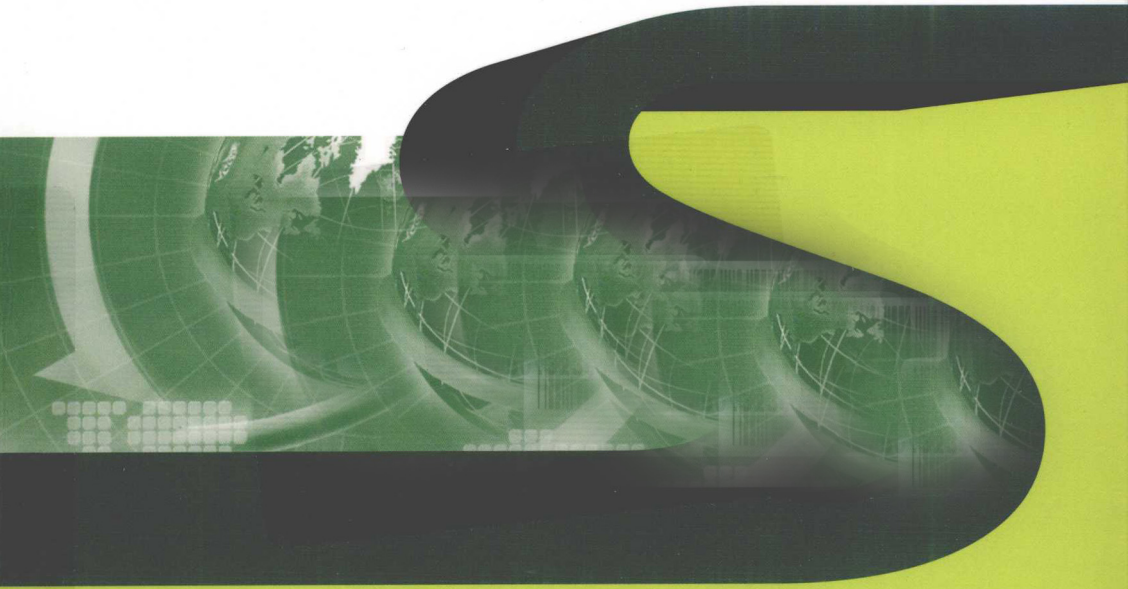
网络信息系统生存性增强技术研究

王莉 著

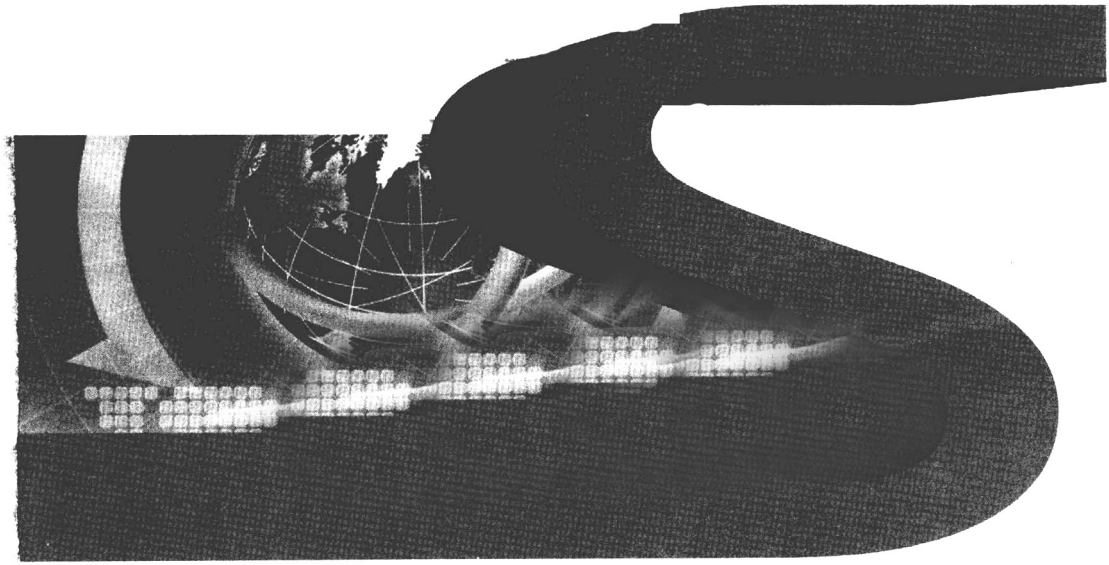


ANGLUO XINXI XITONG SHENGCUNXING
NGQIANG JISHU YANJIU

西南交通大學出版社
Http://press.swjtu.edu.cn

网络信息系统生存性增强技术研究

王莉 著



WANGLUO XINXI XITONG SHENGCUNXING
ZENGQIANG JISHU YANJIU

西南交通大学出版社
·成都·

图书在版编目（CIP）数据

网络信息系统生存性增强技术研究 / 王莉著. —成都：西南交通大学出版社，2011.5
ISBN 978-7-5643-1126-1

Ⅰ. ①网… Ⅱ. ①王… Ⅲ. ①计算机网络－信息系统－研究 Ⅳ. ①TP393

中国版本图书馆 CIP 数据核字（2011）第 039148 号

网络信息系统生存性增强技术研究

王 莉 著

*

责任编辑 黄淑文
特邀编辑 黄庆斌
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
成都蓉军广告印务有限责任公司印刷

*

成品尺寸：148 mm×210 mm 印张：5.375
字数：150 千字
2011 年 5 月第 1 版 2011 年 5 月第 1 次印刷
ISBN 978-7-5643-1126-1
定价：20.00 元

内 容 简 介

网络信息系统的生存力，是指系统在遭受攻击、失效或故障等事件的时候，能实时提供用户关键服务的能力。网络信息系统生存性增强技术是信息系统安全领域的研究热点之一。本书的信息系统生存性增强技术研究面向提高信息系统生存能力的目标，着重对增强信息系统生存能力的相关技术和相关算法进行研究。尤其是在前人的基础上，对信息系统的生存性增强技术研究做了一个有效的梳理，并对系统生命周期中非常关注的生存性分析技术以及重配置技术进行了深入的研究。这些研究，无论在理论上还是实用上，都取得了一定突破，对于有效保障开放环境下的信息系统安全具有较好的实用性。

