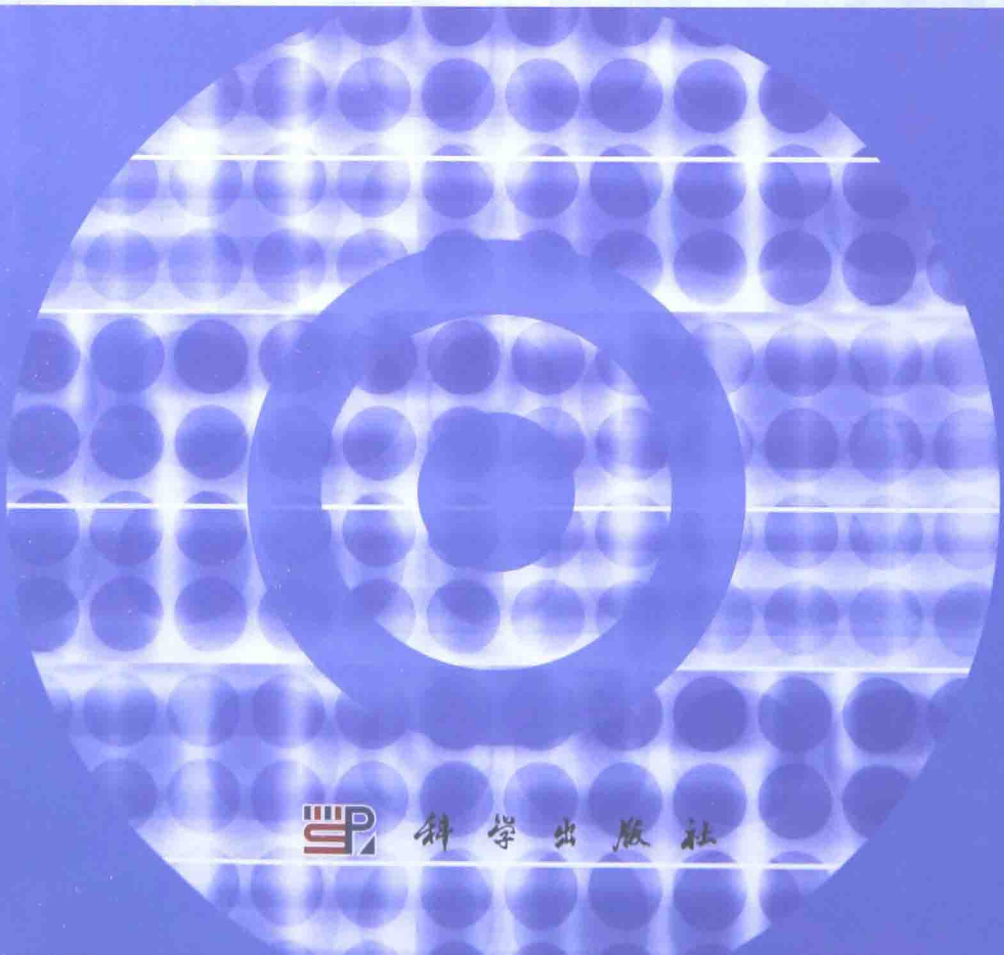
信息科学技术学术著作丛书

中国科学院科学出版基金资助出版

可信网络连接与可信云计算

慈林林　杨明华　田成平　盛　兵　著



科学出版社

信息科学技术学术著作丛书

可信网络连接与可信云计算

慈林林　杨明华　田成平　盛　兵　著

科学出版社

内 容 简 介

本书系统阐述当前可信计算领域的两大热点技术——可信网络连接和可信云计算，全书分为上下两篇。上篇全面系统地介绍可信计算技术背景、网络访问控制技术、可信网络连接技术以及可信连接架构。在此基础上结合实践应用，论述可信网络连接技术原理及实现途径。下篇主要对可信云安全的构建技术、云计算虚拟化技术、可信移动终端技术、基于可信基的数据安全防护技术、基于安全属性的行为度量以及基于控制流的软件动态度量技术进行了阐述，引入了最新研究成果并结合应用实例进行了深度技术剖析。

