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 securityissues. With respect to security, the emerging risks of denialof service (DOS) attacks will evolve into a critical danger asthe availability of mobile networks becomes more and moreimportant for the modern information society. This paperoutlines a critical flaw in GSM networks which opens theavenue for distributed denial of service attacks. We proposea way to mitigate the attacks by adding minimalauthentication 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 ofnumber of subscriptions in most of the European andAsian countries and the new generation of GPRS and 3Gdevices truly enable mobile Internet access. Widespreadacceptance of 802.11 and Bluetooth enable seamlessintegration of laptop, PDA and cell phone platforms withsupport for powerful new mobile applications. Theimmense benefits of ubiquitous networking do come witha unique set of risks.Wireless technology is extremely complex.Unfortunately, radio engineers are almost never securityexperts and the general tendency is to consider thatsecurity will be added later, if required. This is a veryunhealthy way of thinking since security must be"blended" together with the radio technology. Anothermajor mistake that is often done is to consider thatsecurity procedures are sophisticated enough as to deterattacks of any kind. This is wrong. An attacker may neverattempt to attack a strong cryptographic system insteadwill choose the weakest link in the communication chain.That link is the radio domain.This judgment has already resulted in some carelessimplementations, such as the IEEE 802.11b/g WEP andBluetooth [1].

These systems had no initial securityanalysis, with the assumption that commercial securitymechanisms may simply be added at a later stage.This paper is structured as follows: Section 2 describessecurity issues in wireless networks, section 3 outlinesthe current security mechanisms in GSM networks(authentication, encryption, key lengths), section 4describes and ranks according to severity the threats onGSM networks, section 5 gives a detailed anatomy of adenial of service attack on a GSM network and shows theattacker profile and attack economics, section 6 describesauthors' proposed DOS mitigation technique and outlinesthe deployment issues associated with it. Finally, section 7 summarizes the subject of the paper and the main contributions.

Manuscript Received on December, 2012.

K. Vsn Raghu Babu, Final Year B.Tech, Ece, Kl University, Vaddeswaram, Ap, India.

T. Ravi, Associate Professor B.Tech, Dept. of ECE, KLUniversity, Vaddeswaram, AP, India.

II. SECURITY IN WIRELESS NETWORKS

Security in wireless networks is an important issuesince users are likely to put personal, important ormission-critical data over an infrastructure that is nottruly secure. The security weaknesses stem from bothusing multiple incompatible security schemes and designflaws in security protocols, which is inherent. Thegreatest danger is that the user may perceive the entirestructure as secure and may mistakenly trust it to conveyconfidential information. The wireless environment posesmany security issues, such as confidentiality,authentication, integrity, authorization, non-repudiationand accessibility. Other issues may include convenience,speed, ease-of-use and standardization [2]. Therefore, thesecurity strategy must be devised and implemented withrespect to the type of data being transported and theestimated loss in case of eavesdropping or tampering withthe data. We have to also consider the fact that manysecurity issues arise due to poor implementation, featureinteractions, unplanned growth and new flaws createddue to prior attacks (Figure 1). Taking denial of serviceattacks as a reference, although this type of attack doesnot directly corrupt the data, there is no reason not tobelieve that another kind of subversive action is in preparation or in progress [3].

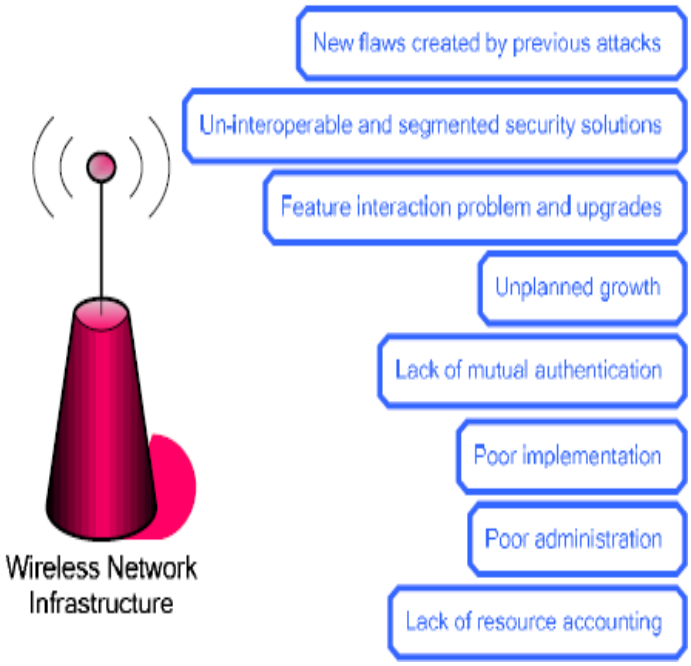

Figure 1. Security issues in wireless networks

To be truly effective, the security strategy must beapplied end-to-end, i.e. from source to destinationregardless of path. For example, WAP provides securityusing WTSL (Wireless Transport Security Layer), butthis is not necessarily end-to-end security sinceencryption takes place only between the mobile deviceand the WAP gateway [5].

