Towards Security and Enrichment of the IP Multimedia Subsystem Based Multiparty Conference

Zeeshan Shafi Khan, Muhammad Sher, Khalid Rashid, Imran Razzak

***ABSTRACT*- Next Generation Networks (NGN) focuses to improve the telecommunication core and access networks and plan to transport all the services by encapsulating them into packets via a single IP based network. IP Multimedia Subsystem (IMS) serves as a Service Delivery Platform for NGN. Conference, one of the main services provided by the IMS, allows the multiple users to communicate at a time. This service is subject to various types of flooding attacks (i.e. Invite Flooding Attack, REGISTER flooding attacks etc), internal threats (i.e. SQL Injection) and session based attacks (Session teardown attack, session modification attack etc). Moreover a single participant of the conference service is fully authorized to refer any number of other participants. It can result in dissatisfaction and conflict among the existing participants of the conference. The referred participant becomes the fully authorized member of the conference which limits the applicability of the conference service in the real life. To mitigate the effect of flooding attacks and internal threats we developed an Intrusion Detection and Prevention (IDP) system. Election based distributed referring authority mechanism is proposed to handle the conflict arise due to the single participant based referring. To span the scope of the conference service in maximum number of real life scenarios parameterized refer request is introduced in the paper. Results are validated through deployment of the proposed solution over IMS testbed.**

***Keywords:* Next Generation Networks, IP Multimedia Subsystem, Service, Conference, Intrusion Detection and Prevention**

I. INTRODUCTION

In future it is planned that all the telecommunication core and access networks will use IP for the transportation. The kind of network in which traffic of all access networks will be transported through IP packet encapsulation is known as Next Generation Networks (NGN). IP Multimedia Subsystem (IMS) provides architecture for fixed mobile convergence that includes variety of protocols. Session Initiation Protocol (SIP) is one of the main protocols of the IMS

A. IMS Architecture

IMS can be divided into three layers. The lower layer or layer one is called as user plan and it accommodates all the IMS users who want to use different IMS services. In order to obtain services an IMS user contacts the layer two known as IMS core where authentication and authorization takes place. IMS core mainly consists of Call Session Control Functions (CSCFs) and databases. Proxy Call Session Control Function (P-CSCF) acts as entry point to IMS core and forwards the request to Interrogating Call Session Control Function (I-CSCF), I-CSCF locates the appropriate Serving Call Session Control Function (S-CSCF) from the databases and forwards request to it. S-CSCF performs authentication by downloading the authentication data from Home Subscriber Server (HSS) and then forwards the request to application server if required. The upper most layer or layer three contains the application servers to provide different kind of services. In this research paper our focus is on Conference server upon which conference service is deployed.

B. IMS conference Service

A conference is a service that allows multiple users to communicate at a time. The conference involves audio, video, or text conference (chatting) [1]. A conference can be loosely, fully distributed or tightly coupled. In this paper our focus is on tightly coupled conference that is controlled by a central point. This central point is responsible to provide services like transcoding, media mixing, notification etc. In IMS conference this central point is called “focus” and it setups a signaling dialogue among all participants. The set of rules related to a conference is known as conference policy. Rules may be related to the membership, access control, usage etc. A server that creates a new conference by assigning it a Universal Resource Identifier (URI) is known as conference factory. Figure 1 shows the conference creation.

A short lived conference that is created without scheduling is known as ad-hoc conference. For scheduled conference we need conference control protocols those are still under researched in IMS. So, our focus is on ad-hoc conferences. In order to invite someone to the conference service a Refer request is generated. Figure 2 describes the referring mechanism in detail.

Manuscript received December 22, 2008.

Zeeshan Shafi Khan is a Research Scholar at International Islamic University Islamabad, Pakistan. His phone number is (+92-321-7625468) and email is (zeeshanshafikhan@yahoo.com).

Prof. Dr. Muhammad Sher is Chairman of Department of Computer Science at International Islamic University Islamabad, Pakistan.

Prof. Dr. Khalid Rashid is Head, Department of Computer Science at COMSATS Institute of Information Technology, Islamabad, Pakistan.

Imran Razzak is a Research Scholar at International Islamic University Islamabad.

