

可信性概念与可信性计算系统的研究^{*}

袁由光 李海山

(中船重工集团七院七〇九所 武昌 430074)

摘 要

正确分析评估计算机系统的可信性,综合权衡可靠性、可用性、安全性、健壮性,构成可信性概念与可信性计算系统研究,旨在探讨一种先进的可信计算系统体系结构,可信计算硬件、软件特性,使其对今后高可信计算机的开发和验证提供理论和方法。

关键词 可信性 可信计算系统 开发与验证

1 问题的提出

在当今知识经济时代,现代化的生产经营无一不是运用信息的过程,高技术局部战争更是信息系统或信息化武器系统的总体对抗。信息是影响各国经济发展、军队战斗力的关键因素(从海湾战争到北约对南联盟的狂轰滥炸,我们更加领悟到了这一点)。而计算机是获取信息、传递信息、处理信息、信息反馈控制与决策、信息对抗的主要设备,计算机系统软、硬件的任何故障都将严重影响信息处理的各个环节,产生重大的经济损失甚至是人员伤亡等无法挽回的结果。长期以来,根据不同应用场合,人们研究了诸如关键任务计算系统、长寿命系统、高可用系统、延迟维修系统、高性能计算系统、安全计算系统等各种不同的计算系统,这些系统具有不同的结构和特点,对可靠性、可用性、安全性、健壮性等有不同的要求,不同的侧重点,但这些系统基本上都只考虑了其中的一个方面或两个方

面,很少综合考虑与权衡各个方面。

随着技术的发展与应用范围的广泛深入,以及武器系统的日趋复杂和庞大,设计和评价一个系统不仅对可靠性、可用性、安全性、健壮性等单个指标有更高的要求,而且要求综合考虑各个指标对系统的影响。然而,长期以来,无论是在航空航天系统,还是在武器控制系统中,对计算系统的确认都只考核个别指标,并且缺乏完整的验证手段和方法,没有完善的理论指导。因此,通过对计算机系统可靠性、可用性、安全性、健壮性等概念以及各指标间相互关系的研究,探索一种具有指导性定义的计算机体系结构,它能根据具体应用的需要综合平衡各指标关系,从而对今后计算机的开发和验证提供理论和方法。使这种研究在综合分析与评估软、硬件计算系统可信性的理论和方法上有所突破,在计算机系统体系结构上有新发展,就成了十分紧迫而重要的研究工作。

随着这一研究工作的深入发展,人们逐渐形成了所谓“可信计算的概念”,进而探讨

^{*} 收稿日期:1999年11月12日

可信计算的定义、内容、指标以及如何正确分析、评估系统的可信性,综合权衡可靠性、可用性、安全性、健壮性等各指标,设计出适合不同应用场合的最优或较优可信系统,并验证系统的有效性、适用性。然而这是一项困难的工作。不幸的是,直到目前为止,对可信计算的概念还不清晰,对有关理论与方法的研究还不深入。但是该研究课题对于提高军事装备的可信性,验证系统的有效性,从而保证军事装备的战备完好性和任务成功性具有重要意义,具有广阔的军事应用前景。在民用航空航天与通信等领域也有广阔的应用前景。

2 国内外研究现状和发展趋势

对可信计算研究是从对容错计算研究开始的,容错计算能提高系统的可靠性或可用性。国外在容错计算的研究和应用方面起步较早,特别是在美国及西欧等发达国家,有一大批高素质的科研人员和一批有相当实力的大公司进行容错技术研究并已形成多种容错产品。其容错理论比较完善,研究手段和设备比较先进,容错计算机和服务器设计方法,体系结构等方面有相当快的发展,已把商用计算机的高新技术和容错技术有机地融合在一起,形成了具有强大处理能力、开放体系结构的容错计算和控制系统。这种系统能满足关键应用、联机事务处理和实时控制中对高性能、高可用性或高可靠性的要求。如 Continuum 容错计算系列是美国 Stratus 容错电脑公司推出的最新容错处理系统,它融合了精减指令集(RISC)技术与 Stratus 的硬件容错技术,采用高性能的 HP-RISC 芯片,系统级的对称多处理器、安装在主机板的高速存贮器和设置专用的 I/O 处理器等多种措施,使 Continuum 具有强大的处理能力,配合 Stratus 独特的硬件容错体系结构,进而保证了 Continuum 的连续可用性。美国 Tandem 公司的 Integrity 系列到 Himalaya 系统服务器都具有强大的处理能力和高可用

