A Novel Approach for Evaluating and Detecting Low Rate SIP Flooding Attack

Abhishek Kumar
Department of Computer Science and Engineering-Information Security
NITK Surathkal-575025, India

Dr. P. Santhi Tilagam
Department of Computer Science and Engineering-Information Security
NITK Surathkal-575025, India

ABSTRACT
Voice over Internet protocol (VoIP) is continuously evolving and changing the face of business telephony. The Session Initiation Protocol (SIP) is a widely used standard in VoIP communications to setup and tear down phone calls. Low rate Denial-of Service (DoS) attack recently emerged as the greatest threat to enterprise VoIP systems. Such attacks are difficult to detect and capable of discovering vulnerabilities in protocols with low rate traffic. In this paper we aim to provide a novel low rate SIP flooding detection scheme using area under curve of monitored dynamic SIP traffic with classification of SIP flooding attacks and its impact on SIP server under low rate DoS attack. Compared to the other detection system our technique achieves advantages of accuracy, fast, light weight, and flexibility to deal with DDoS attack detection. Experimental results show the effectiveness of the scheme.

General Terms
Application Security.

Keywords
VoIP, SIP, Low Rate DoS Attack, Behavior Based Analysis.

1. INTRODUCTION
Voice over Internet Protocol (VoIP) is a technology that is reshaping the future of telephony and in coming decades it will completely replace the Public Switched Telephone Network (PSTN) and the traditional PBX system. While enterprise VoIP offers low cost and various functionality it's also opens the door for external threats. Facilitating the VoIP services to legitimate users would be the main concern about the productivity of future business telephony. Most VoIP services uses the SIP infrastructure, because its simplicity and wide range of features, which makes its service vulnerable. The Registrar server makes it possible for users to alter the address at which they are contactable. This is possible through the SIP client sending a REGISTER request of change of an address to the Registrar server which involves significant computation on Registrar server.

The low rate attack strategies are novel approach to launch flooding DoS attack without sending high rate traffic to the victim. These attacks are mixed approaches between flooding and vulnerability attacks by which attackers get advantages after reducing traffic rate. These low rate DoS attacks degrade the performance of SIP application server and cause in rejection of legitimate requests significantly where results obtained under different hardware and software system specification [3]. This paper is an extended work of [3] and addresses the important issue on how fast and accurately detects the low rate DoS attack on SIP application server.

We use a freely available open source Asterisk SIP server version 1.6.20 [1]. We populated 16000 unique username and passwords in user account and directory data of server. We automate a registration flooding low rate DoS attack scenario and populate a .csv file of 16000 valid and invalid username and passwords to generate legitimate and illegitimate dynamic traffic behavior to SIP application server. Figure 1, shows the notional diagram of DoS attack target (SIP Registrar) of SIP application server. We used very popular traffic automation and generation tool SIPp [2].

In this paper, we focus on behavior based fast detection of low rate DoS attack on SIP server using area under curve. Our method clearly distinguishes the normal traffic behavior, low rate flooding attack (obviously high attack rate also) and flash crowd.

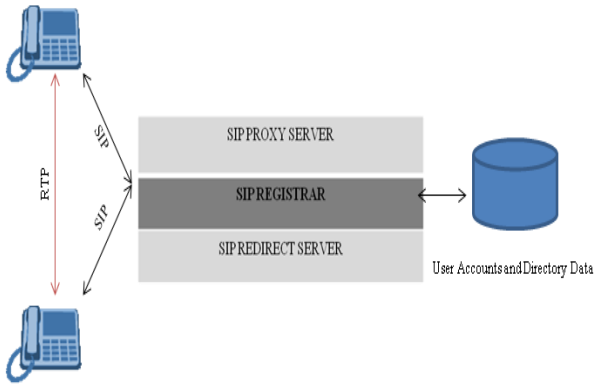

Fig. 1 DoS Attack Target SIP Registrar

The rest of this paper includes following structure; section 2 gives a brief introduction to SIP protocols vulnerabilities and major flooding attacks with threat model. Experimental testbed set up with different modules and proposed detection scheme are described in section 3. Section 4 presents SIP signaling traffic behavior with computer simulated results. Related works are described in section 5. Section 6 is the conclusion and future work.

