互联网环境下的软件可信度量研究

李红霞　陈均明　著

Internet-based software trusted measure

西南交通大学出版社
Http://press.swjtu.edu.cn

互联网环境下的软件可信度量研究

李红霞　陈均明　著

西南交通大学出版社
·成　都·

内容提要

本书是软件可信度量（software trusted measure）领域的最新研究成果，分析了软件可信计算与软件可信面临的问题、软件行为可信、软件可信的技术支撑等方面；研究了软件可信路径渗透、软件可信特征和机理；剖析了软件可信度量可用的模型和软件可信度量的一些方法；重点研究了软件可信树度量方法；设计、测试与分析一个软件可信度量评估系统原型系统。可为进一步深入研究软件可信度量提供参考，也可供相关专业人士使用。

图书在版编目（CIP）数据

互联网环境下的软件可信度量研究 / 李红霞，陈均明著. —成都：西南交通大学出版社，2011.2
ISBN 978-7-5643-0931-2

Ⅰ. ①互… Ⅱ. ①李…②陈… Ⅲ. ①软件工程－研究 Ⅳ. ①TP311.5

中国版本图书馆 CIP 数据核字（2010）第 198605 号

互联网环境下的软件可信度量研究

李红霞　陈均明　著

*

责任编辑　李芳芳
特邀编辑　黄庆斌　顾　飞
封面设计　本格设计

西南交通大学出版社出版发行
（成都二环路北一段 111 号　邮政编码：610031　发行部电话：028-87600564）
http: //press.swjtu.edu.cn
成都蜀通印务有限责任公司印刷

*

成品尺寸：148 mm×210 mm　　印张：6.437 5
字数：178 千字
2011 年 2 月第 1 版　　2011 年 2 月第 1 次印刷
ISBN 978-7-5643-0931-2
定价：18.00 元

序

以计算机为核心的信息系统早已成为当今人类社会的基础设施之一，其重要性完全不亚于电力系统，人们对信息的依赖，也跟对电力的依赖不分伯仲。对于如此关键的基础设施，其安全性是头等大事。因此，信息安全，包括计算机安全、网络安全等，不仅是专业领域中的热点课题，也常常是公共媒体中的热门词汇。

在信息安全领域，近年来“可信（赖）计算”在人们的视界中越来越突出。某种意义上，“可信”概念包含“安全”概念，一个可信的系统，应该是安全的。因此，可以认为：“可信”是“安全”的升华，是一种更高的境界。尽管国际上关于可信计算有不止一个术语，如 Trusted Computing，Trustworthy Computing，还有 Dependable Computing，且各自的含义并不同一，但它们的核心理念是共同的。

既然信息系统是由硬件和软件构成的，那么可信系统就必须保证两者都可信。从计算机诞生之日起，硬件和软件就密不可分，两者相得益彰。然而，相对而言，软件的“软性”，其实也表征了它在逻辑上的极端复杂性，更加难以捉摸。因此，尽管在硬件层面上，可信计算已经初步有了诸如 TPM（Trusted Platform Module）这样的可信平台模块，但在软件层面上，可信计算的进展却显得尤其困难重重。

“可信”这个概念，其反面应该是“不可信”。但是，截然的、全或无性质的二元划分在实践中显得过于武断，是行不通的。因此，针对某种实体如软件，研究其“可信”程度，即它的度量，是十分明智的。

这本书的内容就是关于软件可信度量的。此课题有相当大的难度，却很有意义。因此，虽然作为一项初步的相关工作，书中可能有

些方面略显稚嫩，难免存在诸多的不完善甚至差错，但这个课题的探索本身是难能可贵的，其成果不失参考价值。何况，“可信计算”在国际上尚存在某种程度的争议，反映了问题的复杂性，但无论如何，其理念是完全正确的，很值得探索。也许，人们很难实现完全的“可信系统”、“可信软件”，但可期待不断提高可信的程度，日益逼近这个理想。

其他的，留给读者自己去品味、去评判。

重庆大学 傅鹂 教授

2010 年 12 月 12 日

前　言

信息时代人们对信息系统的依赖程度越来越高。信息系统，特别是运行在信息系统中的各类软件的安全性也受到越来越多的关注。安全设计本身的缺失可能构成新的信息安全风险。新的风险点、新的漏洞、新的攻击技术手段会随时出现。有了广域网后，病毒、黑客和计算机犯罪使得大家对网络的安全产生了恐惧，严重制约了信息化的发展，制约了电子商务、电子政务的发展。病毒和黑客攻击的最终目的是非法进入用户的信息系统，篡改或盗用电脑上的数据。防火墙、杀毒软件等对这些攻击只能被动抵抗。由老三样（防火墙、入侵监测和病毒防范）为主构成的传统信息安全系统，是以防外为重点，而与目前信息安全主要“威胁”源自内部的实际状况不相符合。从组成信息系统的服务器、网络、终端三个层面上来看，现有的保护手段是逐层递减的。人们往往把过多的注意力放在对服务器和网络设备的保护上，而忽略了对终端软件系统的安全保护。

