INTERNATIONAL JOURNAL OF SCIENTIFIC & ENGINEERING RESEARCH, VOLUME 4, ISSUE 1, JANUARY-2013
ISSN 2229-5518

TO Overcome DoS and DDoS Flooding Attacks in IP Multimedia Subsystem (NGN) using the Genetic Intrusion Detection Systems (IDS)

Muhammad Tayyab, Ahmed Mateen Buttar, Milhan Afzal Khan, Muhammad Awais

Abstract

IP Multimedia Subsystem designed by the 3rd Generation Partnership Project to provide the access networks services and telecommunication services, plans to merge services like multimedia, data and voice conversation under one umbrella. In this research, network based anomaly detection system is proposed by using Genetic Algorithm rules to avoid such attacks like IP Spoofing and UDP Flooding which cause the DoS and DDoS attacks keeping in view to secure the IMS and also discussed the complete overview of IMS (NGN) based network architecture, their DoS and DDoS attacks which cause the unavailability of services to the users.IMS inherits many security issues because the No of billions users are in the form to interact with IMS to get large No of services like multimedia, data or voice conversation. Due the large usage of IMS services there is also the availability of malicious user to attack the IMS services and make the services unavailable for the intended user, which reduces the performance of IMS. IMS based abnormality detection method is proposed using GA as abnormality detector. Genetic Intrusion Detection system effectively detects intrusive attack in IMS system and shows low false positive results.

1 Introduction

The IP Multimedia Subsystem standard introduced by the 3GPP is the heart of the future next formation of telecommunication industry. Residentially designed by the 3rd Generation Partnership Project for the better quality of services of multimedia to the intended users, IP Multimedia Subsystem's total functioning is depends on the Session Initiation Protocol for signaling the messages from source to destination and also its execution depends on Internet Protocol. The IMS open core network brought revolution in the fields of telecommunication industry and also introduced the rich multimedia services like video streaming, data sharing and voice calls under one platform.

Muhammd Tayyab MPhil Computer Science in networks from University of Agriculture Faisalabad
Email: mastermind.338@gmail.com
Ahmed Mateen Buttar is Lecturer/Supervisor in University of Agriculture Faisalabad Computer Science Dept.
Email: ahmedmatin@hotmail.com
Milhan Afzal Khan MPhil in Computer Science from University of Agriculture Faisalabad.
Email milhankhan@gmail.com
Muhammad Awais is a Research Scholar.
Email: philpy18@yahoo.com

By adoption these changes come to the new consign of challenge for offering a safe and secured verity of services to the subscribed users. IMS perform functioning on basis of session initiation protocol and internet protocol; it comes into many known security confront with these protocols.
In particular, there has been lot of work is done or in progress in recent past years on both issues and

Providing the resolution for SIP based VoIP protection. There are three primary goals that are most frequently quote for the IMS frame work, Integration of Services, Billing and Charging and Quality of Service (QoS). In concise, the last two objective of IMS shows that next generation network architecture are mainly depends on the packet switched architecture that is based on internet protocol which offers the best service that can never be offered ever before. That's why; most of the VoIP application spreader cannot suggest any announcement for the users understanding or nor can they suggest enhanced value billing and charging edge for the network sources. A vital intention of the IMS standards is to provide the architecture for setting up VoIP and multimedia video streaming applications that offers for both quality of Services and Charging or Billing. The

third aim of IMS standards is to provide mechanism for proficiently incorporating several diverse verities of services that are used to be combined without trouble and harmonized to meet the user's requirements. The main objective of design and practical implementation of IMS is to reduce the requirement to generate the predictable highly definition applications that should be contains all attributes and characteristic in a sole function and do not simply assimilate with other functions (Hunter *et al. 2008).*

1.1 Market Factors and Trends

Tendency in the technology changes, customer/corporate client's trade behavior and prospect, or cost pressures of operators, authoritarian alter, and physical and biased changes are just some of the pressure is going to diverse in the field of telecommunications industry. Even though the uses of services are going increasing rapidly day by day, average revenue earning by per user are going to the downward, driving network operators are now in trying to achieve new mechanism for permanently revenue earning, and profitability (kinder, 2005).