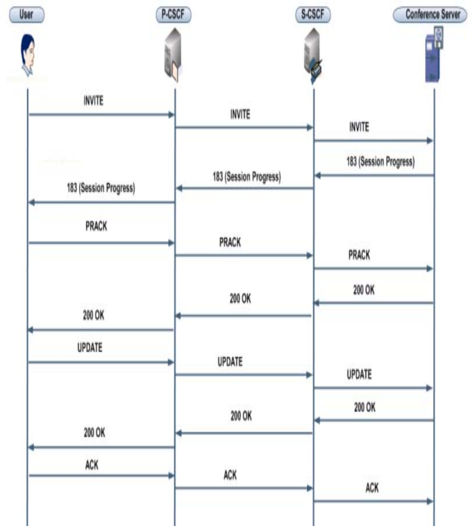


Figure 1: Conference creation using conference factory

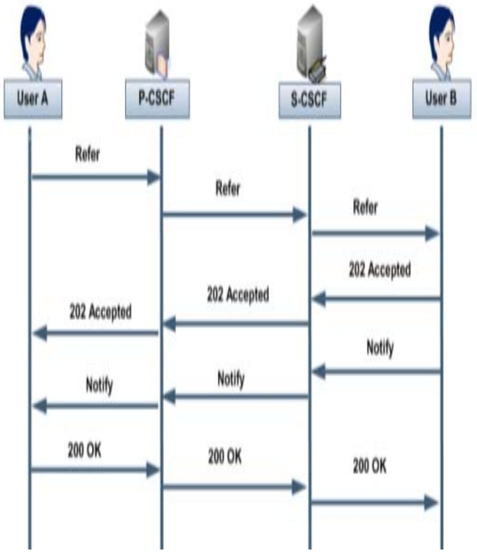


Figure 2: Referring a user to conference

The remainder of this paper is organized as follows. Section II gives high level overview of the related work, section III investigates the problem, section IV describes the proposed solution while section V consists of validity and applicability of the proposed solutions. Section VI concludes the article.

II. RELATED WORK

M. Sher et. al. in 2006 proposed a Transport Layer security (TLS) along with the intrusion detection system to secure the IMS application server against various types of time dependent and time independent attacks. Since SIP is mostly used with UDP so the implementation of TLS is an issue that needs to be resolved [2]. In 2006 Chen et. al. [3], Geneiatakis et. al. [4] and in 2007 Hunter et.al. [5] all investigated the SIP based flooding attacks and focuses on the need of some better solution against these attacks. Alam et.al. in 2006 purpose the idea of narrowcasting [6]. According to them instead of sending their communication to all the participants of the conference, each participant can configure his preferences that to whom he want to send his voice and to whom he don't want to. M. Sher et. al. in 2007 developed an Intrusion Detection and Prevention (IDP) system to secure the IMS application server. It is very difficult to maintain an up-to-date comprehensive list of rules. In this paper the main focus of the authors is on misuse detection only. The anomaly detection is not addressed [7].

III. PROBLEM ANALYSIS

There are many problems with the existing working mechanism of the conference service. A SIP based flood can be launched over the conference service by sending enormous number of invite requests. Since every invite request results in creation of a conference which require considerable amount of resources at the conference server so large number of invite requests may results in denial of service. Moreover internal threats like SQL injection etc. are also alarming and results in destruction at service level.

Conference allows a single participant to invite anyone to the conference through refer request. Therefore an existing participant of the conference can invite such a person who is not acceptable by the other existing participants of that conference. Therefore the other participant may leave the conference due to the inclusion of a new member. So in short single participant based authority may results in conflict and dissatisfaction among the existing participants of the conference.

Whenever a person is referred into the conference it becomes a fully authorized participant of that particular conference. Here fully authorized means that if it is a video conference than that participant has the full authority to watch, listen and speak. We can not restrict it to only watch or speak. In real life there are many scenarios where we need passive participants. Here passive means that the authority of those participants is limited. So this fully authorized mechanism reduces the applicability of the conference service in real life.