本文共有 10 章，其内容主要包括两大部分：（1）生存性分析技术。重点从系统体系结构、攻击者、系统运行状态三个方面对系统的生存能力进行定性分析和定量计算；（2）重配置技术。重点研究了生存性重配置过程相关概念的形式化定义、重配置的策略，并在此基础上，提出了一个面向容错 QoS 的生存性重配置实现模型，最后讨论了动态重配置技术的影响和重配置控制系统的安全问题。

本书可作为计算机应用及相关专业的参考读物，也可作为网络相关从业人员的学习用书。

前　言

交通、通信、能源以及金融服务等关键系统对社会的正常运转是至关重要的。由于社会各领域的基础设施对于网络关键信息系统的严重依赖，使得这些关键信息系统一旦不能提供服务，就会导致非常严重的后果。为了保护这些关键信息系统，人们最大限度地采取了安全措施，但没有一项安全措施能完全确保无边界网络中的信息系统免遭攻击。生存性学科则可以在系统遭受攻击、故障或失效时有效确保传递关键服务和维持系统的完整性、私密性以及性能等关键特性。

目前，众多的研究者和研究机构对信息系统生存性进行了研究，并且在生存性的定义、生存性分析等领域作出了极大的贡献。同时，信息系统生存性的增强技术也很快成为了研究的热点。

但是，信息系统生存性的研究历史并不长，也远未达到成熟阶段，表现在信息系统生存性的定义和特点没有统一，增强信息系统生存能力的技术没有深入研究，更多的还是停留在理论研究上，距离可真正进行实际应用还有很大的差距。

针对目前生存性研究存在的不足，作者对信息系统的生存性增强技术进行了探讨，主要有如下贡献：

（1）从系统的生命周期观点提出了一个全面增强系统生存能力的技术框架。该框架将系统的生存能力增强技术划分为生存性设计、生存性测试、生存性分析以及生存性提高技术等。这个框架为生存性的增强技术研究指明了方向。