1.2 Maturity of VOIP Services and Technology

In contrast with all further service and technology providers, IP and the Internet services have continuous to acclimatize, expand, and breed in the No of architecture it can be elated crossways, functions which are to be supported by them, and devices within which it is included (kinder, 2005).

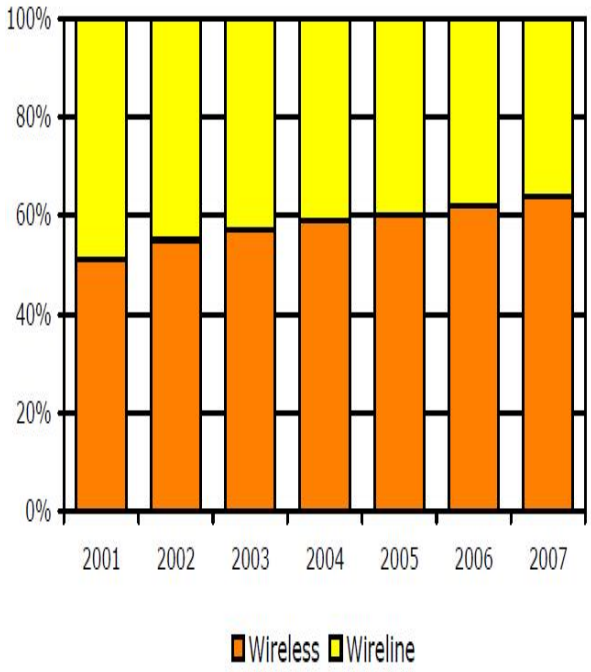

Fig 1: Increasing of proportion of wireless subscribers.(Kinder, 2005)

2. Migration from Public Switch Telephone Network to Next Generation Network

The NGN stands for a fusion of currently, so this is time to move towards from public switched telephone network traditionally network future packet based IP network for providing the rich set better quality of services of multimedia to the users of the internent. The financial and authoritarian preparations for the both networks PSTN or NGN have traditionally been very dissimilar. What are happened when these two traditional worlds strike? Most of the networks providers over the last ten years hold many of the most key components of an NGN for the further deployment. Nearly all, if not all, of the technology essential for Internet Protocol based network connection has been accessible for five to ten years to the end user for the verity of services like multimedia, telecommunication services etc. Highly formatted mechanism to connection have been unhurried to organize, yet where the technology standards have been grown up or within coming distance of development (Marcus 2006).

3. IDPS Technologies

By using the Intrusion Detection System with IMS Frame Network we can deal with no trouble that DOS and DDOS attacks from the regular users. In Intrusion Detection System there are set of laws set for the nasty users to do not go into the IP Multimedia Subsystem Network to build the services engaged for the planned users. An Intrusion Detection System the tools or software's which are to be used in network to scrutinize the network data traffic for the nasty use or policy violate and constructs the statistical reports to the management systems to take action alongside the intrusion. The primary goal of Intrusion Detection Systems is to spotting the likely incident, sorting information regarding them and reporting endeavors (Scarfone, 2007).

3.1 Key Functions Supported by IDPS Technologies

There is something fascinating to notice which shows that there is something going erroneous and probably take action on. By executing the intrusion detection system with some rules to explore the spiteful traffic in IMS frame work, can simply mitigate the DOS and DDOS attacks. IDPS is the procedure of scrutinizing the trials going on into computer design architecture or network and examining them from malicious indication of likely events, that are contravention and forthcoming intimidation that breaches computer based security set of standards , suitable use strategy, or standard rules of security practices that are mostly used in network from avoiding the anomalies. Intrusion detection and prevention system is the procedure for detecting the intrusion and anomalies in network and also trying to prevent from the identified probable happenings. Intrusion detection systems (IDS) are mainly paying attention on identifying probable happenings logging information of malicious user, trying to stop them from logging the systems which they want to attack, and also providing the information regarding the anomalous behavior to network security administrators for performing the right job to make the services available to the end users (Scarfone, 2007).

