Abstract

Traditional public switched telephone networks (PSTN) are replaced more and more by VoIP services these days. Although it is good for saving costs, the disadvantage of this development is that VoIP networks are less secure than the traditional way of transmitting voice. Because VoIP networks are being deployed in open environments and rely on other network services, the VoIP service itself becomes vulnerable to potential attacks against its infrastructure or other services it relies on.

This thesis will present a discussion of security issues of the Session Initiation Protocol (SIP), the signalling protocol for VoIP services. The main focus is on active attacks against the protocol that aim to reduce the service's availability – so called Denial of Service (DoS) attacks.

Existing countermeasures and detection schemes do not adequately differentiate between DoS attacks. However, the differentiation is important with respect to performance loss, as various protection schemes involve more computationally intensive processes.

Based on that discussion, this thesis attempts to provide an ontological approach to describing, and eventually preventing attacks from having their intended effects.