False base station attack in GSM Network Environment

Mishra Sandip D., Dr. Nilesh K. Modi

Abstract— **In this paper, we have discussed about attacks performed on false base station. In GSM network environment all the communication has restricted between mobile station and base station which call has been transferred. This GSM network has few draw back which are discussed in this paper. This is also about how call has been forwarded to mobile switching center and base station. GSM network contains about different types of encryption and decryption mechanism between call transfers. The attack makes intruders to impersonate GSM base station and make it impersonate user to get connect within base station. In this case all the integrity of original base station has been occupied by the false base station and then call has been conducted to make some fake communication. In this type of situation attacker make a fake call and sending fake sms or mms type of data. Also attacker can access and trace location of any particular mobile subscriber.**

In this case secret key of USIM has been cracked to authenticate false base station. Some time false base station can behave as repeater and can transmit some requests in the network and the target user which are in the peripheral of that base station and modify or ignore certain service requests and/or paging messages related to the target user. An attack requires a modified base station and makes it vulnerable to that a user can be enticed on a false base station.

Index Terms—**Authentication and Key Agreement (AKA), Evolved packet system (EPS), Extensible Authentication Protocol (EAP), Global System for Mobile Communication (GSM), Universal Mobile Telecommunications Systems (UMTS)**

I. INTRODUCTION

The demands on mobile communication and networks have been constantly increasing. Originally the need was simply to have a phone system that could meet most of the requirements of the standard plain old telephone service (POTS) in most homes. The original first generation mobile communication system, such as the advanced mobile phone system (AMPS), were analog cellular networks which met this need without considering the inherent issues that arise due to using a wireless medium as opposed to a wired one. Security was a major issue that was not properly addressed when developing the 1G system and therefore the phones were susceptible to cloning. This was due to the phones broadcasting their identities without encryption or integrity when phone calls are placed. Attackers could then take this information and apply it to their own phone to then use it to connect to the provider network allowing them to call anywhere without having a legitimate account with the provider. The cloning defrauded many providers of large amounts of money while inappropriately making unauthorized use of their resources. There are many benefits and requirements of security in mobile wireless communication.

The second generation of mobile communications (2G) strove to solve the phone cloning issue and while meeting the expanding requirements of consumers with GSM/2G networks. Global system for mobile communications (GSM) networks also addressed some of the issues with using a wireless medium when sending information. The new network authenticates the user against the network in a cryptographically secure method to limit the potential of phone cloning security issues as well as ensuring that the network resources are not accessed inappropriately. This made phone cloning a much more difficult proposition for attackers to inappropriately make use of provider networks while allowing providers to be much more certain that their resources were not being fraudulently used by unauthorized devices. The problem with GSM networks was that they did not appropriately protect the user from many other types of attacks such as the false base station attack that would allow an attacker to listen in or modify the communication from the GSM user. The false base station attack and other security issues in GSM networks were attempted to be resolved by providers with the third generation of mobile communication (3G).

3G mobile communications allowed for much better use of the spectrum available allowing much "smarter" devices to be on the network. Even though the cloning issue was mostly resolved with the GSM networks there were other security issues that needed to be addressed in universal mobile telecommunications systems (UMTS) networks. To address these new issues the 3rd generation used mutual-authentication between the mobile device and the provider network. The UMTS networks also have much higher speeds for IP communication to allow for users to make extensive use of the network resources. The next generation of mobile communication will make even further use of the available spectrum and increase the ability of smart devices to do much more robust communication with media and other applications. The authentication in the fourth generation (4G) is still going to be the same authentication protocols as the USIM 3G to make certain that resources are not misappropriated. (4G) long term evolution (LTE) networks will a low wider bandwidths, higher efficiency and a fully IP network for all communication. GSM networks have by far the largest installed base of users with over 5 billion GSM

Manuscript received Nov, 2014.