性。另外,还有根据应用环境不同采用各种不同设计思想和方法来提高系统或某关键部件的可靠性或可用性。有对服务器中关键部件如网络控制器、磁盘控制器采用冗余设计和热拔插技术;在数据存贮上采用 RAID 技术;而更多的则是利用容错思想,采用商业系统进行集成,组成双机容错服务器。如采用双控制器磁盘阵列,两台服务器通过 SCSI 总线连接到一个磁盘阵列子系统,备援服务器通过网卡并经由 SCSI 通道和一个网络上的监视器侦测主服务器故障。发现故障,备援服务器则接替主服务器管理各种系统资源。以上这些系统往往在可信性的某一指标上能达到很高标准,能有效满足某些方面的应用需要,但由于其它方面欠考虑往往限制了其应用范围。

当前由于各企事业单位更清楚地认识到计算机的稳定性直接影响到企业的商誉和运作,构筑高可信性系统的需求日益高涨,在商用上越来越多的服务器厂商开始采用“集群技术”,利用 LAN 等网络,将多个同种计算机连接起来,作为一个整体进行信息处理、运用。通过采用故障自动恢复中间件;故障防范运行机制;用 RAID 和工具保护数据等措施提供高可用性系统。以前,高可用性的用户多选择 Unix 服务器,不少用户对 NT 服务器的可用性心存疑虑。尔后由于微软推出了集群软件 MSCS,提高了 NT 集群的地位和竞争力,成为许多要求高可用性用户的重要选择,IT 业界也普遍看好。微软将 MSCS 作为 Windows NT4.0 企业版的标准附件。除 MSCS 外,NT4.0 企业版还增加标准附件事务处理(TP)监控器 MSTs 和消息连接中间件 Message Queue Server (MSMQ)等,以提高系统的可用性。集群软件对于处理器等硬件故障以及由 OS 应用等偶发原因所造成停机故障自动恢复非常有效。一旦“心跳信号”中断或检测到主服务器上的进程发生了故障,就将应用切换到“待机”服务器。还有一种提高可用性的方法是利用具有通信功能的中

间件,如 TP 监控器和对象请求代理(ORB)等。在多台服务器运行的分布环境下,当某一服务器发生故障时,TP 监视器和对象请求代理自动切换客户端访问的服务器,继续进行处理。Borland 的三层系统构筑支持工具“Entera”将应用分割成多个构件,每个构件都装载到两个以上的应用服务器上。假若一台应用服务器发生故障,某个构件被停掉时,服务器的“Entera”在同一机器上重新启动该构件。如果应用服务器彻底停机时,客户端的 Entera 将访问对象切换到别的应用服务器。若能在故障发生前消除引发故障的原因,就能降低系统停机的危险。最近在系统管理工具中,出现了具有支持“预防性维护”功能的产品。如 MpWalker 不仅能检测故障的发生,而且具有能检测故障发生“征兆”的“预防性维护”功能。时刻记录平时的使用状况,一旦实测值开始脱离平均运行状况,就向系统管理人员发出警告。但如果在节假日运行状况变化的系统中,不随之改动基准值,就会误报。实际上,这些都是以软件的方法来解决系统运行中出现的问题,然而由于应用的原因而造成的系统停机,即使是由“待机”服务器来执行该应用,仍然会停机。再者,并不是对所有的软件产品都能进行故障切换。如用微软的 MSCS 可以对 Oracle 进行故障切换,但对资源进行分组等设置作业非常麻烦,发生一点问题就会失败。能检测到的故障也有一定限度,如微软的 MSCS 不能检测接在 LAN 上的网卡(NIC)故障,而康柏的 Ipwatcher 软件则可用于 NIC 故障检测。另外,为了活用集群软件,在系统设计时要注意,为了尽量缩短从故障切换到恢复的时间,程序和事务处理要尽可能变小。

随着 Internet 的普及,保密、防信息泄漏等安全技术越发受到人们的重视,在这方面的研究目前正方兴未艾。在安全性方面,今日的国际信息安全产业已初具规模,各大跨国公司纷纷介入这一新兴的庞大市场。IBM 公司积极开展电子商务协议、SET 和 CA 等方

面的研究;HP 公司推出国际密码构架 ICF、“虚拟保险箱”、“B1 级安全操作系统”等安全产品。SUN 公司积极推广其 JAVA 产品和相关的 JAVA 安全产品,以及 FIRE - WALL1 防火墙;DG 公司积极倡导其 NUMA 产品和 B2 级安全操作系统,以及完整的信息安全解决方案;CA 公司积极推广其 UNICENTER TNG,支持防火墙、一次身份认证等信息安全模块。GEMPLUS 公司新推出的智能卡,支持 2048 比特的 RSA 公开钥匙密码算法。各大跨国公司均有自己强大的信息安全实验室。如 IBM 公司的苏黎士实验室、HP 公司的伦敦信息安全实验室等。出现了许多信息安全和网络安全专业公司。

