of the mechanisms described above. The intruder uses the eavesdropped response data to impersonate the target user towards the network and the other party.

$Risk_{DREAD} = (2 + 10 + 5 + 1 + 10) / 5 = 5.6$

O. Hijacking outgoing calls in networks with encryption disabled

This attack requires a modified BTS/MS. While the target user camps on the false base station, the intruder pages the target user for an incoming call. The user then initiates the call set-up procedure, which the intruder allows to occur between the serving network and the target user, modifying the signaling elements such that for the serving network it appears as if the target user wants to set-up a mobile originated call. The network does not enable encryption. After authentication the intruder cuts the connection with the target user, and subsequently uses the connection with the network to make fraudulent calls on the target user's subscription.

$Risk_{DREAD} = (4 + 10 + 5 + 1 + 10) / 5 = 6$

P. Hijacking outgoing calls in networks with encryption enabled

This attack requires a modified BTS/MS. In addition to the previous attack this time the intruder has to attempt to suppress encryption by modification of the message in which the MS informs the network of its ciphering capabilities.

$Risk_{DREAD} = (4 + 10 + 5 + 1 + 10) / 5 = 6$

Q. Hijacking incoming calls in networks with encryption disabled

This attack requires a modified BTS/MS. While the target user camps on the false base station, an associate of the intruder makes a call to the target user's number. The

intruder acts as a relay between the network and the target user until authentication and call set-up has been performed between target user and serving network. The network does not enable encryption. After authentication and call set-up the intruder releases the target user, and subsequently uses the connection to answer the call made by his associate. The target user will have to pay for the roaming leg.

$Risk_{DREAD} = (4 + 10 + 5 + 1 + 10) / 5 = 6$

R. Hijacking incoming calls in networks with encryption enabled

This attack requires a modified BTS/MS. In addition to the previous attack this time the intruder has to suppress encryption.

$Risk_{DREAD} = (4 + 10 + 5 + 1 + 10) / 5 = 6$

S. Threat Ranking

Table 3 summarizes the threats and their ranks. It is easily observable that the most serious threat is the denial of service attack.

Table 3. GSM threat ranking

Threat	Rank
Denial of Service Attacks	8.2
Hijacking outgoing calls in networks with encryption disabled	6
Hijacking outgoing calls in networks with encryption enabled	6
Hijacking incoming calls in networks with encryption disabled	6
Hijacking incoming calls in networks with encryption enabled	6
De-registration Spoofing	5.8
Location Update Spoofing	5.8
Camping on a False BTS	5.6
User impersonation through eavesdropped authentication response	5.6
Passive Identity Caching	5.2
Encryption Suppression	5.2
Active Identity Caching	5
Eavesdropping on User Data by Suppressing Encryption	5
Suppression of Encryption between Target User and True Network	5
Eavesdropping on User Data by Forcing the Use of a Compromised Cipher Key	5
User impersonation with compromised authentication vector	5
Compromised Cipher Key	4.8

V. Denial of Service Attacks in GSM networks

A. Anatomy of a DOS attack

Denial of service attacks may take several forms of which the most common are causing the network not to transmit messages it should be sending in order to provide a service to legitimate clients or causing the network to send messages it should not. One obvious cause of DOS attacks is that the preliminary communication takes place before authentication and the network commits valuable resources to not-yet-authenticated clients [3]. As such, the network cannot distinguish legitimate traffic from the rogue traffic and there isn't much that can be done.

