Mitigating Denial of Service Threats in GSM Networks

Valer BOCAN[*] and Vladimir CREȚU[**]

[*] *Department of Computer Science and Engineering, Politehnica University of Timişoara, Bd. V. Pârvan, 300223 Timişoara, Romania, E-mail: vbocan@dataman.ro, WWW: http://www.dataman.ro*

[**] *Department of Computer Science and Engineering, Politehnica University of Timişoara, Bd. V. Pârvan, 300223 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

1. 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 done more often than not 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: part 2 describes security issues in GSM networks (authentication, encryption, key lengths); part 3 describes a flaw in the channel assignment protocol in GSM networks and estimates the losses that can be incurred as a result of an attack; part 4 describes our proposition regarding DOS attacks in GSM networks and finally part 5 summarizes the main subject of the paper and our contributions.

2. Security in GSM 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 (see 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]. 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].

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 about 1 billion users worldwide, GSM is a potential target for several kinds of attacks. The easiest attacks to mount are the low tech ones, 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].

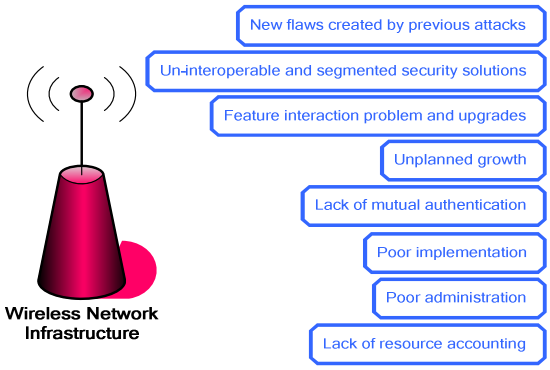

Figure 1. Security issues in wireless networks

2.1. Authentication

Client authentication is performed by a simple challenge-response algorithm as shown in the 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. 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 Project [9] suggests default implementations for A3 and A8 as a simple series of XOR operations, fact which demonstrates our point. 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 1.84×10^{19} ($2^{128/2}$) rather than 65536 ($2^{32/2}$). For more information on birthday attacks see [10].

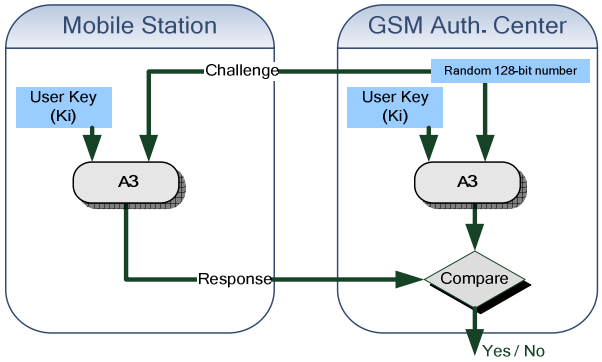

Figure 2. Authentication in GSM networks

2.2. 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 [12]. 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.

2.3. 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 [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 no. 1 (cited from [14]) shows security requirements for different 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 1.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

3. DOS attacks in GSM networks

3.1. 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. As outlined in [3], one obvious cause of DOS attacks is that the preliminary communication takes place before authentication. The network cannot distinguish legitimate traffic from the fake one and there isn't much that can be done.

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

- *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 other cellular systems, the security only relates to the radio link and is intended to stop all but the most determined eavesdroppers. Since radio resources are limited, GSM has a very good resource accounting feature; however, in case of a misbehaving mobile station there is nothing that can be done in terms of resource containment, as we will see below.

The typical scenario for the preliminary part of a mobile-originated call is as follows (see figure 3):

- The MS requests assignment of a control channel from the BSC.
- 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.
- 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.
- The BTS acknowledges the receipt by sending a CHANNEL ACTIVE ACKNOWLEDGE message.
- The BSC sends the IMMEDIATE ASSIGNMENT COMMAND message to the BTS which in turn informs the MS upon the allocated channel.

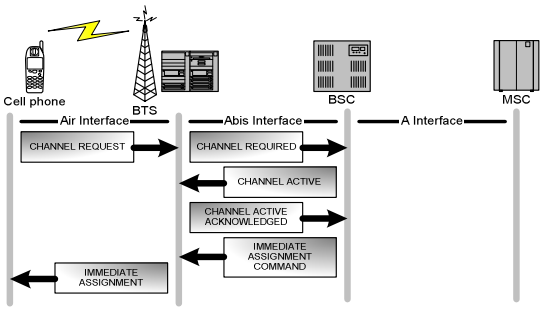

Figure 3. Channel assignment process in GSM

At this point, at the request of an **unauthenticated** mobile station (client from our perspective), the BSC has allocated a signaling channel from the pool of available channels. The mobile station is now responsible for complying with the rest of the protocol, namely requesting a service type.

The entire design relies on the fact that the mobile station will correctly follow each protocol step. What happens if a malicious mobile station repeats the above scenario 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 locally congested 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 (see figure 4).