2. VULNERABILITY AND SIP FLOODING ATTACK
Session Initiation Protocol (SIP) is a simple and textual based protocol having less secure authentication and authorization mechanism. Due to this inherent property of SIP, it is vulnerable to unauthorized privilege access, denial of service attack and

unstable system behavior. DoS attack on the SIP infrastructure is the easiest way to exploit vulnerability. Some DoS attack exploits the vulnerability of the SIP protocol RFC specification and other exploits the SIP protocol implemented by the different vendors. According to [4], there exist different classes of DoS attack which either consume the server resources for fake computations or under utilize the network bandwidth. To reduce the chances of falling victim to this type of attack, a number of measures can be taken. Proxy servers and firewalls can be implemented on a network to prevent UDP from being used maliciously and filter unwanted traffic. For example, if an attack appeared to come from one source previously, you could set up a rule on the firewall that blocks UDP traffic from that IP address. In this paper we focus on detection of registration flooding and authentication flooding attack on SIP server.

2.1 Signaling Flooding Attack

A. SIP Registration Flooding Attack. A user agent send REGISTER request to SIP server when they initially want to communicate with other user and at regular interval as shown in Figure 2. An attacker can easily spoof large number of location addresses and send request to REGISTRAR with invalid username and passwords. In response attacker receives the 401 UNAUTHORIZE messages and again send the invalid MD5 digest calculated by hash function with nonce, realm, username and password values as shown in Figure 2. Here we assume the attacker know the username and locations of valid users. When SIP server receive the calculated MD5 digest it will match the received digest to digest calculated by server, while doing so server lookup the database of users and engaged in calculating digests. Due to excessive calculation of unwanted MD5 digest and to lookup user directory server incur high load on server and cross the threshold value of packet processing and hence cause the DoS attack.

B. Authentication Flooding Attack. The authentication mechanism used by SIP is based on HTTP Digest mechanism based on challenge/response model. In order to verify the valid password sent by client, SIP server needs to compute MD5 Digest response to match the received response. The attacker machine needs not to calculate the MD5 Digest response using the realm, nonce, username and passwords values. An attacker can easily send the random Digest values stored. Using this mechanism an attacker can send more requests per second to target server to keep server busy.

C. INVITE Flooding Attack. The SIP infrastructure is also vulnerable to INVITE flooding attack. A VoIP server should have a security feature to blocks flooded call request from unregistered clients. So, an attacker registers first after spoofing a legitimate user, and then sends flooded INVITE requests in a short period of time with different rates. This impacts significantly the performance of SIP server.

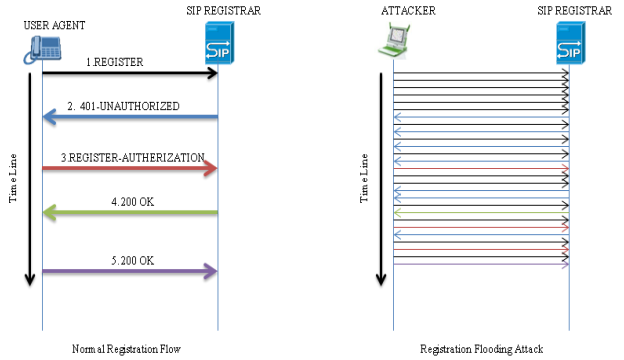

Fig. 2 Normal Registration and Registration Flooding Attack

D. PING Flooding Attack. VoIP protocol uses ping message in the application layer to check out the reachability of server, like SIP OPTIONs message. A router or firewall do not allow (Internet Control Message Protocol) ICMP ping in many production network for security reason. However a VoIP system should allow ping message in application layer for more reliable serviceability, but an attacker can misuse this message and can flood the SIP server with various ping messages. Beside of these major flooding attacks, an attacker can flood valid or invalid call control messages like SIP INFO, NOTIFY, Re-INVITE etc. after call set up.

2.2 Threat Model

SIP is vulnerable to many network anomalies as mentioned in section 2. Such attacks can be easily launched on SIP server using openly available traffic generator tools such as SIPp [2]. Stateful SIP proxy server maintains the transaction state for each request for some time. SIP REGISTRAR server rejects many legitimate REGISTRATION request if the attack rate is even low. Attackers can launch low rate DoS attack instead of high rate flooding attack because it is difficult to detect and its impact of request rejection on server is significant [3]. Thus the low rate SIP REGISTRATION flooding attack is deteriorating VoIP network. We focus our discussion on the low rate REGISTRATION flooding attack.