With respect to computer networks, Spatscheck and Peterson consider that there are three key ingredients for defending against DOS attacks [8]:

- *accounting* for all consumed resources per client;
- *detection* when the resources consumed by any given client exceed some limit;
- *containment* – the ability to reclaim the tied resources after detecting an attack by dedicating minimum additional server resources to the task and thus avoiding to fall for a follow-up denial of service attack;

Although the GSM technology was designed with security in mind and that was touted as one of the reasons for its superiority over analog systems, we cannot talk about end-to-end security as the security mechanism relate to the radio domain only. As radio resources are limited, GSM has efficient resource accounting that in part relies on the mobile stations to function properly. This implies that mobile stations must strictly adhere to standards, which is the case today. However, as with any software driven device, chances are that the software or the firmware will eventually be reverse engineered and the modified version will not adhere to the standard. This is one of the greatest challenges in terms of protecting the integrity of the infrastructure.

The typical scenario for the preliminary part of a mobile-originated call is as follows [6]:

Step 1: The mobile station (MS) requests the assignment of a control channel from the base station controller (BSC) (Figure 3).

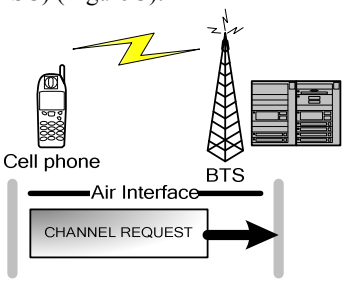

Figure 3. CHANNEL REQUEST message

Step 2: The BTS decodes the CHANNEL REQUEST message, calculates the timing advance (the MS↔BTS distance) and forwards the complete information to the BSC by a CHANNEL REQUIRED message. The type of requested service is also indicated (Figure 4).

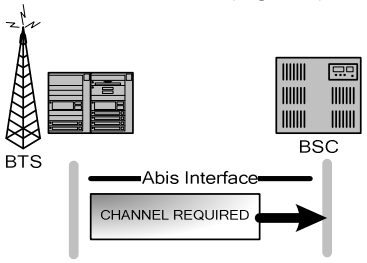

Figure 4. CHANNEL REQUIRED message

Step 3: After receiving and processing a CHANNEL REQUIRED message, the BSC informs the BTS what

channel type and which channel number shall be reserved by a CHANNEL ACTIVE message (Figure 5).

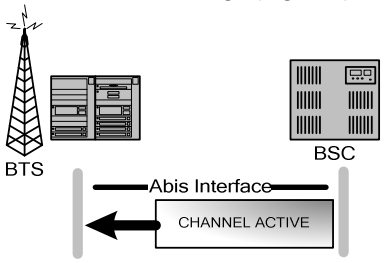

Figure 5. CHANNEL ACTIVE message

Step 4: The BTS acknowledges the receipt by sending a CHANNEL ACTIVE ACKNOWLEDGE message (Figure 6).

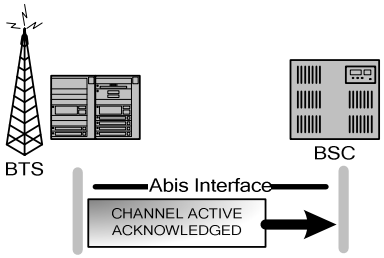

Figure 6. CHANNEL ACTIVE ACKNOWLEDGED message

Step 5: The BSC sends the IMMEDIATE ASSIGNMENT COMMAND message to the BTS which in turn informs the MS upon the allocated channel (Figure 7).

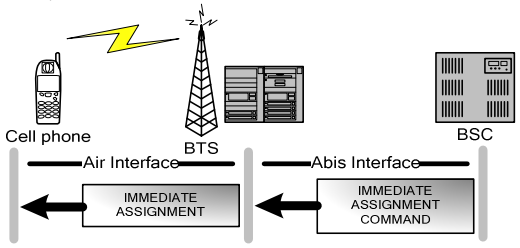

Figure 7. IMMEDIATE ASSIGNMENT message

The complete message exchange of the channel assignment process is shown in Figure 8.

