计算机工程与应用 2010 46 (1): 90-94 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

基于CPK的可信平台用户登录认证方案

马宇驰，赵 远，邓依群，李益发

解放军信息工程大学 信息工程学院 应用数学系，郑州 450002

收稿日期 2008-7-10 修回日期 2008-11-10 网络版发布日期 2010-1-7 接受日期

摘要 用户登录身份认证是建立操作系统可信性的一个非常重要的环节，是建立可信计算环境的基础。首先讨论了认证的相关技术，介绍了CPK（组合公钥）原理，然后根据可信计算组织的规范，利用CPK算法和动态验证码的技术，提出了一种基于CPK的可信平台用户登录认证方案，该方案属于双因素认证方案，将认证和授权严格分开，并启发式分析了方案的特色和安全，最后在串空间模型下证明了方案的安全性，取得了比TCG标准中引用的方案更好的性能。

关键词 可信计算 组合公钥（CPK） 身份认证 可信登录 串空间模型

分类号 TP311

Trusted computing platform login authentication scheme based on CPK

MA Yu-chi，ZHAO Yuan，DENG Yi-qun，LI Yi-fa

Department of Applied Mathematics，Information Engineering Institute，PLA Information Engineering University，Zhengzhou 450002，China

Abstract

Identity authentication for user login is very important to the operation system，and is the basis for building the trus-ted computing environment.The related technology of authentication is discussed.The theory of CPK（Combination of Public Key） is introduced.In addition，according to the standards of the Trusted Computing Group（TCG），using CPK and dynamic authentication code technology，a trusted computing platform login authentication scheme based on CPK is proposed.The scheme is double ingredient，separates authentication and warrant strictly.This paper not only shows a heuristic analysis about the characteristic and security of the scheme，but also，in strand space model，proves the security of the scheme，which indicates the scheme is more secure than the corresponding scheme presented in TCG standard.

Key words trusted computing Combination of Public Key（CPK） identity authentication trusted login strand space model

DOI: 10.3778/j.issn.1002-8331.2010.01.029

通讯作者 马宇驰 mayuchi9111027@hotmail.com