计算机工程与应用 2010 46 (5): 80-82 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

一种基于SGC-PKE的SIP可认证密钥协商方案

张 睿[1]，蒋 华[1，2]，杨亚涛[2]
1.西安电子科技大学 通信工程学院，西安 710071
2.北京电子科技学院 通信工程系，北京 100070

收稿日期 2008-8-18 修回日期 2008-11-11 网络版发布日期 2010-2-8 接受日期

摘要 会话初始协议（SIP）在许多领域已经开始发挥重要的作用。作为下一代互联网中的核心协议之一，SIP实体间通讯的安全性成为了至关重要的问题。通过对SIP现有的安全机制进行分析和比较，在此基础之上提出了一种新的基于自生成证书公钥加密体制（SGC-PKE）的可认证密钥协商方案，保证了SIP消息在传输过程中的完整性和机密性，并克服了使用公钥基础设施（PKI）带来的缺点。

关键词 会话初始协议 自生成证书公钥加密算法 双向身份认证 密钥协商
分类号 TN915.9

SIP authenticated key agreement scheme based on SGC-PKE

ZHANG Rui[1]，JIANG Hua[1，2]，YANG Ya-tao[2]

1.College of Communication Engineering，Xidian University，Xi’an 710071，China
2.Department of Communication Engineering，Beijing Electronic Science and Technology Institute，Beijing 100070，China

Abstract
Session Initiation Protocol（SIP） has played an important role in many fields.As one of the core agreements of the next generation Internet，however，SIP security is to be a crucial issue.In this paper，the existing SIP security mechanisms are analysed，and a new SIP authenticated key agreement mechanism based on Self-Generated-Certificate Public Key Encryption scheme（SGC-PKE） is presented，which assures the integrity，confidentiality and non-repudiation during the transmission of SIP message and overcomes the disadvantage of Public Key Infrastructure（PKI）.

Key words session initiation protocol self-generated-certificate public key encryption scheme mutual-authentication key agreement

DOI: 10.3778/j.issn.1002-8331.2010.05.024

通讯作者 张 睿 channel_vison@163.com