计算机工程与应用 2010 46 (5): 96-99 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

一种基于身份的SIP认证与密钥协商机制

周计成，徐开勇，赵 彬，吴 平

解放军信息工程大学 电子技术学院，郑州 450004

收稿日期 2008-8-25 修回日期 2008-11-6 网络版发布日期 2010-2-8 接受日期

摘要 随着SIP协议在网络通信中的广泛应用，特别是向移动领域扩展，网络中大量使用无线设备，终端的运算与存储能力有限。对SIP的安全方案进行了讨论和分析，提出了一种基于身份的认证与密钥协商方案，保证了SIP消息传输过程中的完整性和真实性，并在该过程中进行了密钥协商。方案中不需要公钥证书，用户用身份标识SIP URI作为公钥，降低了对终端计算、存储能力的需求和通信开销，具有简单高效的优点。

关键词 会话发起协议 安全机制 基于身份的密码学 身份认证 密钥协商

分类号 TP393.08

Identity-based authentication and key agreement scheme of SIP

ZHOU Ji-cheng，XU Kai-yong，ZHAO Bin，WU Ping

Institute of Electronic Technology，PLA University of Information Engineering，Zhengzhou 450004，China

Abstract

Along with Session Initiation Protocol（SIP） application in network communication widely，especially in mobility area，many wireless equipments are used.These devices have limited capacity of storage and computing.In this paper，the security schemes of SIP are discussed and analyzed.Furthermore，a new authentication and key agreement scheme based on identity is proposed，which assures the integrity and authenticity of SIP message during transmission and consults with share key.The scheme doesn’t need any public key certificate；user’s SIP URI is used as his public key.It needs less storage，computing capacity and communication cost，so it is simple and effective.

Key words Session Initiation Protocol（SIP） security mechanism Identity Based Cryptography（IBC） authentication key agreement

DOI: 10.3778/j.issn.1002-8331.2010.05.029

通讯作者 周计成 testforngn@sina.com