本书可作为高等院校工科专业研究生和高年级本科生的教材，也可供相关领域的科研和工程技术人员参考。

图书在版编目(CIP)数据

可信网络连接与可信云计算/慈松林等著. —北京：科学出版社，2015
(信息科学技术学术著作丛书)
ISBN 978-7-03-[illegible]-4

Ⅰ.可… Ⅱ.慈… Ⅲ.计算机网络-安全技术 Ⅳ.TP393.08

中国版本图书馆 CIP 数据核字(2014)第 304861 号

责任编辑：魏英杰 邢宝钦 / 责任校对：桂伟利
责任印制：赵 博 / 封面设计：陈 敬

科学出版社出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

新科印刷有限公司 印刷
科学出版社发行 各地新华书店经销

*

2015 年 1 月第 一 版 开本：720×1000 1/16
2015 年 1 月第一次印刷 印张：25
字数：508 000

定价：128.00 元

(如有印装质量问题，我社负责调换)

《信息科学技术学术著作丛书》序

21世纪是信息科学技术发生深刻变革的时代，一场以网络科学、高性能计算和仿真、智能科学、计算思维为特征的信息科学革命正在兴起。信息科学技术正在逐步融入各个应用领域并与生物、纳米、认知等交织在一起，悄然改变着我们的生活方式。信息科学技术已经成为人类社会进步过程中发展最快、交叉渗透性最强、应用面最广的关键技术。

如何进一步推动我国信息科学技术的研究与发展；如何将信息技术发展的新理论、新方法与研究成果转化为社会发展的新动力；如何抓住信息技术深刻发展变革的机遇，提升我国自主创新和可持续发展的能力？这些问题的解答都离不开我国科技工作者和工程技术人员的求索和艰辛付出。为这些科技工作者和工程技术人员提供一个良好的出版环境和平台，将这些科技成就迅速转化为智力成果，将对我国信息科学技术的发展起到重要的推动作用。

《信息科学技术学术著作丛书》是科学出版社在广泛征求专家意见的基础上，经过长期考察、反复论证之后组织出版的。这套丛书旨在传播网络科学和未来网络技术，微电子、光电子和量子信息技术、超级计算机、软件和信息存储技术，数据知识化和基于知识处理的未来信息服务业，低成本信息化和用信息技术提升传统产业，智能与认知科学、生物信息学、社会信息学等前沿交叉科学，信息科学基础理论，信息安全等几个未来信息科学技术重点发展领域的优秀科研成果。丛书力争起点高、内容新、导向性强，具有一定的原创性；体现出科学出版社“高层次、高质量、高水平”的特色和“严肃、严密、严格”的优良作风。

希望这套丛书的出版，能为我国信息科学技术的发展、创新和突破带来一些启迪和帮助。同时，欢迎广大读者提出好的建议，以促进和完善丛书的出版工作。

中国工程院院士
原中国科学院计算技术研究所所长
李国杰

前　言

随着信息技术的飞速发展，世界已全面进入信息化时代。然而，全球信息系统安全形势日益严峻。美国总统奥巴马上任后不久就明确表示：网络安全是美国面临的最严峻的国家安全挑战之一。目前有相当一部分人简单地认为只要研制出有自主知识产权的CPU、操作系统及数据库，我国信息系统的安全问题就能解决。事实上，这只能解决部分问题。目前信息系统存在的问题主要表现在：系统越来越庞大，各种控制越来越复杂，互通互联越来越广，洋葱头似的安全保护机制运行效能低下，管理成本越来越高，兼容性越来越差。信息系统在安全方面暴露的问题集中表现为病毒成千上万且层出不穷；被动式防御手段力不从心；安全防护模型越来越“脆弱”；漏洞越堵越多、防火墙越砌越高；安全策略越来越复杂。头疼医头、脚疼医脚的办法已不能从根本上解决信息系统的安全问题。其根源是系统的不完备性和软件生产方式的先天缺陷。此外，在设计计算机体系结构时，硬件自身防护能力存在不足。现有的大量软硬件在线使用且无法替换，陷入不能不用也不得不用的窘境。面对这种现状，只有采用主动与被动相结合的解决办法。借鉴人类防病、治病的思路，关键在于提高自身免疫力。因此，必须为信息系统构建安全基因。

信息系统安全主要包括设备安全、数据安全、内容安全和行为安全等。硬件安全和操作系统安全是信息系统安全的基础；加密是数据安全和内容安全的保障；网络安全是信息系统安全的关键。信息系统安全必然要从被动防御向主动防卫转变，从关注脆弱性安全向关注结构性安全转变，从关注外部威胁向关注提高自身能力转变。早期的查漏洞、打补丁、防火墙等方法，都是被动防御的产物。虽然信息系统的纵深防御已采取了多层措施，但仍不能从根本上解决问题。可信计算技术是在主动防卫的思路下发展起来的，按照生物基因与现代精细化管理思路，为计算机建立可信任根。从信任根芯片、主板、BIOS和操作系统做起，建立信任链，一级保证一级，逐级安全加固，提高系统安全性。可信计算从信任根入手，通过完整性度量和标签机制建立基础信任体系。正是这一思想推动了可信计算技术的发展。当前可信计算技术已成为信息安全领域的关键技术。国内有专家形象地将基于信任根的标签机制和可信性增长称为“安全基因”。