At the end of the channel assignment process, following the request of an **unauthenticated** mobile station (client from our perspective), the BSC has

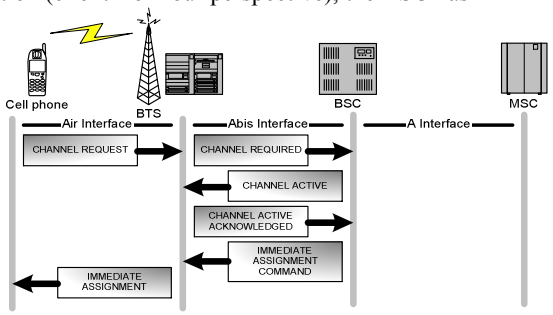

Figure 8. Channel assignment process in GSM

allocated a signaling channel from the pool of available channels. The mobile station is now responsible for complying with the rest of the protocol, the first step being the request of a service type.

Instead of relying on authentication, the design relies on the fact that the mobile station will correctly follow each protocol step. What happens if a malicious mobile station repeats the scenario above and requests several signaling channels without ever continuing the protocol path to the end? Since the number of signaling channels is limited, the network becomes congested locally and legitimate requests are denied due to the lack of available channels. The BSC will eventually time-out the incomplete requests and free the resources, but this is not exactly resource containment since the attack itself is not detected. The available traffic channels will never be serviced to legitimate clients since all signaling channels would be unavailable (Figure 9).

Even if the network did a minimal authentication against the mobile station by asking the IMEI number or the power levels of six neighboring cells, the attack would still be possible since the mobile station has complete control over those and may report false values for power levels and IMEI numbers by generating them on-the-fly or cycling them from a precompiled list. Some mobile phones manufacturers have decided to store the IMEI number in the write-once memory, thus the physical modification of the IMEI is impossible. This does not necessarily hinder the possibility to report back false information.

It is interesting to note that strengthening the SIM security does not improve things from the security standpoint. While the deployment of a SIM-based security solution would be relatively cheap, this will be ineffective as the attack is aimed against the call set-up protocol itself and not the SIM.

B. The Attacker Profile

The recent history recorded many attempts to protect the information by hiding it or at least hardening the ways to discover it. This is what is known as security through obscurity and it is most likely the main source of problems for any system that attempts to secure the data. The security mechanism will eventually be discovered, leaked to interested groups and exploited.

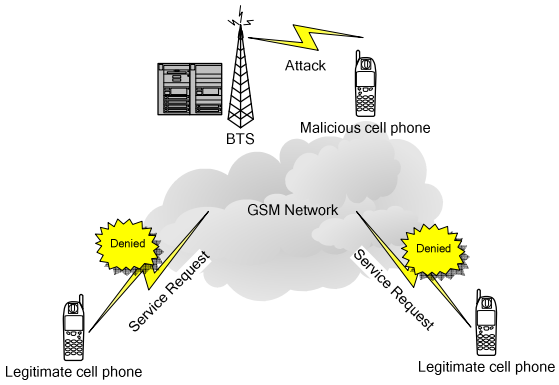

Figure 9. Denial of service attack in a GSM network

Most of the individuals that attack computer or telephony systems have personal motives. Some of them will try to exploit weaknesses for financial gain (free access to resources, free long distance calls, free calls to premium numbers, etc.) and some will present the exploits to relevant groups for fame. Although the attacks are serious and inflict losses on the network operator, denial of service attacks are by far the worst threat. An individual targeted against a vulnerable organization can paralyze the traffic on large areas of the network, causing difficult to estimate financial loss.

In order to successfully attack a GSM network, the intruder must first be able to tamper with the phone firmware in such a way that makes the attack possible. This is no trivial task that requires extensive knowledge of the particular implementation of the mobile device, embedded code and GSM technicalities. This is the most challenging aspect and fortunately not many individuals have that kind of expertise.

The intruder must also get an understanding of the network topology. If the targeted area is local, a simple walk through the city is sufficient to determine the approximate spots where the base transceiver stations (BTS) are located and where the malicious mobile stations will operate. The intruder must not necessarily be present as the mobile phone can be preprogrammed to launch the attack and the city landscape provides plenty of places to hide such small devices.

