

Threats and Countermeasures in GSM Networks

K. Vsn Raghu Babu, T. Ravi

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.

Manuscript published on 30 December 2012.

* Correspondence Author (s)

K. Vsn Raghu Babu*, Final Year B.Tech, Ece, KI University, Vaddeswaram (A.P), India.

T. Ravi, Associate Professor B.Tech, Department of ECE, KI University, Vaddeswaram (A.P), India.

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC-BY-NC-ND license <http://creativecommons.org/licenses/by-nc-nd/4.0/>

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, this 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, there is no reason not to believe that another kind of subversive action is in preparation or in progress [3].

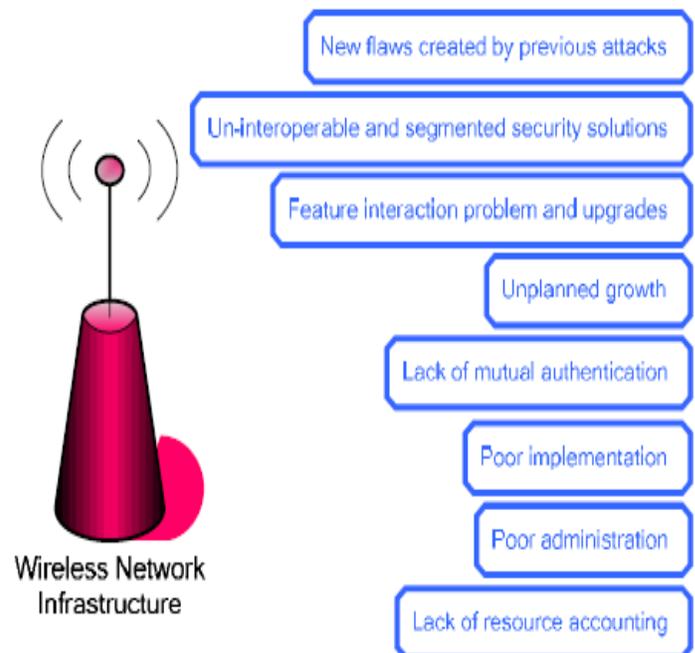


Figure 1. Security issues in wireless networks

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 WTLS (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 (Ki), 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 fixed 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 afterthought.
- 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. 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]. 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. 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 (Ki) 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 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 is 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 $1.84 \times 10^{19} (2^{128}/2)$ 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 into two frames at a time (2×114 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.

A disagreement between cellular telephony 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.

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.

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 rouge 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 (IMSIdetach) 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. $RiskDREAD = (3 + 10 + 4 + 1 + 10) / 5 = 5.6$

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. $RiskDREAD = (2 + 8 + 5 + 1 + 10) / 5 = 5.2$

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. $RiskDREAD = (2 + 8 + 4 + 1 + 10) / 5 = 5$

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. $RiskDREAD = (2 + 10 + 3 + 1 + 10) / 5 = 5.2$

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. $RiskDREAD = (2 + 8 + 3 + 1 + 10) / 5 = 4.8$

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.

$RiskDREAD = (2 + 10 + 2 + 1 + 10) / 5 = 5$

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.

$RiskDREAD = (2 + 10 + 2 + 1 + 10) / 5 = 5$

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.

$RiskDREAD = (2 + 10 + 2 + 1 + 10) / 5 = 5$

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.

$RiskDREAD = (2 + 10 + 2 + 1 + 10) / 5 = 5$

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.

$RiskDREAD = (2 + 10 + 5 + 1 + 10) / 5 = 5.6$

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.

$RiskDREAD = (4 + 10 + 5 + 1 + 10) / 5 = 6$

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.

$RiskDREAD = (4 + 10 + 5 + 1 + 10) / 5 = 6$

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.

$$\text{RiskDREAD} = (4 + 10 + 5 + 1 + 10) / 5 = 6$$

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.

$$\text{RiskDREAD} = (4 + 10 + 5 + 1 + 10) / 5 = 6$$

S. Threat Ranking

It is easily observable that the most serious threat is the denial of service attack.

IV CONCLUSION

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 simultaneously disabling one or more cells, depending on the particular network configuration.
- Since no communication fees are involved (no actual call is made), the effective financial 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 Politecnica, 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.

AUTHOR PROFILE



Kollipara. VSN Raghun Babu was born in Amaravathi, Guntur. He is now pursuing B.Tech Degree in Electronics And Communication engineering from K L University of Guntur. He is interested in Communications and Networking.



Krishnam Raghavendra Sujith born in Kurnool in 1991, pursuing B.tech Degree Electronics and communication engineering in K L University Vijayawada, Andhra Pradesh. Interested in wireless networks.



Kota. Samba Siva Rao was born in 1991 at Vijayawada. He is now pursuing B.Tech Degree in Electronics & Communication Engineering in K L University. He is interested in Communication and Networking.



Tummati Ravi is working as associate professor in K L UNIVERSITY. He is interested in Image Processing.