Identifying and Removing DDoS Attacking UMTS Network for Simless Nodes

Yasmeen Patel
PG Student
Department of Computer Science and Engineering
Nagpur Institute of Technology

Mr. Jagdish Pimple
Lecturer
Department of Computer Science and Engineering
Nagpur Institute of Technology

Abstract

In this paper we consider security of internet access over the Third Generation (3G) telecommunication systems. We Consider Universal Mobile Telecommunications System (UMTS) is selected as the most popular system among 3G systems. Here we detecting and removing DDos attack in UMTS network. The study then focuses on network access security mechanism of UMTS denial of service, identity catching, and redirection as the most significant attacks against authentication mechanism. Furthermore, we provide some solutions and methods to improve and prevent these attacks in UMTS system. The Universal Mobile Telecommunication System, more commonly known as UMTS, is now the world's leading mobile telecommunication system serving over 4 billion subscribers worldwide. UMTS has got much popularity as the earlier GSM system failed to cope up with higher data rate demands and faced some major security flaws. Although the UMTS system is able to mitigate most of those security flaws, yet it is not invincible to the new threats emerging with new and more sophisticated technologies. Many different kinds of security breaches are possible against UMTS networks. In this short technical essay, we will focus only on the Denial of Service (DoS) attacks on the UMTS access network, we replace GSM network with UMTS network because of security flaws. Distributed Denial of Service (DDoS) attacks exhaust victim's bandwidth or services. In this paper, different types and techniques of DDoS attacks and their countermeasures are reviewed. We also discuss some traditional methods of defence such as trace back and packet filtering techniques so that readers can identify major differences between traditional and current techniques of defence against DDoS attacks. Before the discussion on countermeasures, we mention different attack types under DDoS with traditional and advanced schemes while some information on DDoS trends in the year 2012 Quarter-1 is also provided. We identify that application layer DDoS attacks possess the ability to produce greater impact on the victim as they are driven by legitimate-like traffic making it quite difficult to identify and distinguish from legitimate requests. The need of improved defence against such attacks is therefore more demanding in research. The study conducted in this paper can be helpful for readers and researchers to recognize better techniques of defence in current times against DDoS attacks and contribute with more research on the topic in the light of future challenges identified in this paper.

Keywords: packet filtering, packet dropping, UMTS network, client's nodes, time frame based technique

I. INTRODUCTION

The growing popularity of mobile devices has led to the rise of mobile malware. It is also one of the reason why amount of new mobile malware families, which are secretly connected over the internet to a remote command and control server. Through mobile device an attacker can spread classic DENIAL OF SERVICE attacks that are distributed through pcs. 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 equipment's 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

Users of mobile devices also suffer from various DOS attack .DOS attack which are targeting mobile devices are jamming attack, flooding attack, and blocking attack. Here in our paper the DDOS attack works on single node. In network the DDos attackers are placed the are installed in the computers as name zombies. They attack on single node in the network. This single Node provides service to the other node in the network. The attacker attack on the nodes which provide services and Make the node overload with the message packet. Due to heavy load the node fails to give response to other nodes in the network which sends request. The attacker delays the request of client node in the network.

To resist the Dos attack we scan the nodes one by one. But scanning one by one is very time consuming, so we switched toward the DDos attack . In DDOS attack scanning starts with group of node and extra packet is drop and congestion is control. Distributed denial of service (DDoS) *attack* aimed to remove 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

II. LITERATURE SURVEY

A. Abusing Mobile Devices for Denial of Service Attack:

(Liberious Vokorokos, Pvol Drienik, Olympia fortotira, IEEE January 22-24, 2015) Say that growing popularity of mobile devices leading to mobile malware. Which are secretly connected over the internet and control server this. Here we presents proof of concept which is used to abuse mobile devices capability for malicious purposes, Distributed denial of service attack is presented using smart phones with android operating system against wireless network. DDos was successful against whole network as all network element is connected via access point where congestion mechanism happen .thus we will successful in overload the server connection.

B. A Denial of Service Attack to UMTS Networks Using Sim-less Devices:

(ALlesso Merio, Mauro Migliard, Nicola, Franscesco palmerie and castigilione, member IEEE, may-june 2014) Says that one of the fundamental elements in cellular network is the authentication procedure performed by subscriber identity module and hence protect from the unauthorized usage. Here we present a new kind of denial of service attack based on properly crafted sim-less devices which create bottleneck in the network.umts protocol flaws is used to launch dos attack. If attacker disposed the list of IMSI .The request packet is attached with IMSI to force umts to start communication this indicate the effectiveness in Ddos attack.

