Return Routability Check Filtering to Prevent Denial-of-Service Attacks on Session Initiation Protocol (SIP)-Based Systems

Technology #m07-043

“Lead Inventor: Henning Schulzrinne, Ph.D.

Session Initiation Protocol (SIP) Requires Differentiating Safe Traffic from Denial-of-Service (DoS) Traffic

Session Initiation Protocol (SIP) is an application layer protocol for establishing multimedia sessions. In SIP deployments, there is a need to differentiate between legitimate SIP traffic from denial-of-service (DoS) traffic, and determine the time and type of DoS attack. Further, it is imperative that DoS traffic has a minimal impact on the performance of SIP-based systems.

Detection and Prevention of DoS Attacks in a SIP-Based Systems

The technology describes a mechanism to determine the type of attack on a SIP-based system using return routability check filtering. This mechanism prevents user datagram protocol (UDP) based attacks by a SIP digest authentication mechanism. A null-authentication mechanism is used to filter a no-shared secret attack.

Applications:
• Detecting and preventing DoS attacks in a SIP-based systems
• Carrier-class SIP deployments need a DoS detection and filtering mechanism

Advantages:
• Distinguishes between trusted traffic and DoS traffic
• DoS attack form can be determined
• Difficult for attackers to launch DoS attacks against carrier class SIP systems


Licensing Status: Available for Licensing and Sponsored Research Support

Inventors

Henning Schulzrinne