4. Networking Attacks in IMS

By means of the maturity of technology changes in networks and function changes, network assaults are very much growing both in services, shapes and sternness. Intrusion detection system is the key component in the field of network security in order to provide the security solution in network design and also plays vital role in the field of network security for detecting the anomalies. Foremost IDS main function is to debugs anomalies from different normal audit data traffic and this can be taken as serious issues in the network and need to act in order to safe from those anomalies in future. IDS are the one of important technology in the field of computer science and brought the revolution in this field, which can sense, avert and maybe respond to against the anomalous behavior (Gandhi and Srivatsa 2008).

5. Denial of Services Attacks in IMS

Denial of service anomalies persists to terrorize networks and computers whether they are connected to the internet. As reported submitted by the CSI/FBI 2003, 42% of users of internet and computer network pointed out DoS anomalies were a foremost issue for them which they faced. Economic retards due to denial of services anomalies that were the 2nd major reason of revenue loss in business industry. CERT explains the denial of services anomalies as "the avoidance of sanctioned way in to a system resource or slowing the system from its operational functioning" and also cause for the unavailability of services. Though extra nomenclatures for denial of systems anomalies subsist, denial of services anomalies are classically estranged into two wide ranging classes: logic based irregularities, that make use of vulnerabilities in a system's software to leave it powerless to act to suitable user requirements; and flow based attacks, which tire out on hand resources, such as CPU utilization, usage of network bandwidth, system storage devices again depicting the objective machine insensitive to desires (William *et al* 2008*).*

6. Problem Statements

Without having any doubt in mind, there are fabulous challenges both technical and in business aspect in the deployment of IMS in real world or in commercial area. Telecommunications business industry are always in trying and struggling to provide the new set of services as the users demand and keep pace with increasing the service demand in the communication business industry. With subscribers demanding the new rich multimedia services and with the prices go down

due to the larger services providers in the telecommunication industry, the old telecommunication business standards need to be updated for achieving the user's requirements. IMS is the open core network provides the possibility to either compete or integrate with over-the top (OTT) application providers.
Internet and cellular companies have combined together for transforming the communication to the end user, and due to the large development such as the cloud computing, IPTV, Wireless Broadband, location services and in the telecommunication industry there is need to establish a one infrastructure for sharing the large no of services like multimedia, Data and Voice conversation under one umbrella.IMS research offers a portfolio of the market research services in this area to address your needs in understanding these trends and market imlications.IMS is not commercially adopted in the market and due to this reason it is a very good domain for research point of view. The objective of this research is to secure the IMS framework from the IP Spoofing and UDP flooding attacks which cause the DoS and DDoS attacks and makes the service unavailable for the indented users. These attacks would be mitigated using the IDS with the help of GA Rules which I implemented in IMS frame work.

7. Problem Solutions

In this research I discussed the complete overview of IMS architecture, its services like multimedia, data sharing, instant messaging, video call etc., also discussed the attacks which cause the DoS and DDoS make the services unavailable for the intended users. IMS standard introduced by the 3GPP is network that provides the lot of services under one umbrella but unfortunately 3GPP not providing the any service mechanism or any security standard which prevent the IP Multimedia Subsystem from the malicious users whose are always in trying to destroy services and make the services unavailable for the end users. This is main problem and main issue in IP Multimedia Subsystems which I discussed in my research and proposed the mechanism based on the Genetic Algorithm Rules with the help of Intrusion Detection system that detect the anomalies or malicious traffic that affect the services of IMS and also reduce the performance of IMS.

Addressing all those methods and signifying a new method on IP systems that can search the system IP on the network much faster than the existing methods. Such method has its own time variation in maintenance of a network which is frequently dependent on total number of nodes. In this research I proposed mechanism for detection UDP Flood and IP Spoofing attacks on main key component Proxy Call Session Control Function which is the entry point to IMS to get the services of IMS. There are many research has been carried out on the DoS and DDoS in IMS in order to protect the SIP signals in IMS but no any research carried out in order to protect the main key component PCSCF in IMS form the UDP and IP Spoofing attacks which makes the service unavailable to the users or reduced the performance of IMS.