3. DETECTION SCHEME AND EXPERIMENTAL CONFIGURATION

In this section, we describe our proposed detection scheme design and experimental testbed configuration for computer simulation results. Our proposed detection scheme is combination of three modules running on server side and developed in Perl language as shown in Figure 3. The first module is internet packet filter and captures all SIP packets coming through the internet and it also capture the response generated by the SIP REGISTRAR. The second module takes input from the first module and makes n samples of attributes with transaction IDs for each delta t duration (in our case it is 10 seconds). The third module calculates the three parameters, Hash Computation Efficiency (HCE), Successful URI Binding Efficiency (SUBE) and Registration Drop Efficiency (RDE) and

also determines the area under curve of these parameters on the scale of 0 to 1 over n samples. To know more about parameters refer [3].

1. Hash Computation Efficiency (HCE). The ratio of third REGISTER request [Fig. 2] with MD5 digest to responded fourth "200 OK" messages. This parameter shows the positive attitude of SIP server.
2. Successful URI Binding Efficiency (SUBE). Ratio of total number of successful URI binding is to total number of request received. This parameter shows the positive attitude of SIP server.
3. Registration Drop Efficiency (RDE). Ratio of total number of rejected URI binding is to total number of request received. This parameter shows the negative attitude of SIP server.

$$AUCHCE = \sum_{n=1}^{m} HCEn \quad (1)$$

$$AUCSUBE = \sum_{n=1}^{k} SUBEn \quad (2)$$

$$AUCRDE = \sum_{n=1}^{r} RDEn \quad (3)$$

$$AV = AUCHCE + AUCSUBE - AUCRDE \quad (4)$$

We calculate area under curve (AUC) for each 10 second interval by each parameter as shown in equation 1, 2 and 3. The total number of samples (m, k and r) for each parameter may be slightly differing. But for each value of n, all parameters belong to same transaction. The attitude value (AV) calculated in equation 4. Further explanations of these values are described in section 4.

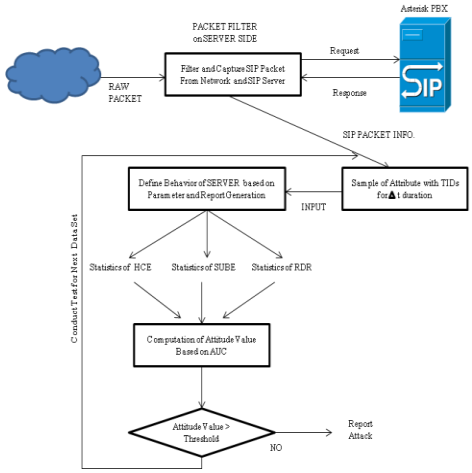

Fig. 3 Detection Scheme Design

3.1 Configuration Module

In our experiment we used SIPp tool with Transport Layer Security (TLS) support as an attack traffic and legitimate traffic generation module. We wrote a XML scenario of REGISTER packet for attacking purpose as well as for legitimate request. For attack generation module, we added 16000 illegitimate user's credentials in our CSV file, which is an input of created XML attack scenario. As a client configuration module for legitimate request we have separate CSV file with valid extension number, location, username and password. This tool is capable to generate normal call flow in a real world call scenario, to analyze the performance of detection scheme under attack scenario. The normal flow depends on the organization of service provider and different configuration and specification of SIP server.

In our experiment we used open source version of ASTERISK 1.6 as a SIP server. We compiled and run a C code to add 16000 users in SIP database to configure SIP.conf file and EXTENSION.conf file.

3.2 Experimental TestBed

For our experiment we used following test bed setup:

1. Legitimate Traffic Generator. This module is responsible to generate all legitimate REGISTER request to SIP server. We generate uniformly distributed normal traffic.

2. Attacker. We have implemented attacker as a different instance of SIPp[2].This module is responsible to to generate low rate flooding and flash crowd requests to SIP server.