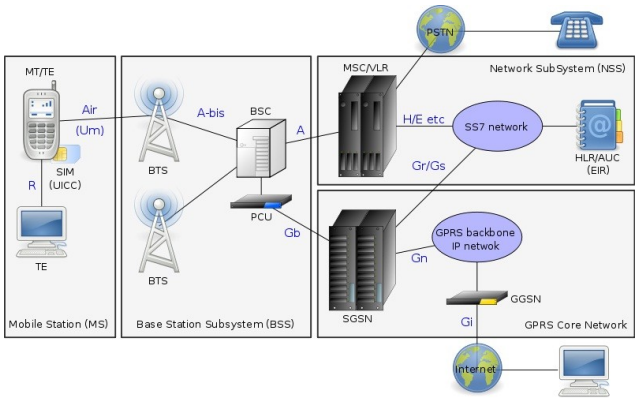
Mishra Sandip D., *Computer Science, Asstant Professor, Narsinhbhai Institute of computer studies, kadi, Mehsana, India-+91-9427317940, Research scholar, Karpagam University*

Dr. Nilesh K. Modi, *Computer Science, Professor & Head, Narsinhbhai Institute of computer studies, kadi, Mehsana, India-+91-9427317940 Research Guide, Karpagam University*

devices in use around the world [1]. This large market of devices has made it a business requirement of all providers to allow for the legacy GSM system to be integrated into new systems to ensure that these users can use the network resources and be billed appropriately for that usage. The interoperation of legacy systems needs to be executed with the utmost care to ensure that issues in the legacy system do not manifest themselves in the new integrated system. There are many security concerns when integrating legacy systems and the evolution of those systems to handle new requirements. The authentication done in the GSM network was maintained in the new UMTS networks to allow these devices to connect. This integration allows some of the security issues in GSM networks to be exploited in the new network. This work discusses authentication in mobile wireless networks as well as the needs of those networks to interoperate and the security issues brought about by that integration. The authentication protocols in the new generations of mobile wireless networks are designed to interoperate (not replace) the existing protocols as the infrastructure for the existing system is deployed nationally and is very expensive to replace requiring time, effort and expense. Therefore the integration of the different protocols to allow this interoperation gives the mobile operators the ability to upgrade their networks while still maintaining coverage for their customers. It worth mentioning that, the integration of the old (flawed) security protocols is not always a right option. For instance, the new authentication protocol described by IEEE 802.11i to protect stationary wireless networks replaced (not interoperate) the legacy Wired Equivalent Privacy (WEP) due to the problems found in the earlier algorithms and protocols. Eric, at al [2] compared between the interoperation solution in mobile networks and the replacement solution employed in stationary wireless networks. In this paper, the interoperation will be described considering security flaws brought about by integrating the old protocols into the new systems. This will include a description the authentication and key agreement (AKA) protocols of the legacy SIM based 2G GSM networks, and the modern USIM based 3G UMTS networks, 4G LTE networks and WiMAX networks. The protocols and methods used for the integration of the legacy systems into the modern AKA systems will discussed. In order to protect the integration in mobile wireless networks against these security flaws in SIM based networks two solutions are proposed. This paper is organized as follows. Section 2 describes the SIM based authentication mechanism used in GSM networks. The USIM based authentication mechanism used UMTS 3G, LTE 4G, and WiMax 4G networks are described in Section 3. Section 4 describes the mobile user hand-over between different network, and the related security issues. Two solutions are proposed to the problem of integration in mobile wireless networks in Section 5. Section 6 concludes this work. [3]. This paper is discussing about attacks performed on GSM and UMTS network.