IV. PRPOSED SOLUTIONS

In order to handle different types of flooding attacks and internal threats we developed an Intrusion Detection and Prevention (IDP) system. To reduce the chances of conflict among the existing participants of the conference service, we offer an election based distributed referring authority mechanism and to maximize the scope of the conference service in the real life we introduced the concept of parameterized referring. Details of the each solution are described as under:

A. *Intrusion Detection and Prevention (IDP) system:*

Flooding attacks and internal threats like SQL injection etc. are very alarming and require a comprehensive solution. We in this paper developed an IDP system to mitigate the effect of these attacks. This IDP system is deployed as a middle layer between IMS core and application plane. The distinct feature of this IDP system is that it includes both misuse detection and anomaly detection modules.

a) Misuse Detection Module: It is one of the main module of the proposed IDP system that detects the attack and penalize the attacker before serving the request.

b) Attack Rules: It is the comprehensive list of the rules related to every type of possible attack. Rules are defined with respect to the role.

c) Blacklist: It contains the list of the users who try to attack over the network. These users are blocked for particular period of time.

d) Anomaly Detection: It inspects the effect of the request on the application server and tries to find the attack after the application server serves the request. Detail architecture of the middleware is given in the figure 4.

When a request from a user reaches to the IMS core, S-CSCF detects whether this request is for conference application server or not. If this request is for conference server than first it forwards towards the misuse detection module of the IDP system. This misuse detection module is equipped with the set of rules about each type of attack. This module after receiving the request first matches it with the blacklist. If that user's ID exists in the blacklist the request is discarded. If the user does not exist in the blacklist then the misuse detection module matches it with the attack rules. If the request matches with any of the attack rules it is considered as an attack and discarded immediately. After discarding the requests the attacker is put into the blacklist for certain period of time. Here we also described the mechanism for the blacklist timings. The blacklist timings depend upon the attacker. If it is that particular user's first attempt to attack, it is blacklisted for few minutes but if that user again tries to attack after getting out from the blacklist than it is blacklist timings are doubled from the previous timings. For this purpose a counter is initialized for every attacker whenever it makes first attempt to attack. With every subsequent attack request the counter is incremented by one and the blacklist timings are doubled from the previous timings.

If the request does not match with any of the attack rules it is considered as a legitimate request and forwards towards the conference server. Conference server serves the request. Since it is very rare that the misuse detection module is equipped with all the rules related to an attack, so it is possible that it fails to identify few attack requests. To handle this situation the anomaly detection module of the IDP comes into action. The server after serving the request sends its initial state (state before serving the request), current state (state after serving the request) and the request itself to the anomaly detection module of the IDP. Anomaly detection module verifies that whether the request did the same for which it is supposed to do. If request results in some undesirable action it is considered as an attack and the anomaly detection module updates the rules of the misuse detection module as well as ordered the misuse detection module to put the attacker into the blacklist. This feature limits the attacker to attack only once. If the attacker tries to repeat the same attack, misuse detection module will detect it due to the updation of the rules. The detailed architecture of the IDP system is shown in the figure 3.

B. Election Based Distributed Referring Authority:

Conference service allows a single participant to refer anyone to the conference. Therefore a participant may refer such a person who is not acceptable by the other participants of the conference. This situation can result into conflict. In order to prevent the conference service from these types of conflicts and to create the friendly environment among the conference participants we developed an election based distributed referring authority mechanism. Whenever a participant wants to refer a person it initiates an election by sending a refer request to the conference server. Conference server starts polling by sending a Poll request to all the existing participant of the conference. All the participants are required to cast their vote either with "yes" or "no". Yes for allowing the refer request and no to reject it. If a participant does not reply within the specified period of time it is automatically considered as "yes". After receiving responses from all the participant or at the end of the specified time, the conference server counts the votes. If a certain percentage (i.e. 60%) of the members replied in "yes" the refer request is entertained else it is discarded and the initiator is notified. Initiator's response is always counted as "yes". Figure 4 explains the scenario in details.

