通信学报
Journal on Communications
主管单位：中国科学技术协会
主办单位：中国通信学会

杨力,张俊伟,马建峰,刘志宏.改进的移动计算平台直接匿名证明方案[J].通信学报,2013,(6):69~75

改进的移动计算平台直接匿名证明方案

Improved direct anonymous attestation scheme for mobile computing platforms

投稿时间： 2012-06-26

DOI：10.3969/j.issn.1000-436x.2013.06.008

中文关键词：可信计算 远程证明 直接匿名证明 密钥协商

英文关键词:trusted computing remote attestation direct anonymity attestation key agreement

基金项目:长江学者和创新团队发展计划基金资助项目(IRT1078)；国家自然科学基金资助项目(U1135002, 61202390, 61202389, 61173135, 61100230, 61100233)；陕西省自然科学基础研究计划基金资助项目(2012JM8025, 2011JQ8003, 2011JM8004, 2012JQ8043, 2012JM8030)

作者	单位
杨力，张俊伟，马建峰，刘志宏	西安电子科技大学 计算机学院，陕西 西安 710071

中文摘要:

分析了Ge等人提出的直接匿名证明方案的安全缺陷，指出该方案的认证协议在用于远程证明时不能抵抗重放攻击和平台伪装攻击。提出一种改进的直接匿名证明的认证协议，引入会话密钥协商机制，增强互认证功能。分析表明，改进方案在正确进行直接匿名证明的前提下，满足不可伪造性和匿名性，能够抵抗重放攻击和平台伪装攻击，协议性能满足移动计算平台的可信验证需求。

英文摘要:

The security flaws of a direct anonymous attestation scheme proposed by Ge, et al. Were analyzed, and the result shows that the authentication protocol of the scheme is vulnerable to reply attacks and platform masquerade attacks when being used for remote attestation. An improved direct anonymous attestation authentication scheme with the involvement of key agreement was proposed to provide the property of mutual authentication. The analysis shows that the proposal can realize direct anonymous attestation with the properties of forgery-resistance and anonymity, and resist reply attacks and platform masquerade attacks; the scheme is effective and suitable for the mobile trusted computing platforms.

查看全文 查看/发表评论 下载PDF阅读器

关闭