II. GSM NETWORK ENVIRONMENT

Mobile service providers needed to secure their networks from attack and misappropriation of networking resources. In the attempt to achieve the goals set out in GSM of protecting access to mobile services and to protect any relevant item from being disclosed on the radio path [3]; the GSM security protocols were developed. There are many technical constraints that needed to be addressed when adding security to mobile communication. When authenticating against a mobile wireless network the mobile equipment needs to be able to send from one base station to another without a loss of communication or interruption to an active connection. The requirement to roam without interruption was a major factor in development of mobile networks that would allow a user to be able to authenticate to and use all parts of the network seamlessly. A major difficulty faced by mobile networks is the ability for a user to roam from one network to another network operator which allows mobile network providers to bill foreign users and systems. The authentication protocol deployed to address these problem was the SIM based GSM protocol. In GSM networks, a mobile station is connected to visit network by several radio link to a particular base station. Multiple base stations of the network are connected with Radio Network Controller (RNC) and multiple Radio Network Controller (RNC) is controlled by a GPRS Support Node (GSN) in the packet-switched case or a Mobile Switching Center (MSC) in the circuit-switched case (shown in Figure). The Visitor Location Register (VLR) and the serving GSN keep track of all mobile stations that are currently connected to the network. Each subscriber can be identified by its International mobile subscriber identity (IMSI).



[Figure-1 GSM Network Communication]

To protect against fake profiling attacks, this permanent identifier is sent over the air interface as infrequently as possible. In this case, locally valid Temporary Mobile Subscriber Identities (TMSI) is used to identify a subscriber whenever possible. Every UMTS subscriber has a dedicated home network with which he shares a long term secret key Ki. The Home Location Register (HLR) keeps track of the current location of all subscribers of the home network. Mutual authentication between a mobile station and a visited network is carried out with the support of the current Serving GSN (SGSN) or the Mobile Switching Center or Visitor Location Register respectively. GSM supports encryption of the radio interface as well as integrity

protection of the signaling messages. For a detailed description we refer to [13].

III. FRAUDS USING FALSE BASE STATION

Using false base station it can forward call to premium rate numbers. This is used for Bogus registration details of customer and that cannot be detected after computing any kind of theft. Using this attack it can also make roaming fraud for with paying service. Using this type of attack it can make terminal theft. This will also make multiple calls forwarding for making service enable like conference calls.[12,10] This thing can generate folloing type of attacks in GSM network environment:

A. Compromising authentication vectors in the network:

The intruder possesses a compromised authentication vector, which may include challenge/response pairs, cipher keys and integrity keys. This data may have been obtained by compromising network nodes or by intercepting signaling messages on network links.

B. Impersonation of a user:

This is the capability whereby the intruder sends signaling and/or user data to the network, in an attempt to make the network believe they originate from the target user. The required equipment is again a modified MS.

C. *Eavesdropping*

This is the capability that the intruder eavesdrops signaling and data connections associated with other users. The required equipment is a modified MS.

D. *Impersonation of the network*

This is the capability whereby the intruder sends signaling and/or user data to the target user, in an attempt to make the target user believe they originate from a genuine network. The required equipment is modified BTS.

E. *Man-in-the-middle*

This is the capability whereby the intruder puts itself in between the target user and a genuine network and has the ability to eavesdrop, modify, delete, re-order, replay, and spoof signaling and user data messages exchanged between the two parties. The required equipment is modified BTS in conjunction with a modified MS.

An attack that makes modified Base Transreceiver Station or Mobile Switching Center and exploits are the weakness that a user can be enticed to camp on a false base station. false Base Transreceiver Station or Mobile Switching Center can act as repeater for some time and can relay some requests in between the network and the target user, but eventually modify or ignore certain service requests and/or paging messages related to the target user. An attack that requires a modified Mobile Switching Center and exploits the limitation that the network cannot validate the messages it receives over the radio interface. The intruder spoofs a deregistration request (IMSI separate) to the network. The network deregisters the user from the visited position area and instructs the Home Location Register to do the same. The user is consequently inaccessible for mobile concluded services. The user spoofs a location update request in a different location area from the one in which the user is roaming. The network registers in the new location area and the target user will be paged in that new area. The user is subsequently unreachable for mobile terminated services. An attack that requires a modified Base Transreceiver Station and exploits the weakness that a user can be enticed to camp on a false base station. Once the target user camps on the radio channels of a false base station, the target user is out of reach of the paging signals of the serving network in which he is registered. A passive attack that requires a modified MS and exploits the weakness that the network may sometimes request the user to send its identity in cleartext. 3G: The identity confidentiality mechanism counteracts this attack. The use of impermanent identities allocated by the helping network makes passive eavesdropping disorganized since the user must wait for a new registration or a mismatch in the serving network database before he can capture the user's permanent identity in plaintext. The inefficiency of this attack given the likely rewards to the attacker would make this scenario unlikely. An intruder entices the target user to camp on its false Mobile Switching Center and subsequently requirements the target user to send its permanent user identity in cleartext perhaps by forcing a new registration or by claiming a short-term identity mismatch due to database failure. 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.

