Security Challenges in 3G Systems

Mohammad Islam[†] **and Vineet Kumar Verma**[††]**,**

[†]Galgotia College of Engineering & Technology, Gautam Budha Technical University, Greater Noida, India.
[††]Noida Institute of Engineering & Technology, Gautam Budha Technical University, Greater Noida, India.

Summary
This study explains the authentication and encryption scheme used in GSM. It explains the different possible attacks on cellular systems, which include SIM cloning, eavesdropping, location tracking, SMS ping, SMS denial of service, authentication denial of service and SMS spam. It classifies these attacks on the basis of target of the attack, type of attack, motivation and severity. It points out the vulnerabilities that are exploited by attacks on cellular systems. It shows that the existing security schemes do not provide adequate security and that there is a need to develop new mechanisms that are better suited to the wireless environment. The study also looks into how risk analysis, risk modeling and fuzzy logic can be applied to security in 3G systems. It proposes a fuzzy logic based risk model to secure Short Message Service in GSM based cellular networks. The proposed model uses a hybrid approach towards risk modeling.

Key words:
3G, GSM, Fuzzy Logic, Cellualr System, SMS, Mobile Network.

1. Introduction:

Cellular telephones are increasingly becoming a crucial part of our daily lives. As of May 2011, the total number of cellular phone users worldwide was 4.8 billion and this was growing at the rate of 52.49 % every 12 months. In the India, the industry is signing up new subscribers at the rate of one every two seconds, putting it on track to reach 851.70 million customers sometime later this year. According to the Cellular Telecommunications Industry Association (CTIA) [1], the cellular industry in the United States grew 25.3 percent in 2010, adding 93 million additional wireless subscribers, for a total of 302.1 million customers. Average usage grew 40.5 percent in 2010 to 180 minutes a month compared to 130 minutes a year ago. The average monthly bill rose 4.6 percent to $41.24 in 2011. Industry revenues for 2010 increased to $40 billion from $33.1 billion in 2009. More than 31 percent of the U.S. population now has active wireless service. Data based services like web browsing and e-mail are now being provided over cellular phones. Wireless connections to the Internet, electronic mail and other data services are further boosting usage. These trends are encouraging for both consumers and the industry, as more affordable plans with more minutes become the standard. In fact wireless service is increasingly becoming an alternative to wire-line services. The concept – “The office is where the cellular phone is.” – is taking root.

The cellular networks used in United States are AMPS, GSM, TDMA, CDMA and PCS. Europe and Asia primarily use GSM. This study mainly concentrates on GSM networks since they are used widely throughout Europe and Asia and their subscriber base in the United States is also increasing. It gives an overview of the security mechanisms in GSM. It enumerates and classifies the several possible attacks on cellular devices. It also sites instances of such attacks that have been conducted on cellular devices.

2. Need For Security In Cellular Systems

Cellular systems need to be secure because of the following reasons:

- The operator must be able to ensure that only legitimate users use the service and that she is able to bill the right person for the service rendered.
- The subscriber wishes to protect his privacy. This includes but is not limited to privacy of the subscriber’s location, privacy of the communication that is being conducted over the wireless link and protection from unsolicited messages and calls.

2.1. Essential Features of a Security Scheme

A security scheme must:

- Have a strong authentication mechanism to protect the operator against fraud and misuse of service
- Have a suitable encryption/decryption scheme to make the wireless link as secure as a wired link to prevent eavesdropping
- Prevent operators from compromising each others security, either inadvertently or because of competitive pressures
- Address the generation and distribution of keys
- Support interoperability between cellular networks without compromising security

Manuscript received October 5, 2012
Manuscript revised October 20, 2012

- A security scheme must not:
- Add enormous delays to the call setup time and degrade the quality of the subsequent communication
- Drastically increase the bandwidth requirements of the channel
- Add excessive complexity to the system
- Increase the error rates of the system
- Render the system cost ineffective

2.2. Overview of Security Mechanism in GSM

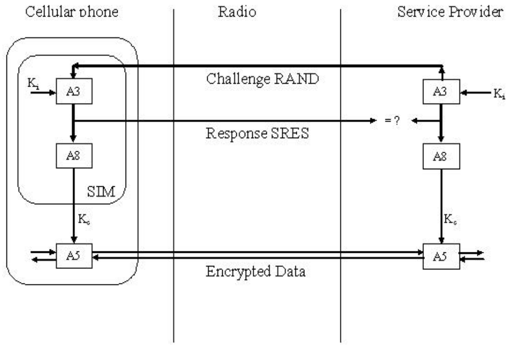

Figure 2.1: Security mechanism in GSM

The security mechanisms of GSM are implemented in three different system elements:

- Subscriber Identity Module (SIM)
  The SIM contains the Individual 3G Subscriber Identity (IMSI), the individual subscriber authentication key (K_i), the ciphering key generation algorithm (A8), the authentication algorithm (A3) and the personal identification number (PIN).

