Session Initiation Protocol (SIP) Flooding Prevention

S.Subapriya
Computer Science Department, Prist University,
Trichirapalli, Tamil Nadu , India
Subapriya1987@gmail.com

S.Dlip Kumar
Computer Science Department, Prist University
Trichirapalli, Tamil Nadu, India.
sdprist@gmail.com

Abstract

The IP multimedia subsystem (IMS) is a Next Generation Network (NGN) that integrates wireless, wire line and internet technologies. IMS enables the convergence of voice, data and multimedia services such as Voice over IP (VoIP), Video over IP, push-to-talk, presence or instant messaging services. The Voice over IP (VoIP) is one such as the IMS are deployed in order to provide cheap and at the same time high quality services to their users. At parallel this open based emerging technology has the security challenges from the multiple communication protocols like HTTP, SMTP and SIP etc. Session Initiation Protocol (SIP) is used for VoIP connection establishment and signaling handshakes, since it is the most flexible and lightweight protocol and it is text based protocol is flexible enough to easily incorporate and provide different services In this paper have presented a security model to protect SIP from single and distributed flooding attacks.

Keywords— IDPS, SIP, Flooding attacks, Bloom Filter , Packet Monitoring Method , CAPCHA.

INTRODUCTION

The IP Multimedia Subsystem (IMS) provides a powerful framework for the deployment of Next Generation Networks (NGN). The IP Multimedia Subsystem standardized by the 3rd generation partnership project (3GPP) and 3GPP2 is a internet technologies. In 2003, the Third Generation Partnership Project 2 released a comprehensive security defense for IMS that addressed the issues of SIP vulnerabilities. Nevertheless, this does not have a security mechanism for detecting and preventing flooding attacks. By using Intrusion Detection and Prevention System (IDPS) with IMS can be utilized for detecting the SIP DOS and DDOS flooding attacks. An Intrusion Detection System there is set of laws for the nasty users to do not go into the IMS. SIP is text-based, which makes it simpler to understand than most bit-oriented protocols, where Knowledge of the significance of each bit position, according to the rules and syntax of the protocol is required. The transport of SIP messages can be carried by transport-layer over IP protocols, such as SIP over UDP or TCP. SIP uses the requests as REGISTER, INVITE, ACK, and RESPONSE". The SIP requests are evaluate by a hashed based filter relied on Bloom filter, presented in the IDPS architecture.

Intrusion Detection and Prevention System (IDPS)

The threats in SIP/IMS environments are originate from different layers, since the attacker attempts to exploit more than one of the protocol's vulnerabilities. Therefore, it is important for the IDPS to be able to detect such behaviors before they become a threat for the higher layers and affect multimedia services

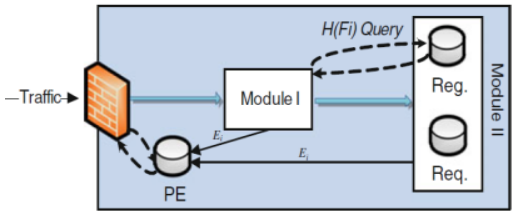

Fig 1. IDPS Mechanism

It consists of two distinct modules: the first one is responsible for registration requests while the other module for all remaining requests. It has been designed not only to prevent spoofing attacks, such as SIP signaling , UE, and User ID impersonation, MitM, but also attacks against system's availability known as flooding attacks. It is true that many flooding attacks utilize spoofed messages and they can therefore be mitigated. However, they can be also launched without spoofed messages, for instance though a security tunnel. Every E_i passes through the spoof checking module which decides whether the message is legitimate, and thus, whether it will be forwarded to the second module or it will be dropped according to some rule of the Policy Enforcer (PE). The latter holds a blacklist of known malicious E_i . An incoming message is firstly checked for existence in the PE's list. Only the non-listed messages should be forwarded and handled by the next modules.

Afterward the legitimate E_i is fed to the second module which consists of two tables: the registration table for holding registration messages data and the request table

IJERT

that holds the data of all the other requests in fig.1 A bloom filter is a data structure that can be utilized for testing the existence of an element x_i in a set X. Every x_i is hashed through λ different hash functions. The result of every hash function points to a specific position of a vector of m bits. The vector's length is equal in bits as the output of the hash functions. Initially, all the vector's bits are zero. When a hashoutput points to a specific position, it turns the null bit to 1 in Fig.2.

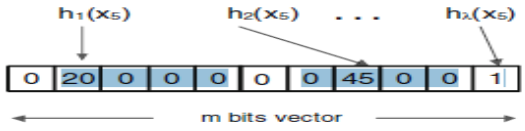

Fig .2 Counting bloom filter

A x_i exists in the set/vector when all λ outputs point to positions with all of them having a value of 1.A more advanced bloom structure is the counting filter. The conventional filter does not allow any other operations (e.g., subtraction or summation) than simply turning the zero bits to 1.

Mechanism message handling pseudo-code

Output: The extracted Ei tuple from incoming traffic

Input : An Ei that shall be blacklisted or a legitimate Ei

That shall be inserted to the second module's table

Module(Ei);

If module 1== 1 /* module1 return 1 when message shall be routed and 0 otherwise*/

then

```
Hash  = H( | Ei.MAC | |Ei. Ip| |Ei.Id|);
If Ei. method = REGISTER
        Insert _reg_table(Hash , Ei);
else
        Insert_request_table(Hash, Ei);
else
        drop_packet(Ei);
        update_PE(Ei);
```

Limitations of Intrusion Detection and Prevention System (IDPS)

- The number of the received requests with the number of 200 OKs and ACKs and thus detect deviations from the normal traffic. Moreover, they are only focused on the INVITE request flooding attack case.
- In other case a flooding detection model is introduced based on priority queues. Furthermore, the attacker can bypass the mechanism by flooding the server and consequently the two queues, both with INVITE requests and response (e.g. 100, 200, 180 etc).
- Bots will affect the request server.
- Fragmented attacks.
- Authenticate user can mistend the traffic to some other gateway or proxy.
- It cannot prevent flooding attacks and MitM in all remaining layers.