可信计算技术是有效解除计算机网络和终端威胁的方法之一。传统的信息安全措施不外乎“堵漏洞、做高墙、防外攻”等老三样，但最终的结果是防不胜防。主要原因是不去控制发生不安全问题的根源，而是在外围进行封堵。国家信息化专家咨询委员会专家沈昌祥院士认为：为了解决 PC 机结构上的不安全，应在世界范围内推行可信计算。

Internet 环境下，计算机系统是否可信，包括硬件、网络、操作系统、中间件、应用软件、信息系统使用者以及它们之间的交互的复杂系统等是否可信，在这条链上的任何一个环节出现问题，都会导致计算机系统的不可信。可信计算旨在能有效地解决计算机结构上的不安全，并从根本上提高系统的安全性。可信计算改变人们传统的信息安全思维方式，从终端开始防范攻击，提高终端系统的安全性，使得信息系统中每个使用者都经过认证和授权，其操作都符合规定，就不会

产生攻击性事故。可信计算试图从终端入手解决整个信息系统的安全问题 。目前国内外可信计算的研究主要集中在硬件层面和网络层面。

以通信、存储和计算为核心的信息基础设施已经渗透到政治、经济、军事、文化以及社会生活的各个层面，成为当代生产力发展和人类文明进步的强大动力。软件是信息基础设施的灵魂，随着计算机系统和计算机网络在社会各个领域的广泛应用以及人们对功能需求的不断增加，互联网环境下，对于越来越复杂的各种应用软件，软件内部存在危机、缺陷、漏洞、错误、软件外部存在病毒、恶意代码入侵，软件系统变得日趋庞大和难以驾驶，系统越来越脆弱，它们很多时候不以人们期望的方式工作，经常发生各种故障和失效，直接或间接地给用户带来损失，可信软件与系统的设计和开发成为一个基本问题，尤其是在开放和分布的 Internet 环境下，问题更加突出。如何进行软件可信度量是一个值得高度重视的问题，但国内外在这方面的系统研究还正处在探索阶段。

需要指出的是：软件可信性的研究与硬件级和网络层面的可信计算有较大的不同，特别是软件的开发存在大量人工因素的介入。所以在软件可信性定量化研究过程中，需要考虑如何刻画各种人为因素，这也是该研究方向的一个难点。有鉴于此，本书以软件工程为背景，信息管理与信息安全领域知识为依托，在软件可信性定量化研究方面进行了初步探索。

本书从可信计算的目的和思路谈起，综述了中外各个科研院所关于可信计算的研究发展状态、软件可信计算的研究发展状态。本书从多个角度描述了可信与可信计算各自的含义，从服务提供者的可信、网络信息传输的可信、终端用户的可信等方面探讨了可信网络的内涵，从软件内外部情况分析了软件可信面临的问题，从软件质量、系统、网络行为、用户使用等不同角度分析了什么是软件可信。分析了软件可信行为特征、软件可信的技术支撑。

本书探讨了与可信路径密切相关的几个概念、分析了可信路径的含义，论证了主流平台中 Linux、NT 系列 windows 中可信路径渗透情

况，阐释了软件可信的基本要素、属性情况、概念模型等软件可信特征和机理，分析了分布式可信模型、主观可信管理模型、可信证据模型、可信评估模型、软件可信分级模型，以便为后面建立软件可信树评估模型做铺垫和准备。本书研究了开放式网络环境下的可信度量方法、基于Agent软件协同服务的可信度量方法、决策树方法、专家评分法、模糊数学方法、支持向量机的模糊数学建模方法和等级度量方法等可支持可信度量的一些方法，为后面建立软件可信树的方法做知识准备。