The intruder must also be motivated, depending on the magnitude of the attack. It is improbable that a single individual may be motivated enough to try to mount a significant attack on a GSM network, especially considering the high cost involved. However, the intruder may be backed up and supported by self-motivated criminal organizations.

C. *Attack Economics*

Due to the ubiquity and the high market value of the GSM networks, the attacks that could potentially bring them down are enticing for criminal organizations. The economics of attacks on GSM networks seems no different than those targeted against computer networks, as follows:

- Attacks that cause total failure of services produce huge revenue losses, not to mention the social impact of the attack.
- When communication is sorely needed, for instance after a terrorist attack or a natural disaster, the DOS attack on the GSM network may have dire consequences. Such lack of communication may cause loss of lives and properties.
- Attacks that cause partial or intermittent service failure are very difficult to spot. A client willing to use the GSM network may have a hard time initiating calls. Piece by piece the trust is eroded and customers may find their way to the competition.

VI. PROPOSED DOS MITIGATION TECHNIQUE

If someone went to your door and asked for something valuable, would you give him that something without asking for his identity? Would you assume that whoever knocked on your door is an honest individual? No matter how hard this is to believe, that is exactly what happens when initiating a call in a GSM network.

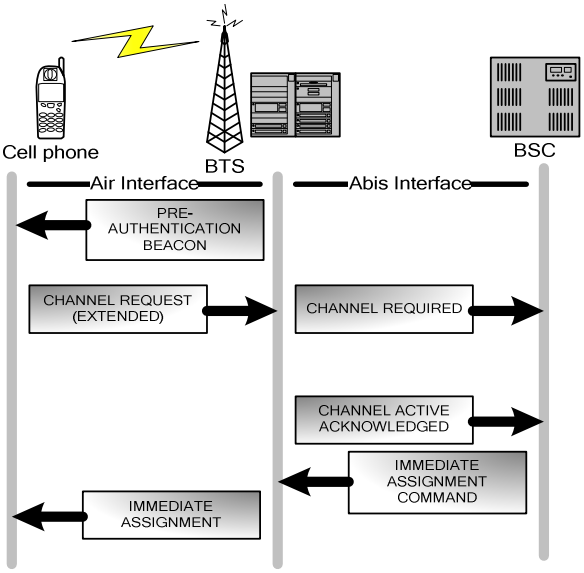

Figure 10. DOS-resistant channel assignment process in GSM

In the process of initiating a call, during the VEA (Very Early Assignment) no authentication or ciphering is performed [7]. The first message sent by the mobile is CHANNEL REQUEST and it is just 1 byte long. It contains the reason for the request (answer to paging, emergency call, etc.) and an identifier for the channel type that the mobile station prefers. The problem with this approach is that the BSC commits its valuable resources to unauthenticated mobile stations which may misbehave. In order to thwart a potential DOS attack, there must be a minimal form of authentication at the time of requesting a communication channel.

We propose a new DOS-resistant channel assignment process for when the system is under attack, as shown in Figure 10.

When the cell congestion threshold is reached, at certain intervals the BTS broadcasts a message called

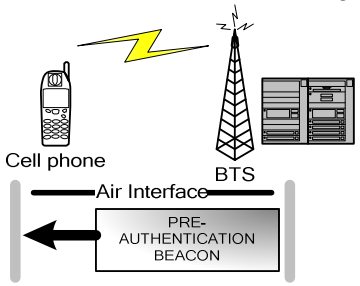

Figure 11. PREAUTHENTICATION BEACON message

PRE-AUTHENTICATION BEACON that delivers a short-lived 128-bit nonce, similar to the one used in the

authentication phase (Figure 11). The nonce has an associated time-to-live value determined by the BSC, so that it is used for a limited amount of time.

