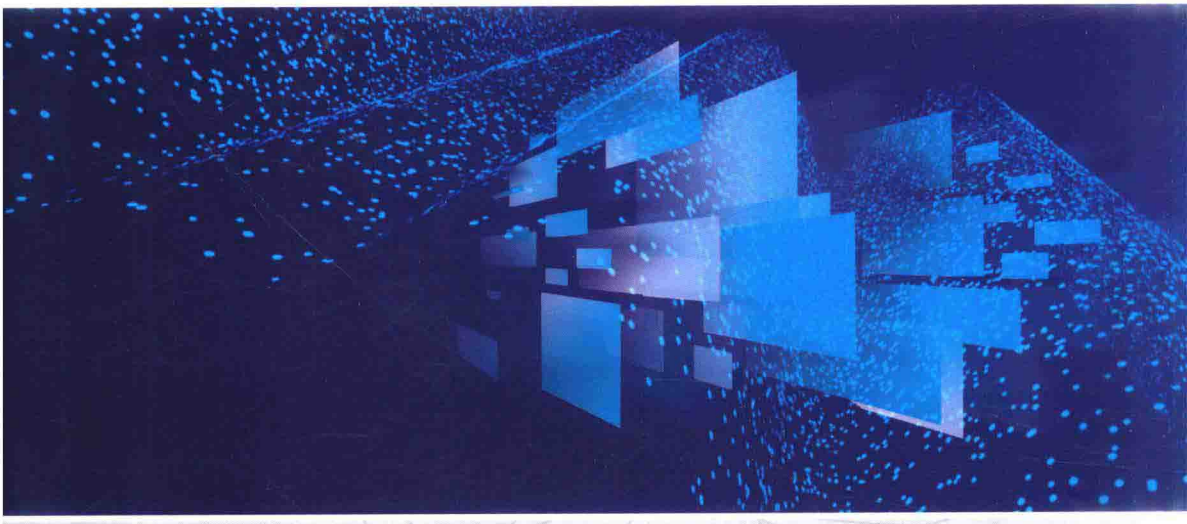
基于虚拟可信平台的软件可信性研究

郝瑞 著

RESEARCH ON SOFTWARE TRUSTWORTHINESS BASED ON VIRTUALIZED TRUSTED PLATFORM



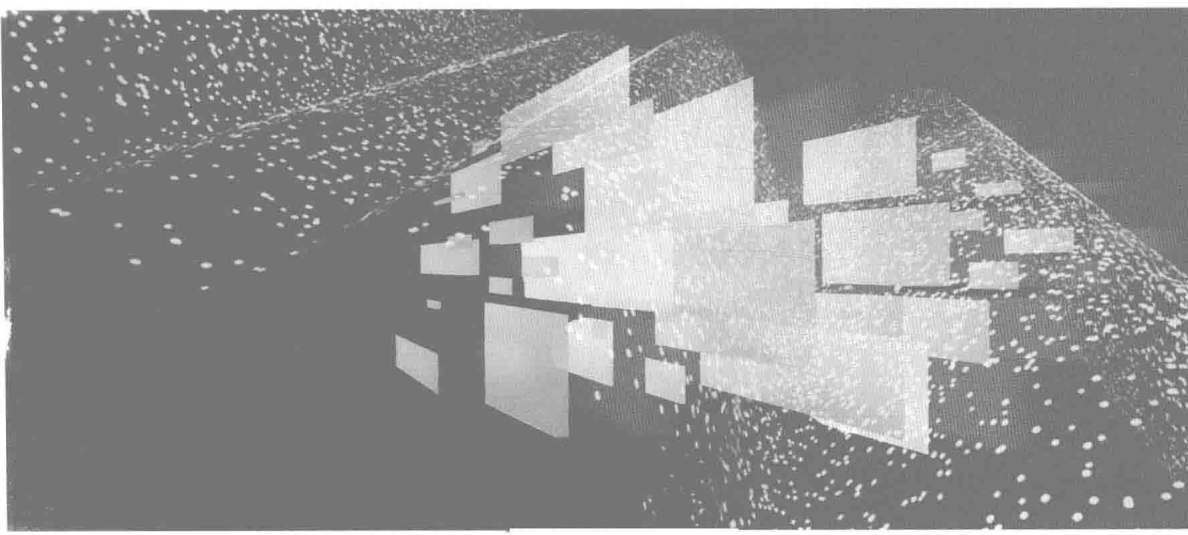
WUHAN UNIVERSITY PRESS
武汉大学出版社

国家自然科学基金（61202365）
虚拟现实技术与系统国家重点实验室开放基金（BUAA-VR-17KF-14）
山西省留学基金（2009-28）
社科联重点课题（SSKLZDKT2014047）