本书将软件可信性质区分软件可信必备性质、运用相关标准评判可信程度的性质、可由专家评判可信等级的软件可信性质，同时将三类性质分别阐述了量化方法。采用模糊数学法和等级度量方法，将软件可信程度采用离散方式分等级进行度量。本书借鉴较为成熟的决策树方法，在总结前人对软件可信属性的零散研究基础上，提出了软件可信树方法，初步地构建了软件可信树体系结构框架；对软件可信树进行了剖析，总结出了软件可信度量评估的步骤。辅以专家评分的半定量化手段，本书对软件可信性量化研究进行了探索，运用软件工程方法，分析、设计、开发了一个评价软件可信性的原型系统。在对软件可信度量评估系统实现的基础上，进行了系统功能测试，对测试结果进行了纵向与横向的对比分析，得出了测试后的结论。

本书书稿由李红霞和陈均明共同完成，由李红霞完成第1、2、3、4、5、8、9、10、11章，陈均明完成第6、7章，李红霞负责本书的全面主持主导工作。

感谢西南交通大学出版社万方老师、黄庆斌等编辑们的辛勤劳动和选题开发中心副主任顾飞先生。感谢重庆大学傅鹂教授在百忙之中审阅我们的书稿并给我们的书写序，感谢重庆工商大学屈莲华副教授在我们修改书稿时提出的校正意见。在此，向所有关心和帮助过我们的家人、朋友、领导和同事表示由衷的谢意！

书中如有错漏和不足，敬请读者指正，谢谢！

李红霞

2010年8月

目　录

第 1 章　研究背景和意义

互联网作为计算机技术与通信技术融合的产物，经过 40 多年的发展，已经成为最大的人造信息系统。随着电子商务、电子政务和跨域的资源共享等新的应用模式不断涌现，人类对计算机系统的依赖性越来越强，其可信性就变得越来越重要。多个数据资料或文献表明[1~23]，计算机系统尤其是大规模计算机系统的可信性正面临严峻的挑战，如果不能妥善地解决计算机系统的可信性问题，信息社会的前景将不容乐观。

当前大部分信息安全系统主要是由防火墙、入侵监测和病毒防范等组成。这些安全手段是从互联网（Internet）中共享信息服务和电子商务的平等交易等的安全需求中假定而来的，其很重要的一个前提是用户不确定和没有一个明确的边界。因此这些常规的安全手段只能是以共享信息资源为中心对非法用户和越权访问进行封堵，以达到防止外部攻击的目的，而对共享源的访问者源端不加控制，加之操作系统的不安全导致应用系统的各种漏洞层出不穷，无法从根本上解决安全问题。

终端和服务器之间通过身份认证和授权共享资源，但是在事务交互过程中服务器无法判断对方是否是真正的可以信任：如请求是否是病毒和木马所发起、是否存在信息泄漏或者被对方恶意欺骗的可能等。因此服务器需要了解远程计算机的环境是否可信，然而当前网络体系结构都不能满足这种要求。如果待接入设备已经受到了攻击，再利用已经被攻破的接入设备作跳板，进而攻击受保护的网络，从而引起严重的安全问题，会对企业应用环境的安全造成极大的威胁。因此，从终端安全入手才能更好地解决整个信息系统的安全问题，也只有立足于终端，从源头上抓起，才能构筑起全面高效的安全防护系统。针对

于此，目前出现了几种安全接入技术，从终端就开始安全分析，尽可能地将不信任的访问操作控制在源端，以保护整个企业网络环境的安全。目前具有代表性的技术包括：思科的网络接入控制技术（Network Admission Control，NAC），微软的网络接入保护技术（Network Access Protection，NAP）以及 TCG 组织的可信网络连接技术（Trusted Network Connection，TNC）。这些技术的主要思路是从终端着手，基于安全管理员指定的组织安全策略，对接入保护网络的主机的相关安全属性进行检查，对于不符合安全策略的终端通常根据组织的不同要求采取不同的措施，拒绝其接入网络或对其隔离、补救。互联网环境下作为系统终端可信计算的重要组成部分的软件系统的可信性已经成为一个亟待解决的问题。

互联网软件的可信问题源于互联网环境的资源行为不可控性和不确定性，这与互联网资源本身的开放性、动态性与资源的成长性、自治性和多样性等自然特性有着密不可分的关系。同时，由于应用规模的不断扩大、所涉及资源的种类和范围的不断扩大、应用复杂度的提高以及计算模式的革新，都对互联网环境下的软件系统可信保障提出了更高的要求。

