文章编号:1001 - 9081(2009)04 - 0915 - 05

可信计算发展综述

熊光泽,常政威,桑 楠
(电子科技大学 计算机科学与工程学院,成都 610054)
(gzxiong@uestc.edu.cn)

摘 要:可信计算是当前计算机科学的一个研究热点,对可信计算的发展进行了综述。阐述了可信性的起源与内涵,总结了可信计算领域的国内外研究进展。针对安全关键系统,着重介绍了各种高可信保障技术。最后,探讨了可信计算的发展趋势。

关键词:可信性;可信计算;安全关键系统;多级高可信保障
中图分类号:TP309 **文献标志码**:A

Survey on dependable computing

XIONG Guang-ze, CHANG Zheng-wei, SANG Nan
(*School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu Sichuan* 610054, *China*)

Abstract: This paper surveyed the development of dependable computing. The basic concepts of dependability were explained, and current research works of dependable computing were introduced. High dependability safeguard techniques for safety-critical systems were proposed. Some future research directions of dependable computing were presented.

Key words: dependability; dependable computing; safety-critical system; multi-level high dependability safeguard

0 引言

计算机从诞生以来,在发展的过程中其体积不断缩小,计算能力则不断提高。近年来,伴随着网络和移动通信技术的快速发展,计算系统已经渗透到人类的生活、生产等各个社会领域,呈现出无处不在的特点,逐渐走向普适计算的模式。

随着计算机广泛应用于诸如航空航天、核反应堆、国防建设以及与国民经济相关的重要领域,人类的生活乃至生存空间对计算机技术及其相关产品的依赖程度越来越高,这些计算机系统中的任何隐患都会对人们带来严重的甚至是灾难性的后果。近年来,这样的事例层出不穷,例如:

1992 年,法国伦敦由于救护派遣系统全部崩溃,导致多名病人因为抢救不及时而失去生命。

1996 年,欧洲航天局首次发射阿丽亚娜 5 号火箭失败,其直接原因是火箭控制系统的软件故障,导致直接经济损失 5 亿美元,使耗资 80 亿美元的开发计划延迟了三年。

2003 年,在美国电力检测与控制管理系统中,由于分布式计算机系统试图同时访问同一资源引起软件失效,造成美国东北部大面积停电,损失超过 60 亿美元。

人类社会对各种计算系统的可依赖程度越来越高,用户对于计算服务的"可信性"也越来越关注,可信计算已成为当前的一个热点研究领域。本文通过综述可信计算的起源、发展与研究现状,分析了相关的实现技术与存在的问题,从而提出此领域亟待研究的理论与技术问题。

1 可信性的起源与内涵

1.1 可信性的起源

可信计算(Dependable Computing)最早出现于 20 世纪 30 年代 Babbage 的论文"计算机器"中[1]。在 20 世纪中期出现的第一代电子计算机是由非常不可靠的部件构建的,为确保系统的可靠性,大量切实可行的可靠性保障技术诸如错误控制码、复式比较、三逻辑表决、失效组件的诊断与定位等被用于工程实践中。J. von Neumann 和 C. E. Shannon 与他们的后继者则逐渐提出并发展了基于不可靠部件构建可靠系统逻辑结构的冗余理论[2]。1965 年,Pierce 将屏蔽冗余理论统一为失效容忍(Failure Tolerance)。1967 年,Avizienis 与 Schneider 等人则把屏蔽冗余理论连同错误检测、故障诊断、错误恢复等技术融入到容错系统的概念框架中[3]。

与此同时,国际上也成立了一些可信性研究机构专门研究高可信保障技术,如 IEEE-CS TC 于 1970 年成立了"容错计算"研究小组,IFIP WG10.4 于 1980 年成立了"可信计算与容错"研究小组,它们的成立加速了可信性相关概念走向一致。Laprie 于 1985 年正式提出可信性(Dependability)以便与可靠性(Reliability)相区别。同时期,RAND 公司、纽卡斯尔大学、加利福尼亚大学洛杉矶分校等探索性地研究了如何综合错误容忍和信息安全防卫于系统设计中。

1992 年,Laprie 把恶意代码和入侵等有意缺陷与偶然缺陷并列,丰富了可信性的内涵,并在他的著作《Dependability: Basic Concepts and Terminology》中对可信性进行了系统地阐述。

1.2 可信性的内涵

可信计算从出现到现在,已经有三十多年的历史了,在它不同的发展阶段中,研究的内容和重点在不断地演变。直到目前为止,可信性这一概念,还没有达成一个被广泛接受、良好形式化的定义,可称为"Dependability"、"Trustworthiness"、"High Confidence"[4]。相应地,可信计算也有"Dependable

