ijecs open access www.ijecs.in

International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 9 September, 2014 Page No. 8331-8335

Defense Mechanism for Denial of Service Attack to UMTS Networks Using Sim-Less Devices

V. Palaniyappan [#1], M.Duraipandian [*2], K.Malarvizhi[*3]

[#1] pursing M.E (CSE) from VSB College of Engineering Technical Campus, Coimbatore, Affiliated to ANNA UNIVERSITY, Chennai, Tamil Nadu, India
Palanid.006@gmail.com

[*2] working as Assistant Professor in VSB College of Engineering Technical Campus, Coimbatore, Affiliated to ANNA UNIVERSITY, Chennai, Tamil Nadu, India
durainithi@gmail.com

[*3]working as Associate Professor in VSB College of Engineering Technical Campus, Coimbatore, Affiliated to ANNA UNIVERSITY, Chennai, Tamil Nadu, India
malarvizhik.se@gmail.com

ABSTRACT

One of the basic security element in cellular networks is the verification procedure functioned by means of subscriber identity module that is necessary to give access to network services and hence secure the network from unauthorized usage by implementing different types of parameters. The large amount of computing power available in modern clustered HLRs, it is also essential to consider the counter-intuitive result summarizes and showing that the more busy the HLR is, the more difficult is disrupting its services. The cellular infrastructure as a whole and thus in the measure needed by its defense, namely: 1.The complexity and the high level of programmability of latest mobile phones and 2.The interconnection between the cellular network and the internet. The awareness of this attack can be exploited by many applications both in security and in network equipment manufacturing sectors.

INDEX TERMS: Authentication, DOS, UMTS, Subscriber identity module, critical infrastructure, Parameter turning.

1. INTRODUCTION

MOBILE phones based on cellular networks are one of the most successfully deployed technologies of the last decades and coverage of cellular networks in the world has generally become persistent. Both an effect and a cause of this success may be seen in the evolutional cycle of the network technologies. In this state, mobile communication networks have gained the role of critical infrastructure for the global community like transport or electricity so that many individuals and business activities relying on them for their day-to-day operations. The complexity of the mobile network structure may hide both unknown and known vulnerabilities that proper analysis tools and formal techniques can unveil. Within protocol-specific vulnerabilities, the same network complexity may also hide potential performance bottlenecks in signalling protocols or control applications components that can be broken by several kinds of Denial of Service (DoS) attacks in order to tear down critical service subsystems or overwhelm them with large number of requests, arduous the resources needed to ensure network operations. The effects, in terms of coverage, of DoS attacks gradually increase when moving from physical (i.e., using a radio jammer) towards the upper layers (i.e., affecting application-level subsystems serving large portion of the cellular network). The potential impact of these attacks on mobile phone networks has not been sufficiently assessed and needs further study.

To this aim, this work, by focusing on the node attachment procedure in Universal Mobile Telecommunications System (UMTS) infrastructures, show that it is likely to mount a full-fledged DoS attack potentially capable of shutting down large sections of the network coverage without the need of hijacking or controlling actual users' terminals, as well as that the number of devices necessary to make such an attack

effective is limited to a few hundred ones. The presented attack does not require the use of real mobile handsets equipped with valid Subscriber Identity Module (SIM) modules and needs only a limited number (a few hundreds) of UMTS radio interfaces, ultimately located on a single ad-hoc device.

2. INTRODUCING THE UMTS NETWORK

Universal Mobile Telecommunications System (UMTS) is a major update to GSM standard which worth it the third generation (3G) epithet. Instead of other GSM updates like GPRS and EDGE, UMTS requires new base station equipments and new frequency band for its operation. In respect to 2G technologies it is characterized by greater spectral efficiency and higher throughput bandwidth ranging from 348kbps of first UMTS release, called R99, to actual 42Mbps of HSPA+. Bandwidth increment is also what drives marketing during early stages of this new technology; great emphasis has been posed by MNOs on services like mobile TV and video calling but their effort has not really been appreciated by end user: in fact, nowadays the main utilization of 3G networks is for plain internet access. UMTS introduction highly affects the radio access portion of the network, the core part, on the other side, remained the same as in GSM/GPRS in order to facilitate the switch from old technologies to the new one. A typical GSM/UMTS Public Land Mobile Network (PLMN) consist at least of the infrastructures depicted. It is mainly split up in three different portions:

- The Mobile Station (MS) or User Equipment (UE).
- The Radio Access Network (RAN) which is called GSM/EDGE Radio Access Network (GERAN) or UMTS Terrestrial Radio Access Network (UTRAN) based on the used technology.
- The Core Network (CN) or Network Switching Subsystem (NSS) with fully separated packet and circuit switched domains.