可信计算概念可以追溯到1983年美国国防部的TCSEC准则。1999年，IBM、Intel和Microsoft等企业成立了TCPA(2003年改为TCG)，主要致力于制定可信计算的工业标准及规范。可信计算组织认为，可信计算现阶段的主要目标是确保系统数据的完整性，提供数据的安全存储、平台身份和可信性的远程证明。

可信计算技术与产品主要用于安全风险管理(发生安全事件造成的损失降至最小)、安全检测与应急响应(及时发现攻击并采取相应措施)等。

可信计算组织用行为定义可信:如果一个实体的行为总是以预期的方式达到预期目标,那么它是可信的。这个定义特别强调了行为的可预期性。ISO/IEC 15408 标准定义可信为:参与计算的组件,其操作或过程在任意的条件下是可预测的,并能够抵御病毒和物理干扰。IEEE CS 可信计算技术委员会认为,所谓可信是指计算机系统所提供的服务可以证明其是可信赖的,即不仅计算机系统提供的服务是可信赖的,而且这种可信赖是可证明的。我国学者认为,可信计算系统是能够提供系统的可靠性、可用性、信息和行为安全性的计算机系统。系统的可靠性和安全性是现阶段可信计算最主要的两个属性。可信计算是一套全新的信息安全技术,主要包括信任根技术、可信软件栈、可信存储、可信服务、可信行为度量、可信软件证明、可信网络连接、TPM 虚拟化和可信云计算等。利用信任链模型构建可信系统是可信计算的核心思想。可信计算组织在信任链中采用度量完整性来确保 BIOS、OSLoader 和 OS 的数据完整性。但是,这种完整性只能说明软件未被修改,并不能说明这些软件没有安全缺陷,更不能确保这些软件运行时的安全性。基于数据完整性的度量是一种静态度量方法,对于操作系统动态加载的模块则难以度量。因此,还需要基于软件行为进行动态度量,不仅包括启动时度量,还包括运行时度量。

目前可信计算组织在信任链中采用度量数据完整性的方法,虽然存在不足之处,但是它足以确保系统资源的数据完整性和抵御大量计算机病毒等恶意软件的攻击,在很大程度上提高了计算机的安全性。完整性度量在系统结构方面的完整性证明更为重要。在网络环境下的可信安全信息系统应满足以下目标:一是计算平台能够向交互者提供可验证的平台完整性信息;二是支持数据的安全保护;三是提供用户程序的安全隔离;四是支持用户和应用程序之间的安全交互;五是具有兼容性。目前的研究主要是结合可信计算和虚拟化技术,使用可信的虚拟机监控器(包括系统管理程序、信任管理、隔离服务管理、存储管理、安全 GUI、虚拟 TPM 管理和强制访问控制等)为受保护的应用程序提供隔离的运行环境。随着云计算的出现,TPM 的虚拟化、信任机制性能扩展和可信计算基的代码最小化与可信证明等问题的研究也越来越重要。基于云计算的可信技术研究已成为当前可信计算研究领域的一个热点。

可信计算虽然已提出多年,但仍面临诸多技术挑战,如可信计算基的膨胀问题等。随着信任根对下一级软件模块的度量和加载,可信计算基也逐渐增大。系统越大信任链越长,可信计算基也越大,可信度就会越低,这是因为可信计算基的膨胀会导致平台的度量变得非常复杂、难以测量。此外,还存在操作系统安全问题、内存隔离问题和运行时度量问题等。目前,可信计算中的软件可信性度量是按数

据完整性度量来进行的，并不是真正软件的动态可信性度量。因此，它只能确保软件的静态可信，而不能确保软件的动态可信。于是，如何进行软件的动态可信性度量，就成为确保软件安全的关键。软件动态可信性是指软件运行时所表现的行为可信性，既包括可靠性，又包括安全性。在可信软件开发方法学上还需开展可信软件开发过程控制、软件行为描述语言和语义模型、可信软件验证方法、基于构件/服务的可信软件系统管理等方面的研究。