- GSM handset or 3G station
  It contains the ciphering algorithm (A5)

- GSM network
  It contains the authentication/encryption algorithms (A3, A8 and A5). The Authentication Centre (AUC), which is part of the Operation and Maintenance Subsystem (OMS) of the GSM network, consists of a database of identification and authentication information for subscribers. This includes the Individual 3G Subscriber Identity (IMSI), the Temporary 3G Subscriber Identity (TMSI), Location Area Identity (LAI), and the individual subscriber authentication key (K_i) for each user.

Security in GSM consists of the following aspects:

- Subscriber Identity Authentication
  GSM network uses a challenge response mechanism for subscriber authentication. The network sends a 128 bit random number (RAND) to the 3G station. The 3G station computes a 32 bit signed response (SRES) by encrypting the random number (RAND) using the authentication algorithm A3 parameterized by the individual subscriber authentication key (K_i). Upon receiving the signed response (SRES) the GSM network repeats the calculation of SRES to verify the identity of the subscriber. The individual subscriber authentication key (K_i) is never transmitted over the radio channel. In fact, it never leaves the SIM since the A3 algorithm is present in the SIM itself. If the received SRES matches the calculated value, the 3G station has been successfully authenticated, else the connection is terminated and authentication failure is signaled to the 3G station.

- Signaling and Data Confidentiality

  Both the SIM and the GSM network generate the encryption key (K_c) using the A8 algorithm, parameterized by the random number RAND and the individual subscriber authentication key (K_i). On the 3G station the generation of the encryption key (K_c) takes place within the SIM, since the A8 algorithm is also present in the SIM. Hence the individual subscriber authentication key (K_i) never leaves the SIM. The encryption key (K_c) is used to encrypt and decrypt data that is sent between the 3G station and the base station.

- Subscriber Identity Confidentiality

  Subscriber identity confidentiality is provided by using the Temporary 3G Subscriber Identity (TMSI) during course of a phone call. The Individual 3G Subscriber Identity (IMSI) is used during set up of the call throughout the authentication process. Once the subscriber has been authenticated she is assigned a Temporary 3G Subscriber Identity (TMSI) and the TMSI is used to identify the user for the remainder of the call. Hence user anonymity is maintained.

- Security while Roaming

  GSM allows operators to inter-operate without revealing the authentication algorithms and the individual subscriber authentication key (K_i) to each other. GSM allows triplets of challenges (RAND), signed responses (SRES) and communication keys (K_c) to be sent between operators over connecting network. Thus a GSM network can authenticate a user of another GSM network without requiring to know the individual subscriber authentication key (K_i) of that user.

2.2.1 Overview of A3/A8

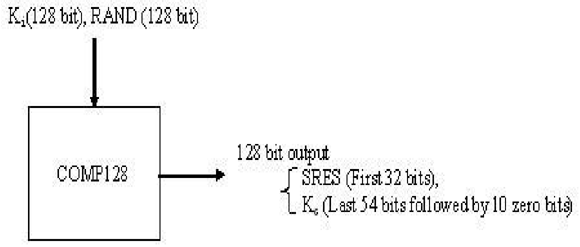
K_i(128 bit), RAND (128 bit)
COMP128
128 bit output
SRES (First 32 bits),
K_c (Last 54 bits followed by 10 zero bits)

Figure 2.2: COMP 128 Calculations

Most GSM networks use COMP 128 for A3 and A8 [6]. COMP128 takes 128-bit random challenge (RAND) and the individual subscriber authentication key (Ki) as input and produces a 128-bit output. The first 32 bits of this output is the signed response (SRES). Ten zero bits are appended to the last 54 bits of the output to obtain the session key (Kc). Thus, it is evident that the strength of the 64-bit key has deliberately been reduced to 54 bits.

2.2.2 Overview of A5

The A5 algorithm [7] is the stream cipher used to encrypt over-the-air transmissions.