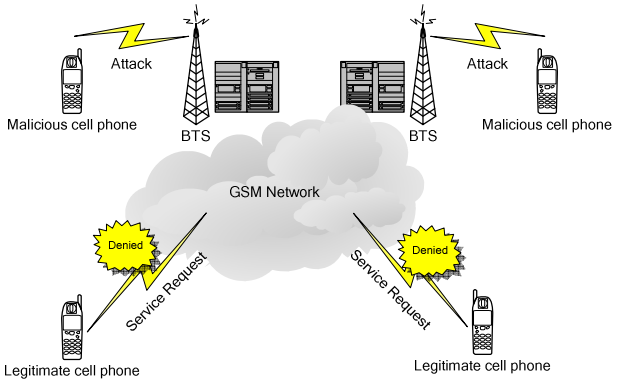

Figure 4. Denial of service attack in a GSM network

Even though the network would do a minimal authentication against the mobile station by asking the IMEI number or the power levels of the 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. Newer models (such as those from Nokia) store the IMEI number in a write-

once memory, thus the physical modification of the IMEI is impossible. This does not necessarily hinder the possibility to report back fake data.

One may suggest that a possible remedy would be strengthening the SIM security. While this would be the preferred method because the deployment would be relatively cheap, this will be useless as the attack is aimed against the call set-up protocol itself and not the SIM.

3.2. The attacker profile

The natural question that arises is what could possibly be an "attacker" or a "malicious mobile station"? The protocols in general are designed assuming that the parties involved behave in-line with the protocol specification. When one of the parties misbehaves, the results are unpredictable.

It is possible to modify portions of the mobile station firmware and determine it to perform the attack as described in the previous paragraph. Having several such mobile stations placed in strategic points within the network and coordinated to mount an attack would most certainly mean denying services of the GSM network for as long as the attack is in progress.

3.3. The economics of DOS attacks

Due to the ubiquity and the high market value of the GSM networks, the attacks that could potentially bring them down can be regarded as enticing. 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 and thus the customer trust is eroded, driving him/her to the competition.

4. Mitigating DOS Attacks

We have shown so far that a denial of service attack is possible because the base station controller (BSC) does not know the identity of the mobile station that makes the request. 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 5.

When the cell congestion threshold is reached, at certain intervals the BTS broadcasts a message called PRE-AUTHENTICATION BEACON that delivers a short-lived 128-bit nonce, similar to the one used in the authentication phase. The nonce has an associated time-to-live value determined by the BSC, so that it is used for a limited amount of time. When a new challenge is generated, the BSC will compute the expected response for each registered user key (K_i) for easier matching.

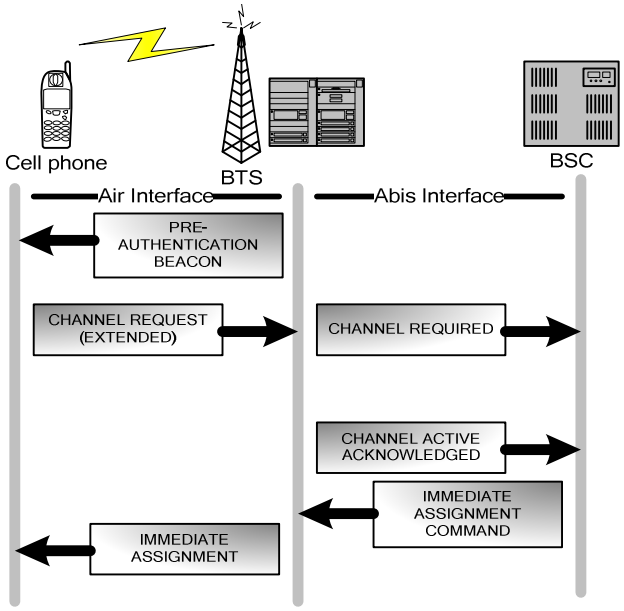

Figure 5. DOS-resistant channel assignment process in GSM

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. 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 6.

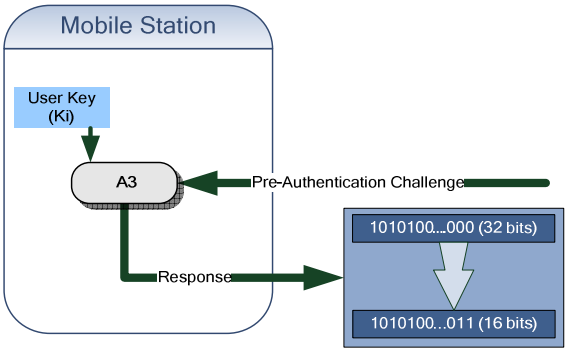

Figure 6. Computing the pre-authentication response

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. We understand that the changes needed in the existing GSM infrastructure are not negligible and the difficulty that lies beneath deploying the new channel assignment protocol 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 extant security mechanisms, so that the incurred changes are minimal. In our design we use the user key (K_i) and the A3 algorithm, both implemented into the SIM.

5. 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. More over, 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 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 difficult to deploy, the proposed technique adds resistance to DOS attacks.

6. 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”, Georgia State University, Atlanta, 2001

[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 (Release 6)”

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

[11] Steve Lord, “Bugwatch: GSM security flaws exposed”, http://vnunet.com/News/1138556, VNU Business Publications Limited, 2003

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

[13] Emmanuel Gadaix, “GSM and 3G Security”, eGlobal, April 2001

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