基于虚拟可信平台的软件可信性研究

郝瑞 著

RESEARCH ON SOFTWARE TRUSTWORTHINESS BASED ON VIRTUALIZED TRUSTED PLATFORM



武汉大学出版社

图书在版编目(CIP)数据

基于虚拟可信平台的软件可信性研究/郝瑞著. —武汉：武汉大学出版社,2017.5

ISBN 978-7-307-19320-8

Ⅰ.基… Ⅱ.郝… Ⅲ.软件开发—研究 Ⅳ.TP311.52

中国版本图书馆 CIP 数据核字(2017)第 108681 号

责任编辑:唐 伟 责任校对:李孟潇 版式设计:马 佳

出版发行:**武汉大学出版社** (430072 武昌 珞珈山)

(电子邮件:cbs22@whu.edu.cn 网址:www.wdp.com.cn)

印刷:虎彩印艺股份有限公司

开本:720×1000 1/16 印张:9 字数:125 千字 插页:1

版次:2017 年 5 月第 1 版 2017 年 5 月第 1 次印刷

ISBN 978-7-307-19320-8 定价:30.00 元

版权所有，不得翻印;凡购我社的图书，如有质量问题，请与当地图书销售部门联系调换。

序

21 世纪是信息化时代，信息成为一种重要的战略资源，信息技术改变着人们的生活和工作方式，社会的信息化程度大大提高，信息产业已经成为世界第一大产业。信息的获取、处理和安全保障能力成为一个国家综合国力的重要体现。当前，信息技术与产业欣欣向荣，处于空前繁荣的阶段。但是，危害信息安全的事件不断发生，信息安全的形势非常严峻。近年来，可信计算技术正在以不同方式应用于构造信息安全解决方案，能够行之有效地提高计算平台的安全性。本书旨在开展虚拟可信平台的软件动态可信理论模型的研究，可以促进可信计算技术，尤其是动态可信评测技术的健康发展，所研究的成果不仅具有重要的理论价值，更对技术实践有很好的指导意义。我相信这本书会使许多人受益，也祝愿我们的作者能在虚拟化和可信计算技术的发展中不断有新的进步和贡献。

李学龙　博士

中国科学院博士生导师

国家“千人计划”专家

国家杰出青年科学基金获得者

摘　要

可信计算技术从硬件结构层有效提高计算机平台的安全性，目前已成为信息安全领域新的研究热点。随着虚拟化技术的快速发展和广泛应用，将虚拟化技术与可信计算技术结合构建虚拟可信平台是业界实现可信计算最为有效的一种解决方案。但是目前虚拟可信平台的发展还存在一些问题：一是物理平台至虚拟平台的信任链扩展不足，无法保障虚拟客户系统的可信性；二是理论研究滞后于技术实现，至今尚未建立公认的基于虚拟可信平台的软件可信性度量模型。

针对上述问题，本书对基于虚拟可信平台的软件可信性度量模型进行了研究，并提出两阶段层次化虚拟可信系统度量模型——TSVTMM，基于该模型提出了基于软件可信属性完整性度量方法，并对 TCG 标准数据封装进行改进，提出了针对可信软件完整性度量列表(TSIML)的数据封装存储方案。根据 TCG 动态度量的实际需求提出了软件行为动态可信评测方法以及利用模糊理论和模糊支持向机(FSVM)的特点，提出一种新的隶属函数构造方法 KDFSVM，从而提高了软件行为的预测精度和识别率。本书主要研究成果及创新点如下。

(1)针对 TCG 信任链扩展无法保障虚拟客户系统的可信性，笔者提出了两阶段层次化虚拟可信系统度量模型 TSVTMM。TSVTMM 根据应用软件的两个执行状态——装载和运行，整体上分为完整性度量和动态可信性评测两个阶段，并采用不同的方式和策略对软件的装载及运行加以控制。完整性度量阶段是对将要装载的应用软件可信属性信息进行完整

此为试读，需要完整PDF请访问：www.ertongbook.com

性验证。动态可信评测阶段是在软件运行期间通过对其实际行为的监控、动态分析、态势预测，实现软件行为动态可信性评测。并将 TCG 信任链扩展至 TSVTMM，从而保证了 TSVTMM 自身的安全。该模型容易实现，具有良好的可扩展性。

(2)针对 TCG 标准数据封装在平台配置更新失效的问题，笔者提出基于 TSIML 新的数据封装存储方案。采用相对固定的虚拟底层环境状态执行标准封装，结合易变的客户虚拟机状态进行属性封装，从而解决了客户虚拟机状态因频繁变化所引起的多次封装问题。

(3)从软件行为的可信性入手，根据 TCG 动态度量的实际需求，笔者提出了软件行为动态可信评测方法。通过软件在运行时对其行为轨迹进行度量，根据软件实际行为是否符合预期的可信策略进行动态分析评测，将可信度量机制的粒度细化到软件行为的层面。实验结果表明该方法在有限的样本条件下，在软件行为模式学习、识别和预测方面具有良好的性能。

(4)为了提高模糊支持向量机 FSVM 对软件行为识别的精度，笔者提出一种基于模糊理论新的模糊隶属函数的构造方法 KDFSVM。该方法对传统的距离模糊隶属度 DFSVM 进行了改进，引入各样本点紧密程度 ρ 和 k 最近邻点中属于同类的比率 p 来构造隶属度。实验结果表明采用 KDFSVM 算法对软件行为预测分类的准确率明显提高。