Solution

To evaluate the solution for the drawback of utilising bloom filters

We establishment a Packet Monitoring System. SIP is a 3-way handshake procedure. The caller generates a SIP INVITE message and forwards it to the appropriate SIP server, which locates the receiver (callee) and sends the call towards his device. The callee whenever receives such a request responds with a 200 OK message, considering that accepts the message. Afterwards, the session is established since the callee receives the final SIP ACK generated by the caller.

Consequently to monitor these types of different SIP messages, we utilized three distinct "tables". The tables hold counters in their entries to enumerate the incoming messages. Every new message is hashed by two or more functions in order to recorded it in the entries of the appropriate table. As input to hash functions are used the headers the headers "Call- Id" and "From" (identifies uniquely a session). The hash function output points to a table position, in which the corresponding counter is increased by 1.

IJERT

Packet Monitoring Method pseudo-code

For each incoming message check the type

If type is request

Check the Method

If method is invite

Update bloom filter (increase by one the appropriate entries of the filter)

else if method is ACK

Update bloom filter (increase by one the appropriate entries of the filter)

If method is RESPONSE

Update Bloom filter (increase by one the appropriate entries of the filter)

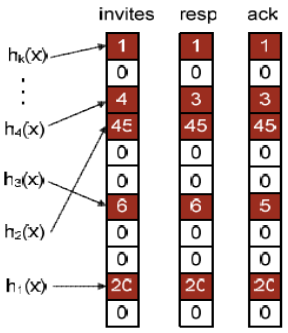

Fig .3 Packet Monitoring Method

A model has a completed session, called session distance and defined as follows

Dist = Num of INVITEs - 0,5*(Num of OK + Num of ACK)

Since the Dist value remains zero, a successful session has been established. Any other positive value represents uncompleted or dropped sessions

Session_distance = #invite $_i$- (0.5 * (# resp $_i$ + # ack $_i$)

3D-CAPCHA solve the bots that affect the request server

3D-CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart)is a mechanism that can differentiate machines bots from human users and has successfully reduced bots server that affect request.

Different types of captcha have been designed for protecting various Internet resources like online accounts, and emails. A few notable design examples include, asking users to identify garbled string of words or characters, identify objects in an image rather than characters, identify videos, and identify textual captcha that involves clicking on the images rather than typing the response. The other type of CAPTCH is displaying to the user a simple mathematical equation and requiring the user to enter the solution as verification and an alternative method such as understanding the meaning e.g., a logic puzzle or trivia question, or instructions on how to create a password. Although CAPTCHAs were designed by Optical character Recognition OCR software for document scanning. Through captcha we detect the bots that affect the request server.

Conclusion and Future Work.

The IMS architecture is standardized to access multimedia services (such as data, voice and video), and Our objective is to extend the SIP security solutions identified suggest that security mechanisms cannot provide 100% protection against SIP flooding attacker, but threats can be mitigated significantly by mechanism .In order to cover the rest of the attacks that can be launched against such infrastructures.

References

[1] .Sengar, H., et al.: Detecting VoIP floods using the Hellinger distance.IEEE Trans. Parallel Distrib. Syst. 794–805 (2008)

[2]. J. N. Gross. Captcha Using Challenges optimized for distinguishing between humans and machines. U.S.Patent Application, 2009.

[3] Wan, X.Y., et al.: A SIP DoS flooding attack defense mechanism based on priority class queue. In: IEEE International Conference Beijing, China, 25–27 June, pp. 428–431 (2010)

[4] Muhammad Sher, Thomas Magedanz, Yacine Rebahi, "Detecting Flooding Attacks Against IP Multimedia Subsystem (IMS) Networks" 2008 IEEE .

[5] 3GPP, "IP Multimedia Subsystems (IMS)", TS3GPP, "IP Multimedia Subsystems (IMS)", TS 23.228 V6.7.0 (2004-09).

[6] T.Dagiuklas, S.Ehlert, G. Kambourakis, C. Lambbrinoudakis, D. Geneiatakis, S. Gritizalis,. "Survey of Security Vulnerabilities in SIP Protocol", IEEE Communication Surveys Volume 8, No.3 ISBN 1553-877Xpp 68-81 (2006).

[7] D. Geneiatakis, N. Vrakas and C. Lamrinoudakis, "Utilizing Bloom Filters for Detecting Flooding Attacks against SIP Based Services",Accepted for publication in Computer and Security, Elsevier.

[8] D. Sisalem, J. Kuthan and S. Ehlert, "Denial of service attacks targeting a SIP VoIP infrastructure: atttack scenarios and prevention mechanisms.

IEEE Network, 20 (5):26-31,2006

[9]. Bloom B. Space/time trade-offs in hash coding with allowable errors. Communications of the ACM 1970;13:422–6.

[10]. Y. Soupionis, G. Tountas, and D. Gritzalis. Audio CAPTCHA for SIP-Based VoIP. In SEC 2009, IFIP, pages25–38. Springer, 2009.

IJERT