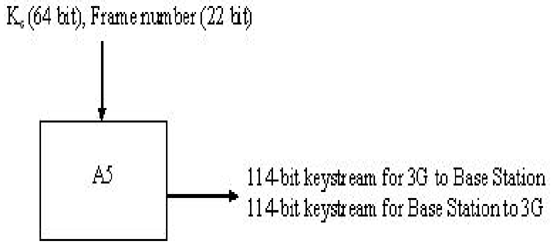
K_c (64 bit), Frame number (22 bit)
A5
114-bit keystream for 3G to Base Station
114-bit keystream for Base Station to 3G

Figure 2.3: Keystream Generations

The stream cipher is reinitialized for every frame sent. The stream cipher is initialized with the session key (Kc), and the number of the frame being decrypted/encrypted. The same Kc is used throughout the cellular call, but the 22-bit frame number changes with each frame sent. This generates a unique keystream for every frame.

The A5 algorithm uses 3 Linear Shift Feedback Registers (LSFR) of different lengths. The sum of the lengths of the 3 LSFRs is 64 bits. The outputs of the 3 registers are XORed together and the result represents one keystream bit. The LSFRs are 19, 22 and 23 bits long with sparse feedback polynomials. All three registers are clocked, based on the middle bit of the register. A register is clocked if its middle bit agrees with the majority value of the three middle bits.

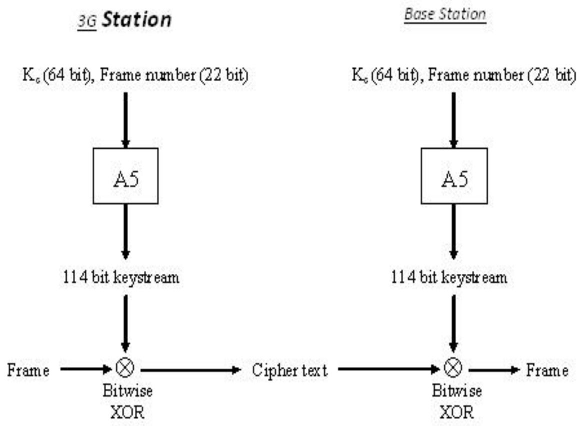

Figure 2.4: Frame Encryption and Decryption

The three LSFRs are initialized using the session key, Kc, and the frame number. The 64-bit Kc is first loaded into the register bit by bit. The LSB of the key is XORed into each of the LSFRs. The registers are then all clocked with the majority clocking rule disabled. All 64 bits of the key are loaded into the registers the same way. The 22-bit frame number is also loaded into the register in the same way with the majority clocking rule enabled. After the registers have been initialized with the Kc and the current frame number, they are clocked one hundred times and the generated keystream bits are discarded. This is done in order to mix the frame number and keying material together. Now 228 bits of keystream output are generated. At the 3G station, the first 114 bits are used to encrypt the frame from the 3G station to the base station and the next 114 bits are used to decrypt the frame from base station to 3G station. At the base station, the first 114 bits are used to decrypt the frame from the 3G station to the base station and the next 114 bits are used to encrypt the frame from base station to 3G station. Each bit of the frame is XORed with a bit of the keystream to obtain the cipher text. After this, the A5 algorithm is initialized again with the same Kc and the number of the next frame.

3. Attacks on Security in Cellular System

3.1 SIM Cloning

As explained above the SIM card is the basic key that uniquely identifies a subscriber to the GSM network. If a SIM can be cloned, it renders the authentication scheme of GSM completely useless. The authentication (A3/A8) and encryption algorithms (A5) of GSM have not been made public by the GSM MoU. It has been proven time and again that security by obscurity is no security at all. The strength of an algorithm must rely on the secrecy of its private key and not on the secrecy of the algorithm itself. Opening an algorithm to public scrutiny and evaluation, results in extensive cryptanalysis of the algorithm by the entire international research community. In the absence of this evaluation, the algorithm is prone to have several flaws and would be an easy target for hackers. This has been proven once again in the case of GSM.