8. Purposed Solution for detection IP Spoofing Attacks in IMS Using GA based IDS.

In this research work I proposed the solution to overcome IP Spoofing and UDP flooding attacks which cause DoS and DDoS floods in IMS introducing the Genetic Intrusion Detection System with GA rules. GA will be used for developing simple rules for monitoring the network traffic with the help of Intrusion Detection System. These rules will be used to distinguish the regular network connection from the irregular network connection. These irregular connections pass on to events with chance of intrusions. In this research I focused on the key point of IMS architecture known as Proxy Call Session Control Function this is the entrance point to the IMS core architecture and this will be my primary responsibility to secure this section. Intruders can attack to this entrance point to corrupt the performance of IMS core network.

GA abnormality detection system used in IMS framework to produces the rules which will use to match only the irregular connections and this method is used to overcome the IP spoofing and UDP Flooding attacks from IMS which cause the DOS and DDOS Flooding attacks. With the intrusion detection system send appropriate reports to administrator of IMS network for further necessary action. Experiments are applied on the IMS core networks and the results shows that IMS is free from DOS and DDOS attacks. By implementing this mechanism it will be very difficult for the malicious user to attack the IMS

and make the services unavailable for the intended user.

8.1 IP Spoofing Attacks

The idea of IP spoofing is firstly launched in 1980 in educational ring. This method is used to append the illegal access to the users to access the network services, where the impostor sends the messages or data packets to the computers with the IP address which signify that message or data packets in this traffic is come from the reliance source or from the reliance host. To engage in IP spoofing, hackers always in trying to detached the system and must be familiar with verity of method to know the IP address of the wounded computer to attack and then make the modification the header so that it seems that the traffic is coming from the reliance host, make the service unavailable to the users.

8.2 Proxy Call Session Control Function in IMS

Technology propensity are rising and altering frequently and rate of change is not the issue of years, months or weeks but the days. The similar is as true for malevolent users. With the entrance of new services, information and devices, the chance of malicious users and attackers are rising day by day which cause delay to in attack difficulty. Due to the malevolent behavior on the network reduce the performance of services. Among them DoS and DDoS attacks are very famed in the form of network nodes.

Like several other IP networks, IMS network is susceptible to number of security Issues. The 3GPP IMS and related specifications like ETSI TISPAN is incorporated with necessary support for signaling protection and for media traffic but this safety measure not fulfill the all security requirements. They do not provided the security mechanism against denial-of-service (DoS) attacks and DDoS or many other anomalies. DoS and DDoS attacks are design to make the services unavailable for the intended users. Conventional DoS and DDoS attacks are ready by develop a buffer overflow, exhausting system resources and exploiting a system bug which results in that system is not functionally more or services are unavailable for the users.

In this research I focused on the main key point of IMS that is Proxy Call Session Control function. I First tried to secure the PCSCF from DoS and DDoS attacks to make services live for the users. The main attacks which I discussed in my research is UDP Flood and IP Spoofing that cause the DoS and DDoS which reduce the performance of IMS architecture and ake the service unavailable for the end user.

PCSCF is the entry point to the IMS Framework. User with their equipments like laptop, cell phone interacts with the IMS networks through PCSCF for getting the services like data, video calls and multimedia services. Securing PCSCF is my major responsibility because IMS will be faces many threads in security. PCSCF is susceptible with dissimilar types of attacks. IMS is currently based on SIP, IP or RTP protocols for the communication with user or for the signaling purpose. That's why it intrinsic the defenseless related to these protocols. Some of the possible attacks that may disgrace the performance of IMS due to these protocols are described in the Fig 2.