1.1 研究背景

在信息时代，人们对信息系统的依赖程度越来越高。信息系统，特别是运行在信息系统中的各类软件的安全性也受到了越来越多的关注。安全设计本身存在的不完备性可能构成新的信息安全风险，因此，新的风险点、新的漏洞和新的攻击技术手段会随时出现。自从有了广域网后，病毒、木马、黑客和计算机犯罪使得大家对网络的安全产生了恐惧，这严重制约了信息化的发展，制约了电子商务、电子政务的发展。病毒和黑客攻击的最终目的是非法进入用户的信息系统，篡改或盗用计算机上的数据。防火墙、杀毒软件等只能对这些攻击被动抵抗[24~44]。

自从20世纪90年代中期计算机开始向大众市场普及以来，安全问题便一直困扰着厂商与用户。在计算机普及的初期，主要依靠口令字、非标准存储格式等方法保护秘密信息，其安全原理是依靠信息的合法拥有者与系统外部人员之间掌握“钥匙信息”的不对称性来实现的。随着网络的兴起，实体之间交换敏感信息需要新技术来进一步确保安全，于是古老的密码技术得到了迅猛的发展，依靠密码算法与密钥相结合来确保信息的机密性、完整性、实体身份的唯一性和操作与过程的不可否认性，称这个阶段为密码保护技术阶段。过去，只有政府机构、商业银行、证券交易所、大型网站和一些技术密集型企业才会对信息安全提出要求，个人消费者还停留在“是否能拥有一台计算机”的阶段，自然不会未雨绸缪地思考安全问题。在这一阶段，提高信息安全的唯一办法是使用专门的硬件设备（防火墙等）来防护，并成立专门的信息部门对信息安全进行管理和完善，而仅此一项各单位每年的投资就相当惊人。随着网络互联互通，特别是因特网的普及，全球范围内基于信任前提的网络设备与协议的标准化，构建化使得信息交换极其容易，同时也造成密码保护成为不可加载或容易旁路的技术。在计算机普及之后，个人消费者也开始注重信息的安全性，但黑客入侵活动也变得猖獗，虽然当时的破坏仅限于摧毁、窃取用户的数据，损失有限，但用户开始受到了这个问题的困扰。当电子商务、网上银行逐渐流行的时候，安全问题就与个人消费者利害关系紧密相关，然而计算机防范黑客入侵的技术并没有本质提高。显然地，计算机将在未来生活中变得越来越重要，若不及时提高安全技术，那么这将会导致严重的问题，甚至反过来制约计算机功能应用的拓展。

在当今的信息技术的环境下，网络威胁包括来自内部与外部的威胁、主动攻击与被动攻击带来的威胁。网络威胁存在的隐蔽性、体制性、边界模糊性、突发性和易被忽视的特点要求我们引起高度重视。同时，伴随着人类对网络办公自动化依赖性的增强，依赖性必然产生脆弱性（技术的脆弱性、社会的脆弱性、人的脆弱性）。安全设计本身存在的不完备性可能构成新的信息安全风险。因此，新的风险点、新

的漏洞被发现，新的攻击技术手段被利用等管理安全问题会随时出现[1~23]。虽然来自网络的安全威胁日益增多，但很多威胁并不是以网络入侵的形式进行的，而是来自于内部合法用户的误操作或恶意操作。所以安全管理要求考虑网络系统的安全配置、正常运行、安全操作、应急响应和安全审计等一系列问题。

如果要打造真正安全可靠的计算机，就必须弥补上述所有可能的攻击漏洞。对应的方案分别如下：对内存中的数据加以保护，防止未经授权的非法窥探；创建可信任的输入/输出系统，防止敏感的密码信息在键盘输入或屏幕输出时被入侵者获取；创建封闭性的程序执行，确保程序指令能够按顺序执行而不会受到其他因素干扰。由于自身内部环境无懈可击，因此入侵者难以实行正常的漏洞攻击，系统的安全性也将提升到一个全新的高等级。

由老三样（防火墙、入侵监测和病毒防范）为主要构成的传统信息安全系统，是以防外为重点，它与目前信息安全主要威胁源自内部的实际状况不相符合。从组成信息系统的服务器、网络和终端三个层面上来看，现有的保护手段是逐层递减的。人们往往把过多的注意力放在对服务器和网络设备的保护上，从而忽略了对终端的保护。恶意攻击手段变化多端，而老三样则是采取封堵的办法。例如，在网络层（IP）设防，在外围对非法用户和越权访问进行封堵。这种封堵的办法是捕捉黑客攻击和病毒入侵的特征信息，但其特征是已发生过的滞后信息，不能科学预测未来的攻击和入侵。人们于是将底层的计算技术与密码技术紧密结合，从而推动信息安全技术研究目前进入信任计算技术阶段[24~44]。

