Chapter 6
Detecting Denial of Service Attacks on SIP Based Services and Proposing Solutions

Zoha Asgharian
Iran University of Science and Technology, Iran

Hassan Asgharian
Iran University of Science and Technology, Iran

Ahmad Akbari
Iran University of Science and Technology, Iran

Bijan Raahemi
University of Ottawa, Canada

ABSTRACT
One of the main goals of employing Next Generation Networks (NGN) is an integrated access to the multimedia services like Voice over IP (VoIP), and IPTV. The primary signaling protocol in these multimedia services is Session Initiation Protocol (SIP). This protocol, however, is vulnerable to attacks, which may impact the Quality of Service (QoS), which is an important feature in NGN. One of the most frequent attacks is Denial of Service (DoS) attack, which is generated easily, but its detection is not trivial. In this chapter, a framework is proposed to detect Denial of Service attacks and a few other forms of intrusions, and then we react accordingly. The proposed detection engine combines the specification- and anomaly-based intrusion detection techniques. The authors set up a test-bed and generate a labeled dataset.

DOI: 10.4018/978-1-60960-836-1.ch006

Copyright ©2012, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
The traffic generated for the test-bed is composed of two types of SIP packets: attack and normal. They then record the detection rates and false alarms based on the labeled dataset. The experimental results demonstrate that the proposed approach can successfully detect intruders and limit their accesses. The results also confirm that the framework is scalable and robust.

INTRODUCTION

The Session Initiation Protocol (SIP) is an application layer protocol standardized by the Internet Engineering Task Force (IETF) for creating, modifying and terminating sessions (Rosenberg et al, 2002, Ehlert, Geneiatakis & Magedanz, 2009). SIP is structured as a layered protocol, meaning that its behavior is described in terms of a set of independent processing stages with only a loose coupling between each stage (Ehlert, Geneiatakis & Magedanz, 2009).

The lowest layer of SIP is the syntax parsing and encoding layer and the second one is the transport layer. It defines how a client sends requests and receives responses, and also, how a server receives requests and sends responses over the network. The third layer is the transaction layer. Transactions are a fundamental component of SIP. A transaction is a request sent by the client transaction layer to the server transaction layer, along with all responses to that request which are sent from the server transaction layer back to the client transaction layer. The transaction layer handles application-layer re-transmissions, matching of responses to requests, and application-layer timeouts. The layer above the transaction layer is called the transaction user (TU). When a TU wishes to send a request, it creates a client transaction instance, and passes the request along with the destination IP address, its port, and its transport layer information (Figure 1).

In 2005, the US National Institute of Standards and Technology declared DoS attacks to be a serious threat for the SIP infrastructures (Ahson & Ilyas, 2009). A DoS attack makes a particular network node unavailable by flooding it with illegitimate packets in order to seize its bandwidth, memory and CPU processing power. DoS attacks can be classified as illustrated in Figure 2. The attacks categorized into two broad groups: intentional attacks and non-intentional attacks. Non-intentional attacks are usually the result of implementation bugs or configuration errors. However, intentional or malicious attacks are initiated purposefully by intruders. Intentional attacks can be further subdivided into flooding and protocol misuse attacks. Flooding attacks are also referred to as exhaustion or depletion attacks because of their goal of depleting one or more resources of the victim and making it incapable of conducting its regular tasks, and processing the incoming requests (Sisalem, Floroiu, Kuthan, Abend & Schulzrinne, 2009).
Guarding Corporate Data from Social Engineering Attacks
www.igi-global.com/chapter/guarding-corporate-data-social-engineering/20671?camid=4v1a