C. Evaluation of Security Attacks on UMTS Authentication Mechanism:

(Mojtaba Ayoybi Mobarhan, Moastafa Ayoubi Mobarhan member IEEE, July 2012) In this approach secret key mechanism is used. Due to the importance of the secret key Says this study security of internet access over the Third Generation (3G) telecommunication systems is considered and Universal Mobile Telecommunications System (UMTS) is selected as the most popular system among 3G systems. We focuses on network access security mechanism of UMTS, called Authentication and Key Agreement (AKA). In addition, twenty types of important attacks and threats in UMTS system are presented and classified based on three major security factors; authentication, confidentiality, and data integrity. The evaluations finally show that the authentication factor is more interesting than other factors for hackers. Then, we describe four attacks named; man-in the-middle, denial of service, identity catching, and redirection as the most significant attacks against authentication mechanism. Furthermore, we provide some solutions and methods to improve AKA In first measure, we can use a protocol that has already been proposed and we can enhance it order to assure adequate protection for the master key. This protocol is the Enhancement Mobile Security and User Confidentiality for UMTS that was proposed for the protection of IMSI. Whenever possible a temporary identity the TMSI, is used. Furthermore, the TMSI is sent encrypted over the radio link. Correspondingly, we propose that the AV be generated using a TK, instead of the K. For the establishment of the secret key TK we propose adapting the EMSUCU protocol. A new TK will be generated each time the Enhanced EMSUCU protocol is performed. As we discussed in section 3, in the UMTS security standard when the crypto period of the keys pair CK, IK has expired the ME will delete their value.

D. Denial of Service Attack on Umts Network:

(Kazi walli ullah IEEE member, November 13, 2011) Say that the Universal Mobile Telecommunication System, more commonly known as UMTS, is now the world's leading mobile telecommunication system serving over 4 billion subscribers worldwide. UMTS has got much popularity as the earlier GSM system failed to cope up with higher data rate demands and faced some major security flaws. Although the UMTS system is able to mitigate most of those security flaws, yet it is not invincible to the new threats emerging with new and more sophisticated technologies. Many different kinds of security breaches are possible against. To set up the communication unprotected message is send by server to the client due to unprotected signaling message make the UMTS network, vulnerable to Dos attack.Threfore some mechanism is developed to protect the attack. UMTS networks. In this short technical essay, we will focus only on the Denial of Service (DoS) attacks on the UMTS access network.

E. Dos attack Exploiting Signaling in UMTS and IMS:

(1Georgios Kambourakis, 1Constantinos Kolias, 1Stefanos Gritzalis, Jong Hyuk Park IEEE member, 2009) says that, The Universal Mobile Telecommunication Standard (UMTS) is continuously evolving to meet the growing demand of modern mobile and Internet applications for high capacity and advanced features in security and quality of service. Although admittedly enhanced in terms of security when compared to 2G systems, UMTS still has weaknesses that can lead to security incidents. Here we investigate the vulnerabilities of the UMTS security architecture that can be exploited by a malicious individual to mount Denial of Service (DoS) attacks. Our focus is on signaling-oriented attacks above the physical layer. We describe and analyze several novel attacks that can be triggered against both core UMTS architecture as well as hybrid UMTS/WLAN realms. An additional contribution of this paper is the presentation of an extensive survey of similar attacks in UMTS and related protocol infrastructures such as IP Multimedia Subsystem (IMS). Finally, we offer some suggestions that would provide greater tolerance to the system against DoS attacks.

F. On Detection of Signaling Dos Attack on 3G Wireless Network:

(Patrick P. C. Lee, Tian Bu, and Thomas Woo IEEE member, 2007)
Says that third generation 3g based CDMA and UMTS are growing throughout the world. Because of their complex signaling and limited bandwidth .here we find the dos attack called signaling attack using simulation devices by real traces we are able to demonstrate the impact of signaling. By using intrusion detection algorithm which are signature and volume based. we use trace driven simulation we can identify the attack Our detection mechanism is robust as it is depend solely on additional signaling and based on any assumed attack strategy.

