计算机工程　2007 33 (20): 156-158　ISSN: 1000-3428　CN: 31-1289/TP

安全技术

一种柔性可信计算机模型与实现方法

周振柳1，陈　楣1,2，池亚平3，刘宝旭1，许榕生1

(1. 中国科学院高能物理所计算中心，北京　100049；2. 福州大学，福州　350002；3. 北京电子科技学院，北京100070)

收稿日期　修回日期　网络版发布日期 2007-10-11　接受日期

摘要　基于可信计算组织提出的可信计算原理和安全技术规范，设计了一种柔性可信计算机模型(FTPC)，阐述了该模型的信任机制和实现方法。FTPC通过增强传统BIOS的安全功能，以BIOS核心代码为可信根核，将可信计算模块(TPM)封装成块设备，并通过计算机USB接口实现TPM与BIOS和操作系统的交互。FTPC采用实体的身份认证、完整性度量和密封存储等技术，无需改变现有计算机硬件体系结构即可支持可信计算，FTPC具有易实施和应用灵活的特点。

关键词　可信计算模块(TPM)；可信计算；柔性可信计算机；BIOS；用于度量的核心可信根

分类号　TP393.08

DOI:

通讯作者:

作者个人主页: 周振柳1;陈　楣1;2;池亚平3;刘宝旭1;许榕生1