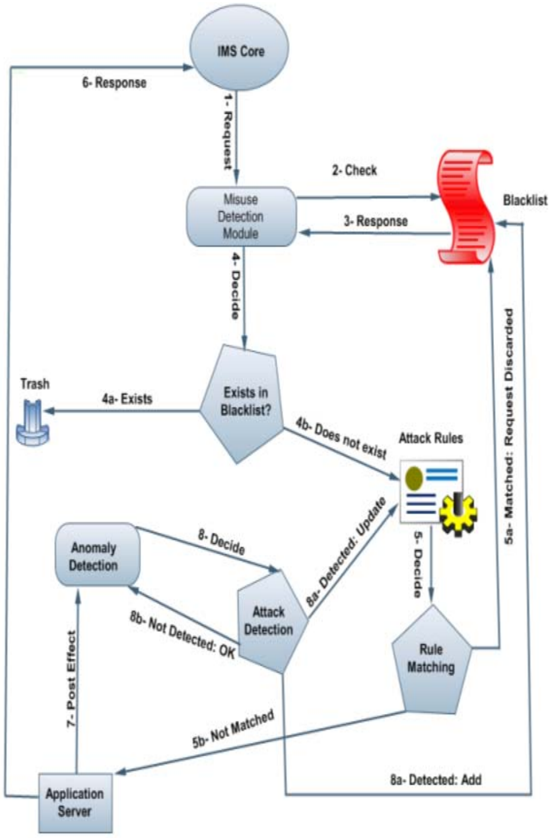


Figure 3: Architecture of Proposed Intrusion Detection and Prevention System

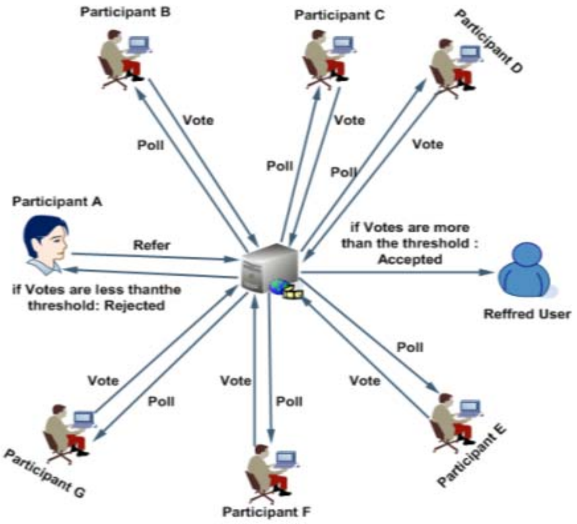


Figure 4: Election Based Distributed Referring Authority Mechanism

C. Parameterized Refer Request:

Whenever a participant refers to some other person into the IMS conference, it becomes the fully authorized member of the conference. There are many scenarios where we want to invite few persons as a passive member of the conference. Here passive means that the participant is not fully authorized for all types of action. The authority of the participant is limited i.e. only to watch the conference (Listening and speaking is not allowed). To accommodate these types of scenarios in the IMS conference we proposed a parametrized refer request mechanism. Whenever a participant launches a refer request it also specify the authority of the referred user along with the refer request. Here authority represents the actions that referred participant can take (watching, listening, speaking etc.). The details are shown in the figure 5. This mechanism reduces the load from the network by allowing only few users to send the media. Scalability that is the major problem with the conference server can be achieved through this mechanism by adding more and more passive users. If all the participants are allowed to speak in a conference then the decision about turn to speak may results in conflict. Since this mechanism can also reduce the number of users allowed to talk so this problem can be solved up to great extent.

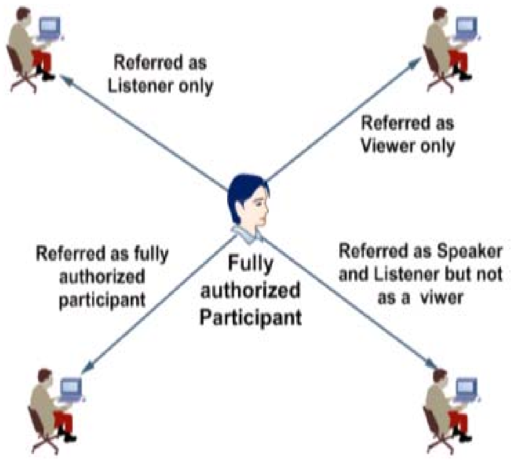

Referred as Listener only
Referred as Viewer only
Referred as fully authorized participant
Fully authorized Participant
Referred as Speaker and Listener but not as a viwer

Figure 5: Referred for Limited Access to the Conference

V. VALIDATION AND APPLICABILITY

In order to validate the proposed solutions we deploy them over the prototype of the IMS testbed. First we deploy the IDP system over the testbed and launches different types of attacks. We found that every attack request that matches with the attack rules of the misuse detection module is discarded and that user is put into the blacklist. In few cases misuse detection module fails to detect an attack due to unavailability of rules. In this case anomaly detection module identifies the attack and put the attacker into blacklist through misuse detection module and updates the rules of the misuse detection module. After that we repeat the same attack and we find that this time the misuse detection component detects the attack. Figure 6 shows the IMS tesbed along with the IDP system.