III. SECURITY MECHANISMS IN GSM NETWORKS

Security and confidentiality in GSM were some of thereasons for which it was considered superior to othermobile communication systems and the tremendoussuccess has inspired other systems such as Code DivisionMultiple Access (CDMA), Personal Handy PhoneSystem (PHS), and Digital Enhanced CordlessTelecommunications (DECT). Another greatenhancement over traditional mobile systems was theintroduction of the SIM (Subscriber Identifier Module)card which clearly separated the mobile device from thesubscriber. The SIM card contains the InternationalMobile Subscriber Identity (IMSI) and a SubscriberIdentification Key (Ki), both used to authenticate theclient against the GSM network. GSM security relies onthree algorithms: A3 and A8 for authentication and A5for encryption.

With more than 1 billion users worldwide, GSM is apotential target for several kinds of attacks. The easiest tomount are the low tech attacks, such as call forwarding topremium numbers (depending on the network operator),bogus registration details, roaming fraud and terminaltheft. Fraud management systems monitor a variety ofindicators, such as multiple calls at the same time, largevariations in revenue paid to other parties, largevariations in duration of calls (very short or very long),changes in customer usage (indicating that a mobile hasbeen stolen or is being abused) and closely monitoringcustomer 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 secureas the fixed network to which it connects.
- GSM infrastructure does not address active attacks, such as identity cashing, camping ona false BTS, eavesdropping, etc.
- Lawful interception was considered as an after-thought.
- Cryptographic and authentication mechanismsare 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 thatinfluence the security in GSM networks. Thefirst capability is the easiest to achieve. Subsequentcapabilities imply more investment from the attacker andwe assume that an intruder having a certain capabilityalso has all lower ranked capabilities [13].Eavesdropping and user impersonation were two issuesknown at the time 2G security was developed. 3Gsecurity however aimed at protecting against all issues.

A. Authentication

Client authentication is performed by a simplechallenge-response algorithm. TheGSM Authentication Center (AuC) generates a random128-bit number and sends it to the mobile station viaradio link. This number and the subscriber key (Ki) arefed 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 SRESbased on the same inputs and it is now capable ofdeciding 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 areoperator specific and they are best kept secrets. This isobscurity rather than security. It is well known the factthat a secret authentication or encryption algorithm maybe vulnerable since it does not benefit from theexperience of the cryptanalytic community who may tryto uncover flaws and errors in design.

In the software world, when a program claims toemploy a new secure algorithm that is several times asfast as DES or AES, chances are that the algorithm isnothing more than a series of XORs. The requirement torun on a smart card (such as the SIM) has a severe impacton the practical implementation. Thus, 3rd GenerationPartnership suggests default implementations for A3 andA8 as a simple series of XOR operations, fact whichdemonstrates our point [9]. Surprisingly, the fact theSRES in only 32 bit long has little impact on the securityin the case of a birthday attack since this quantity is usedin conjunction with the random key from the AuC and thenumber of successful eavesdrops is thus 1.84 x 1019(2128/2) rather than 65536 (232/2). For more information onbirthday attacks see [10].

B. Encryption

Unlike A3 and A8, the GSM standard specifies the A5algorithm, used for encrypting the speech, data andsignaling information over the radio link. Theinformation is encoded two frames at a time (2 x 114bits), one for uplink and the other one for downlink. Inthe initial design (called A5/1), the session key K ismixed with the frame counter to initialize a set of 3registers that will produce the 228 bit output by XORingthe LFSR with the plaintext.

A partial source code implementation of the GSM A5algorithm was leaked to the Internet in June 1994.Rumors go that this implementation was an early designand bears little resemblance to the A5 algorithm currentlydeployed. Nevertheless, insight into the underlyingdesign theory can be gained by analyzing the availableinformation. The details of this implementation, as wellas some documented facts about A5, are summarized.

A disagreement between cellular telephonemanufacturers and the British government centering onexport permits for the encryption technology in GSM wassettled by a compromise in 1993. Western Europeannations and a few other specialized markets such as HongKong would be allowed to have the GSM encryptiontechnology, in particular the A5/1 algorithm. A weakerversion of the algorithm (A5/2) was approved for export to most other countries, including Central and EasternEuropean nations [11]. This is mainly a political issuewhich involves privacy rights of the individual, theability of law enforcement agencies to conductsurveillance and the business interests of corporationsmanufacturing cellular hardware for export.The simple design of A5/1 eventually proved insecureand it was broken around April 1998 by Ian Goldberg andDavid Wagner who also succeeded to break the A5/2algorithm in as few as 5 clock cycles. This is veryuncomfortable for anyone who uses the GSMinfrastructure for private communication.For domestic uses, the GSM security proves far betterthan the analog cellular systems. The use ofauthentication, encryption and temporary identificationnumbers ensures the privacy and anonymity of users aswell as preventing fraudulent use.

