Abstract

Session Initiation Protocol (SIP) is an application layer protocol for multimedia sessions developed by IETF. It is a signaling protocol for voice over IP (VoIP). Originally, SIP was specified as a client server protocol to set up multimedia communications. However, recent proposals suggest using SIP in a peer-to-peer setting. The initiators of P2P SIP claim higher robustness against failure as well as easier configuration and maintenance as in the main motivation for peer-to-peer SIP. Clearly, a peer-to-peer setting imposes new security threats to SIP communications; design decisions that affect security, which include node-ID computation, overlay routing, authentication of nodes, SIP message semantics, and representation of identity. For instance, the lack of a central authority makes authentication of peers a hard problem. Without authentication, adversary nodes can spoof identity and falsify messages in the network. The peer-to-peer network may be affected by attacks like bootstrapping, identity enforcement, free riding, and anonymity. The requirements for secure network are secure node-ID assignment, secure routing table maintenance and secure message forwarding. In our project, we focus on providing secure node-IDs. Solely the IP address (without port) is used for node-ID generation. It is suggested as a better choice than using a combination of IP address and port which is being originally used.

Reference


Index Terms

Computer Science
Multimedia

Communication

Key words

VOIP
Session Initiation Protocol
P2P SIP

SIP Components

SIP Messages

RAT