III. COMPARATIVE STUDY OF LITERATURE SURVEY

Sr.no	*Title of Paper*	*Author Name*	*Method /Algorithm used*	*Drawbacks*
1.	*Abusing mobile devices for Denial Of Service Attacks*	*Liberious Vokorokos Pvol Drienik,Olympia fortotiraI IEEE member, January 22-24, 2015)*	*Ping Flood Method is used which provide attack.*	*The Server is able to response even if the network is LAG.*
2.	*A Denial of Service Attack to Umts Networks Using Sim-less DevicesEvaluation of Security Attacks on Umts Authentication Mechanism*	*ALlesso Merio Mauro Migliard,Nicola, Franscesco,palmerie andcastigilione, member IEEE, may-june 2014*	*UMTS radio interface is used to inject the signaling traffic*	*The device is not owned by user it is placed by attacker which is dangerous and create cyber warfare.*
3.	*Evaluation of security attack on umts Authenticartion Mechanism*	*AyoubiMobarhan,Moastafa Ayou Mobarhan member IEEE, July 2012*	*Authentication and Key Agreement protocol is used which is based on secret key*	*Threats were found and presented.*
4.	*Denial of Service Attack on Umts Network.*	*Kazi walli ullah IEEE member november 13, 2011*	*Radio Resource Control Device is used to establish connection.*	*Packet is sent which is not encrypted which results in packet sniffing and spoofing.*
5.	*Dos Attack Exploiting Signaling in Umts and IMS.*	*GeorgiosKambourakis, Constantinos Kolias, 1Stefanos Gritzalis, Jong Hyuk Park IEEE member, 2009)*	*128bit Symmetric Secret Key is used.*	*Weakness found in signaling due to which attackers become more powerful*
6.	*On Detection of Signaling Dos Attack on 3G Wireless Network*	*Patrick P. C. Lee, Tian Bu, and Thomas Woo IEEE member, 2007)*	*Radio channel is used along with RNC and Base stations.*	*This attack is based on assume attack strategy which create false positives.*

IV. PROBLEM STATEMENT

In the earlier scenario, to mount dos attack against mobile network is not the big deal. In order to make the attack successful the methodology based on GSM is required. In this work we have explored the different approach. First approach is the use of cellular device to establish the connection but this approach is failed because the requesting packet is not encrypted which shows all information including IMS number due to which packet spoofing attack occurs. Similarly in second approach using ping flood attack the DDOS is successful in creating the load on server but due to mobile devices attacker has possibility cheap and create botnet for Denial of service attack .they create extra traffic on network which is the drawback of this approach. In the next approach Key agreement protocol is used to create the Ddos attack .The result of this attack is make the resources and services available to authorize client. But this approach is weak because threats were found. In the next approach 3g along with umts network is used to resist DDos attack and add some security features for network. After surveying related work it is found that some malicious hazardous addition flaws are exploited the network..Due to which weakness found in signaling.

V. PROPOSED APPROACH

In our approach we propose a method by which DDOS attacks can be detected and removed in sim-less device environments. Our approach will be based on a time based tracking system, which will check the number of packets arriving in a particular time frame, and then take an action.on the basis of digital signature packets is searched. If the nodes are sending packets in a particular signature, then we can decide that the particular set of nodes is performing DDOS attack and we can remove them from the network. This will help us to improve the efficiency of the network, by reducing the overall delay and energy consumption needed to transfer a packet successfully from source to destination.

UMTS security is built on the success of GSM by retaining its strong security features and advantages. Although GSM security has been very successful compared to 1G, one of the purposes of the UMTS security design was to address its original and noticed GSM weaknesses. The following are some of these weaknesses and threat Unidirectional Authentication and Key Agreement (AKA) protocol. Possibility of replay attacks.

- Cipher keys and authentication data are transmitted in clear between and within networks.
- Encryption does not extend far adequate towards the core network and data is transmitted in Clear on the microwave links.
- 2G systems do not have the flexibility to upgrade and enhance security functionality overtime. Therefore, 3G defined the UMTS system to improve security of communication systems. It provides a high level of security in comparison with GSM. It also prepares significant improvements to overcome the vulnerabilities in the 1G and 2G systems. These improvements include mutual authentication, freshness and liveliness assurance of AKA, sufficient and suitable Integrity Key (IK) and Cipher Key (CK) sizes (128 bits) and data integrity of signaling messages in radio interface. The following are the major aims of carrying out this work.

1) The most important security mechanisms of the UMTS system are presented.
2) Most efficient attacks on UMTS system are studied and analyzed.
3) UMTS attacks are classified based on three major factors and demonstrate authentication is more attractive than others for attack.