（2）为了采取合适的措施来增强系统的生存性，本书将信息

系统生存性分析问题划分为系统体系结构、攻击行为和系统状态三个子问题，并分别提出各自的模型。三个模型充分考虑了导致系统生存能力变化的因素。从系统的体系结构来看，对系统的生存性恢复操作必然会体现在系统的体系结构变化上，因此，提出了一个改进的复杂矩阵跟踪系统的体系结构变化，通过判断系统的服务路径是否可达来定性判断系统服务是否可生存；将程序切片思想引入了体系结构，讨论了一种定量的生存性分析方法；从攻击者攻击行为来看，假设攻击行为是破坏关键服务的最主要原因，因此，引入攻击树来模拟攻击行为，并定量计算系统的生存能力；从系统状态来看，提出采用 U 函数方法来定量计算多状态系统的生存能力。

（3）作为一种重要的生存性增强技术，本书详细地研究了面向生存能力的重配置技术，首先给出了重配置的形式化定义，然后详细讨论了重配置的步骤、重配置的特点以及重配置的操作，并在讨论传统的重配置操作基础上，基于乐观估计错误影响范围，提出了一种简单有效的重配置操作。该操作大大降低了重配置的操作成本。

（4）为了确保重配置技术能增强系统的生存能力，如何选择一个合理的、有效的重配置策略是个非常紧迫的问题。基于最大构件生存能力的重配置策略和最大配置依赖的重配置策略的比较分析，提出了一个面向 QoS 的重配置策略。实验表明该策略能获取最大的配置成功率，并且极大地降低了重配置的操作次数。最后，提出了一个面向 QoS 的重配置操作实现模型，并讨论了其实现细节和相应的实现算法。

（5）尽管重配置机制在很大程度上保障了系统的生存能力，但在实际的重配置操作过程中，重配置操作可能对系统产生功能或性能上的影响，如果这些影响不能够系统地进行评估并有效加

以控制，将给系统带来严重的威胁。本文详细分析了两种重配置影响，给出了两种重配置影响控制实现方式，并提出一种重配置调度算法，进一步减少了重配置程序的运行开销。

（6）面向生存性的重配置系统安全研究：重配置系统是一个置于被重配置的信息系统上的一个控制系统，其特殊的重要地位非常容易遭受外在的攻击，导致重配置的操作无法进行，更为严重的是攻击者可能获取重配置系统的控制权，从而可以采取随意的重配置操作，给信息系统带来更加灾难性的后果。本文从攻击角度出发，分析了检测-响应系统中的攻击行为，并针对其中攻击管理存在的问题，讨论了重配置系统自身的安全隐患，给出了一系列的安全保障机制维护了重配置系统的安全。

王 莉

2011年4月

目　录

第1章 绪 论

1.1 网络信息系统生存性概述

本书所指的网络信息系统（Network Information System，NIS）是指可以通过其他系统被人们访问的信息系统，即这些系统并非是一个孤立的封闭系统，而是与外界存在着信息交流[1]。网络信息系统已经广泛地应用于能源、交通、电讯、制造、金融服务、医疗和教育等领域。在21世纪的今天，网络信息系统已经逐渐成为社会各领域不可或缺的关键设施，它的使用程度成为衡量一个国家现代化和综合国力的重要标志[2, 3]。随着我国计算机网络和信息系统建设的快速持续发展，各个社会职能部门对网络信息系统的依赖程度也越来越大[4]。由于严重的依赖程度以及网络环境的异常复杂性，使得这些关键信息系统的安全问题成为迫在眉睫和不可回避的问题。

网络信息系统的安全运行，不仅取决于提供服务功能的构件自身的可靠性，还有赖于系统运行平台的稳定性。信息系统可运行在内网、外网以及公网上，这些网络提供异构的工作平台，包括不一样的操作系统、硬件产品以及不同的通信协议等。信息系统的重要运行环境Internet，是一种开放和标准的面向所有用户的技术，其资源通过网络共享。资源共享和信息安全是自 Internet 问世以来，一

直存在的一对矛盾体。随着计算机网络资源共享的进一步加强，信息安全问题也日益突出，网络黑客攻击（特别是大规模 DoS 攻击）、大规模蠕虫病毒的无规律性连续侵袭或意外的安全事故已经造成了巨大的经济损失，未来可能的网络恐怖活动甚至信息化战争使得运行在网络上的信息系统安全状况非常令人担忧。

