Abstract

As VoIP (Voice-over-IP) Services are becoming more popular, various types of attacks against them are increasing. SIP (Session Initiation Protocol) is the main protocol that is used in VoIP. SIP is subject to various types of attacks including DoS (Denial-of-Service) attack. This paper reports our experiment of simulating VoIP system using existing open source tools and technology. The simulated VoIP system is used to demonstrate a normal VoIP communication, launching DoS flooding attacks against SIP and implementing a successful Snort-based Intrusion Detection System (IDS) capable of catching suspicious SIP messages. Additionally, we propose a new VoIP architecture, which is based on buffering all incoming messages from clients with the intention of processing the messages in the buffer before they are forwarded to the destination.

References


Index Terms

Computer Science  Security

Keywords

VoIP; DoS; denial of service attack; snort; IDS; intrusion detection system; SIP; session initiation protocol.