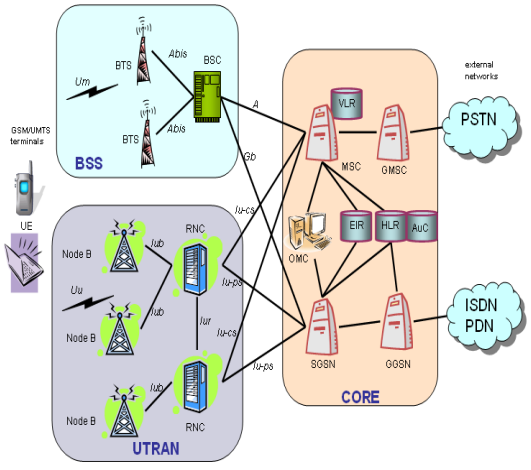

Fig.1. Structure of UMTS network

3. DDOS

Distributed denial of service (DDoS) *attack* aimed at cloud computing is some sort of malicious activity or a typical behavior, which cooperate the availability of the server's resources and prevents the legitimate users from using the service. DDOS attacks are not meant to alter data contents or achieve illegal access, but in that place they target to crash the servers, generally by temporarily interrupting or suspending the services of a host connected to the Internet. DOS attacks can occur from either a single source or multiple sources. Multiple source DOS attacks are called distributed denial-of service (DDOS) attacks.

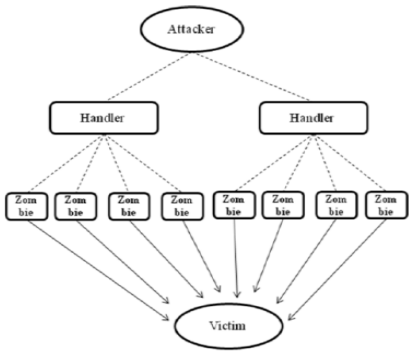

Fig.2. Architecture of DOS

3.1 Types of DDOS Attacks

DDOS attacks can be classified into generally three types:

- **Volume Based Attacks** - This type of attack includes UDP floods, ICMP floods, and other spoofed packet floods. The aim of this attack is to inundate the bandwidth of the attacked site.
- **Protocol Attacks** - This type of DDOS attack consume the resources of either the servers or of intermediate communication equipment, such as routers, load balancers and even some firewalls. Some few examples of protocol attacks include Ping of Death, SYN floods, Smurf DDOS, disjointed packet attacks. Protocol base attacks are usually calculated in Packets per second.
- **Application Layer Attacks** - Perhaps the most dangerous type of DDOS attack, application layer attacks are consist of seemingly sensible and effortless requests. The focus of these attacks is to crash the web server. Application layer attacks include Zero-day DDOS attacks, Slowloris, DDOS attacks that target Apache, Windows or Open BSD vulnerabilities. The Application layer attack is calculated in Requests per second.

4. RELATED WORK

For some reason each new radio access technology has to be deployed along side existing ones, leading to hybrid architecture where some network components are shared among different technological infrastructures. All of these aspects represent a significant increase in the dangerousness of the attack when compared to the existing one and can make the described devices on attractive target also for the cyber-warfare or cellular network production industry.
Attacker Model: Signaling–oriented DoS attacks that can affect both UMTS and UMTS/WLAN integrated systems.
Black hole attack Model: An attacker with a false BS equipment moves close to its target victims. The victim is connected to its fake equipment the attacker would simply