The origin of the breach was when the Smartcard Developed Association (SDA) discovered the cryptographic algorithms used inside the SIM's and cellular phones. The SDA first verified that the algorithms were accurate. The exact details of the algorithms were not known to the public but the verified algorithms matched the facts that were publicly known. Next the SDA brought in David Wagner and Ian Goldberg, researchers in the Internet Security, Applications, Authentication and Cryptography (ISAAC) group at the University of California, Berkeley. Within a day, Wagner and Goldberg had found a fatal cryptographic flaw in COMP128 (A3/A8), the algorithm used for authentication inside the SIM. They created a system to exploit the flaw by repeatedly asking the SIM to identify itself; by processing the responses they were able to extract the secret from inside the SIM.

The crack was based on a speculated implementation of the COMP128 implementation. This speculated implementation was derived from information on the internal details of COMP128 from public documents, leaked information and several SIMs the researchers had access to. The speculated algorithm was verified to be correct by comparing the output of the software implementation to the responses produced by a SIM known to implement COMP128.

A theoretical analysis of the algorithm, uncovered a potential vulnerability in the algorithm. The attack was a chosen-challenge attack. The SIM is presented specially chosen challenges. The SIM uses the COMP128 algorithm to determine the signed response to the chosen challenge. By analyzing a series of such challenges the value of the secret key can be determined.

3.1.1 Cloning with Physical Access to SIM

If one has physical access to a SIM, them all one needs is an off-the-shelf smartcard reader and a computer to direct the operations.

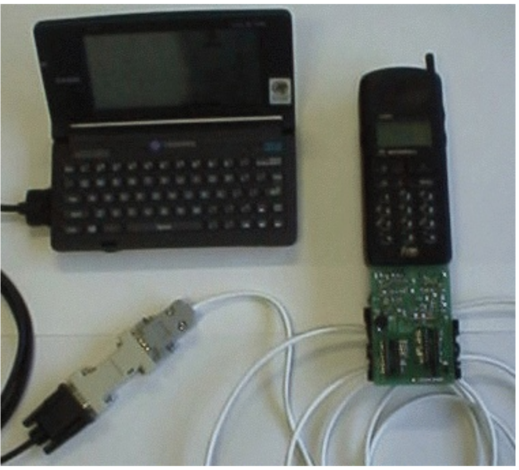

Figure 3.1: A Cloned GSM Cellular Phone

The attack requires the SIM to be queried about 150,000 times. So, a smartcard reader that can issue 6.25 queries per second could complete the attack in about 8 hours.

3.1.2 Possible Damage by SIM Cloning

Cloning a SIM renders the GSM authentication mechanism useless. The attacker in possession of the cloned SIM can use the services of the GSM network at the cost of the real subscriber. It can also result is a great loss of revenue for the service provider since, he can no longer be sure as to how many the calls the true subscriber has made. It may also lead to a disgruntled customer, who may lose faith in the service provider after such a security breach and switch to a different provider, thus causing further loss of revenue for the service provider.

The attacker who has a cloned SIM can also eavesdrop on the conversation of the true subscriber. If the attacker monitors a call right from the start and gets hold of the random challenge (RAND), it is very easy for her to obtain the session key since she knows the individual subscriber authentication key (Ki) and the algorithms A3 and A8. The financial or tactical damage arising out of this depends on the sensitivity of the information being exchanged during course of the conversation.

In all likelihood, the most rampant misuse of SIM cloning would be achieved by a "customer" arranging for his own SIM to be cloned. The customer could then use the 2 SIMs in 2 different cellular phones. Currently most cellular operators charge a rental fee for sharing of airtime between two phones. Thus, producing a loss of revenue for the service provider.

Another scenario that should be considered is the possibility of prepaid SIMs being cloned, together with their pre-paid airtime. Those networks deploying handset-based pre-paid solutions would be vulnerable to this type of attack, because it would be difficult for the network to prevent the pre-paid airtime being re-used by these identical SIMs. Besides if there are multiple cloned SIMs in existence, it would be impossible to identify the authentic one and the owner of the authentic SIM may lose her prepaid airtime to one of the cloned SIM users.

3.2 Eavesdropping

This is the most classical form of security violation. Every pair of communicating entities wishes to maintain a certain level of confidentiality of its communication. The attackers goal is to gain as much information about the conversation as she possibly can.

3.2.1 SIM Cloning Attack

If the attacker has managed to clone the SIM of one of the parties involved in the conversation it is pretty easy for her to eavesdrop on the conversation. The attacker monitors the activity of the user whose SIM she has cloned. She must get hold of the random challenge (RAND) that is sent across during the call setup phase. Knowing the RAND and the individual subscriber authentication key (Ki), the attacker can compute the session key Kc that is to be used during the conversation. Knowing the session key, the attacker can eavesdrop on all the data that is being sent across the wireless link.