为了保护这些关键信息系统，人们做过很多努力，从协议规划、服务模式、网络管理等方面进行了合理设计，而且提出了众多的安全措施，包括加密、访问控制、防火墙、入侵检测、病毒防护等，这些传统的安全技术试图通过加固使得系统难以突破，或者通过检测发现系统中已经侵入的所有攻击，它们为保护信息系统安全作出了很大的贡献。但实践证明，要识别一个动态变化的系统的全部漏洞是不可能的，要识别未来所有可能的攻击手段也是很困难的。近年来，虽然安全技术在不断提高，但网络安全事件及其对社会造成的影响并没有完全消失甚至没有减少。其主要原因在于：① 现有的安全措施自身存在缺陷，其发生机制和所采用的技术有待完善；② 目前的安全措施侧重于对特定系统的组成构件的保护，却忽视了系统是有机整体的事实；③ 各种安全机制自身也可能是攻击者的目标，也是需要保护的对象，但在实际应用中却往往疏于防范。④ 目前网络与信息系统日益朝着大规模、高度分布式的方向发展，已经跨越了传统的网络边界，演变成无边界网络系统。传统的基于网络边界和安全域划分的安全观念已经不适应网络形势的发展。

更何况，网络信息系统的复杂性和开放性，使其完全可以成为一个开放的复杂巨系统[5]，虽然各种安全措施在不同层面上加固了系统，一定程度上能保障系统顺利实施，但这些措施在一个层面上的使用可能在其他层面上带来新的漏洞。也就是说，现在已经不存在哪个网络信息系统对于计算机化的攻击是免疫的，不存在绝对安全的网络信息系统。

一方面，由于网络信息系统规模大，技术复杂，涉及人员多，也使其安全保障困难，而要达到一定安全标准，所需的投入也相当大。这就要求在网络信息系统的安全建设中，需要权衡安全、成本、效率三者的关系。实际上，绝对的安全是没有的，网络信息系统也不是“越安全越好”。不同的网络信息系统，对于信息安全的要求是不同的。因此，必须根据网络信息系统的实际要求做到恰到好处。在进行网络信息系统的安全设计时，应该根据实际应用情况，协调好安全、成本、效率三者的关系。如果一个网络信息系统的安全保密性能超出了安全保密的管理要求，这不但没有必要，而且还会造成资金上的浪费。

另一方面，传统的安全措施关注网络信息系统安全的检测和防御问题，采用的安全技术主要研究信息的机密性。但是当前网络信息系统关心的重点已经从单个部件的安全转而关注信息的可获取性和服务的可持续提供。即系统在提供服务的过程中，当攻击、故障或某种特殊的安全事故突破了既定的安全防线，使系统某些组成部分受损时，采取何种方法保证网络信息系统的关键服务持续提供，如何在系统性能下降时，或者说，系统暂时通过降级服务满足了用户需求时，如何尽快恢复受损的部件，提高系统应对未来攻击或故障的能力，换句话说，如何增强系统自身生存力已经成为网络信息系统安全关注的重心。

所谓信息系统的生存力，就是指系统在遭受攻击、失效或故障等事件的时候，能实时地提供用户关键服务的能力[6]。信息系统的生存性主要研究系统在受到外在作用力的情况下，通过调度其现有资源，持续提供关键服务的能力，而提供关键服务的质量取决于当时系统的状态，但至少应该满足关键服务的最低需求。

增强信息系统的生存能力包括两个层面的含义：

一是增强系统持续提供服务的能力。即增强系统在面临攻击、

失效和偶发事件的情况下持续提供服务的能力。

二是提高系统的生存演化能力。即使当前系统能提供服务，但系统状态已经受损，如果不采取补救措施，在未来某个时刻，系统无法持续维持服务的概率增大，从而破坏潜在的生存能力，因此必须考虑生存性补救措施，来帮助系统自恢复。