IV. HACKING THE SIGNALING NETWORK

In the air interface waves between the Mobile station and the Base transceiver station are not the only vulnerable point in the GSM system. The transmissions are encrypted only between the MS (mobile station) and the BTS. After the Base transceiver station (BTS), the traffic is transmitted in plain text within the operator's network. This will opens new possibilities of hijacking of network. If the attacker can access the operator's signaling network, he will be able to listen to everything that is transmitted, including the actual phone call as well as the RAND, SIGNED RESPONSE (SRES) and Kc. Accessing the signaling network is not very difficult. Although the BTSs are usually connected to the BSC through a cable, some of them are connected to the BSC through a microwave.[11] This link would be relatively easy to access with the right kind of paraphernalia. The microwave link might be encrypted, however, depending on the hardware manufacturer, thus making it slightly more difficult to monitor it . It is really a question about whether the attacker wants to crack the A5 encryption protecting the session of a specific MS or the encryption between the BTS and the BSC and gaining access to the backbone network. The ability to tap on to the data transmitted between the BTS and BSC would enable the attacker to either monitor the call by eavesdropping on the channel throughout the call or he could retrieve the session key, Kc, by monitoring the channel, interrupt the call over the sky and decrypt it on the fly.

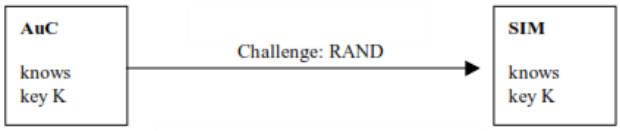
The GSM measurement requires the phone to validate to the network interface, but does NOT require the network to validate to the phone. This well-known security hole can be exploited by an International mobile subscriber identity(IMSI)-catcher. The service provider cannot observe the use of International mobile subscriber identity(IMSI)-catcher. An International Mobile Subscriber Identity(IMSI)-catcher is a device for forcing the transmission of the International Mobile Subscriber Identity(IMSI) and intercepting GSM mobile phone calls. The International Mobile Subscriber Identity(IMSI)-catcher acts as a base station and logs the International Mobile Subscriber Identity(IMSI) numbers of all the mobile stations in the area, as they attempt to attach to the International Mobile Subscriber Identity(IMSI)-catcher. It allows forcing the mobile phone connected to it to use no call encryption (A5/0 mode), making the call data easy to intercept and convert to audio. The basic principle of GSM is, a mobile station always connects to the base station which provides the best reception. An attacker can easily enforce this kind of a setting, i.e., make a victim device connect to him instead of a real base station by drowning the real base stations that are present by sending its beacons with higher transmitting authority. Thus the International Mobile Subscriber Identity (IMSI)-CATCHER creates the same scenario and acts as a fake base station, so the victim's mobile attaches with the hackers International Mobile Subscriber Identity (IMSI)-CATCHER assuming it as the real base station. [3] Now during the connection setup the attacker sends the security capabilities of the victim mobile station to the attached visitor network. The attacker sends the TMSI of the victim mobile station to the visited network, which he obtained during the connection setup. If the current TMSI is unknown to the attacker, he sends a faked TMSI. If the network cannot resolve the fake TMSI, it sends an identity request to the attacker. The attacker replies with the International Mobile Subscriber Identity (IMSI) of the victim. The visited network requests the authentication information about the victim device from its home network. The home network provides the authentication information to the visited network. The network sends RAND and AUTN to the attacker. The attacker disconnects from the visited network. Thus attacker obtains an authentication token. [5]

