计算机工程与应用 2007 43 (16): 165-168 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信与安全

基于嵌入式技术的信任根研究

林小茶，李 光

北京信息工程学院，北京 100101
华北计算技术研究所，北京 100083

收稿日期 修回日期 网络版发布日期 2007-5-19 接受日期

摘要 可信计算近年来发展迅速，被认为最有可能从根源上解决计算机的安全问题，信任根是可信计算的根本。简要介绍了可信计算的发展历史，分析了可信产品市场不景气的原因，从可信计算信任根的角度入手，提出了两种采用嵌入式技术来实现信任根的方案，并给出了方案的详细设计思想。

关键词 可信计算 信任根 可信平台模块 嵌入式技术

分类号

Study of TPM based on embedded technology

LIN Xiao-cha，LI Guang

Beijing Information Technology Institute，Beijing 100101，China
North China Institute of Computing Technology，Beijing 100083，China

Abstract

With rapid development in recent years，the trusted computing technology has been recognized as a method to solve the computing security problems from the root，while the root of trust is the base of the trusted computing.This article briefly introduces the development history of the trusted computing，then analyzes some reasons of depression in the trusted product market，and finally digging into the root of trust，proposes two proposals for realizing the root of trust based on embedded technology，and supports these two proposals with detailed design concept as well.

Key words trusted computing root of trust Trusted Platform Module（TPM） embedded technology

DOI:

通讯作者 林小茶