以上两个层面含义相辅相成，互相作用。前一层含义是系统必须具备的基本能力，不管发生什么事情，系统的某些组成部分可能受损，但通过相应手段，仍然可以响应系统的关键服务，或提供关键服务的替代服务，服务的等级可以完全一致，也可能有所降低，但毕竟是完成了相关服务的提供，因此从这个层次上来讲，可以认为系统的生存策略是成功的。就像一个人，如果其手受伤了，不能提重物，但也不至于影响到这个人的性命，因此可以认为这个人是具有生存性的。第二个层面强调系统的自适应、自演化能力。在上例中，人毕竟是受了伤，不同于一个健康人，必须外敷药，内调理，以此来增强自身的适应能力，尽快恢复受伤的手。可以看出，前一层含义是基础，是系统必须达到的目标，后一层含义是前一层含义的不可或缺的保障措施，它能保证信息系统的持续演化，不至于终止信息系统生存期。再用上例，手受伤不治疗，会影响到身体的其他器官，逐渐恶化，最终导致性命丢失，不再具有生存能力。同样地，系统的生存性也是随着系统的演化而延续，不具有演化能力的系统其生存能力也是暂时的。

因此，类比于生物体，信息系统在漫长的进化过程中，如何适应各种恶意攻击事件、突发意外事故，如何提高自身的演化能力来适应变化的环境，对这些问题的深入研究，是加强信息系统安全的有效手段，尤其是增强关键领域信息系统生存能力必须面临的有效方法。

本书将面向提高信息系统生存能力的目标，着重研究增强信息

系统生存能力的相关技术和相关算法。尤其是在前人的研究成果的基础上，对信息系统的生存性增强技术做了一个有效的梳理，并对系统生命周期中非常关注的生存性分析技术以及重配置技术进行了深入的研究。这些研究，无论在理论上还是实用上，都取得了一定的突破，对于有效保障开放环境下的信息系统安全具有较好的实用性。

1.2 网络信息系统可生存性的研究现状

正因为网络信息系统生存性概念具有丰富的内涵和不同的安全理念，而且信息系统生存性的研究与关键信息基础设施保护紧密相连，因而引起了广泛关注。无论是在国际还是在国内，关注的部门也越来越多，投入的资金、研究的队伍也越来越大[7, 8]。

对生存性的研究最早源于海军战船在遭遇持续的损害时，如何阻止其沉没；而当轮船下沉时，如何挽救船员的生命。在一战和二战时，研究开始细化，研究领域也延伸到了航空领域。20 世纪 60 年代末，美国军方标准正式定义生存性是指系统为完成其任务抗恶劣环境的能力。目前生存性的研究主要集中在汽车、建筑、战争、电信等领域。网络信息系统的生存性研究相对较新，信息系统的生存性概念由 Barnes 等人于 1993 年首次提出。

目前，研究人员在充分吸收包括容错、QoS、可靠性等多个领域的研究成果的基础上，对网络信息系统的生存理论及技术展开了大量研究。从目前的文献来看，研究重点主要体现在以下几个方面：对信息系统生存性概念的理解和认识，给出了一些定义和描述[9~11]；信息系统生存性分析技术研究[12~14]；信息系统存活性

的度量方法研究[15, 16]；可生存信息系统的设计[17]等。人们在不断寻求开放互联网络环境下的容错（Fault Tolerance）、容入侵（Intru-sion Tolerance）、容攻击（Attack Tolerance）的解决方案过程中，逐渐形成了网络系统生存性研究的理论和技术框架，为后续的研究奠定了坚实的基础。

1.2.1 网络信息系统生存性概念

虽然生存性概念已经广泛应用在军事领域[18]或电信领域[19]，但是由于信息系统的复杂性，使得信息系统生存性概念在很长一段时间内没有一个统一的标准。而因为信息系统和武器系统等传统行业领域存在巨大差异，将以往军事领域或者电信领域的生存性概念应用于信息系统将存在着缺陷。CMU/SEI 研究小组给出的定义是：可生存性是指在遭受攻击、故障或意外事故时，系统能够及时地完成其关键任务的能力。1997 年 Ellison[20]给出了针对信息系统的生存性定义，指出了信息系统生存性包含的若干基本概念，如生存性涉及的攻击等事件、关键服务以及实时性等。这个定义在日后的研究中被广泛引用。不少学者在 Ellison 定义的基础上，拓展了信息系统的生存性定义，如 Moitra[21]认为生存性是系统能抵抗攻击以及被攻击后仍能提供服务的程度；Wilson[22]认为系统生存性是指在确定的故障等事件下，系统仍能保持工作状态的能力。