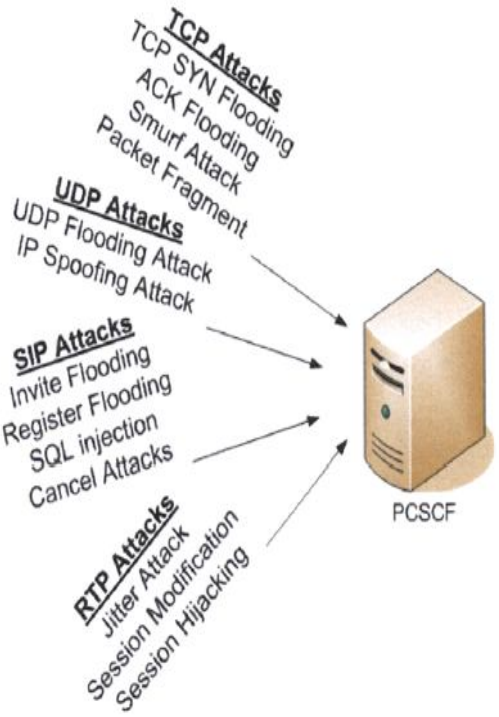

Fig 2: Intruders that attacks PCSCF in IMS core

Network based anomaly detection mechanism works on every data packet that is received. We have used the same mechanism in our proposed approach. The methodology is mentioned in Fig 14. USERS communicate with IMS through PCSCF. The packets are received at PCSCF through Gm reference point. The anomaly detection will work like that:

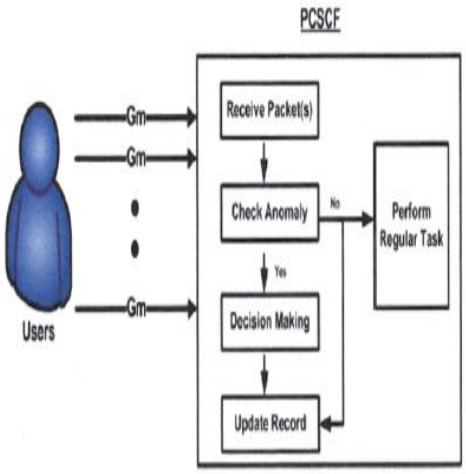

Fig 3: Anomaly Detection in PCSCF

1) Create the initial data set. There are four attributes or characteristic of each data set (i.e.) Source IP Address, Destination IP address and Destination Port and Duration of connection.
2) There is also some blacklisted IP address is entered in IDS.
3) There are some ports which is used by the different server in IMS given as under.
    - P-CSCF uses 4060
    - I-CSCF uses 5060
    - S-CSCF uses 6060
    - HSS uses 3868,3869,3870
4) Suppose that the new packet is received from the user. Compare the packet with each data set and if the packets information is matched with data set then proceed else reject that packet.
5) Store the number of attributes of packet received positive in an array and then verify them.
6) Find the maximum matched found.

The Example of Data set is given as under.

if { source IP address 10.96.134.32; destination IP address:

172.16.111.3; destination port number: 8080; connection time: 10.1 seconds }

then {stop the connection}

This rule can be explained as follows: if there exists a network connection request with the source IP address 10.96.134.32, destination IP address 172.16.111.3, destination port number 8080, and connection time 10.1 seconds, then stop this connection establishment. This is because the IP address 10.96.134.32 is recognized by the IDS as one of the blacklisted IP addresses; therefore, any service request initiated from it is rejected.

In this approach, the network traffic in IMs Framework used for GA is a pre-classified data set that distinguishes b/w normal and anomalies. This data set information is gathered using network sniffers Snort. The data set is physically confidential based on expert person's information. It is used for the strength assessment during the implementation of GA. By initial GA there are only small set of anomalies rules are used, we can also get the larger data set rules based on anomalies detection which is more enough for the GA to detect the anomalies. By implementing the IDS with GA rules i can say that now P-CSCF which is main key component of IMS frame work is now protected from the anomalies and now free from the UDP and IP Spoofing attacks. When attackers try to fetch the information from the IMS by using the UDP flooding attacks technique or by using the IP Spoofing technique, Installed IDS at the key component of P-CSCF in IMS provides the information about those attacks in the form of statistical reports.