3. Attack Detector. This module is responsible to perform all steps mentioned in detection scheme and report anomalies if exist.

4. SIP Server. This module works as a REGISTRAR. Here we used the open source version of Asterisk 1.6.20 [1] as a SIP server.

5. Hardware Specification. The testbed has been designed in our NITK Information Security Lab. All modules are operated in Linux machine. The SIP server machine is Intel(R) Core 2 Duo, 2.0 GHz processor with 2 MB RAM and L2 cache running Linux Fedora Core 13 with Kernel version 2.6.23.142. The Attacker and legitimate traffic generator is Intel(R) Core(TM), 3.0 GHz with 1 GB RAM and 4096 KB cache running Linux Fedora 8 with kernel version 4.1.2-33.

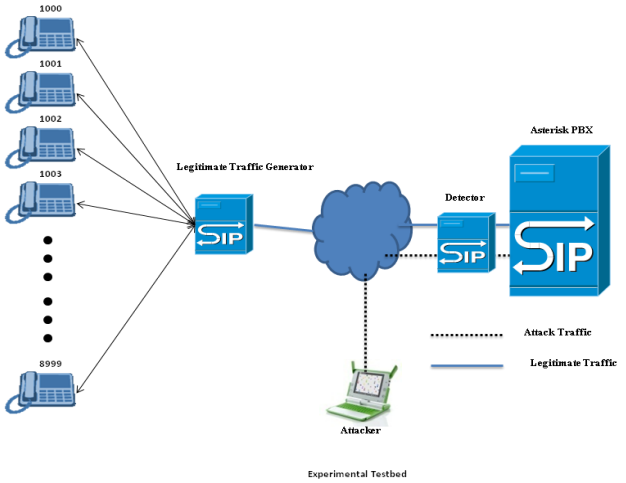

Fig. 4 Experimental Testbed

4. PERFORMANCE EVALUATION

Now, we present the performance of our proposed detection scheme. As for given hardware specifications of SIP server machine, maximum valid registration request processed by REGISTRAR is 20 REGISTER packet/sec in no attack scenario. For analysis purpose we present all statistics in Figure 5 A, B, C, D, E, F, G, H and I. Where A, B and C shows the performance of HCE parameter under normal condition (request rate uniformly distributed between 1 to 20 REGISTER per second), under low rate attack (flooding rate is comparable to normal condition) and under flash crowd (20-40 REGISTER per second) respectively. Performance of SUBE parameter under normal condition, low rate attack and flash crowd are presented in D, E, and F of Figure 5 respectively. Figure G, H and I present performance of RDE parameter under all three condition.

According to our SIP server specification and experiment, SIP server is capable to process 20 legitimate REGISTER packet/sec for 16000 configured phones in normal condition. For good accuracy and due to frequent change in network traffic, we have taken 136 samples of SIP attribute data set in duration of 30 minutes.

4.1 Behavior under normal condition

From Figure 5.A, the average area under curve by HCE is 1317.97 which is 97.62% of 1350.In ideal case this value should be 100%, but it is due some fluctuation in normal condition. Here area under curve is cumulative sum of trapezoidal shape made over 136 samples. In Figure 5.D, SUBE cover 98.41% of the total area in normal condition. From Figure 5.G it is clear that, the RDE cover only 1.58% of total area in normal scenario, which should be very less in ideal condition. For accurate detection of attack, the sum of positive attitude (HCE and SUBE) must be less than negative attitude (RDE). But here positive attitude is much more than negative one which shows good accuracy of our scheme. So behavior under normal condition is:

$$HCE + SUBE >> RDE$$

4.2 Behavior under low rate DoS attack

Now we analyze effectiveness our detection scheme under low rate attack. For low rate attack, we injected illegitimate requests which rate is less than or equal to normal condition rate. From Figure 5.B, 5.E and 5.H, it is clear that the positive attitude is very less than negative attitude in comparison with normal condition. From Figure 5.B we can see the HCE cover only 277.23 which is 20.23% of total area. Figure 5.E shows that area covered by SUBE is only 35% of total. Both positive attitude values are less than that of normal condition. In Figure 5.H, the negative attitude RDE cover 64.68% of total area.