3.2.2 Attacking the Signaling Network

In GSM, only data sent over the wireless link is encrypted. Traffic over wired lines within the operators network is transferred in plaintext. Thus, if the attacker can get access to the signaling network of the operator then she can listen to everything that is transmitted, which includes the phone conversation and also RAND, Kc, and SRES.

Another form of attack would be to try and gain access to the Authentication Center (AUC) database or the Home Location Register (HLR). Access to either of these will give the attacker the individual subscriber authentication key (Ki) for all subscribers of that network. However the AUC and the HLR are generally more secure than the rest of the GSM network and hence such a break-in is less likely.

3.2.3 Possible Damage by Eavesdropping

Eavesdropping on a private conversation violates the privacy of the parties involved in the conversation. The financial or tactical damage arising out of this depends on the sensitivity of the information being exchanged during course of the conversation. For example, sometimes eavesdropping may just give the attacker some local gossip. However in cases where important financial information is being transferred over the conversation, the attacker may gain information of significant financial value. In military circles, access to a conversation about tactical defense/attack decisions may give the attacker significant advantage in the battlefield and render the victim vulnerable to defeat.

3.3 Location Tracking

Wireless 3G communication technologies rely on one key element to function: constant knowledge by the transmitting or switching system of the location of a cellular phone for the purpose of routing incoming communications. Even when they are not in use, these units regularly and automatically emit positioning signals. Unfortunately for privacy, these signals can be used for purposes far different than the original goal of routing communications

3.3.1 Location Management in GSM

When a 3G station is powered on, it performs a location update procedure by indicating its Individual 3G Subscriber Identity (I3SI) to the network. The first location update procedure is called the I3SI attach procedure. The 3G station also performs location updating, in order to indicate its current location, when it moves to a new Location Area or a different Public Land 3G Network (PL3N). This location updating message is sent to the new 3G Switching Center (MSC)/Virtual Location Register (VLR), which gives the location information to the subscriber's Home Location Register (HLR). If the 3G station is authorized in the new MSC/VLR, the subscriber's HLR cancels the registration of the 3G station with the old MSC/VLR. A location updating is also performed periodically. If after the updating time period, the 3G station has not registered, it is then deregistered. When a 3G station is powered off, it performs an IMSI detach procedure in order to tell the network that it is no longer connected.

During course of a phone call, subscriber identity confidentiality is provided by using the Temporary 3G Subscriber Identity (T3SI). The Individual 3G Subscriber Identity (I3SI) is used during set up of the call throughout the authentication process. Once the subscriber has been authenticated, she is assigned a Temporary 3G Subscriber Identity (T3SI) and the T3SI is used to identify the user for the remainder of the call. Hence anonymity of the user is maintained. However an attacker who is monitoring activity on the 3G device right from the start of a call can still keep track of the user. The service provider needs to monitor the location of the user as mentioned above and can definitely isolate the position of the user depending on the location from which the user signal is originating, This information can of course be misused.

3.3.2 Possible Damage by Location Tracking

It is frightening to imagine that someone could be monitoring one's every move. One's life will no longer remain private if someone can find out and keep a record of where one has been every moment of one's life. This information can be used for personal financial gain by the attacker. It can also be used to jeopardize the physical well being of an individual, for example, try to assault a person when she is in a desolate area. Another example is that paparazzi could misuse the location service, to track and haunt celebrities.

3.4 SMS Ping

Short Message Service (SMS) is a service that allows short text messages to be sent to a subscriber's cellular phone. As is common in the 3G phone industry, SMS text messages can be used by network operators to change the functionality of phones. Thus, a malformed message could cause phones to lock up. This can be used by an attacker to lock up a cellular phone or a set of cellular phones.

3.4.1 Possible Damage by SMS Ping

SMS ping can be used to launch a denial of service attack on the cellular phone or a set of cellular phones. Most GSM providers allow sending of SMS messages through e-mail. It is very easy and inexpensive to send a single e-mail that would lock up a cellular phone. The e-mail with this locking SMS message could be sent to a number of cellular phones or all the cellular phones in a particular number range. It is not too difficult to write a simple program or script to send out such messages. A cellular phone that has been locked by such an attack will be unable to receive or make calls until the phone is reset by removing and reattaching the phone's batteries. This attack, which locks a phone, may go undetected until the user tries to use the phone. Until that time the user may have missed a lot of legitimate calls. The damage due to such an attack can range from a mere irritant value to huge financial losses due to missed calls. Besides it may result in customer frustration and dissatisfaction with the service rendered by the GSM provider.

