

信息与网络安全

一种基于SIP安全认证机制的研究

姬宁<sup>1</sup>;林晓<sup>2</sup>;普杰信<sup>2</sup>

河南科技大学电子信息工程学院<sup>1</sup>

收稿日期 2006-9-21 修回日期 网络版发布日期 2007-3-14 接受日期

**摘要** 目前,会话初始协议(SIP)大部分认证机制只提供了服务器到客户端的认证,HTTP摘要认证便是其中的一种。分析了这种机制容易遭受服务器伪装攻击和密码窃取攻击的缺陷,提出了一种弥补这些缺陷的安全认证机制。试验表明该算法具备较高的效率。

**Abstract** At present, most of the session initial protocol (SIP) authentication schemes only provide client-to-server authentication. And HTTP digest authentication is one of them. The weakness of this scheme in server spoofing and password guessing attacks was analyzed, and a more secure strategy was proposed which avoided these shortcomings. The experimental result illustrates that this proposed algorithm is effective.

**关键词** [会话初始协议](#) [认证](#) [HTTP摘要](#) [安全](#)

**Key words** Session Initial Protocol (SIP); authentication; HTTP digest; security

分类号

**DOI:**

通讯作者:

姬宁 [hkdjining@yahoo.com.cn](mailto:hkdjining@yahoo.com.cn), [hkdjining@sina.com](mailto:hkdjining@sina.com)

作者个人主页: 姬宁 林晓 普杰信

扩展功能

本文信息

▶ [Supporting info](#)

▶ [PDF](#) (847KB)

▶ [\[HTML全文\]](#) (0KB)

▶ [参考文献\[PDF\]](#)

▶ [参考文献](#)

服务与反馈

▶ [把本文推荐给朋友](#)

▶ [加入我的书架](#)

▶ [加入引用管理器](#)

▶ [引用本文](#)

▶ [Email Alert](#)

▶ [文章反馈](#)

▶ [浏览反馈信息](#)

相关信息

▶ [本刊中 包含“会话初始协议”的相关文章](#)

▶ 本文作者相关文章

· [姬宁](#)

· [林晓](#)

· [普杰信](#)