So in low rate attack scenario, the sum of positive attitude is less than negative attitude. So behavior under low rate attack condition is:

$$HCE + SUBE < RDE$$

4.3 Behavior under flash crowd

Our detection scheme also detect flash crowd (20-40 REGISTER request per second), however our aim was to detect low rate DoS attack. From Figure 5.C, 5.F and 5.I, it is clear that the positive attitude values are less than the negative attitude value. From Figure 5.C, the HCE cover only 37.03% of total area which is more than attack scenario but less than normal condition. Whereas area covered by SUBE is 16.65% in Figure 5.F, which is very less than normal condition. From Figure 5.I, area covered by negative attitude RDE is 83.34% of total which is also much more than normal condition. So behavior under flash crowd is:

$$HCE + SUBE < RDE$$

Table [1], shows summary of the effectiveness of our detection scheme under normal condition, low rate DoS attack and flash crowd.

5. RELATED WORK

To the best of our knowledge, no detection scheme is designed to detect the anomaly behavior of SIP server (particularly for SIP REGISTRAR with LOCATION SERVER) against low rate DoS attack. As a result, not much experiment is done to analyze the behavior of SIP server under low attack rate scenario, which significantly degrades the performance of server. The author of [5], experimentally analyzed the behavior of SIP server which is based on HD with probability distribution model. The result show good capability to detect low rate DoS attack for INVITE flooding, however scheme will be ineffective if attacker simultaneously flood the four SIP attributes that are used to build probability distribution model as mentioned in [6]. The important work done in [6], their scheme integrated with two techniques sketch and Hellinger distance with voting procedure which takes significant time for calculation. They focused on INVITE flooding attack and did not mention how fast their detection scheme works.

6. CONCLUSION AND FUTURE WORK

In this paper we have experimentally shown the behavior of SIP REGISTRAR under normal condition, low rate DoS attack and flash crowd. The overall calculation time it takes to define behavior of server after module I is 2 to 4 seconds (according to our system configuration). Since our detection scheme is strongly capable to detect low rate DoS attack it also gives high accuracy of detection in high rate flooding attacks as well. Our detection scheme have very low overhead and accurate to detect low rate DoS attack against SIP Server.

Our detection mechanism force to build the strong mitigation techniques for different protocol supporting server of VoIP infrastructure under low rate DoS attack. In future we will extend our detection scheme for all low rate DoS attack mentioned in this paper and define protocol state machine to mitigate it.

7. ACKNOWLEDGMENTS

I would like to appreciate co-author of this paper and Department of Computer Science and Engineering-Information Security, NITK Surathkal for valuable support in this research.

Table 1 Summary of performance evaluation of detection scheme

Behavior under conditions	HCE	SUBE	RDE	Attitude Value	Anomaly Detection
Normal	97.62%	98.41%	1.58%	+194.45	No
Low rate attack	20.23%	35.31%	64.68%	- 9.37	Yes
Flash crowd	37.03%	16.65%	83.34%	-29.66	Yes