3.5 SMS Denial of Service

The SMS service has become very popular with cellular phone users. It enables users to receive text messages on their cellular phone like a pager. If the message is from another cellular phone, then the user can even reply to the message. This feature is really useful in public places like cinema halls, theatres, etc. where is would be inappropriate to conduct a conversation over the cellular phone. The cellular phone user could receive and send SMS messages through the cellular phone without disturbing the people around her. SMS messages can also be used to get web-updates, such as stock quotes or weather forecasts or weather warnings. Many service providers provide a means of sending SMS messages through the Internet. The person who wants to send an SMS message to a cellular phone user simply has to send a message to a special e-mail address. The email would be sent to the cellular phone user as an SMS message.

In most cases, this e-mail address can be easily deduced from the phone number of the cellular phone. This would allow someone on the Internet to launch a SMS Denial of Service attack on the cellular phone. The attack would simply send a flood of SMS messages through e-mail to the target cellular phone. The bandwidth of the wireless channel used by a cellular phone is very small as compared to the bandwidth of a typical Internet connection. It is very easy to flood the cellular phone using just a few machines or maybe even a single machine. As compared to this, to effectively bring down a target on the Internet one would need to launch a Distributed Denial of Service attack involving of thousands of machines. Thus, it is much easier to launch a DoS attack on a cellular device as compared to a host on the Internet. By launching such an attack on a larger scale, maybe targeting thousands of cellular phones belonging to the network, the entire wireless network of a service provider may be clogged.

3.5.1 Possible Damage by SMS Denial of Service Attack

A SMS Denial of Service attack can cause damage in several ways. The attacker could simply flood cellular phone bandwidth, preventing the cellular phone from carrying on with any useful communication. If there is a limit on the capacity of SMS messages that can be stored by the cellular phone, this could be easily exceeded, thus blocking out legitimate SMS messages. Some providers charge the users for every SMS update. An SMS flood could cause the user to exceed his quota and get a bill for all the junk messages sent to her. The customer is obviously going to contest such a bill, thus causing the provider to lose bandwidth and revenue on SMS messages that the user did not want to receive. An intangible loss would be the loss of customer confidence in the service provider's system and may even lead to the service provider losing a customer.

3.6 Authentication Denial of Service

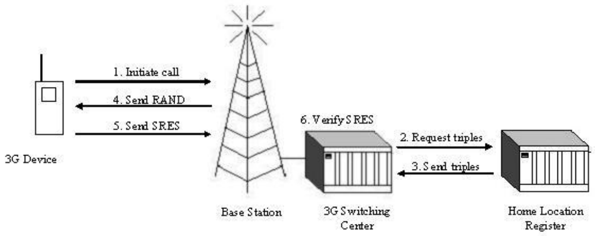

Figure 3.2: Authentication Procedure in GSM

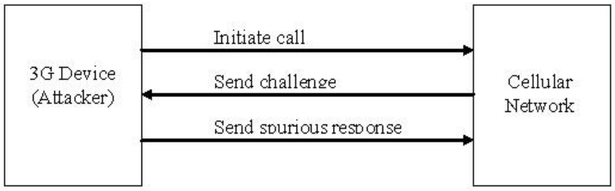

Figure 3.3: DoS by Spurious Authentication

In this form of attack, the attacker repeatedly asks the cellular network to authenticate her. Authentication requires the cellular phone to communicate with the cellular network, thus consuming the cellular bandwidth for the duration of the authentication. Besides, even though the authentication eventually fails, the cellular network still has to go through the steps 1 to 6 each time authentication is requested. This would consume a lot of resources in the cellular network. If the attacker has access to multiple such spurious wireless devices, she could repeatedly request authentication from the cellular network, thus degrading the quality of service or even denying service to legitimate users.

3.6.1 Possible Damage by Authentication Denial of Service Attack

Given sufficient resources the attacker can generate so many spurious authentication requests, that the network will be virtually inoperable. Most of the bandwidth will be consumed by the spurious authentication attempts, precluding legitimate users from using the service. The entire cellular network can be brought down by this kind of attack. This could cause losses to the order of millions of dollars. The customers could also suffer significant loss due to inability to use the phone when needed and failure to receive financially important incoming calls. A response to this kind of attack could be very difficult since the attacker may actually have a team of accomplices that are constantly on the move with these spurious wireless devices.