在可信网络连接方面，可信计算组织制定的可信网络连接(TNC)规范采用了一整套标准接口和协议，将传统的网络安全技术(防火墙、入侵检测等)与可信计算技术相结合，把可信硬件 TPM 集成到可信网络连接结构中，此外，还包括虚拟化技术、基于标签的交换技术以及基于标签的云计算访问控制技术等。

本书从可信网络技术入手，全面介绍国际可信计算组织和中国国家信息标准有关可信网络连接方面的相关知识，内容包括理论基础、技术规范、技术原理、技术实现、编程示例和实践应用。在此基础上，针对目前云计算技术的大规模推广应用背景及云计算在可信性和安全性问题所面临的严峻挑战，重点对可信云安全构建技术、云计算虚拟化技术、可信移动云终端技术、基于安全属性的行为度量技术与基于控制流和可信计算基的软件动态度量技术进行阐述，引入最新研究成果并结合应用实例进行技术剖析。全书共 9 章，分上下两篇。上篇为可信网络连接技术；下篇为可信云计算技术。除了第 1 章介绍可信计算技术的基础知识，第 4 章介绍可信计算规范之可信网络连接架构标准外，其余各章均为近年来研究成果的总结。其中，第 2 章为网络访问控制技术；第 3 章为可信网络连接技术；第 5 章为可信网络连接原型与实现；第 6 章为云安全概述；第 7 章为云计算虚拟化技术；第 8 章为可信移动终端技术；第 9 章为可信云计算技术。第 3 章、第 5 章、第 7 章和第 9 章是本书的重点。本书旨在总结作者所在团队多年来在该领域理论与技术方面的研究成果，同时也积极吸纳国内外在该领域的突出成果，特别是我国学者的研究成果。希望能抛砖引玉，达到百花齐放、百家争鸣的效果。为从事该领域研究的科研技术人员，高等学校的教师、研究生和本科生提供更多借鉴和参考。希望本书能为我国在信息安全研究方面取得新的更大成绩做出一点积极的贡献。

在开展可信计算技术研究的过程中，我们得到了信息安全专家沈昌祥院士的精心指导，也包括他对本书的悉心指教。此外，我们还得到了武汉瑞达信息安全公司、浪潮集团超越公司、迈普网络公司、中船重工 716 研究所等单位的大力协助与联合攻关，还有研究院科研团队多位同仁与研究生的大力参与，主要包括葛根焰、杨银刚、黄亮、程宾、柳伟、闫永航、杨斌、王云会等。他们为本书的完成做了大量的辛勤工作，在此表示感谢。此外，本书的出版还得到了中国科学院科学出版基金(2014 第 041 号)，国家 863 计划(编号：2013AA7072017B)，以及国家核高基重大

专项(编号:2014ZX01040501-002)的支持,在此一并表示感谢。

由于作者学术水平有限,书中难免会有不妥之处,恳请读者批评指正,在此致以衷心的感谢。

2014 年 7 月于北京

目　录

下篇　可信云计算技术

上　篇

可信网络连接技术

第 1 章　可信计算概述

2001 年，发生在美国纽约的“9・11”事件震惊了全世界。2002 年美国专家爱德・约敦写了一本名为《字节战争》的书，引起了巨大轰动。这主要是因为他对“9・11”事件的深度剖析引发了许多思考。他鲜明地指出 IT 领域将成为未来的重要战场，阐明如何应对 IT 领域“9・11”型的难预料性、突发性、灾难性事件。他还进一步指出：如果说第一次世界大战是化学家发明引起的战争，第二次世界大战是物理学家发明引起的战争，那么未来的世界大战如果发生，就将是 IT 专家发明引起的战争。

面对“后 9・11”时代，爱德・约敦突出强调我们正进入信息时代，正处在一个高技术、快变化、难预测、恶性事件频发的世界。在这个世界里，IT 领域面临的威胁比以往更加严重。系统安全、风险管控、应急体制、恢复机制、系统鲁棒性和灾难抢救都应适应这种严峻形势。在新时期，IT 系统已然成为国家关键基础设施的重要组成和人们生活必不可缺的部分。网络空间已成为涉及国家安全的新领域。IT 系统安全、基础信息设施安全、信息安全，以及个人隐私安全等都显得特别突出、重要。因此，应高度重视 IT 系统安全问题，寻求解决之道。