收稿日期:2008 - 10 - 06;**修回日期**:2008 - 11 - 30。 **基金项目**:国家 863 计划项目(2006AA01Z173)。

作者简介:熊光泽(1938 -),男,四川丹棱人,教授,博士生导师,CCF 高级会员,主要研究方向:高可信计算、嵌入式实时计算、普适计算;常政威(1981 -),男,河南安阳人,博士研究生,主要研究方向:可信计算、嵌入式实时系统;桑楠(1964 -),男,四川营山人,教授,博士研究生,主要研究方向:可信计算、嵌入式实时系统、软件工程。

"Computing"[5-6]，"Trusted Computing"[7]和"Trustworthy Computing"[8]等多种叫法，不同的学者从不同的角度和层次对可信性的相关概念和可信计算的发展进行了阐述。

文献[6]从可信硬件、软件、系统和网络等方面介绍了可信计算的概念与发展。文献[5]从差错源的变化、复杂性的迅速增加和计算设备总量的增加这三个方面分析了可信计算的产业趋势。文献[7]全面总结了可信计算的不同发展阶段，对当前网络环境下可信计算的研究内容进行了分析和点评。文献[9]从密码学、可信计算、网络安全和信息隐藏等方面综述了信息安全技术的研究进展，将可信计算看作解决安全问题的一个新方案。文献[4, 8, 10]分别介绍了高可信软件工程，可信网络和可信中间件的发展。

文献[11]对"Dependability"、"Trustworthiness"和"High Confidence"等几个概念从目标和面临威胁两方面进行了比较，认为它们是互相等价的。

本文中，可信性采用"Dependability"的表述。简言之，"可信性"指系统在规定时间与环境内交付可信赖的服务的能力。可信性是一个复杂的综合概念，其中包含了特征属性、降低或损害因素以及提高方式，如图1所示。

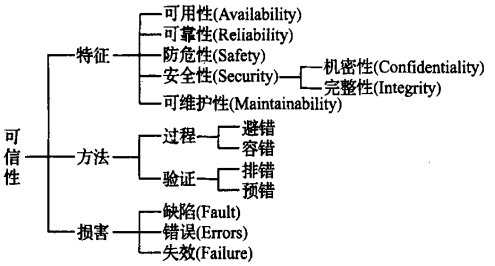

图1 可信性的特征、实现方法及损害

1.2.1 特征

广义地讲，可信性所包含的特征属性有：可用性(Availability)、可靠性(Reliability)、防危性(Safety)、安全性(Security)、可维护性(Maintainability)，其中安全性又可进一步细分为机密性(Confidentiality)与完整性(Integrity)。

可用性表示系统在给定时间内可运行的概率，它通常用来度量可延迟或短暂停止提供服务而不会导致系统发生严重后果的品质。

可靠性则是指系统在给定的环境及时间区间内连续提供期望服务的能力。

防危性是指系统在给定的时间内不发生灾难性事故的概率，用来度量可继续提供正常功能或以不破坏其他系统及危害人员生命安全的方式中断服务的能力。

安全性是指系统防止敏感信息与数据被未授权用户非法读写的能力，包括防止授权用户抵赖其已进行过的访问。安全性可进一步细分为机密性与完整性，其中机密性是指系统保护敏感信息与防止数据非法泄露的能力，而完整性则是指系统保持敏感数据一致性的能力。

可维护性是指系统易于修理和可进化的能力。

1.2.2 损害

服务是指系统根据用户的输入或其他外部条件而进行的一系列操作。正确的服务是指正确实现系统功能的服务。失效(Failure)指系统实际所交付的服务不能完成规定的功能或不能达到规定的性能要求，即正确服务向不正确服务的转化。系统失效则是指系统的实现未能与系统需求规范保持一致，或系统规范未能完全描述系统本身应具有的功能。失效的根源是由于系统(或子系统)内部出现了错误的状态，错误到达服务界面并改变服务时便产生失效。缺陷是导致错误发生的根源，它一般处于静止状态，当缺陷产生错误时，称缺陷被激活。

错误(Error)是指在一定的运行条件下，导致系统运行中出现可感知的不正常、不正确或未按规范执行的系统状态。错误最终能否导致系统失效由系统组成、系统行为和应用领域决定。应用于不同领域的系统，错误产生的后果也不尽相同，例如，秒级的服务器响应延迟在实时系统中被认为是性能失效，而通用系统中则是可接受的。因此，系统状态在不同的用户看来，并非都是错误。

缺陷(Fault)是指因人为的差错或其他客观原因，使所设计的系统中隐含有不正确的系统需求定义、设计及实现。这些缺陷将有可能导致系统在运行中出现不希望的行为或结果。缺陷是造成错误出现的原因，其来源十分广泛。