drop every packet that is transmitted from and towards the UE. This could be described as a variation of a black hole attack and could be conceived as the higher layer equivalent of radio jamming.
SIM: Attack does not require the use of real mobile handsets equipped with valid Subscriber Identity Module (SIM) modules and needs only a limited number (a few hundreds) of UMTS radio interfaces.
EIR: The IMEI is checked against the equipment identity register (EIR), in order to banish stolen or out-of requisites hardware from the network. In order to avoid its use as a way to track users in their movements by unlawfully eavesdropping radio traffic, another identifier called Temporary Mobile Subscriber Identity (TMSI).
To overcome the demerits of above described schemes, we are proposing a avoiding the usage of device in possession of unaware users, measuring the time delay by assigning the different types of parameter values.

5. ANALYSIS OF AIR INTERFACE

We now analyses the peculiarities of GSM and UMTS air interface protocols to evaluate their limits in terms of number of attach requests sent to the base station per second. In this process the only device communicating with the target cell.

5.1. GSM AIR INTERFACE

The GSM air interface has been designed to take advantage of both Frequency Division Multiple Access (FDMA) like previous 1G technologies and Time Division Multiple Access (TDMA). Multiple frequencies are mainly used to boost cell capacity in terms of concurrent calls, time division and different carrier frequencies that the MS swipes during its boot-up procedures. This particular air resource.

5.2. UMTS AIR INTERFACE

UMTS is a mobile cellular system designed to remove GSM inefficiencies related to synchronization between all devices in the RAN. For this reason it substitutes the TDMA protocol with a particular form of Code Division Multiple Access (CDMA) that is Wideband CDMA (W-CDMA), which allows Node B to transmit simultaneously to multiple mobile phones on the same carrier frequency as long as different channelization codes are used. This codes also known as Walsh Hadamard sequences are multiplied with the bit sequence coming out from the channel coding block: the resulting sequence has an higher rate than the input one and UMTS specification fixes it at 3:84Mcps where the c" stands for chip.

5.3. UMTS ATTACK LIMITS

The complete UMTS location update procedure is very similar in its phases. The first message that deviates from a standard location update flow is the same as in GSM, that is, the authentication response message. Unlike GSM, however, this time the attacker has to reply to the authentication request with a wrong challenge response SRES because, at this stage, the UMTS protocol stack does not allow a MS-initiated connection release: neither at RRC layer 2, nor at RLC one.

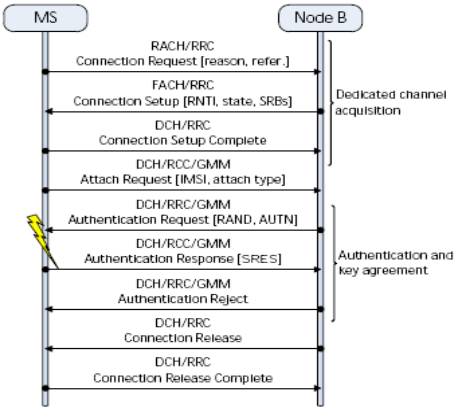

Fig.3. Message exchange between MS and Node B during the attack

6. PROPOSED WORK

The aim of the proposed scheme is to provide a security application which accurately detects and blocks DoS attack creating nodes in a UMTS network. The aim also measures the time delay by assigning the different types of parameter values. The application could be easily deployed in the network. Here we are proposing two main algorithms, UMTS integrity algorithm used to compute message authentication code and AKA algorithm used for authentication process.

A. ALGORITHMS

A.1. AKA ALGORITHM

In the attach procedure CN may require MS' authentication: this is the case when, for example, IMSI is used as identity declaration. The authentication process begin with MSC asking HLR authentication information for a given IMSI;HLR verify the presence of the IMSI in its database and, aided by AuC, generates a random RAND, which is processed by digest algorithm along with the IMSI's private key Ki thus obtaining an expected response XRES and a ciphering key Kc. (RAND, XRES, Kc) is the authentication triplet sent back to MSC which, in turn, sends RAND to mobile and receives back SRES as a response: MSC finally claims the user as authentic if and only if XRES = SRES. All the computations on the MS side is performed by the SIM card which is the only other element, apart from HLR, that knows both the digest algorithm and the private key Ki.