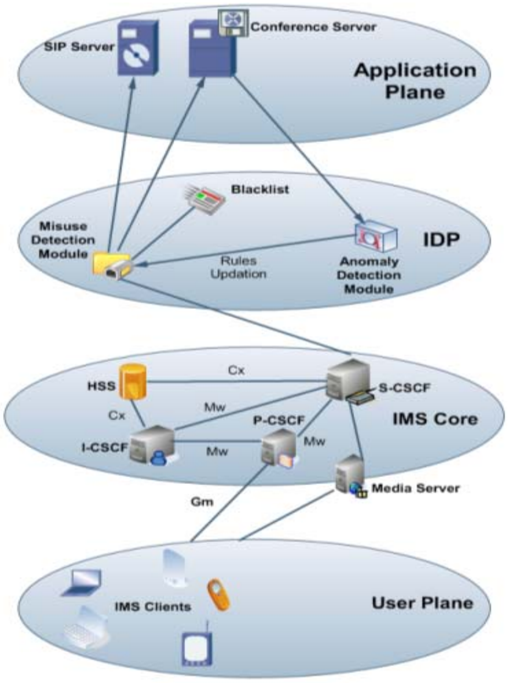


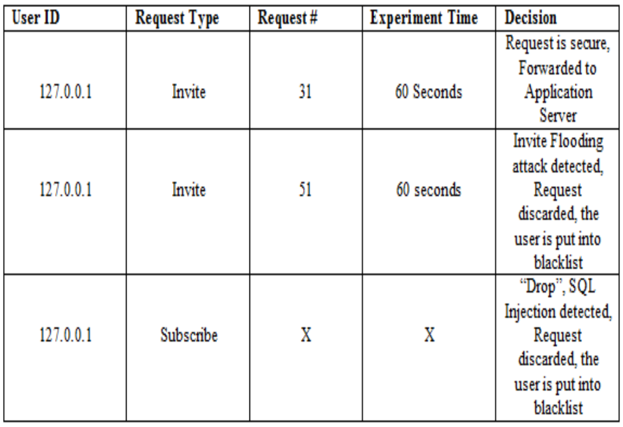
Figure 6: IMS testbed along with proposed IDP system

First we configure set of attack rules against various types of attack at the misuse detection module of the IDP system. Few of the rules are given in simple text at below:

1) If a user sends more than 50 Invite requests within 60 seconds consider it as Invite flooding attack
2) If a user sends more than 5 Refer requests in 60 seconds consider it Refer flooding attack
3) If a request contains “Drop” consider it as SQL Injection attack

After that we perform various experiments by sending different number and different types of requests. The results are described in Table I.

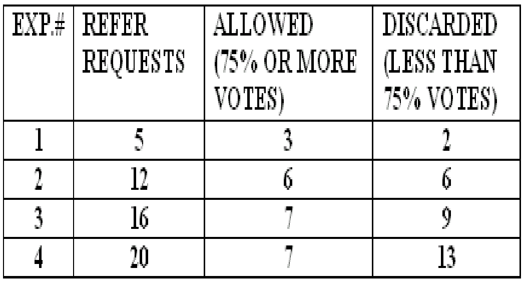
Table I: Performance of the IDP System



User ID	Request Type	Request #	Experiment Time	Decision
127.0.0.1	Invite	31	60 Seconds	Request is secure, Forwarded to Application Server
127.0.0.1	Invite	51	60 seconds	Invite Flooding attack detected, Request discarded, the user is put into blacklist
127.0.0.1	Subscribe	X	X	"Drop", SQL Injection detected, Request discarded, the user is put into blacklist

In the next experiment we evaluate our election based distributed referring authority mechanism. For this experiment the threshold value is set to 75%. We launched 5 refer requests in a conference of 10 participants. Out of these 5 refer requests 3 got more than 75% votes so they became the member of the conference and the 2 requests fail to gain 75% vote so they are discarded by the conference server. We repeat this experiment with different values and table 1 shows the results.