缺陷是产生错误的根源，但并非所有缺陷都能产生错误。通常，缺陷处于静止状态，当缺陷由于系统或子系统在特定环境下运行而被激活时，将导致系统或子系统进入错误的状态，当一个或多个错误进一步在系统或子系统中传播并到达服务界面时，将导致系统或子系统失效。一部分系统失效是非常危险的，如果这类失效在系统范围内得不到很好的控制，将最终导致灾难性事故发生。图2为缺陷、错误及失效之间的关系。

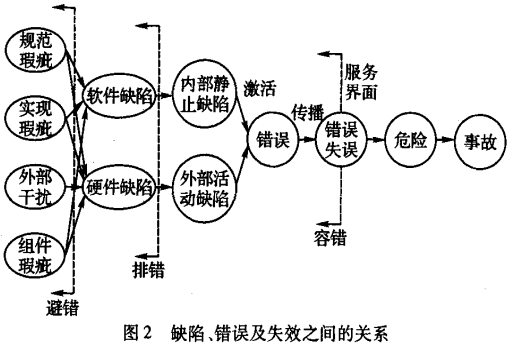

图2 缺陷、错误及失效之间的关系

1.2.3 可信性保障技术

高可信保障技术可分为避错、容错、排错和预错四种。

1)避错。其目的是尽量避免将缺陷引入系统，主要应用于系统的设计和维护阶段。在系统的设计阶段，从需求分析、系统定义、系统设计到代码编制，每个步骤都必须最大限度地保证其合理性和正确性，以避免缺陷的引入。

2)容错。容错是一种通用的可信性保障机制，其目的是使系统在运行中出现错误时能够继续提供标准或降级服务。容错技术能够处理多种类型的缺陷和错误，如硬件设计缺陷和软件设计缺陷。通常，容错被分为硬件容错、软件容错和系统容错。常用的容错方法都包含错误检测、错误处理、错误恢复三个过程，其中错误检测是设计容错系统的关键。当系统中出现错误状态时，不同的应用需采用不同的错误处理手段，如核电系统出现致命错误时应紧急停堆，而对于飞行中的飞机当检测到有致命错误发生时，显然不能简单关闭发动机，而应采取其他错误处理手段来保证飞机的安全。

3)排错。其目的是发现错误后及时排除，这一技术通常应用于系统的测试和维护阶段。通过模拟真实工作环境进行系统测试，发现错误并分析产生错误的原因，然后改进系统以

消除、减少错误的产生。在高可信的软件开发工程中,测试开销要占80%以上,这充分体现了测试的重要地位。

4)预错。其目的是预测系统内与错误相关的各个方面,以保证满足规定的标准。在系统的运行过程中,系统可以通过分析当前所获得的系统状态信息,预测可能发生的错误,并采取措施加以避免。这一技术必须依靠正确的系统状态分析,也是该类技术实施时最难以解决的问题。

图3则表示了以上四种可信性保障技术在系统开发过程中不同阶段的应用情况。在具体的工程实际中,设计人员首先根据系统的应用领域、功能和性能需求、成本限制和资源限制等诸多因素,确定系统的失效语义。然后,根据失效语义,与多种合适的可信性保障手段相结合,处理在系统生命周期的不同阶段出现的缺陷和错误,从而保障系统的可信性。

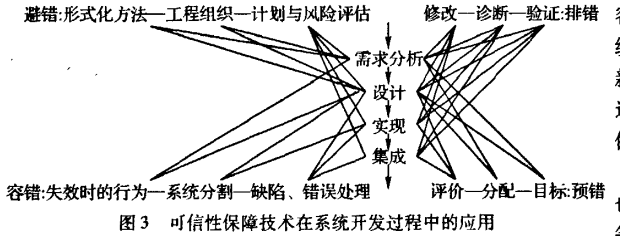

图3　可信性保障技术在系统开发过程中的应用

2　可信计算研究进展

从上个世纪末以来,可信计算经历了从出现到发展壮大的过程,世界范围内许多大学、研究机构和相关企业都有研究小组和实验室从事这方面的研究。

我国也加强了可信计算基础理论和自主关键技术的研发,尤其是在安全和可靠性方面,发展比较迅速,并取得了一系列的成果。

2.1　国外研究进展

1999年IEEE太平洋沿岸国家容错系统会议改名为可信计算会议。2000年IEEE国际容错计算会议(FTCS)与国际信息处理联合会IFIP的10.4工作组主持的关键应用可信计算工作会议合并,更名为IEEE/IFIP可信系统与网络国际会议(International Conference on Dependable Systems and Networks, DSN),如今已成为可信计算领域每年一度的顶级会议。2000年12月11日美国卡内基梅隆大学与美国国家宇航总署(NASA)的Ames研究中心联合成立了高可信计算联盟(High Dependability Computing Consortium),包括Adobe、惠普、IBM、微软和SUN在内的12家公司,麻省理工学院、乔治亚理工学院和华盛顿大学等高校都加入了其中。2004年,IEEE可信与安全计算汇刊(IEEE Transactions on Dependable and Secure Computing)创刊,标志着可信计算开始成为一个独立的学科,对它的基础研究、实验研究和工程研究已在全世界全面展开。

