计算机工程　2007 33 (15): 152-154　ISSN: 1000-3428　CN: 31-1289/TP

安全技术

一种基于TPM芯片的计算机安全体系结构

邢启江1,2，肖 政3,4，侯紫峰3，姜永华2

(1. 山东工商学院计算中心，烟台 264005；2. 海军航空工程学院电子信息工程系，烟台 264001；3. 中国科学院计算所，北京 100080；4. 中国科学院研究生院，北京 100039)

收稿日期　修回日期　网络版发布日期 2007-7-31　接受日期

摘要　针对现行通用个人计算机基于开放架构、存在诸多攻击点等安全问题，提出了一种基于TPM安全芯片的新型计算机体系结构。设计并实现了基于安全芯片的软件协议栈TSS，在安全芯片中使用软件协议栈，通过核心服务API来调用核心服务模块，解决远程通信的平台信任问题。设计并实现了基于多协议的授权和认证管理，实现上层应用和TPM之间的授权会话及授权认证，从而保证计算机能够完成安全计算和安全存储的工作，使计算平台达到更高的安全性。

关键词　TPM安全芯片；软件协议栈；可信计算；安全体系结构

分类号　TP303

DOI:

对应的英文版文章：15-54

通讯作者:

作者个人主页: 邢启江1;2;肖 政3;4;侯紫峰3;姜永华2