A.2. UMTS INTEGRITY ALGORITHM

The purpose of the integrity protection is to authenticate individual control messages. The integrity key IK is generated during the authentication and key agreement procedure, similarly as the cipher key CK. The integrity protection mechanism is based on the concept of a message authentication code. This is a one-way function, which is controlled by the secret key IK. The algorithm for integrity protection is based on the core function as the encryption.

B.SYSYEM MODULES

B.1. UMTS NETWORK

B.2.ATTACKING THE UMTS NETWORK

B.3.ASSESSING THE UMTS RADIO INTERFACE

B.4.DOUBLING THE ATTACK POWER USING SIMS

B.5.PARAMETER ASSIGNMENT

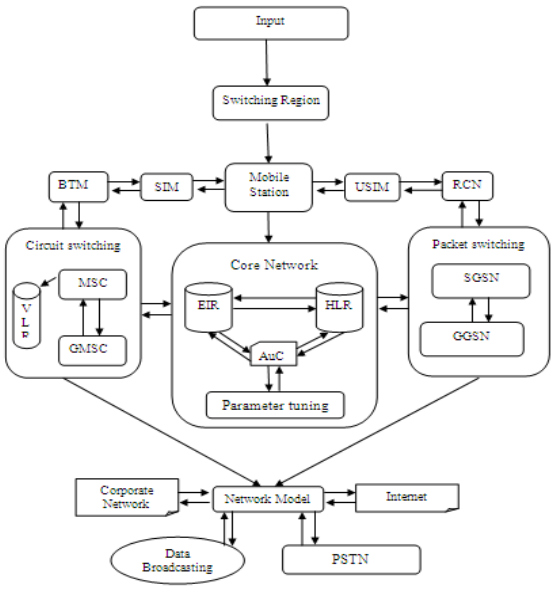

Fig.4. System Architecture

7. CONCLUSION

In this paper explores the scope of the UMTS based DoS attack. The classification of UMTS based DoS attack and some detection technique. An evaluation on DoS attack was discussed. In order to cope with the above timing limits, we envisioned an ad-hoc attacking device, equipped with multiple UMTS radio interfaces and no SIM modules. The Subscriber Identity Module is required to grant access to network services and hence protect the network from unauthorized users by assigning different types of parameters.

REFERENCES

[1] "A Denial of Service Attack to UMTS Networks Using SIM-Less Devices" Alessio Merlo, Mauro Migliardi, Nicola Gobbo, Francesco Palmieri, and Aniello Castiglione, Member, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 11, NO. 3, MAY-JUNE (2014).

[2] Y.-L. Huang, F.-Y. Leu, I. You, Y.-K. Sun, and C.-C. Chu. (2014). "A secure wireless communication system integrating RSA, Diffie-Hellman PKDS, intelligent protection-key chains and a Data ConnectionCore in a 4G environment."

[3] Y.-L. Huang, F.-Y. Leu and K.-C. Wei, "A secure communication over wireless environments by using a data connection core," Math. Comput. Modelling, vol. 58, no. 5, pp. 1459–1474, 2013.

[4] 3GPP. TS 23.401 | General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access. Http://www.3gpp.org/ftp/Specs/html-info/23401.html.

[5] K.W. Derr. Nightmares with Mobile Devices are Just around the Corner! In Portable Information Devices, 2007. PORTABLE07. IEEE International Conference on, 2007.

[6] C Johnson, H Holma, and I Sharp. Connection setup delay for packet switched services. 2005.

[7] Harri Holma and Antti. Toskala. WCDMA for UMTS. Wiley Online Library, 2002.

[8] L.R. Knudsen and C.J. Mitchell. An analysis of the 3gpp-MAC scheme. In Daniel Augot and Claude Carlet (Eds.) Workshop on Coding and Cryptography, WCC 2001, Les Ecoles de Cotquidan, 2001.

[9] T. Iwata and T. Kohno. New Security Proofs for the 3GPP Con_dentiality and Integrity Algorithms. In W. Meier and B. Roy (Eds.) Proceedings of FSE 2004, Lecture Notes in Computer Science, Springer-Verlag, 2004.