可生存性的中心思想是即使在遭受入侵后，或者系统的重要部分遭受到损害或摧毁时，系统依然能够完成任务，并具有在一定的时间内修复被损坏服务的能力。需要注意的是，可生存的是系统的服务而不是系统本身。响应时间（及时性）是可生存性的一个非常重要的指标，服务应该在系统要求或者用户所期望的时间内可用。攻击、故障或意外事故代表着所有潜在的对系统有着威胁的事件。

可生存系统并不是特别着重于如何区分这些事件，重点在于如何去分辨这些事件给系统带来的不同的影响。另外，系统在继续提供服务的同时一定要保证系统的基本属性，比如数据完整性、机密性和可用性，并且网络性能的下降不应该被用户觉察到。如果系统不能保证这些属性，即使系统能够继续工作，也不认为该系统具有可生存性。

上述定义虽然给出了信息系统生存性的定性概念，但都缺乏具体的性能指标用于判定系统的生存性。Knight[23]认为生存性是系统的一个重要特征，而且这个特征是可以度量的，他详细给出了一个生存性系统必须满足哪些必要的特征。这种利用各种规范来定义生存性的方式有利于生存性的评价和定量分析。杨超[24]在 Knight 的基础上利用一个 8 元组对系统的可生存性给出了形式化定义。Westmark[25]对各种生存性定义进行了归纳总结，将网络系统的生存性定义为包含系统、威胁、自适应性、服务可持续性和实时性等 5 个关键部分。基于这 5 个部分来定义信息系统的生存性将有助于度量生存力。

信息系统存活性的描述性以及形式化的定义，使得定性或定量评估网络信息系统的可生存性成为了可能，同时也为增强信息系统的生存能力指明了方向。

1.2.2 生存性分析

生存性管理不仅仅强调对系统的服务和数据的保护，同时还提高了系统识别、抗击攻击的能力，最后可以恢复受损的服务和资源。而信息系统的生存性管理离不开系统的生存性分析。与安全性分析相比，网络信息系统的生存性分析所涉及的故障类型与脆弱性要广泛得多[26, 27]，因此进行网络系统的生存性评估的难度也远远大于安

全性评估。CERT Coordination Center 提出了网络生存性分析（Survivable Nerwork Analysis，SNA）方法，用于评估现有系统的生存性能，从而提高系统在遭受危险时的生存能力。后来很多学者融入了传统的安全性评估方法，提出了基于攻击状态图的方法来分析系统忍受攻击的能力[28]，使用故障注入的方法[29, 30]，将故障及入侵事件注入系统模型中，从服务抵抗这些故障的能力来进行生存性分析。这些方法存在一个前提，即故障及入侵的情况都是已知的，由此计算的结果无法让人信服。

文献[16]借助于配置的概念，将系统服务甚至整个系统的故障归结到原子服务（某个硬件、软件或它们的组合）中去，简化了复杂变化的攻击及入侵情况，将整个系统视作层次化的结构，从而给出了一种服务可生存性的定量表达。

鉴于生存性分析在评估系统生存能力上的重要性以及生存性分析方法的缺乏，本书将在第 4 章，提出一种全面的生存性分析方法，即从系统自身体系结构、系统遭受的外部环境的变化、系统在遭受危险时呈现的状态这三个方面来全面评估当前系统的生存能力，最后还针对系统的演化特征，提出了一种基于演化过程的生存性分析思路，为后续生存性增强提供了强有力的依据。

1.2.3 生存性度量

由于目前很多生存性方法仅仅给出了定性的生存性评估，对于一些比较关键且敏感的系统，用户可能需要确切地知道系统生存程度的具体值。Knight 和 Sullivan[31]提出了一种度量网络系统可生存性的方法，该方法将系统的存活性分析过程形式化地描述了出来，有助于加深理解系统存活性的影响因素。网络系统的可生存需求以一个四元组{E，R，P，M}来表示，符合此需求的网络系统是可生