C. Key Length

When designing or deploying cryptographicalgorithms, the natural question that comes is how longshould the key be?

Unfortunately there is no singleanswer to this question as there are several variables,such as the value of the protected data, secrecy time andan approximate estimation of the attacker resources. Theworld renowned cryptologist Bruce Schneier emphasizesthe close relationship between the value of the data andthe effort to encrypt it. For instance, a customer list maybe worth $1000. Financial data for an acrimoniousdivorce case might be worth $10,000. Advertising andmarketing data for a large corporation might be worth$1,000,000 and the master keys for a digital cash systemmight be worth billions of dollars [4, 14]. Similarly, thereis also a relationship between the secrecy time and theeffort to encrypt the data. In the world of commoditytrading, secrets only need to be kept for minutes. In thenewspaper business, today's secrets are tomorrow'sheadlines and the U.S. Census data are required by law toremain secret for 100 years. Table 2 (cited from Ref.[14]) shows the security requirements for different kindsof information.Going back to the GSM system, if we overlook theproven security flaws in the A5 design and consider thekey length as the only security factor, it is interesting tosee how long it would take to decrypt a message with agiven key length, assuming a cracking machine capableof 1 million encryptions per second [12]. The timerequired to break a 128 key is extremely large. Forcomparison, the age of the universe is believed to be 1.6 *10^10 years. Assuming that the effective key length of theA5 algorithm is 40 bits, it currently provides adequateprotection for information with a short lifetime; howeverit shouldn't be used to transfer confidential informationwith 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 andcategorize them. In this paper we will use a threat rankingmethodology named DREAD.

A. The DREAD Threat Ranking

Howard and LeBlanc introduced a risk assessmentmethodology called DREAD [17]. This alarmist, butappropriate, name is an acronym from the followingterms:

• 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 anexploit. High reproducibility is important for mostattackers to benefit.

• Exploitability

How much effort and expertise is required to mount anattack? For example, if a novice programmer with a homePC 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. Alsoconsider what degree of authentication and authorizationis required to attack the system. For example, if an anonymous remote user can attack the system, it ranks10, while a local user exploit requiring strong credentialshas a much lower exploitability.

• Affected users

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

• Discoverability

This is probably the hardest metric to determine andwe always assume that a threat will be taken advantageof, 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 DREADthreat ranking methodology to some known GSMsecurity flaws in order to determine which one of themshould be addressed first in the event of an infrastructureupgrade. Some of the following security flaws arementioned in [13].

B. Denial of Service Attacks

The GSM radio interface is vulnerable to denial ofservice attacks as scarce resources such as signalingchannels are blindly granted to anyone who requeststhem. Flooding the signaling channels with rouge orlegitimate requests essentially means that the trafficchannel is paralyzed. The flood on the signaling channelmay be caused by a misbehaving mobile station [16] or by genuine requests [15]. The next section contains anextensive description of denial of service attacks.RiskDREAD = (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 isdetached from the visited location area and is thusinaccessible to network paging requests. The net result isthat all mobile terminated services will fail.RiskDREAD = (3 + 10 + 5 + 1 + 10) / 5 = 5.8

D. Location Update Spoofing

This attack is similar to the previous one. The attackerspoofs a location update request in a different locationarea from the one in which the user is roaming. Again,the net result is that all mobile terminated services fail.RiskDREAD = (3 +10 +5 +1 +10)/5= 5.8

E. Camping on a False BTS

The mobile phone can be enticed to camp on a rogueBTS, making it inaccessible to paging signals of theserving network. Alternately, the rogue BTS may act as arelay and let traffic through at will. This attack requires amodified BTS.RiskDREAD = (3 + 10 + 4 + 1 + 10) / 5 = 5.6

F. Passive Identity Caching

Under certain circumstances, the network may requestthe user to send its identity in plain text. A modifiedmobile station can be used to cache the information forother uses. RiskDREAD = (2 + 8 + 5 + 1 + 10) / 5 = 5.2

G. Active Identity Caching

This attack is similar to the previous one, except thatthe user may be enticed to camp on a false BTS which inturn continuously requests that the mobile identity be sentunencrypted. RiskDREAD = (2 + 8 + 4 + 1 + 10) / 5 = 5