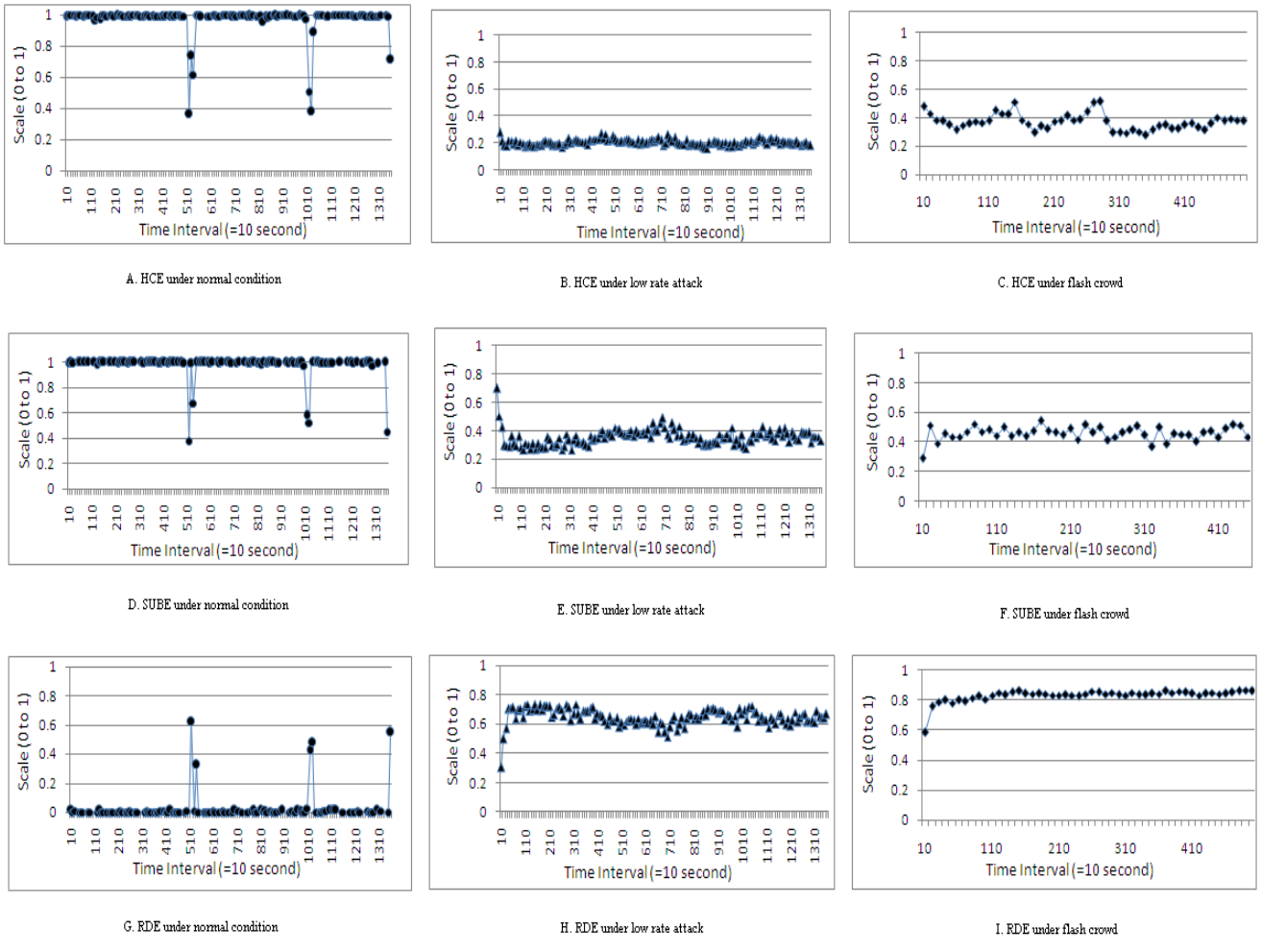

Fig. 5 A. HCE under normal condition, B. HCE under low rate attack, C. HCE under flash crowd, D. SUBE under normal condition, E. SUBE under low rate attack, F. SUBE under flash crowd, G. RDE under normal condition, H. RDE under low rate attack, I. RDE under flash crowd

8. REFERENCES

[1] Asterisk, The Open Source Telephony Projects, http://www.asterisk.org.

[2] R. Gayraud et al., "SIPp", http://sipp.sourceforge.net

[3] A. Kumar, S. Thilagam, A. Pais, V. Sharma, K. Sadalkar, "Towards Evaluating Resilience of SIP Server Under Low Rate DoS Attack", Proceeding AIM Advances in Information Technology and Mobile Communication. 2011 AIM '11. Springer-Berlin Heidelberg, CCIS-Vol. 147, pp. 336–339, (2011).

[4] Al-Allouni, H.,Rohiem, A.E.,Hashem, M.,El-moghazy, A.,Ahmed, A.E., "VoIP Denial of Service Attacks Classification and Implementation"., National Radio Science Conference, 2009. NRSC '09. pp 1–12, (2009).

[5] H. Sengar, "Overloading Vulnerability of VoIP Network". Dependable Systems and Networks, 2009. DSN '09. IEEE/IFIP International Conference, pp 419–428, (2009).

[6] J. Tang,Y. Cheng, C. Zhou, "Sketch-Based SIP Flooding Detection Using Hellinger Distance".,Proceeding GLOBECOM'09 Proceedings of the 28th IEEE conference on Global telecommunications. pp 3380–3385, (2009).