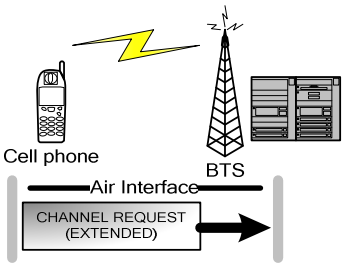

Figure 12. CHANNEL REQUEST (EXTENDED) message

When a new challenge is generated, the BSC will compute the expected response for each registered user key (K_i) for fast subsequent key matches.

The 128-bit nonce is large enough to prevent precomputation of a statistically significant key space, especially given the limited power available in mobile stations. The mobile station stores the latest challenge received and will use it for subsequent channel requests for the time designated by the TTL value. The pre-authentication phase works much like the authentication itself, except that the response is shortened to lower the amount of traffic on the signaling channel (Figure 12). We propose that the response be reduced to 16 bits out of the original 32, and that gives us a space of 65536 values, enough to avoid occasional matches, should the malicious client send a burst of fake requests with random responses. This process is shown in Figure 13.

The extended CHANNEL REQUEST message sent via a random access channel (RACH) must hold both the reason for requesting the resource (as it did in the original version) and the 16-bit pre-authentication response.

Associating this minimal form of authentication with each request for resource assignment at the BSC level ensures that resources cannot be depleted by a single misbehaving mobile station.

A. Deployment issues

As with any upgrade to the network infrastructure (other than software upgrades) the deployment process poses difficulties.

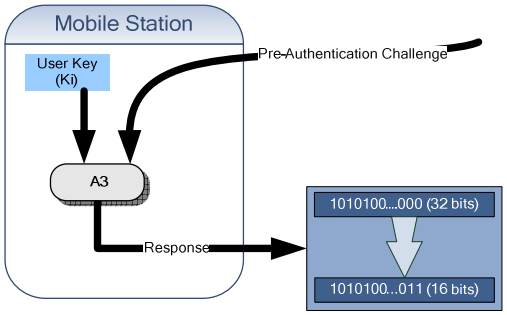

Figure 13. Computing the pre-authentication response

The cost associated to the deployment process must not exceed the benefits. However, in some extreme cases where security is at risk, compromises must be made.

The original GSM security design is very poor and the designers left almost no room for future enhancements. The changes are not negligible and the difficulty that lies beneath deploying the new channel assignment protocol and possibly other countermeasure is enormous. However, given the dangerous potential of the anonymous DOS-attacks possible under the current design, we argue the need to make the switch as soon as feasibly possible.

Considering that the subscriber identity module (SIM) is especially hardened against reverse engineering, our proposition relies on security mechanisms already in place and that will ease the integration of the modified protocol with the existing infrastructure. In our design we use the user key (K_i) and the A3 algorithm, both found in the SIM.

VII. CONCLUSIONS

Security in wireless networks is a complex thing. Whereas in a wired network tapping is usually done by physically accessing the communication links and securing those may improve information security to some extent, in case of wireless networks the information is broadcast over the radio waves and it is readily available to whoever wants to listen. Moreover, radio resources in wireless networks are a valuable commodity and any interference may threaten the availability of network services, hence the need for authentication and resource containment.

With respect to security, we have emphasized the obscurity that surrounds the protocols used for authentication and encryption in GSM networks. This inevitably leads to flawed designs, which poses great risks to anyone who puts personal, important or mission-critical data over such infrastructures.

We have ranked the threats by their damage potential, using the DREAD methodology developed at Microsoft. According to our findings, we argue that the denial of service attack is the most serious one and needs to be addressed first.

We have shown that the GSM technology is vulnerable to denial of service attacks and the resources needed to mount such an attack are dangerously low:

- The attack is possible because the call set-up protocol allocates resources without a minimal authentication.
- A single attacker is capable of disabling an entire GSM cell.
- Since no communication fees are involved (no actual call is made), the effective cost of launching a devastating attack is zero.