H. Encryption Suppression

As the mobile station has no way of authenticatingmessages over the radio interfaces, it may be enticed tocamp on a false BTS and communicate with the attackerin an unencrypted mode. The attacker can spoof thecipher mode command and it maintains the call for aslong 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 thepossession by the intruder of a compromisedauthentication vector and thus exploits the weakness thatthe user has no control upon the cipher key. The targetuser is enticed to camp on the false BTS/MS. When a callis set-up the false BTS/MS forces the use of acompromised 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 thatexploits the weakness that the MS cannot authenticatemessages received over the radio interface. The targetuser is enticed to camp on the false BTS. When the targetuser or the intruder initiates a call the network does notenable encryption by spoofing the cipher modecommand. The attacker however sets up his ownconnection with the genuine network using his ownSubscriptionn. The attacker may then subsequentlyeavesdrop 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 falseBTS/MS. When the target user or the genuine networksets up a connection, the false BTS/MS modifies theciphering capabilities of the MS to make it appear to thenetwork that a genuine incompatibility exists between thenetwork and the mobile station. The network may thendecide to establish an un-enciphered connection. Afterthe decision not to cipher has been taken, the intrudermay 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 andthe possession by the intruder of a compromisedauthentication vector and thus exploits the weakness thatthe user has no control the cipher key. The target user isenticed to camp on the false BTS/MS. When the targetuser or the intruder set-up a service, the false BTS/MSforces the use of a compromised cipher key on the mobileuser while it builds up a connection with the genuinenetwork 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 possessionby the intruder of a compromised authentication vectorwhich is intended to be used by the network toauthenticate a legitimate user. The intruder uses that datato impersonate the target user towards the network andthe 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 theweakness that an authentication vector may be usedseveral times. The intruder eavesdrops on theauthentication response sent by the user and uses thatwhen the same challenge is sent later on. Subsequently,ciphering has to be avoided by any of the mechanismsdescribed above. The intruder uses the eavesdroppedresponse data to impersonate the target user towards thenetwork 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 thetarget user camps on the false base station, the intruderpages the target user for an incoming call. The user theninitiates the call set-up procedure, which the intruderallows to occur between the serving network and thetarget user, modifying the signaling elements such thatfor the serving network it appears as if the target userwants to set-up a mobile originated call. The network
does not enable encryption. After authentication theintruder cuts the connection with the target user, andsubsequently uses the connection with the network tomake 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 tothe previous attack this time the intruder has to attempt tosuppress encryption by modification of the message inwhich the MS informs the network of its cipheringcapabilities.
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 thetarget user camps on the false base station, an associate ofthe intruder makes a call to the target user's number. Theintruder acts as a relay between the network and thetarget user until authentication and call set-up has beenperformed between target user and serving network. Thenetwork does not enable encryption. After authenticationand call set-up the intruder releases the target user, andsubsequently uses the connection to answer the call madeby his associate. The target user will have to pay for theroaming leg.
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 tothe previous attack this time the intruder has to suppressencryption.
RiskDREAD = (4 + 10 + 5 + 1 + 10) / 5 = 6

S. Threat Ranking

It iseasily observable that the most serious threat is the denialof service attack.

IV CONCLUSION

Security in wireless networks is a complex thing.Whereas in a wired network tapping is usually done byphysically accessing the communication links andsecuring those may improve

information security to someextent, in case of wireless networks the information isbroadcast over the radio waves and it is readily availableto whoever wants to listen. Moreover, radio resources inwireless networks are a valuable commodity and anyinterference may threaten the availability of networkservices, hence the need for authentication and resourcecontainment.With respect to security, we have emphasized theobscurity that surrounds the protocols used forauthentication and encryption in GSM networks. Thisinevitably leads to flawed designs, which poses greatrisks to anyone who puts personal, important or missioncriticaldata 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 ofservice attack is the most serious one and needs to beaddressed first.We have shown that the GSM technology is vulnerableto denial of service attacks and the resources needed tomount such an attack are dangerously low:

- The attack is possible because the call set-up protocol allocates resources without a minimalauthentication.
- A single attacker is capable of simultaneously disabling one or more cells, depending on the particular network configuration.
- Since no communication fees are involved (noactual call is made), the effective financial costof launching a devastating attack is zero.

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

REFERENCES

[1] Alan Burnett, Securing the Wireless Internet, Roke Manor Research Ltd, UK, 2003
[2] UpkarVarshney, "Network access and security issues in ubiquitous computing", Workshop on Ubiquitous Computing Environment, Cleveland, 2003
[3] ValerBocan, "Developments in DOS research and mitigating technologies", PeriodicaPolitehnica, 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.

Kollipara. VSN Raghu 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.

KrishnamRaghavendraSujith 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.