面对“后 9・11”时代的种种威胁，人们期盼构建可信的信息系统、可信的网络、可信的环境，获得可信的服务。可信计算技术由此得到了快速的发展。

1.1　信息安全威胁

随着信息技术的发展，现代社会的方方面面都越来越依赖计算机。特别是近十年来，在互联网技术的推动下，计算机越来越多地被应用到社会、经济、政治、教育、文化和军事等各个领域，计算平台的安全性变得越来越重要。然而，自从计算机问世以来，安全问题就一直伴随着计算机的发展而存在。特别是，计算机软件的人工编程模式和互联网的自由发展方式都使漏洞、病毒及攻击无法避免。近年来，随着软件工具的发展，软件漏洞、病毒的数目急剧增加。移动互联网的快速发展，也使得针对软件的攻击范围不断扩大，造成的安全危害日趋严重[1]。

软件安全漏洞产生的根源在于，软件系统的超级复杂性和程序正确性证明的无法实现。Linux 内核 2.6.27 版本的代码库的代码量就已经超过 1000 万行。据统计，一个主流 UNIX/Linux 或 Windows 系统均有上亿行代码。研究表明，典型的产品级软件每千行代码就有一个与安全相关的漏洞。由此推算，一个主流应用

软件就可能隐藏了 10 万个以上的安全漏洞。常见的软件漏洞威胁主要有缓冲区溢出、恶意文件执行、SQL 注入、不安全对象引用、跨站脚本攻击(XSS)、不安全的身份鉴别、多级存储和加解密过渡等。这些漏洞的数目并没有因软件补丁增加而减少,相反呈急剧上升之势。图 1-1 是国家互联网应急中心(CNCERT)给出的 2002～2008 年软件漏洞增长情况。根据中国国家信息安全漏洞库(CNNVD)统计,截至 2014 年 7 月底,CNNVD 漏洞总量已达 68165 个。目前,中国已是网络攻击的主要受害国。仅 2013 年 11 月,境外木马或僵尸程序控制服务器 IP 数目为 3618,控制了境内近 90 万个主机 IP。

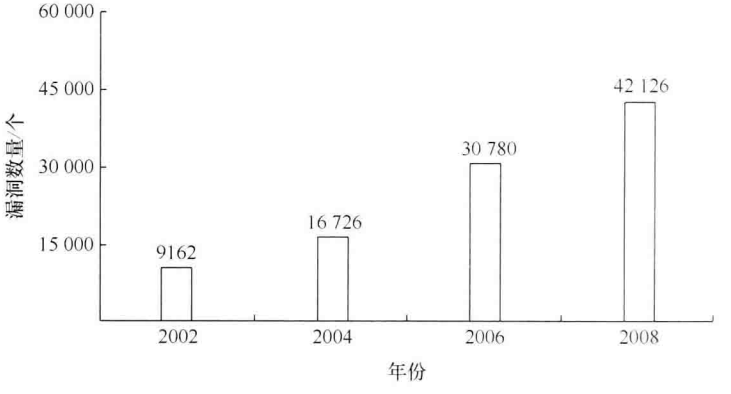


图 1-1 CNCERT 报告的软件漏洞统计数据

软件漏洞的泛滥为黑客提供了可乘之机。由于需要进行频繁的补丁更新和版本更新,人们采取事后修正的策略,并没做到预先防御,所以实际上绝大多数系统都存在或多或少的漏洞。与服务器相比,客户端系统更容易受到攻击。据初步统计,当前世界每 20 秒就有一起黑客侵入事件发生,仅美国每年造成的经济损失就超过 100 亿美元。

2014 年 5 月 15 日,中国互联网络信息中心(CNNIC)发布报告称,2013 年互联网国家级有组织的网络攻击频发,如"棱镜门"事件中披露的美国国家安全局进行的网络监控项目等。此次 CNCERT 公布的大量数据显示,中国境内遭受网络攻击的情况也十分严重,CNCERT 详细列举了国内机构、企业遭受境外攻击的具体案例。数据显示,仅 2013 年的前两个月,就有境外 5324 台主机通过植入后门对中国境内 11 421 个网站实施远程控制。其中,位于美国的 1959 台主机控制着中国境内的 3579 个网站,位于日本的 132 台主机控制着境内的 473 个网站。按照所控制的境内网站数量统计,美国位居第一。此外,针对中国网上银行、支付平台、网上商城等的钓鱼网站有 96%位于境外,其中位于美国的 619 台服务器承载了 3673 个针对境内网站的钓鱼页面,美国服务器承载钓鱼页面数量占全部钓鱼页面数量的 73.1%。