Swedish IT Security Network for PhD students (SWITS 2008)

19-20 May 2008, Örebro

Two Layer Denial of Service Prevention on SIP VoIP Infrastructures

Ge Zhang
Privacy and Security Research Group, Karlstads University

Abstract

The emergence of Voice over IP (VoIP) has offered numerous advantages for end users and providers alike, but simultaneously has introduced security threats, vulnerabilities and attacks not previously encountered in networks with a closed architecture like the Public Switch Telephone Network (PSTN). We propose a two-layer architecture to prevent Denial of Service attacks on VoIP systems based on the Session Initiation Protocol (SIP). A first line Bastion host provides essential security checks against well-known TCP/IP related attacks and detects and prevents SIP message flooding against the host. In the second line of defense, we enhance the SIP proxy with additional security modules that provide specialized SIP-related security features. The architecture is designed to handle different types of attacks, including request flooding, malformed message sending, and attacks on the underlying DNS system. The effectiveness of the prevention mechanisms have been tested both in the laboratory and on a real live VoIP provider network. Finally, I will also present our consideration of the performance enhancement of our architecture (especially on the throughput).

Keywords: VoIP; SIP; Denial of Service; Flooding protection; Security; Malformed messages; DNS cache