1983年美国国防部制定了世界上第一个计算机可信性评价标准,即《可信计算机系统评价准则》(Trusted Computer System Evaluation Criteria, TCSEC)[12],1985年又对它进行了修订。IBM、HP、Intel、微软等知名IT企业于1999年成立可信计算平台联盟(Trusted Computing Platform Alliance, TCPA)以来,可信计算从学术界一步步走向产业界。2003年TCPA改组为可信计算组织TCG,全球IT行业内几乎所有的著名公司都加入了TCG这一组织。在欧洲,2006年1月启动了名为"开放式可信计算"(Open Trusted Computing)的研究计划,已有23个科研机构和工业组织参与。

2.2　国内研究进展

可信计算是国家的中长期发展规划中优先发展的研究领域,在"十一五"期间,我国在可信计算的一些关键技术尤其是软件领域启动了一批重大科研项目。国家高技术研究发展计划(863计划)于2007年启动了重点项目"高可信软件生产工具及集成环境",主要目标是在高可信软件生产的关键技术方面取得突破。国家自然科学基金委员会于2007年底启动了"十一五"重大研究计划"可信软件基础研究",由著名计算机软件专家何积丰院士任首席科学家,实施周期6年,计划经费1.5亿元,如此大规模资助软件基础研究在我国还是首次[13]。

为了反映国内在相关领域的工作进展和最新研究成果,《计算机学报》于2007年10月份出版了"可信计算专辑",从容错和安全两个方面,报道了国内在集成电路、软件、系统和网络可信性,以及信息安全理论与工程等方面的最新进展[14]。《Journal of Computer Science and Technology》近期也将出版一期专刊,重点关注高可信软件系统的软件工程研究进展。

同时,从2004年开始,与可信计算相关的学术会议也在不断召开。由中国计算机学会容错计算专业委员会等主办,2008年在重庆召开了第三届全国可信计算学术会议,在郑州召开了第三届中国可信计算与信息安全学术会议。

从20世纪90年代以来,随着计算机网络的快速发展,针对日益严峻的计算机病毒、非法入侵等安全隐患,越来越多的机构和人员加入到了信息安全的研究队伍中,在密码算法、信息隐藏与检测算法、安全协议、安全评估、系统安全、网络安全和信息安全应用系统等方面取得了很大的进展[9,15]。

对可靠和容错计算[16]方面的研究,主要集中在集成电路测试[17]和软件测试[18],软、硬件验证[4],软件容错[19]、硬件容错[20]、系统结构容错[21]和网络容错[22]等方面。

目前,在可信计算领域,国内的研究机构主要有中科院计算所、国防科技大学、北京大学、华东师范大学、电子科技大学、武汉大学、哈尔滨工业大学、哈尔滨工程大学、西北工业大学等。国内的联想、同方、方正、浪潮等公司也加入了可信计算的研发队伍中,并已开始推出自己的可信芯片和计算机。

3　安全关键系统的高可信保障技术

安全关键系统(Safety Critical Systems)是指系统功能一旦失效将引起生命、财产的重大损失以及环境可能遭到严重破坏的系统,这类系统广泛存在于航空航天、国防、交通运输、核电能源和医疗卫生等诸多安全关键领域中,对高可信的需求是不言而喻的。

对于安全关键应用而言,系统高可信的重心是防危(Safety),但同时也需要可靠性与安全性等保障。

一个系统可靠并不意味着防危,如即将爆炸的核电系统继续发电满足其可靠性需求,但却与防危性目标相违背;一个系统防危也不一定可靠,如核电系统无论在什么情况下总是采取停堆措施,显然该系统具有极高的防危性,但却失去了系统应有的可靠性(一般故障下应继续发电)。除此之外,防危性也需要可靠性的支持,例如用于核电紧急停堆的防危系统一旦启动后,将希望该防危系统是可靠的,直到核反应堆完全关闭。

同时,安全关键系统中的安全关键组件必须具有较高的

机密性和完整性,保证软件及其使用的数据不会被非授权代理篡改。否则,正在执行的组件将不满足其规定的安全需求,甚至导致灾难性事故的发生。

电子科技大学从"八五"期间开始,以高可信嵌入式实时操作系统为突破口,面向航空、核电、交通等任务关键领域,从可靠性、防危性、安全性等可信性属性出发,在操作系统内核、中间件、构件、应用软件以及现场网络等多个层面开展研究,构建了一个面向安全关键系统的多级高可信保障体系,如图4所示。经过近二十年的研究和沉淀,在高可信嵌入式操作系统、高可信软件的测试与评价等关键技术领域取得了突破。