8.3 Snort Intrusion Detection System

Snort is stands for supersonic naval Ordnance Research Track. Snort is the leading open source intrusion detection and prevention system used for detecting the malicious traffic and reported that traffic to network administrator to take action against that malicious users. It is also employing the lots of preventative measures such as firewalling, patching and also intrusion detection. Detection system from anomalies can give you assurance that your system is more effective from attacker, If not then providing the valuable information about what you need to improve.

Summary

With the increasing of usage of cellular devices day by day and user eagerness of getting the wide range of services like multimedia, instant message sharing, video call etc. in his hand or just in the way where they are. It is necessary for the telecommunication industry to introduce such platform where the users get the all type of services within no time. IP Multimedia Subsystem is one the suitable example of such platform where the users gets the all type of multimedia services, data sharing, and video call streaming with no time also with the better Quality of Services and also in very low rate.IMS infrastructure provides all the services under one umbrella. Although IMS is still not practically implemented in real life as main transporter networks and its broad level execution are some years away. Next Generation Network is a packet based network architecture sends data in the form of packets to destination in predefined timeline, which is used to provide services like telecom Services and able to make use of several broadband services, QoS enabled transport technology in which service related functions are independent from basic transportation related technology. Though, the IMS framework supports the concept of combinational services such as Presence, Location, and Push-to-Talk that can be influenced for new applications. The IMS architecture is a product of the 3GPP standards organization. Formerly brought up in 3GPP Release 5, the IMS is designed as a cover to the Packet-Switched Domain, most frequently positioned over IP.

As a key technique or component in network security domain is Intrusion Detection System (IDS) that plays very important role of detecting a variety of anomalies and makes safe the networks from the intruders. Foremost function of IDS is to find out anomalies from among normal audit data traffic and this can be considered as classification problem and need to act in order to safe from those anomalies in future. Without having any doubt in mind, there are fabulous challenges both technical and in business aspect in the deployment of IMS in real world or in commercial area. Telecommunications business models are struggling to keep pace with increasing service demand. With subscribers expecting rich multimedia services and competition eroding prices, the old business models need to be updated. IMS core opens the possibility to either compete or integrate with over-the-top (OTT) application providers.

Due to the larger architecture and service feature in IMS framework, there are also some attraction are existing for the malicious users or anomalies to attack the IMS network and make the service unavailable for the users, one main objective is also of destroying the services of IMS. That type of attacks are knows as Denial of Services attacks. In this research a Genetic Intrusion detection based solution is proposed for detecting such attacks and make the services of IMS is available all time for all users. In this research I discussed the UDP flood and IP spoofing attacks both have the connection less architecture and can easily access the IMS network services by using the different techniques. Here intrusion detection based mechanism for the malicious traffic with some set of Rules of Genetic algorithm at the key component of IMS Proxy call session Control Function which is also the entry point to IMS. User cannot subscribe the IMS services without the PCSCF. By implementing the Intrusion based detection system with some certain rules in Open IMS core environment results shows that the IMS is free from the DoS and DDoS attacks at the PCSCF point which causes the service engaged for the intended users.

Ref Literature Cited:

[1] [1] Hunter M.T., R. J.Clark., and F. S.Park., 2007. Security Issues with the IP multimedia Subsystem. *Workshop on Middleware for next-generation converged networks and applications*, PP: 9.

[2] [2] Kinder N., 2005. IMS-IP Multimedia Subsystem. *Proceedings of the International Multi Conference of Engineers and Computer Scientists*. PP: 657-668.

[3] [3] Marcus.S.J., ITU Workshop., 2006. What rules for IP-enabled NGNs? *INTERCONNECTION IN AN NGN ENVIRONMENT. Geneva,* Document: NGN/ 02.

[4] [4] Scarfone K., 2007. *Guide to Intrusion Detection* and *Prevention Systems. National Institute of Standard and Technology) Special* Publication, *PP:* 800-94.

[5] William W., D.J. Fired., and R.K. Cunningham., 2008. Detecting Flood Based Denial of services Attacks with SNMP/RMON. *The First International Conference on Availability, Reliability and Security*. PP: 45-60.