综上所述，通过开展基于虚拟可信平台软件可信性度量模型的研究，从而构建虚拟可信执行环境，可以促进虚拟化技术和可信计算技术更好的结合。

ABSTRACT

Trusted computing technology from the hardware structure layer effectively improves the security of the computer which has become one of the new hot spots in new hotspot in the field of information security. With rapid development and wide application of virtualization technology, it is the most effective solution of trusted computing to combine virtualization technology and trusted computing technology in industry. But, there are still some problems in the development of virtualized trusted platform. Firstly, the lack of trust chain extension of the physical platform to a virtual platform can not ensure the trustworthiness of the virtual client systems. Secondly, theoretical researches are behind technical practice. There are not yet generally accepted software measurement models founded based on virtual trusted platform.

In order to solve above problems, a two-stage strategy virtualized trusted system measurement model-TSVTMM is proposed. Based on the model, the integrity measurement method for the software trustworthiness properties is proposed; TCG standard data sealing is improved and the solution of data sealing for the trust software integrity measurement list(TSIML) is proposed; The dynamical trusted evaluation of the software behavior is proposed based on the actual demand of TCG dynamic measurement; The new construction method of the membership function KDFSVM based on fuzzy theory and fuzzy support vector machine FSVM is proposed in order to improve prediction ac-

curacy and recognition rate of the software behavior. The followings are main research results and innovations:

(1) In order to solve TCG trust chain extension can not ensure the trustworthiness of the virtual client system, the two-stage strategy virtualized trusted system measurement model-TSVTMM is proposed. There are two phases of integrity measurement and dynamic trusted evaluation based on loading and running of the software, and loading and running of the software is controlled in different ways and strategies. In integrity measurement phase, the integrity of the trusted attribute information of the software is verified. In dynamic trusted evaluation stage, the software behavior is evaluated by monitoring the actual behavior, dynamic analysis and trend forecasting. TCG trust chain extends to TSVTMM to ensure own security of TSVTMM. This model is easy to implement, and it has good scalability.

(2) In order to solve the problem of the platform configuration update, the new solution of data sealing is proposed. Standard sealing relatively invariable virtualized underlying states combines with property sealing variable guest virtual machine states. This method solves the problem of the repeated sealing because of frequent changes of the guest virtual machine.

(3) Starting from trustworthiness of the software behavior, according to actual demands of dynamic measurement, the method of dynamic trusted evaluation of the software behavior is proposed. The behavior traces are measured during the software running, and it is judged wether the actual behavior is as expected according to the trusted strategy. The granularity of the mechanism of trustworthiness is refined to the level of software behavior. Experimental results show that the method has a good performance on pattern learning, recognition, and projection of the software behavior under conditions of limited samples.

(4) In order to improve the accuracy of recognition of fuzzy support vec-

tor machine (FSVM) to the software behavior, the new construction method of fuzzy membership function KDFSVM is proposed based on fuzzy theory. The method improve the traditional distance fuzzy membership DFSVM by introducing the tightness of each sample point ρ and p , which is the proportion of k nearest neighbor belonging to the same class, to construct the membership function. Experimental results show that the KDFSVM improves the classification accuracy rate of the Software behavior significantly.

In short, theresearch on software trustworthiness based on virtualized trusted platform can promote a healthy development of virtualization technology and trusted computing technology.

目　录

此为试读，需要完整PDF请访问：www.ertongbook.com

图 目 录

表 目 录

第1章 绪 论

1.1 研究背景和意义

随着计算机技术的发展、网络的广泛普及，当今社会已进入信息化社会，信息化已经渗透到社会的政治、经济、教育、军事、社会生活以及意识形态等各个方面。在信息社会，一方面，信息技术与信息产业的高速发展已成为社会新的经济增长点和重要的战略资源；而另一方面则是破坏信息安全的事件层出不穷，呈现日益复杂的局面，信息安全问题已经变得日益突出。信息的安全保障能力已成为一个国家的综合国力的重要组成部分。信息安全事关国家安全、事关社会的稳定，因此，必须采取有效措施保障我国的信息安全。

纵观信息安全的发展历程，人们最早关注的是信息在通信过程中的安全问题。随着多用户操作系统的出现，人们对信息安全的关注扩大为“机密性、访问控制与认证”。到了20世纪中后期，学术界与军事部门对“信息安全”与“信息系统安全”越来越重视，信息安全逐步发展成为一门独立的学科，许多信息安全标准规范在这一时期大规模有组织地制定，信息安全的研究越来越多地受到信息技术的驱动，新型网络和计算机应用环境下的协议设计和算法逐渐成为热点问题。当今是可信计算时代，当前信息安全的研究已经逐步发展成为可信计算研究时期，可信计

此为试读，需要完整PDF请访问：www.ertongbook.com