Abstract

This paper presents a brief survey about the existing key exchange protocols namely MIKEY, ZRTP and SDES. The core features of these protocols and their suitability to SIP-VoIP Networks are analyzed in this paper. The focused research area in VoIP is related to the Security and Quality of service of the Voice data. Among these areas VoIP security and
An Analysis of VoIP Secure Key Exchange Protocols Against Man-In-The-Middle Attack

classification of voice data turns to be a challenging one. As VoIP delivers the voice packet over the public internet, using the transparent IP protocol suite the confidentiality of the voice data is at risk. Moreover exchanging cryptographic keys to encrypt the media stream in the Session Initiation Protocol has proven to be quite difficult task. There is a need for stronger key management protocols which will secure the voice data from all types of attack and which also provides a feasible key exchange mechanism. Each of these three key management protocols is surveyed and in addition its resistant against Man-In-The-Middle Attack has also been analyzed.

Reference


**Index Terms**

Computer Science

Security

**Key words**

SIP
SRTP
VoIP
ZRTP

SDES
MIKEY