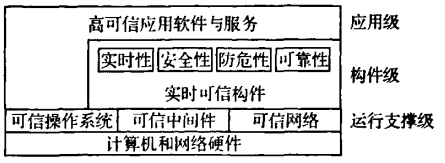

图4 安全关键系统的多级高可信保障体系

3.1 多级高可信保障体系

面向安全关键应用的高可信保障体系构筑于硬件层之上,从运行支撑级、构件级和应用级多个层面上提供多级保障。

3.1.1 运行支撑级

运行支撑级在处理器、存储器、传感器和网络设备等硬件平台上,对传统的操作系统、中间件和网络协议等进行改造,增强其可信性,从而为上层的高可信应用的运行提供支撑。

操作系统是任务关键应用的基础软件平台,它负责管理硬件资源,使应用软件可以方便地使用系统提供的各种可信服务。嵌入式实时操作系统通常包括硬件抽象子层、操作系统内核、文件系统、通信协议和服务接口等组成部分,其中内核是实现可信操作系统的关键,将在3.2节详细介绍。

对分布式安全关键系统而言,中间件需要向应用系统提供可信性支持。文献[23]对安全中间件的关键技术包括体系结构、协议、算法等开展了深入的研究,研究成果已应用于多项科技项目和市场产品中。文献[24]提出了一种实时自适应资源管理中间件,将QoS机制引入到分布式嵌入式系统的可信性确保中,在此基础上构建高效、可移植的应用系统。

在现场总线网络的可靠性保障方面,文献[25]把可用性与可靠性有机结合起来,对系统的可靠性进行综合评价。文献[26]提出了一种基于以太网技术的实时容错现场网络体系结构ARTCA。文献[27]提出了一种高可靠实时通信协议E&TTE,满足了安全关键实时网络的多种传输需求。

3.1.2 构件级

当前的软件构件技术大多关注和强调构件系统功能上的描述,对于系统功能之外的非功能因素,即性能特性却缺乏相应的表达、刻画和保障,无法满足不同应用领域用户的可信性需求。

为此,将系统可信性确保策略与机制独立于功能构件,通过选择、定制及动态绑定策略与机制为应用系统提供性能保障,将可信性(可靠性、防危性、安全性)确保构件设计成一种基于实时中间件的服务,为应用程序各功能构件提供灵活的性能确保服务[24]。

3.1.3 应用级

在运行支撑级提供高可信服务,构件级提供性能(可信性)和功能分离的基础上,可以根据应用系统的定制需求,通过构件的组装高效率、高质量地构造高可信应用软件。在安全关键应用中,根据内部和外部环境的变化,如何自适应地确保软件系统的可信性,仍然需要进一步的研究[24]。

对于高可信应用软件而言,软件的测试与评价是一个难题,本文将在3.3节详细介绍。

3.2 高可信嵌入式操作系统

电子科技大学从实时内核可靠性、防危安全和信息安全的角度,系统地分析和研究了其可信性保障技术,设计并实现了自主研发的嵌入式实时操作系统CRTOSII的内核。

调度算法是实现嵌入式实时操作系统内核的关键。文献[21]改进了传统实时调度算法,使之具有容错特性。文献[28]设计了可支持关键任务优先运行的防危调度算法。

防危核是一种针对软件故障的防危保障机制,文献[29]基于反射技术实现了防危核的原型。文献[28]基于两级调度模型及硬通货内存分配机制,实现了时间与空间隔离的防危保护机制。

安全核是嵌入式操作系统访问控制的核心组件,文献[30]从多安全策略集成性模型、基于反射技术的应用级访问控制、支持动态策略的安全核体系结构等方面进行了研究,在CRTOSII上实现了安全核的原型。

3.3 高可信软件的测试与评价

软件测试是保证软件可靠性的一个重要步骤,文献[31]针对分布式实时软件的可预计和可靠性要求,建立了实时多任务可靠性模型。文献[18]提出了一种基于任务模块软件统计测试的实时多任务软件可靠性验证方法,并提出了一种先验知识动态整合的贝叶斯统计推断验证测试方法。在此基础上,通过多年的持续研究,设计和开发了实时多任务软件的可靠性评价及辅助测试系统SRET。

软件防危性测试的目的是评价软件是否达到系统要求的防危性,文献[18]提出了基于关联风险剖面的软件防危性增长测试方法,建立了基于加速剖面的软件防危性验证测试方法。文献[32]提出了一种适合于防危性测试的增量记忆型的软件测评方法。

