Towards Evaluating Resilience of SIP Server under Low Rate DoS Attack

Abhishek Kumar[1], P. Shanthi Thilagam[1], Alwyn R. Pais[1], Vishwas Sharma[2],
and Kunal M. Sadalkar[1]

[1] Dept. of Computer Engineering, NITK-Surathkal, India-575025
{aksinghabsk, santhisocrates, alwyn.pais,
officialmails.kunal}@gmail.com
[2] Dept. of SERC, IISc. Bangalore, India-560012
vishwas@mmsl.iisc.ernet.in

Abstract. 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 and it noticeably affects the performance of Session Initiation Protocol, SIP, communication. In this paper, we deeply analysis the resilience of SIP server against certain low rate DoS attacks. For this purpose we define performance metrics of SIP server under attack and non-attack scenarios. The performance degradation under attacks gives a measure of resilience of the SIP server. In order to generate normal SIP traffic and the attacks, we defined our own XML scenarios and implemented them using a popular open source tool known as SIPp. The system under evaluation was an open source SIP server.

1 Introduction

Voice over Internet Protocol (VoIP) is a technology that is reshaping the future of telephony. While enterprise VoIP offers low cost and various functionality it's also opens the door for external threats [1]. Most VoIP services uses the SIP infrastructure, because its simplicity and wide range of features, which makes its service vulnerable. To provide a better VoIP services we need to understand the behavior of VoIP server under different attack rates [2] and its countermeasure. The attack rate is comparable with that of normal traffic and hence it is not flooding the target to cause saturation. This qualifies the attacks to be termed "low rate". These 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.

We use a freely available open source Asterisk SIP server version 1.6.20 [3] & [4]. We populated 8000 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 8000 valid and invalid username and passwords to generate legitimate and illegitimate traffic to SIP application server. Fig. 1 (A) shows the notional diagram of DoS attack target (SIP Registrar) of SIP application server.

V.V. Das, G. Thomas, and F. Lumban Gaol (Eds.): AIM 2011, CCIS 147, pp. 336–339, 2011.

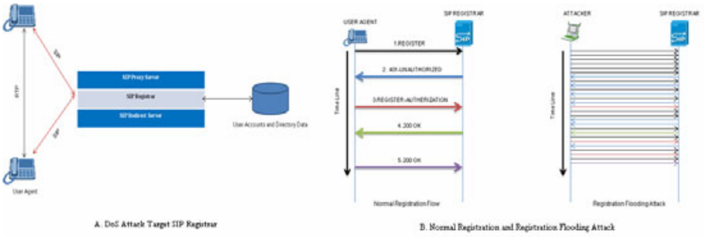

Fig. 1. A. DoS Attack Target SIP Registrar, B. Normal Registration and Registration Flooding Attack

2 Performance Metrics and Experimental Configuration

2.1 Performance Metrics

Our all metrics are SIP based to evaluate the resilience of VoIP SIP server. If any metrics are degraded, it will result to un-resilient SIP server. In our study we define following metrics:

- **Database Lookup Efficiency (R12).** The ratio of total number of first REGISTER request for database lookup by SIP server to total number of responded second "401-Unauthorized or 404- Not found" messages. This will measure the searching efficiency of SIP server for large number of user database in attack and no attack scenario.
- **SIP URI Binding Efficiency (R34).** The ratio of total number of third REGISTER request with MD5 digest to total number of responded fourth "200 OK" messages. This measure defines the digest computation efficiency of SIP server in attack and no attack scenario.
- **Successful Registration Acceptance Rate (SRAR).** Total number of successful URI binding per second. This measure defines the successful acceptance rate in attack and non attack mode. This metric determine the utilization of resources of SIP server.
- **Registration Drop Rate (RDR).** Total number of rejected URI binding per second. This measure defines the registration drop rate in attack and non attack scenario. This metric determine the loss of potential resources of SIP server under flooding attack.

2.2 Configuration Module

In our experiment in Fig. 2, we used SIPp tool [5] with Transport Layer Security (TLS) support as an attack generation and analysis module and an open source version of ASTERISK 1.6 as a SIP server. For attack generation module and client configuration module, we added 8000 illegitimate and legitimate user's credentials in our CSV file respectively, which is an input of created XML attack scenario. We compiled and run a C code to add 8000 users in SIP database to configure SIP.conf file.