Table I1: Election Based Referring



EXP.#	REFER REQUESTS	ALLOWED (75% OR MORE VOTES)	DISCARDED (LESS THAN 75% VOTES)
1	5	3	2
2	12	6	6
3	16	7	9
4	20	7	13

In the last we identify few scenarios for the applicability of the parametrized refer request and validates the proposed mechanism in those scenarios. We take the Campus example where administration and the faculty members start a video conference to discuss few important issues. Latter on the president of the university referred few students into the conference but they were only allowed to watch and listen the conference. They were not allowed to speak in the conference. This feature is obtained through the parametrized refer request.

VI. CONCLUSION

IMS conference service is subject to various types of security attacks. To make this service more resilient against security threats we proposed intrusion detection and prevention system consists of misuse detection and anomaly detection components. To prevent the conflicts among the participants of the conference service an election based distributed referring authority mechanism is developed and at the end to enhance the applicability of the conference service in the real life we proposed a parametrized refer request.

ACKNOWLEDGEMENT

We acknowledge Higher Education Commission (HEC) Pakistan, for providing financial assistance and grant to carry this research. Support and help of the colleagues and friends is highly appreciated. We are very thankful to Fraunhofer FOKUS Communication Research Institute, Germany for technical support on IMS testbed development.

REFERENCES

[1] Miikka Poikselka "IP Multimedia Concepts and Services" 2nd Edition, Jhon Wiley & Sons Ltd. 2006
[2] M. Sher, S. Wu, T. Magedanz, "Security Threats and Solutions for Application Server of IP Multimedia Subsystem (IMS-AS)", IEEE/IST Workshop on Monitoring, Attack Detection and Mitigation. MonAM06, 2006
[3] Chen, E.Y., "Detecting DoS attacks on SIP systems," IEEE Workshop on VoIP Management and Security, Page(s):53 – 58, 3 April 2006.
[4] D. Geneiatakis, T. Dagiuklas, G. Kambourakis, C. Lambbrinoudakis, S. Gritizalis, S. Ehlert, D. Sisalem, "Survey of Security Vulnerabilities in SIP Protocol", IEEE Communication Surveys Volume 8, No.3 ISBN 1553-877X, pp 68-81 (2006).
[5] Michael T. Hunter, Russell J Clark, Frank S. Park, "Security Issues in IP Multimedia Subsystem (IMS)" MNCNA, ACM, 2007.
[6] Mohammad Sabbir Alam, Michael Cohen, & Juli´an Villegas, "Figurative Privacy Control of SIP-based Narrowcasting", and 22nd International Conference on Advanced Information Networking and Applications, 2008.
[7] M. Sher, T. Magedanz, "Developing Intrusion Detection and Prevention System for IP Multimedia Subsystem Application Servers", Journal of Information Assurance and Security, 2007
[8] Mohammad Sabbir Alam, Michael Cohen, Ashir Ahmed, "Design for Controlling Media Privacy in SIP Conferencing Systems", International Conference on Digital Telecommunications, 2006.
[9] Third Generation Partnership Project (3GPP). www.3gpp.org/
[10] Third Generation Technical Project, Technical Specification, "IP Multimedia Subsystems (IMS)", 3GPP, TS 23.228 V6.7.0 (2004-09).
[11] Sher, M.; Magedanz, T.; Penzhorn, W.T., "Inter- domains security management (IDSM) model for IP multimedia subsystem (IMS)", The First International Conference on Availability, Reliability and Security, 2006
[12Rebahi, Y., Sher, M., Magedanz, T., "Detecting flooding attacks against IP Multimedia Subsystem (IMS) networks", IEEE/ACS International Conference on Computer Systems and Applications, 2008
[13] Muhammad T. Alam, Zheng da Wu, "Cost Analysis of the IMS Presence Service", 1st Australian Conference on Wireless Broadband and Ultra Wideband Communication, 2006
[14] Vishal K. Singh and Henning Schulzrinne, "A Survey of Security Issues and Solutions in Presence", www1.cs.columbia.edu/~vs2140/presence/presencesecurity.pdf
[15] Victoria Beltran, Josep Paradells, "Middleware-Based Solution to Offer Mobile Presence Services", Mobilware'08, 2008.