V. ATTACKS ON BASE STATION ALGORITHM

Cryptographic attack against the COMP128 algorithms also known as the GSM MoU Example algorithm, is circulated to members of the GSM MoU and may be used as validation algorithm in a GSM network. COMP128 is not an European Telecommunications Standards Institute (ETSI) standard algorithm and, it has never been suggested by ETSI. Also, COMP128 is not mandated by the GSM MoU for use by its members. The GSM standard was defined so as to allow network operators to choose or design their own validation and cipher key generation algorithm, subject only to meeting the requirements to standard input and output lengths. The attack is a so-called collision attack, one of a class of attacks that have been known for years. The main objective of the attack is to calculate the secret subscriber's authentication key. It exploits weakness in COMP128 which allows information is to be deduced about the key when two different challenges to the card (input values to the algorithm) produce the same output. The attack is independent of the SIM manufacturer's performance of the algorithm and uses no chip card specific properties. It is not suggest that there are any problems in the SIM itself. For example the same attack would apply if the algorithm and key were implemented in a tamper-proof "black box". It is claimed that several challenges are sufficient to derive the key. This may be a little on the confident side. However, accepting it as true, the attack requires physical ownership and continuous examination of the card for some 8 hours. The attack is effective against one SIM, or to precise one subscription at a time. Negotiation of a particular subscriber's key has no impact on keys used by other subscribers, and hence the security offered by network to its subscribers on the whole. Moreover, as interrogation is possible only after verification of user's PIN by the SIM, The attack requires awareness of this secret PIN. For those operators who will not use COMP128, we would advise them in the short term to encourage their subscribers to make use of the SIM's PIN feature. They should also accept measures to ensure that take on phones are not mistreated. In the longer term, they should move to the use of another algorithm.

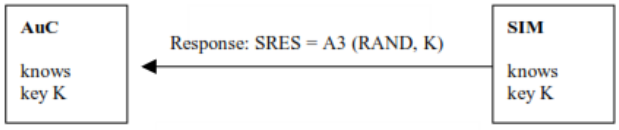
VI. GSM SECURITY USING COMP128 ALGOIRTHM

Each SIM card in its GSM handset has a different 128 bit secret key K, it is unique to only that SIM card only and to an Authentication Centre (AuC) in the network. When a GSM phone call is being set up from the Authentication Centre (AuC) sends RAND number from center, a freshly generated 128 bit random number, via the network and the GSM handset to the SIM:



[Figure: 2 RAND Generation in GSM]

The SIM combines RAND and K using a hash function called A3 algorithm, which gives a 32-bit "signed response" SRES. The SIM sends SIGNED RESPONSE (SRES) back to the Authentication Centre (AuC) via the handset and the network will receive that and conforms that the sender is valid for getting connection to mobile communication network.



[Figure: 3 Response to RAND request using SRES]

The Authentication Centre (AuC) compares SIGNED RESPONSE (SRES) to the value which it computed using its own copy of RAND and K. If they are equal the Authentication Centre (AuC) believes that SIM is authentic and the call is allowed to proceed.

The speech exchanged between the GSM handset and the network is encrypted using an algorithm called A5 which has a 64 bit session key. For each new call the essential A5

session key is generated using a hash function called A8. This takes the same 128 bit challenge and 128 bit key K and produces the 64 bit session key, so no further exchange of data is required for this step.

VII. CONCLUSION

This paper will elaborate about how false base station performs with different subscriber and mobile switching center. How data are lost during transmitting from one location to another location and then it will regenerated from impersonate user using same SIM based authentication. Also this cases a vulnerability of COMP128 algorithm that is to be cracked by any particular attacker. Using this attacker can access call, use call forwarding, and conference call.