[10] Mylonas, S. Dritsas, B. Tsoumas, and D. Gritzalis, "Smartphone security evaluation—the malware attack case," in Proc. Int. Conf. Security Cryptography, 2011.

[11] P. Traynor, M. Lin, M. Ongtang, V. Rao, T. Jaeger, P. McDaniel, and T. La Porta, "On cellular botNets: Measuring the impact of malicious devices on a cellular network core," in Proc. 16th ACM Conf. Comput. Commun. Security, 2009.

[12] c.Johnson, H. Holma, and I. Sharp, "Connection setup delay for packet switched services," in Proc. 6th IEEE Int. Conf. 3G Beyond,2005.

[13] Yu Chen, *Member IEEE*, Kai Hwang, *Fellow IEEE*, and Wei-Shinn Ku, *Member, IEEE* "Collaborative Detection of DDoS Attacks over Multiple Network Domains" IEEE Transactions on Parallel and Distributed Systems.

[14] Collin Mulliner and J-P Seifert. Rise of the iBots: Owning a Telco network. In Malicious and Unwanted Software (MALWARE), 2010 5th International Conference on IEEE, 2010.

[15] Fleizach, M. Liljenstam, P. Johansson, G. M. Voelker, and A.Mehes. (2007). Can you infect me now?: Malware propagation in mobile phone networks. Proc. ACM Workshop Recurring Malcode, [Online].Available: http://doi.acm.org.

[16] Castiglione, G. Cattaneo, A. De Santis, F. Petagna, and U.Ferraro Petrillo. 2006. "SPEECH: Secure personal end-to-end communication with handheld," in Proc. ISSE Securing Electronic Business Processes.

[17] 3GPP TR 33.909 V1.0.0 (2000-12) Technical Report; 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Report on the Evaluation of 3GPP Standard Con_dentiality and Integrity Algorithms (Release 1999).

[18] N. Gobbo, A. Merlo, and M. Migliardi. (2013). "A denial of service attack to GSM networks via attach procedure," Proc. ARES Workshop, vol. 8128, [Online]. Available: http://dx.doi.

[19] 3GPP, (2012). TS 24.008—Mobile radio interface Layer 3 specification; Core network protocols; Stage 3. [Online]. Available: http:// www.3gpp.org.

[20] Tao Peng and Christopher Leckie and Kotagiri Ramamohanarao (2006), "Survey of Network-based Defense Mechanisms Countering the DoS and DDoS Problems," ACM Transactions on Computational Logic.

[21] 3GPP. TS 44.006 | Mobile Station - Base Stations System (MS – BSS) interface Data Link (DL) lay specification. http://www.3gpp.

[22] Patrick Traynor, William Enck, Patrick McDaniel, and Thomas La Porta. Mitigating attacks on open functionality in SMS-capable cellular networks. In Proceedings of the 12th annual international conference on Mobile computing and networking, ACM, 2006.

Authors Profile

V.Palaniyappan received the B.E. degree in computer science and engineering from Karpagam Institute of Technology, Coimbatore, Anna University Chennai in 2013. He is currently pursing M.E (CSE) From VSB College of Engineering Technical Campus, Coimbatore.

Mr.M.Duraipandian received B.E., M.E., Degree in the Branch of Computer Science and Engineering from Kumaraguru College of Technology, Coimbatore. He is currently pursuing his Ph.D in Anna University, Chennai. Presently, he is working as an Associate Professor in the Department of Computer Science Engineering, VSB College of Engineering Technical Campus, Coimbatore. His Ph.D dissertation focused on "Network Security". He is a Fellow member in Indian Society for Technical Education and Computer Society of India.

K. Malarvizhi received the B.E. degree in computer science and engineering from Bharathiar University, Coimbatore in 1993. She Received the M.E. degree in software engineering from Anna University, Chennai in 2005. From 1998 to 2003, she worked at Sri Ramakrishna Engineering College, Coimbatore. She is currently working in VSB College of Engineering. She has 15 years of teaching experience in reputed engineering colleges and 4 years of research experience. Her current research interests focus on wireless networks, delay analysis, high speed networks and optimization techniques.