4 可信计算的发展趋势

本节从可信计算基础理论、可信系统和网络、可信性的评价与验证、可信应用这几个方面,总结当前可信计算研究存在的问题,指出一些有待于进一步研究的方向。

4.1 可信计算基础理论

可信计算概念来源于工程技术发展,到目前为止还没有一个统一的、科学严谨的定义,理论滞后于技术,尚没有公认的可信计算理论模型。因此,必须加强对可信计算基础理论和体系结构的研究,如可信计算的数学模型、可信软件的行为学与进化模型、可信性度量理论、可信网络的信任链模型等。

4.2 可信计算机系统与网络

4.2.1 可信硬件

当前计算机硬件的设计与测试主要是集成电路的设计与测试,它对验证设计的正确性和保证硬件的可信性极为关键。据国际半导体技术蓝图ITRS预测,未来单个芯片上将会集成数十亿个晶体管,可以将数十个乃至上百个处理核放置在单个硅片上,使得多核处理器(Multi-Core Processor)和多处理器片上系统(Multi-Processor System-on-Chip)[33]的出现成为必然。对多核系统的设计验证和测试是保证硬件可信性的关键。对于大规模多核系统,片上互连将成为新的性能瓶颈,片上网络(Network-on-Chip)是一个新的解决方案,对片上网络

的验证与测试、可靠性与容错、安全性等都需要开展大量的研究工作[34]。

4.2.2　可信软件

如果说硬件是计算机系统的基础,那么软件就是计算机的灵魂。随着人们对计算机系统功能需求的不断增加,软件系统变得日趋庞大和难以管理,缺陷和漏洞难以避免,为软件的可信性带来极大的挑战。可信软件的研究对象包括操作系统、中间件、构件、数据库、程序设计语言和应用软件等,其中软件体系结构与构件技术成为开发可信软件的重要途径[4]。

传统软件工程的首要目标是在有限的资源约束条件下开发出功能正确、质量可靠的软件系统,并没有把软件的可信性作为最主要的研究内容。这就需要研究可信软件工程、可信软件生产线、可信的设计规范或者软件开发工具等,从需求分析、设计、开发、验证到测试,改造原有的软件开发步骤,实现一套自动化的可信性保障流程。

4.2.3　可信网络

以因特网为代表的信息网络已成为现代社会最重要的基础设施之一,同时,随着传感器、嵌入式产品、消费电子等设备的大量介入,网络的规模仍在不断膨胀。在网络环境下,网络设备可能会出现故障,个人隐私可能会泄露,网络账户可能会被入侵,每个网络用户都希望网络是安全可靠的,对可信计算的需求更为突出。

如果说以前的网络以高性能为目标,当前的网络则应该提供高可信的服务,如安全性、可生存性和可控性[8]。可信网络的研究内容很多,包括可信网络结构,可信网络协议,可信网络设备等[7]。

4.3　可信性的评价与验证

由于可信性是指系统在规定时间与环境内提供可信赖服务的能力,它包括多个方面的属性。所以,对一个系统的可信性评价并不能简单地用某个单一的标准来衡量,而需要一个具有多方面指标的测度,是一个多目标的决策问题。

在实际的应用环境中,在评估一个系统的可信性时,对于它的若干个属性,并不是一视同仁的。各属性的重要程度,取决于系统的应用需求、设计和开发成本、外在环境等多方面的因素。因此,对可信性的度量和评价实际上是一个综合评价的过程,可以用下式表示[35]:

$$D = \omega_1 R + \omega_2 SE + \omega_3 SA + \omega_4 A + \omega_5 M \quad (1)$$

其中,$\sum_{i=1}^{5} \omega_i = 1, 0 \leqslant \omega_i \leqslant 1$。$D$ 表示一个系统的可信性,R,SE,SA,A 和 M 分别表示系统的可靠性,安全性,防危性,可用性和可维护性的参数值。ω_i 为表示各属性重要性的权值,由设计人员或最终用户根据应用的需求等因素做出权衡。这样,系统在不同的设计和配置下,可以对它的可信性做出定量的比较和分析。对各属性的强调程度与侧重点的不同直接影响到系统的可信性,当各属性彼此矛盾而需要平衡时,上述问题尤为严重。

有了可信性的度量和评价标准,还是远远不够的,如何用定义好的测度,判断一个系统是否真的是可信的,或者达到哪种可信赖的程度,都需要对系统的可信性进行验证。这也是当前可信计算的一个难点。

4.4　可信计算的应用

可信性是一个复杂的概念,对它的研究,还依赖于不同的应用场合需求。例如,对于实时系统而言,如果系统的时限约束没有满足,系统肯定是不可信的,谈论其他的属性如可靠性、防危性等是没有意义的,因此必须考虑实时性与可信性的协同设计。对于依赖电池供电的移动嵌入式产品而言,如何在能耗约束的条件下,提高系统的性能并保持系统的可信性,是一个新的研究课题。随着多核芯片的集成度越来越高,温度管理也是解决此类系统可靠性和防危性的一种重要手段。