3.7 SMS Spam

As mentioned earlier, SMS is gaining immense popularity among cellular phone users. Subscribers use SMS for a wide range of applications from text based paging to wireless web updates. The use of SMS along with the ability to pin point a subscriber's location can be used for targeted marketing campaigns. For example when a user enters a mall, an advertisement for one of the shops in the mall could be sent to the user's cellular phone as an SMS message. The user could receive notification of a special sale or a special offer in a specific shop. A discount coupon could be beamed to the user's cellular phone. A mall in Europe already plans to use this scheme nicknamed “Ads in your pocket”. All this can be very irritating to the subscriber who does not wish to receive such messages. Often the subscriber has a limited number of updates or pays per SMS message received. In such a case the subscriber certainly does not want to pay for junk SMS messages. Even if the subscriber does not have to pay, this kind of messaging can be highly irritating. People often do not wish to be disturbed except for urgent messages. An advertisement SMS message disturbing a person who is in the middle of a movie or a theatre performance can be highly irritating. This is similar to the problem of spam e-mail that one receives on the PC, except that receiving spam as SMS messages on the cellular phones can be much costlier and much more irritating.

3.7.1 Possible Damage by SMS Spam

This kind of attack is higher on irritant value than on financial loss. Although at times the subscriber may end up paying for junk SMS message that she does not want. Thus she would suffer some extra financial burden.

4. Classification of Attacks on Cellular Systems

4.1 Classification based on Target

- Subscriber based attacks
  These attacks are targeted at a particular subscriber. These include but are not limited to eavesdropping, SIM cloning, SMS DoS, location detection, SMS spam. The loss incurred depends upon the type of attack and also on the nature of the information that has been compromised. With a cloned SIM, the attacker could use the service and have the target subscriber billed for it. SMS spam and SMS DoS attacks can be mere irritants. In case of eavesdropping the loss depends on the nature of the information that is compromised. An

overheard domestic conversation may be of little value as compared to sensitive military or financial information that may be leaked out.

- Provider based attacks
  These attacks are targeted at the service provider. They need to be organized at a much larger scale as compared to a subscriber based attack. They would also need specialized equipment for their execution. An example of such an attack is an authentication DoS attack on a service provider. Such an attack could potentially bring down an entire network causing loss of service to thousands of customers and huge financial losses to the service provider.

4.2 Classification based on Type of Attack

- Authentication attacks
  This type of attack targets and breaks the authentication system in a 3G network. Examples of such attacks include authentication DoS and SIM cloning. These attacks would either allow the attacker, unauthorized access to the 3G network or would target the authentication mechanism to deny service to authentic customers. Attacks that try to break the authentication system and gain unauthorized access can be prevented or at least made more difficult by increasing the strength of the authentication algorithms. To increase the strength of the algorithms, one need to increase the key size for the algorithms or increase the inherent strength of the algorithm. To ensure the strength of an algorithm, it would be a good idea to open the algorithm to the international research community for research and evaluation before incorporating it into a standard. It has been proven time and again that security by secrecy of the algorithm itself is no security at all. It may also be suggested that the schemes based on the secret algorithms, be changed to schemes and mechanisms based on open and proven standard algorithms like RSA, DES, AES.

- Encryption Attacks
  In these attacks the attacker tries to crack the encryption used to secure the communication and gain access to the information being transferred. The damage depends on the actual content that gets compromised as a result of the attack. Again, these attacks can be prevented by using industry strength encryption algorithms like RSA, DES and AES, instead of secret proprietary algorithms.

- Denial of Service attacks
  This is the most difficult type of attack to ward off. In this type of attack the security system itself would be used to deny service to legitimate customers. Denial of denial of service is a topic of a lot of research now-a-days. One can however dissuade people from launching such attacks by tracking down and punishing those responsible for such attacks. Another way is to make the equipment that would be required to launch such an attack unavailable to the general public.

- Spam
  It is just a matter of time before the spam mail one gets on one’s e-mail accounts starts moving towards spam messages on one’s cellular phone. Most people expect only the most urgent of messages on one’s cellular phone. Unsolicited messages on one’s cellular phone can be highly irritating. It can be very difficult to filter out spam SMS messages just as it is difficult to intelligently filter out spam mail.