计算机健壮性问题虽然早已提出,但引起人们的充分重视,却是近几年的事情,欧洲阿里亚娜 5 号火箭的爆炸,是因为计算机没有满足健壮性要求导致的。所谓健壮性可理解为:当计算机系统或部件(软件或硬件)接受了无法执行的操作命令时,应能避免系统失效能力。在计算机应用中,不知原因的“死机”现象往往是健壮性问题所引起的。美国卡内几—梅隆大学(CMU)的 Ballista 计算机健壮性研究小组,对各类计算机上的不同 UNIX 操作系统进行了健壮性测试,通过测试寻找典型的与健壮性相关的异常现象有:灾难性异常、重新启动异常、异常中断等,然而有关计算机系统健壮性问题的研究还很不成熟。

上述研究都是人们普遍认识到计算机系统的可靠性、可用性、安全性、健壮性等极端重要,而提出的一些解决方法和手段。

近年来,人们提出研究可信性的概念,试图对可信计算的概念、内容、方法等进行全面系统的研究,找出一种分析、设计和评估可信计算系统的理论和方法。然而,这方面的研究还处于概念阶段,研究文献也不多见。

3 可信性概念与可信性计算系统研究

可信性概念与可信性计算系统研究的目的是通过对计算机系统可靠性、可用性、安全性、健壮性等可信性概念及各指标间互相关系的研究,探索一种具有指导性定义的计算机体系结构,它能根据具体应用的需要综合平衡可信性各指标关系,从而对今后高可信计算机的开发和验证提供理论和方法。

3.1 可信计算概念、理论和方法研究

研究可信计算的概念、定义、内容、指标和方法,研究综合分析及评估软、硬件计算机系统可靠性、可用性、安全性、健壮性等可信性指标的理论和方法,要解决的关键问题首先是建模,以图论、马尔柯夫链或 Petri 网等数学分析方法为工具,建立一种综合考虑可靠性、可用性、安全性、健壮性等可信性指标的数学模型。

目前虽然国际上出现有很多各式各样关于可靠性、可用性的研究及成果,也有大量实用的信息安全方面的产品,但仍没有一种综合考虑可信性各指标的通用性产品出现,更没有理论、方法。我们认为计算系统可信性至少应包括:信息一致、完整、保护和鉴定;访问控制/安全服务;服务可用性;网络管理与控制;损失评估;反应(隔离、校正、行动),包括恢复与重构;易损性评估和规划;入侵探测/威胁报警等一系列内容。因此计算系统可信性的度量单位—可信度应是可靠度、可用度、安全度、健壮度等的综合函数,而且可靠度、可用度、安全度是相互影响的。增大安全度就必需增加软、硬件防范措施,即在串联系统中增加串行元器件,这必将影响到系统的可靠度;而增大可靠度必需增加系统冗余资源,这又可能会影响可用度。

3.2 先进的可信计算系统体系结构研究

研究可信计算系统中基本部件特性、系统构成、重组和恢复策略。研究 COTS 技术在可信计算系统中的应用。

要同时考虑计算机系统的可靠性、可用性、安全性、健壮性等可信指标,就必须研究这样的计算机所具有的特殊体系结构,这

种计算机的基本部件特性,以及在故障情况下的重组与恢复策略,在紧急情况下保证系统安全及避免系统失效的能力。

随着计算机的不断发展,军事装备水平的不断提高,越来越多的民用高新技术正不断进入军事应用领域。民用计算机无论是在硬件设备设计制造,还是软件开发与应用上都有很成熟的技术。充分利用商用成熟技术构造可信计算系统,不仅能保持系统兼容性,避免重复劳动造成资源浪费,而且有利于形成产业化。通过采用开放体系结构,有利于军用计算机产品走系列化、模块化、通用化发展道路;保证足够的技术支持、产品维护和升级服务;紧跟计算机技术发展潮流,保证我军武器装备,信息对抗系统的先进性;有利于技术持续发展,缩短武器系统研制周期,较好地解决服役周期长与计算机更新换代的矛盾。

3.3 可信计算硬件的特性研究

在体系结构研究的基础上,通过对组成系统的基本部件的分析,对严重影响系统可靠性、可用性、安全性、健壮性的模块、材料等硬件构件进行具体研究,以形成一个高可信计算系统框架。