REFERENCES

1. Start 3GPP Technical Specification, "3GPP TS 33.102, V5.3.0, Third Generation Partnership Project; Technical Specifications Group Services and System Aspects; 3G Security; Security Architecture," September 2003
2. E. Barkan, E. Biham, and N. Keller, "Instant cipher text-only cryptanalysis of GSM encrypted communication," in Advances in Cryptology – CRYPTO 2003 , vol. 2729 of LNCS , pp. 600–616, August 2003.
3. D. Fox, "Der IMSI-catcher," DuD, Datenschutz und Datensicherheit, 2002.
4. ETSI Technical Specification, "ETSI TS 100.929, V8.0.0, Digital Cellular Telecommunications System (phase 2+)(GSM); Security related network functions," 2000.
5. U. Meyer and S.Wetzel, "A man-in-the-middle attack on UMTS." In submission.
6. 3GPP Technical Specification, "3GPP TS 35.202 V5.0.0, Third Generation Partnership Project; Techni- cal Specification Group; 3G Security; specification of the 3GPP confidentiality and integrity algorithms; doc-ument 2: Kasumi algorithm specification," Jun 2002.
7. M. G. I. Briceno and D. Wagner, "A pedagogical implementation of the gsm A5/1 and A5/2 "voice pri-vacy" encryption algorithms." http://cryptome.org/gsm-a512.htm, 1999.
8. J. Golic, "Cryptanalysis of alleged A5 stream ci-pher," in Advances in Cryptology ,vol. 1233 of LNCS , pp. 239–255, Springer Verlag.
9. A. Biryukov, A. Shamir, and D. Wagner, "Real time cryptanalysis of A5/1 on a pc," in Advances in Cryptology, proceedings of Fast Software Encryption'00 , vol. 1978, pp. 1–18, Springer-Verlag, 2001.
10. E. Biham and O. Dunkelman, "Cryptanalysis of the A5/1 gsm stream cipher," in Progress in Cryptology, proceeding s of Indocrypt"00, LNCS, pp. 43–51, Springer- Verlag , 2000.
11. P. Ekdahl and T. Johansson, "Another attack on A5/1," Transactions on Information Theory , vol. 49, pp. 284– 289, 2003.
12. I. Goldberg, D. Wagner, and L. Green, "The (real-time) cryptanalysis of A5/2." Presented at the Rump Session of Crypto'99, 1999.
13. S. Petrovic and A. Fuster-Sabater, "Cryptanalysis of the A5/2 algorithm." Cryptology ePrint Archive, Report 200/052, http://eprint.iacr.org, 2000.
14. U. Meyer, K. Kastell, and R. Jakoby, "Secure handover procedures," in Proceedings of the 8th Conference on Cellular and Intelligent Communications , October 2003.
15. Boman, K., Horn, G., Howard, P. and Niemi, V.: UMTS security. Electronics & Communication Engineering Journal, Oct 2002, pp. 191-204.
16. TS 33.401, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE): Security architecture.
17. TS 33.402, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE): Security aspects of non-3GPP accesses.
18. IETF RFC 5448: Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA').

Mr. Sandip Mishra
is presently working as assistant Professor in the MCA Department of S. V. Institute of Computer Studies, kadi, Mehsana, Gujarat, India. He is pursuing Ph.D. in Mobile Security from Karpagam University, Coimbatore, India. He is actively engaged in teaching since three years. His current research interests are in the areas of authentication algorithm for mutual encryption

A researcher and academician, working with highly industry standards having full focused vision to bring the institute at the highest pick of cut-throat academic environment, for the national leverage. Dr. Nilesh Modi having rich experience of around 10 years in academics and IT industry, holding Doctorate in E-Security (Computer Science and Application). Continuing his research on information and communication security, presently he is pursuing post doctoral research on Wireless Communication and Security and pursuing for the Certification as an Ethical Hacker. He is working as a recognized research supervisors for Ph.D. and M.Phil. Programme from more than 03 universities of India. He has good number of research under his name and presented more than 65 research papers in International and National Journals and Conferences. He has reviewed number of Ph.D. & M.Phil. thesis from different universities in India and abroad. He is also working as a manuscript reviewer for the international journal & conference at computer science department, auburn university, Alabama, USA. He is also working as a reviewer for number of national and international journals. He has delivered number of expert talk on eSecurity and hacking in National and International Conferences.