4.3 Classification based on Motivation

- Financial gain
  These attacks are generally aimed at gaining some financial advantage. SIM cloning for unauthorized use of a service is an example of such an attack. So is eavesdropping to gain certain financial or tactical information.

- Disruption
  These attacks are not motivated by financial gain. Their basic aim is to disrupt the service being targeted. Often the aim is just to gain attention of a lot of people or maybe just to prove a point.

4.4 Classification based on Severity of Loss

- Extreme
  These attacks cause extensive financial losses. A Denial of Service attack that brings down the entire wireless network is an example of such and attack. Prevention of such attacks would result in significant financial savings. In some cases, such as in military use of wireless systems, such an attack can have even more severe consequences than just financial loss.

- Moderate
  These are attacks that are comparatively less severe as compared to extreme loss attacks. An

example of such attacks is an eavesdropping attack that compromises sensitive information of a particular user. The financial loss to the individual may be significant but is would be at least a few degrees of magnitude lesser than the loss caused by extreme loss attacks.

- Mild/Irritant
  These attacks would generally just be mere irritants and would not result in significant financial losses. An example of such attacks would be SMS spam attacks.

4. Conclusion.

This study explains the authentication and encryption scheme used in GSM. It explains the A3, A5 and A8 protocols used in the security mechanism in GSM. It explains the different possible attacks on cellular systems, which include SIM cloning, eavesdropping, location tracking, SMS ping, SMS denial of service, authentication denial of service and SMS spam. It classifies these attacks on the basis of target of the attack, type of attack, motivation and severity. It points out the vulnerabilities that are exploited by attacks on cellular systems. It shows that the existing security schemes do not provide adequate security and that there is a need to develop new mechanisms that are better suited to the wireless environment.

It can be extended to proposes a fuzzy logic based risk model to secure Short Message Service in GSM based 3G networks.

Acknowledgment

This work is supported by research team under Noida Institute of Engineering and Technology, Greater Noida, India. Also this work is highly appreciated by research personnel at Galgotia College of Engineering and Technology, Gr. Noida, UP, India. This topic has great work to be extended when implementing risk model against security threats in 3G systems.

References

[1] DavidWagner, GSM Cloning, http://www.isaac.cs.berkeley.edu/isaac/gsm.html, [referred Nov. 2000].

[2] Anon., GSM Cell phones Cloned, http://jya.com/gsm-cloned.htm, [referred Nov. 2000].

[3] Harri Hansen, Security of 3G Systems from a User's Point of View, April 4, 2000.

[4] David Margrave, GSM Security and Encryption, [referred March 2000].

[5] Briceno M. & Goldberg I. & Wagner D., A Pedagogical Implementation of A5/1, http://www.scard.org/gsm/a51.html, [referred April 2000]

[6] Racal Research Ltd., GSM System Security Study, http://jya.com/gsm061088.htm, June 10, 1988

[7] Racal Research Ltd., GSM System Security Study, http://jya.com/gsm061088.htm, June 10, 1988

[8] Harri Hansen, Security of 3G Systems from a User's Point of View, April 4, 2000

[9] 3GPP Technical Specifications Group – Services and System Aspects – Security Working Group, ftp://ftp.3gpp.org/TSG_SA/WG3_Security, [referred Nov. 2000].

[10] Deborah J. Bodeau, A Conceptual Model for Computer Security Risk Analysis, The MITRE Corporation.

[11] David Margrave, GSM Security and Encryption, [referred March 2000]

Mohammad Islam received the B.Tech. degree in Computer Science & Engineering, and M.Tech. degree in Software Engineering from Uttar Pradesh Technical University, Lucknow, India in 2005 and 2011, respectively. During 2005-2009 he stayed in Krishna Institute of Engineering & Technology, Ghaziabad, UP, India on the post of Lecturer and from 2009 to till date he is Assistant Professor in Galgotia College of Engineering & Technology, Greater Noida, UP, India. He have published 6 papers in international journals in different. He is active researcher in his field.

Vineet Kumar has done his B.Tech in Computer Science from College of Technology, Pantnagar, UP, India. Completed his M.Tech in Computer Science from UP Technical University, Lucknow and is pursuing his PhD in Computer Science from MBU, Solan, HP, India. He is Associate Professor in the Department of Information Technology and holds the position of Controller of Examination in NIET. He is a versatile person in research and academics as he have published many research papers in international and national conferences.