研究具有自动故障检测、诊断、重组与恢复的硬件模块,这是保证系统具有高可信性的基础。目前在这方面的研究较多。

高性能计算机系统的安全对我军信息化建设相当重要,特别是在实时高性能计算任务中,如果没有安全保障,花巨资建立的电子信息系统就有战时出问题的潜在危险。尤其是在今天为增强信息战能力,国外正在研究各种信息战手段和武器,诸如高能电磁脉冲武器、计算机病毒武器、网络攻击技术及工具等,目的在于攻击和瘫痪敌方计算机系统。发达国家对计算机信息对抗技术及装备的研究属于高级军事秘密。因为以争夺信息优势为目标的信息战已成为支配未来战场的新的战争形式,由各类电子装备构成的电子信息系统已成为军队作战系统的核心,同时也是实施未来信息战的物质基础和主要载体。它

能对各类战场信息进行截获、综合、处理、传递、控制和利用,为己方武器系统提供目标指示和射击参数,以压制、欺骗、干扰、破坏方式阻断敌方信息源,同时保护己方电子系统免受敌人破坏。

国外,特别是美国,对军用计算机系统的安全性有一套完整的检测与验证标准,建立了各种安全等级。在计算机信息泄露领域有很深的理论研究,在防信息泄露的材料、方法、手段上有很强的技术力量。目前,国际市场上已有截获距离为1000m的计算机泄露信息截获装置出售(但不卖给我国)。据称,美国的截获距离已达到5000m以上。美军的信息对抗能力已达到可靠使用的程度,它可以利用信息对抗在发动实体攻击前,先破坏敌对国家的供电系统和通讯中心,使这个国家陷入瘫痪。

因此,开发研制我军高性能计算机系统时,在重视高可靠性、可用性的同时,充分考虑系统的健壮性、安全性意义重大。

3.4 可信计算的软件特性研究

可信软件模块是构造可信计算系统的基础。可信软件模块必须具有高的可靠性、可用性,同时还应具有安全性和健壮性。因此要研究容错软件、安全软件、健壮软件。

对于可信操作系统的研究,可选择一种稳定性能好的实时多任务操作系统进行改造。保持系统兼容性,保护用户在软件上的投资和软件开发上的自由;同时通过强化操作系统核心,支持相应的硬件容错结构。在操作系统内核增加容错服务子系统,提供对容错硬件资源的直接管理,支持下列容错功能:配对与备份硬件的执行;模块热插拔时的切换与恢复;协助容错硬件对错误隔离、故障检测、诊断与记录;故障设备的I/O重定向。容错服务子系统提供的容错控制与管理进程作为系统进程之一在启动操作系统时创建,由

容错硬件检测装置或模块插入信号启动运行。在操作系统与应用程序间提供应用程序接口,它由系统调用中间件组成。应用程序对系统的调用通过中间件实现,中间件对调用合法性,传递参数等的有效性进行检查,以保证系统不会因函数不利参数传递而引起系统异常,在紧急情况下保证系统安全与避免系统失效。

参考文献

- [1] Karama Kanoun, Mohamed Kaaniche, Christian Beounes, Jean-Claude Laprie, Jean Arlat, "Reliability Growth of Fault-Tolerant Software", IEEE Trans. Reliab. 1993. 6
- [2] Nitin H. Vaidya, Dhiraj K. Pradhan, "Fault-Tolerant Design Strategies for High Reliability and Safety", IEEE trans. Comp. 1993. 10
- [3] 袁由光, 陈以农. 容错与避错技术及其应用. 科学出版社, 1992
- [4] 袁由光. 实时系统中的可靠性技术. 清华大学出版社, 1995
- [5] Y. Deswarte, "A High Safety Multi-processor Architecture". Dig. Gth Int. Symp. Fault-Tolerant Comput. 1976
- [6] B. W. Johnson, J. H. Aylor, "Reliability & Safety Analysis of a Fault-Tolerant Controller", IEEE Trans, Reliab. 1986. 10
- [7] Joanne Bechta Dugan, Salvatore J. Bavuso, Mark A. Boyd, "Dynamic Fault-Tree Models for Fault-Tolerant Computer Systems", IEEE Tran. Reliab. 1992. 9
- [8] Shambhu J. Upadhyaya, Sreejit Chakravaty, "Analysis of a Fault-Tolerance Scheme for Processor Ensembles", IEEE Trans. Reliab. 1992. 6
- [9] Jean Arlat, Alan Costes, Yves Crouzet, Jean-Claude Laprie, Davie Powell, "Fault Injection and Dependability Evaluation of Fault-Tolerant Systems", IEEE Trans. Comput. 1993. 8
- [10] A Reliable Fail-Safe System, IEEE Trans. Comput. 1998. 2