应用系统是可信计算发展的根本目的和推动力。需要面向电子商务、电子政务、军事电子等不同的应用,开展对具体行业和领域的可信计算技术与产品的研究。

5　结语

信息技术的快速发展,使得计算呈现出无处不在的特点,人类社会对计算设备的依赖程度越来越高,计算系统的可信性已引起了学术和产业界的高度关注。可信计算经过近几年的研究与发展,在多个关键技术上取得了进展和突破,出现了许多研究原型系统和商业化产品。通过对可信计算的定义以及关键技术研究现状的分析,可以得出以下结论:

1)总的来说,可信计算还处于发展的初期阶段,还没有形成具有普遍适用性的基础理论体系,无论是学术界还是产业界,对可信计算的认识还没有统一,缺乏切实可行的可信性规范和标准。

2)随着普适计算和网络计算的发展,计算设备得到了广泛的应用,计算系统的可信性面临着严峻的挑战,在软件、硬件、系统及网络等领域,从分析、设计、实现,到验证、测试等研发阶段都有许多关键技术问题尚未解决。

3)经过多年的发展,计算系统的单维可信性保障技术如网络和信息安全、数字系统的可靠性等,已在不同应用领域取得了突破。但对于安全关键系统中多维可信性的综合保障和多目标评价,还需要进一步深入的研究。

4)系统的可信性是个复杂的综合概念,在不同的应用领域和环境下,它与计算系统和设备的实时性、能耗和温度等属性密切相关,存在着互相依赖的关系。面向应用领域的可信计算技术,例如多核芯片、无线网络等特殊环境下的可信性保障技术是需要关注的重点。

参考文献:

[1] LAPRIE J C. Dependable computing and fault tolerance: Concepts and terminology[C]// Proceedings of the 15th IEEE Symposium on Fault Tolerant Computing Systems. Los Alamitos, CA: IEEE Computer Society, 1985: 2-11.

[2] von NEUMANN J. Probabilistic logics and the synthesis of reliable organisms from unreliable components[M]// SHANNON C E, ASHBY W R, MCCARTHY J. Automata studies. Princeton: Princeton University Press, 1956: 43-98.

[3] NELSON V P. Fault-tolerant computing: Fundamental concepts[J]. Computer, 1990, 23(7): 19-25.

[4] 陈火旺, 王戟, 董威. 高可信软件工程技术[J]. 电子学报, 2003, 31(12A): 1933-1938.

[5] SIEWIOREK D, 杨孝宗, CHILLAREGE R, *et al*. 可信计算的产业趋势和研究[J]. 计算机学报, 2007, 30(10): 1645-1661.

[6] 闵应骅. 可信系统与网络[J]. 计算机工程与科学, 2001, 23(5): 21-23.

[7] 周明天, 谭良. 可信计算及其进展[J]. 电子科技大学学报, 2006, 35(4): 686-697.

[8] 林闯, 彭雪海. 可信网络研究[J]. 计算机学报, 2005, 28(5): 751-758.

[9] 沈昌祥, 张焕国, 冯登国, 等. 信息安全综述[J]. 中国科学: E 辑 信息科学, 2007, 37(2): 129-150.

(下转第 931 页)

由表 1 可见,这种混合认证模型充分糅合了严格层次结构模型和分布式信任结构模型的优点,既克服了前者根认证中心的瓶颈效应,又解决了后者在不同信任域的交叉认证中可能存在的不可靠性,是对现有结构模型的改进,具有良好的综合性能。

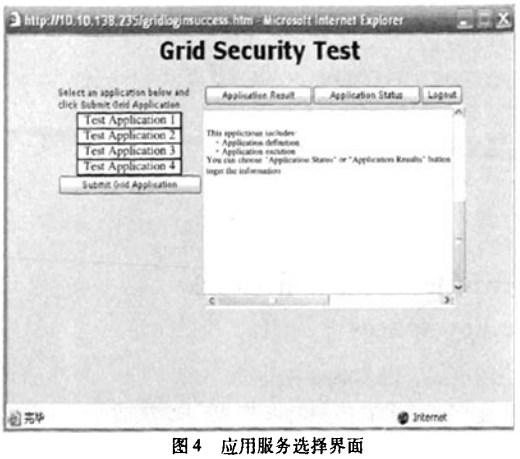

图 4　应用服务选择界面

4　结语

对三级认证子系统和域间认证子系统的仿真验证和性能分析表明:本文所提出的混合认证模型是可行的。在终端用户登录方面,该模型采用的RADIUS认证机制克服了静态口令机制所存在的易被攻破、安全性和计算性能互相钳制等弱点;在 CA 的结构组织上,该模型融合了严格层次结构模型和分布式信任结构模型的优点,具有良好的综合性能。

在混合认证模型中,三级认证服务器之间的交互和协调,以及终端用户的应用功能设计,还有待进一步研究。

参考文献:

[1] HOUSLEY R, POLK W, FORD W, *et al*. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile[EB/OL]. [2008-07-20]. http://www.ietf.org/rfc/rfc3280.txt.

