Abstract

Session Initiation Protocol (SIP) is an open standard protocol and constitutes the provisioning of services like Internet Telephony and Instant Messaging. Vulnerabilities in SIP have made it possible to exploit it and launch many of the known internet attacks and also few specific attacks, thus affecting the services deploying SIP for session management. To maintain the confidentiality and integrity of voice data security mechanisms need to be deployed. Currently available security measures do not take into account real time nature of data and are generic i. e. not optimized for VoIP technology. This paper presents new end to end encryption architecture for securing the VoIP calls which use SIP to establish their session taking into account the real time nature of data.

References

- Liancheng Shan and Ning Jiang, &quot;Research on Security Mechanisms of SIP-based
End to End Encryption Architecture for Voice over Internet Protocol

VoIP System; IEEE 2009 paper 978-0-7695-3745-0/09.
- Arno Wacker, Mirko Knoll, Timo Heiber and Kurt Rothermel, &quot;A new Approach for establishing Pairwise keys for Securing Wireless Networks&quot; in SenSys internal Conference 2005, paper 1-59593-054-X/05/0011

- Prateek Gupta, Vitaly Shmatikov, &quot;Security Analysis of Voice-over-IP Protocols&quot; in conference, paper 0-7695-2819-8/07.

Index Terms

Computer Science
Security

Keywords
End to End Encryption Architecture for Voice over Internet Protocol

Sip Vulnerability  Encryption Algorithm  Voip Exploitation  Voip Communication