Abstract

Voice over IP (VoIP) is a popular communication technology that is on its way to replacing the Public Switched Telephone Network (PSTN). The ubiquitous Internet along with the rise of camera-equipped smartphones and mobile computing devices has allowed VoIP to thrive. The Session Initiation Protocol (SIP) is one of the signaling protocols that makes VoIP possible, allowing it to be more flexible and even cheaper than other means of communication. Unfortunately, as with all IP-based technologies, VoIP systems are threatened by Denial of Service (DoS) attacks.

A variety of solutions exist that attempt to safeguard SIP-based VoIP from DoS attacks, but they are either too simple to be reliable or are too sophisticated to be practical as a first line of defense. This paper presents the design and implementation of DoS Defender, a novel intrusion detection system (IDS) that is fast yet effective at detecting the onset of a DoS attack. DoS Defender employs a neural network for traffic pattern recognition and can be used as part of an automated system for the activation of countermeasures. The system has been evaluated in a simulated environment, where it achieves near perfect precision and recall for detecting DoS attacks.