[2] The Globus Alliance. Globus project[EB/OL]. (2005-08-10)[2008-08-10]. http://www.globus.org/.

[3] PERLMAN R. An overview of PKI trust models[J]. IEEE Network, 1999, 13(6): 38-43.

[4] MOSES T. PKI trust models[EB/OL]. [2008-07-22]. http://www.itu.dk/courses/DSK/E2003/DOCS/PKI_Trust_models.pdf.

[5] ZHU L, TUNG B. Public key cryptography for initial authentication in kerberos (PKINIT)[EB/OL]. (2007-01-05)[2008-07-25]. http://draft-ietf-cat-kerberos-pk-init-16.txt.

[6] RIGNEY C, WILLENS S, RUBENS A, *et al*. Remote authentication dial in user service (RADIUS)[EB/OL]. [2008-07-19]. http://www.ietf.org/rfc/rfc2865.txt.

[7] FOSTER I, KESSELMAN C. The grid: Blueprint for a new computing infrastructure[M]. 2nd ed. San Francisco, USA: Morgan Kaufmann Publishers, 2004.

(上接第 919 页)

[10] 李琪林,周明天.可信中间件—技术现状和发展[J].计算机科学,2008,35(6):15-19.

[11] AVIIENIS A, LAPRIE J C, RANDELL B, *et al*. Basic concepts and taxonomy of dependable and secure computing[J]. IEEE Transactions on Dependable and Secure Computing, 2004, 1(1): 11-33.

[12] Csc-std-001-83. Trusted computer system evaluation criteria[S]. Washington, D C, USA: DOD, 1980.

[13] 刘克,单志广,王戟,等."可信软件基础研究"重大研究计划综述[J].中国科学基金,2008(3):145-151.

[14] 闵应骅,冯登国.《可信计算专辑》前言[J].计算机学报,2007,30(7):1-2.

[15] 冯登国.信息安全[J].计算机学报,2006,29(9):1-2.

[16] 闵应骅.容错计算二十五年[J].计算机学报,1995,18(12):930-943.

[17] 胡瑜,韩银和,李晓维.SoC 可测试性设计与测试技术[J].计算机研究与发展,2005,42(1):153-162.

[18] 覃志东.高可信软件可靠性和防危性测试与评价理论研究[D].成都:电子科技大学,2005.

[19] 张宇,洪炳熔.软件容错技术的研究现状与展望[J].计算机应用研究,1999,16(9):1-3.

[20] 傅忠传,陈红松,崔刚,等.处理器容错技术研究与展望[J].计算机研究与发展,2007,44(1):154-160.

[21] 陈宇.高可靠容错实时系统的支撑技术研究[D].成都:电子科技大学,2003.

[22] 闵应骅.网络容错与安全研究述评[J].计算机学报,2003,6(9):1035-1041.

[23] 向生建.安全中间件系统关键技术研究[D].成都:电子科技大学,2006.

[24] 廖勇.面向新一代航空电子的实时自适应资源管理中间件及算法研究[D].成都:电子科技大学,2006.

[25] 黎忠文,雷航,熊光泽.可降级现场总线网系统可靠性的评价方法[J].电子学报,2001,29(2):147-149.

[26] 陈慧.实时宽带现场网络技术研究[D].成都:电子科技大学,2004.

[27] 杨仕平,桑楠,熊光泽.基于 Ethernet 技术的安全关键实时网络[J].软件学报,2005,16(1):121-134.

[28] 杨仕平.分布式任务关键实时系统的防危(safety)技术研究[D].成都:电子科技大学,2004.

[29] 黎忠文.分布式控制系统中新安全保障技术的研究——安全核技术[D].成都:电子科技大学,2001.

[30] 吴新勇.嵌入式操作系统安全保障技术研究[D].成都:电子科技大学,2004.

[31] 雷航.面向实时系统的软件可靠性评价技术的研究[D].成都:电子科技大学,1997.

[32] 杨仕平,桑楠,熊光泽.安全关键软件的防危测评技术研究[J].计算机学报,2004,27(4):442-450.

[33] JERRAYA A A, WOLF W. Multiprocessor systems on chips[M]. San Francisco, California: Elsevier Morgan Kaufmann, 2005.

[34] PANDE P P, GRECU C, IVANOV A, *et al*. Design, synthesis, and test of networks on chips[J]. IEEE Design & Test of Computers, 2005, 22(5): 404-413.

[35] 徐拾义.可信计算系统设计和分析[M].北京:清华大学出版社,2006.