We have also proposed a way to add pre-authentication information in the GSM channel assignment protocol. Although not easy to deploy, the proposed technique adds resistance to DOS attacks.

REFERENCES

[1] Alan Burnett, *Securing the Wireless Internet*, Roke Manor Research Ltd, UK, 2003

[2] Upkar Varshney, "Network access and security issues in ubiquitous computing", Workshop on Ubiquitous Computing Environment, Cleveland, 2003

[3] Valer Bocan, "Developments in DOS research and mitigating technologies", *Periodica Politehnica, Transactions on Automatic Control and Computer Science,* Vol. 49 (63), 2004

[4] Niels Ferguson, Bruce Schneier, *Practical Cryptography*, Wiley Publishing, Inc., 2003

[5] Ghosh and Swaminatha, "M-commerce Security", *Communications of the ACM*, February 2001

[6] Gunnar Heine, *GSM Networks: Protocols, Terminology and Implementation*, Alcatel SEL Germany, 1998

[7] Alcatel University, *Introduction to the Alcatel GSM Network*, 2003

[8] Oliver Spatscheck and Larry Peterson, "Defending against denial of service in Scout", In *Proceedings of 3rd USENIX/ACM Symposium on OSDI*, pp.59-72, Feb 1999.

[9] 3rd Generation Partnership Project, *Specification of the GSM-MILENAGE Algorithms: An example algorithm set for Authentication and Key Generation functions A3 and A8,* http://www.gsmworld.com/using/algorithms/docs/55205-600.pdf

[10] William Stallings, *Cryptography and Network Security, Principles and Practices, Third Edition*, Prentice Hall, 2003

[11] Steve Lord, "Bugwatch: GSM security flaws exposed", VNU Business Publications Limited, 2003, http://www.vnunet.com/vnunet/news/2121449/bugwatch-gsm-security-flaws-exposed

[12] David Margrave, *GSM Security and Encryption*, George Mason University

[13] Emmanuel Gadaix, "GSM and 3G Security", *Black Hat Conference Singapore*, April 2001

[14] Bruce Schneier, *Applied Cryptography*, John Wiley & Sons, Inc., 1996

[15] William Enck, Patrick Traynor, Patrick McDaniel, Thomas la Porta, "Exploiting open functionality in SMS-capable cellular networks", *12th ACM Conference on Computer and Communication Security*, 2005

[16] Valer Bocan, Vladimir Cretu, "Mitigating denial of service threats in GSM networks", *The First International Conference on Availability, Reliability and Security – ARES*, Wien, Austria, 2006

[17] Michael Howard, David LeBlanc, *Writing Secure Code*, 2nd Edition, Microsoft Press, 2003

Valer Bocan was born in Deva, Romania. He received the title of engineer in Computer Science from the "Politehnica" University of Timişoara in 1999. He is now a doctoral candidate at the Department of Computer Science and Engineering, Faculty of Automation and Computers at University "Politehnica" of Timisoara, Romania. He also serves as a software architect and a security advisor with the IT S&D department of Alcatel Romania. His research interests include security and privacy of computer and communication systems, digital rights management techniques, cryptography, secure software development practices and RFID devices.

Bocan is a member of the IEEE.

Vladimir Cretu was born in Cluj, Romania. He received the title of engineer in Electronic Computers in 1974 and the Ph.D. degree in Computer Science from the "Politehnica" University of Timişoara in 1984. He is now Professor and Head of the Department of Computer Science and Engineering, Faculty of Automation and Computers at University "Politehnica" of Timisoara, Romania. His research interests include real-time and distributed systems, software for data acquisition and processing systems for electrical machines, instrumentation and measurements, data structures, algorithm design and analysis, embedded systems, computer security and software development processes and techniques.

Prof. Cretu is a member of the IEEE, a professional member of the ACM, and a correspondent member of the Romanian Academy of Technical Sciences.