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

王丽娜,高汉军,余荣威,任正伟,董永峰.基于信任扩展的可信虚拟执行环境构建方法研究[J].通信学报,2011,(9):1~8

基于信任扩展的可信虚拟执行环境构建方法研究

DOI：

中文关键词：

英文关键词：

基金项目：

作者	单位
王丽娜	
高汉军	
余荣威	
任正伟	
董永峰	

中文摘要：

为保护虚拟机运行环境及上层服务软件的完整性、安全性，提出了一种基于信任扩展的可信虚拟执行环境的构建方法。首先，建立物理平台配置寄存器（PCR, platform configuration register）与虚拟PCR的映射关系，以此实现虚拟可信平台模块（vTPM）与底层可信计算基的绑定；其次，利用本地vTPM管理器签发证书，完成可信证书链在虚拟机中的延伸。通过物理平台至虚拟平台的信任扩展，虚拟机可以有效的利用TPM提供的相关功能（如远程证明、密封存储等），完成平台环境的证明及私密信息的安全存储，从而构建了可信虚拟执行环境。最后，实现了原型系统并进行了测试，测试结果证明了本系统可以有效地实现虚拟平台的密封存储和远程证明等功能。

英文摘要：

查看全文 查看/发表评论 下载PDF阅读器

关闭