VI. MODULES USED IN THE PROJECT

1) Development of wireless network for simless devices
2) Application of DOS attack from one node
3) Application of DDOS attack from various nodes
4) Detection of DOS and DDOS based on the time frame approach
5) Result analysis and comparison

A. Development of Wireless Network for Simless Devices Module:

We create the wireless network by shutting down the large portion of network without need of controlling user terminal. The attack actual does not required valid handset equipped with SIM it only require the UMTS radio interfaces

B. Application of DOS Attack from One Node Module:

When the setup is ready the single client attacker makes attack on the server node. The node sends continuously the requesting packet to the server which exceeds the capacity of server due to which it fails to response to other requesting node.

C. Application of DDOS Attack from Various Nodes Module:

In this module more than one attacker is placed in the network.at a time more than one attacker node starts attacking the node simultaneously on the server node make the server busy for the longer period of time.

D. Detection of DOS and DDOS Based on the Time Frame Approach Module:

Here we calculate the time required to trace the Dos attack with respect to Ddos attack. In Dos attack the scanning of node starts with node to node which required time while in Ddos attack the scanning is done group by group and search the attacker. As the attacker found the packet that comes from attacker is start dropping.

E. Result Analysis and Comparison Module:

Here the output of Dos and Ddos attack is compare.

VII. METHODOLOGY

In proposed system, we developed the network with sim-less devices. Though mobile devices an attacker can spread classic Denial of Service Attack that are distributed through pcs the aim of the attack is to make the resources un available to the requesting client. In the network the client, machines and single server machine are present. They communicate with each other by sending packets.

When the client requesting the server to provide the service, the attackers starts attacking the server by continuously sending the data packet. They overload the server such that he fails to respond to client machine that request for the service due to which time delay occur and traffic is create in the network. To overcome this drawback the scanning of node is done. The scanning is done by covering maximum node i.e. group of node .In Dos attack scanning id done node to node one by one due to which time required. While in ddos attack Scanning is done group by group which takes less amount of time. During Scanning if attacker found then the packet which is send by attacker is dropped due to which traffic is control and Ddos attack is overcome.

VIII. EXPECTED OUTCOME

A. Reduced Delay:

To analysis the traffic in the UMTS network algorithm is used.to identify the attacker in short period of time we used such technique which reduced delay in finding the attacker. Traffic which is created is overcome and handle quickly.

B. Reduced Energy:

As number of nodes is present in the network large amount of energy is required so to save the energy, when the communicating is not carried out all the nodes goes to sleep mode .they are active only when the communication established.

C. Improved Throughput:

It improved the packet delivery over the communication channel. This system perform well even when traffic is occur over the network and produced maximum throughput

REFERENCES

[1] 3GPP, (2012)Ts.25.214-physical layer procedure(FDD)htttp://www.3gpp.org/ftp//spec/html-Info/25214.htm.
[2] J. W. Hui and P. Thubert, "Compression format for ipv6 datagrams over ieee 802.15.4- Based networks." IETF Proposed Standard, (ISSN: 2070-1721) Available [Online] http://tools.ietf.org/html/rfc6282, Sept.2011
[3] "European project- "enabling the business-based internet of thingand services"." Website [Online] http://www.ebbits-project.eu/news.php,Accessed May 2013.
[4] "Suricata- The Next Generation Intrusion Detection System." [Online] http://www.openinfosecfoundation.org, Accessed May 2013.
[5] R. Tomasi, L. Bruno, C. Pastrone, and M. Spirito, "Meta-exploitation of ipv6-based wireless sensor networks," in 3rd international workshop on Security and Communication Networks - IWSCN, (Gjøvik - Norway),
[6] Sooyeon Shin, Taekyoung Kwon, Gil-Yong Jo, Youngman Park, and H. Rhy, "Experimental Study of Hierarchical Intrusion Detection for Wireless Industrial SensorNetworks," IEEE Transactions on Industrial.
[7] T. Winter, "Rpl: Ipv6 routing protocol for low-power and lossy networks." IETF RFC 6550, Available [Online], http://tools.ietf.org/html/rfc6550, Mar. 2012.
[8] S. Raza, L. Wallgren, and T. Voigt, "Svelte: Real-time intrusion detection in the internet of things." Ad Hoc Netw http://www.sciencedirect.com/science/article/pii/S1570870513001005
[9] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary, "Wireless sensor network security: A survey," Security in distributed, grid, mobile, and pervasive computing, vol. 1, p. 367, 2007.
[10] D. Evans, "The internet of things. How the next evolution of the internet is changing every everything," CISCO white paper, 2011.