1.2 研究意义

人们对计算机系统的依赖性越来越强，但病毒、木马等计算机黑客攻击手段层出不穷地危害和威胁着计算机系统的信息安全，因此计算机系统的可信计算变得越来越重要。

可信计算技术是有效解除计算机网络和终端威胁的方法之一。传统的信息安全措施不外乎“堵漏洞、做高墙、防外攻”老三样，但最终的结果是防不胜防，其主要原因是不去控制发生不安全问题的根源，而是在外围进行封堵。国家信息化专家咨询委员会专家沈昌祥院士认为：为了解决 PC 机结构上的不安全，应在世界范围内推行可信计算。

自 20 世纪 70 年代初期，Anderson 首次提出可信系统（trusted system）的概念以来，信息系统的可信性问题就一直受到学术界和工业界的广泛关注。

可信计算技术是近几年信息安全领域新的研究热点，它的研究旨在能有效地解决计算机结构上的不安全，并从根本上提高系统的安全性。可信计算改变了人们传统的信息安全思维方式，从终端开始防范攻击，提高了终端系统的安全性，使得信息系统中每个使用者都经过认证和授权，其操作都符合规定，就不会产生攻击性事故。“从终端入手才能解决整个信息系统的安全问题。”沈昌祥院士早在 20 世纪 90 年代初期就提出了这一思路。

可信计算技术的实质是要求信息系统中的交易和计算设备要：可信、可靠、安全及受保护。可信，以已知方案运行，并能够事先与该方案进行通信；可靠，总是可用于交易和通信，并可抵抗病毒和其他入侵；安全，能够停止多余的干扰或观察程序；受保护，为了实现计算机保密，只与在常用参数设定范围内的必要人员共享信息。

可信计算平台作为实现可信计算技术的核心，已成为信息系统的基础性和平台性设备。可信计算平台的可信根源来自于可信平台模块 TPM（Trusted Platform Module）。可信平台模块是一种硬件设备，与平台主板相连，用于验证身份和处理计算机或设备在可信计算环境中使用的变量。TPM 和存储在其中的数据与平台所有其他组件分离。可信平台模块（TPM）其本身就是一个小型的控制和管理系统，它作为平台运行时的信任源。系统所有的安全认证和安全调用都通过 TPM 来完成，并建立起一条网络—应用软件—操作系统—硬件—用户的完整的信任链关系。在信任传输的作用下，实现安全机制的整体性检查，

从而确保了各环节的可信性，进而保证了整个系统的可信性。

可信计算平台的主要功能是确保用户身份及权限的真实性、合法性；工作空间的完整性、可用性；确保存储、处理及传输的机密性、完整性；确保硬件环境配置、操作系统内核、服务及应用程序的完整性；确保密钥操作和存储的安全；确保系统具有免疫能力，从根本上防止病毒和黑客。它在构筑信息安全环境、保障源头安全方面起着十分重要的作用。在网络环境下的用户认证不仅可以包括用户的身份信息，而且可以包括 PC 的硬件信息，从而可以更好地保证网络通信安全和身份认证安全，并最终使防病毒、防入侵等最基本的信息安全功能与可信计算平台实现最佳的结合。

互联网作为计算机技术与通信技术融合的产物，经过近 40 年的发展，已经成为最大的人造信息系统。随着电子商务、电子政务和跨域的资源共享等新的应用模式不断涌现，人们逐渐认识到在互联网环境下的软件系统的可信性已经成为一个亟待解决的问题。互联网软件的可信问题源于互联网环境的资源行为不可控性和不确定性，这又与互联网资源本身的开放性、动态性与资源的成长性、自治性、多样性等自然特性有着密不可分的关系。同时，由于应用规模、所涉及资源的种类和范围的不断扩大和应用复杂度的提高以及计算模式的革新，都对互联网环境下的软件系统的可信保障提出了更高的要求。

对我国信息化建设来说，电子政务、电子商务系统、企业信息化系统、军队机要、通信、作战指挥系统等均迫切需要安全、可信的计算平台来构筑安全保障体系。首先，在电子政务系统的建设中，身份认证、授权管理和责任审定需要以可信计算平台为基础。其次，对涉密网和非涉密网进行安全隔离所用到的有关技术措施（如安全网关、安全网闸、安全的防火墙等）更需要以可信计算平台为基础。最后，军队的机要、通信和作战指挥系统的信息化建设是国防建设中的重要内容，其信息安全更是直接关系到国家的生死存亡，它们同样需要以可信计算平台为基础。

Internet 环境下，计算机系统是否可信，包括硬件、网络、操作系