INTRUSION-TOLERANT METHODS WITH APPLICATIONS

容忍入侵方法与应用

郭渊博　王超　著
马建峰　审

国防工业出版社
National Defense Industry Press

INTRUSION-TOLERANT METHODS WITH APPLICATIONS

容忍入侵方法与应用

郭渊博　王超　著
马建峰　审

国防工业出版社
National Defense Industry Press

内 容 简 介

本书系统介绍了容忍入侵系统模型、关键技术和应用等方面的内容。提出了面向服务的容忍入侵模型和系统架构，给出了容忍入侵的可信第三方系统设计方案并进行了形式化描述和规格说明，提出了综合使用“先应式入侵响应”+“数据破坏隔离”的容忍入侵响应模型，建立了容忍入侵系统的广义随机 Petri 网模型；研究了进行容忍入侵系统应用设计时面临的现实问题，给出了基于通用攻击结构的秘密共享设计方案和异步先应式秘密共享方法；提出了多重驱动的自适应重配置容忍入侵安全通信模型，给出了入侵检测与容忍入侵相结合的密码协议安全运行防护方法，提出了基于 Tornado 码的客户—服务器工作模式的分布式容忍入侵数据存储方案，研究了基于规范的容忍入侵中间件方法并在开源的 J2EE 应用服务器 JBoss 中实现了对容忍入侵的功能支持。

本书针对有计算机、通信、密码学技术基础的中、高级读者，适合从事网络信息安全理论研究、工程应用、项目管理人员，以及高校信息安全、计算机、通信等专业高年级本科生和研究生参考使用。

图书在版编目(CIP)数据

容忍入侵方法与应用 / 郭渊博，王超著. —北京：国防工业出版社，2010.5

ISBN 978-7-118-06776-7

Ⅰ. ①容… Ⅱ. ①郭… ②王… Ⅲ. ①计算机网络－安全技术 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2010)第 066756 号

国防工业出版社出版发行

（北京市海淀区紫竹院南路 23 号　邮政编码 100048）

国防工业出版社印刷厂印刷

新华书店经售

*

开本 710×960　1/16　印张 16　字数 265 千字

2010 年 5 月第 1 版第 1 次印刷　印数 1—4000 册　定价 39.00 元

（本书如有印装错误，我社负责调换）

国防书店：(010)68428422　　发行邮购：(010)68414474

发行传真：(010)68411535　　发行业务：(010)68472764

前　言

在信息安全研究领域，尽管人们已经开发了许多安全技术来防止攻击者对系统的破坏，但由于网络的开放性以及攻击技术的快速传播性，使得想开发出绝对安全的信息系统是不可能的。容忍入侵是一种融合了密码技术和容错技术的安全技术，是实现信息可生存性的重要手段。传统的安全技术更多强调如何保护系统以使之免受入侵；而容忍入侵更强调了即使系统的某些部分已经受到攻击者破坏或被攻击者成功控制时，系统如何继续对外提供服务，并保证系统所要求的安全特性。

本书在国家863项目“基于规范的容忍入侵中间件关键技术与平台(2007AA01Z405)”和国家自然科学基金项目(60503012，60842006)等的资助下，研究了容忍入侵设计方法与应用两方面的内容，提出了一种面向服务的容忍入侵模型，研究了实施容忍入侵方法所涉及的两项关键技术——秘密共享和安全群组通信，给出了一种容忍入侵的可信第三方系统设计，提出了容忍入侵的入侵响应模型，研究了容忍入侵系统服务可用性及其量化分析方法，讨论了容忍入侵方法在安全通信系统、密码协议系统、CA系统、数据存储系统、应用服务器中间件等领域的应用。主要内容如下：

(1)提出了一种面向服务的容忍入侵模型，给出了其系统架构，讨论了其中所涉及的一些重要技术。在该模型基础上，设计了一个以容忍入侵为中心，结合防火墙与访问控制系统、分布式入侵检测系统等技术的，具有反馈交互的三层细粒度动态纵深防御安全体系结构。

(2)针对容忍入侵方法在进行系统设计时，很难根据系统配置及安全需求确定存取结构，进而无法直接应用基于存取结构的秘密共享的问题，借助集合论的概念研究设计了一种基于通用攻击结构的秘密共享方案；针对不具同步时钟模型且主机间不存在可靠通信通道的现实分布式容忍入侵系统应用场合，通过引入可由协议事件和系统中各主机本地时钟双重驱动的时间片的概念，定义了异步模型中先应式秘密共享的运行状态及其转换过程，给出了异步环境中一种

实用有效的先应式秘密共享方法。

(3)结合可验证秘密共享技术和知识证明技术,设计了一个计算安全且具有容忍入侵功能的可信第三方系统方案,还使用面向对象的形式化规格说明语言 Object Z 对所设计的容忍入侵可信第三方系统进行了形式化描述和规格说明。

(4)提出了一种容忍入侵的入侵响应模型,利用基于入侵攻击图的"先应式"入侵响应技术,在检测到入侵行为的前期进行防御,在入侵者的攻击目标完全实现之前给予响应,尽量阻止攻击目标的实现;利用基于数据破坏隔离技术的事后入侵响应技术作为第二道防线,即使在前期的入侵响应失效、关键数据已经被破坏的情况下,迅速进行破坏隔离与恢复,保证系统继续向用户提供不间断的服务。还建立了一个入侵者与入侵检测及响应系统之间的博弈模型,推导出了博弈双方的最优混合策略,得到了模型中各方参与者的优化问题的解并给出了相应的物理解释。

(5)分析了容忍入侵系统安全性评估的可能性和必要性。根据容忍入侵系统在入侵到来时可能发生的状态变化,提出了基于系统状态转移图模型的容忍入侵系统安全性分析方法。基于容忍入侵系统所采用的冗余技术,建立了系统的广义随机 Petri 网(GSPN)模型,分别从机密性、完整性、可用性等不同方面定量分析容忍入侵系统的安全性。

(6)针对传统安全通信系统采用静态安全策略,从而缺乏容忍入侵能力和高效性的问题,提出了一种多重驱动的自适应重配置安全通信模型,基于安全策略的冗余和多样性技术,能够根据系统当前安全态势情况及系统资源状态和系统配置变化、用户使用偏好等因素,动态自适应地调整每个会话的安全策略,以便在攻击和系统配置变化的情况下动态调整系统状态。还讨论了模型中的一些关键技术,设计了基于 D-S 证据推理方法的系统安全态势评估模型,和基于层次分析方法的安全策略决策模型。

(7)针对现有对密码协议安全运行防护手段不足的问题,基于纵深防御策略,给出了一种结合入侵检测与入侵容忍密码协议安全运行防护方法;设计了具有特征入侵检测和异常入侵检测两种模式的混合入侵检测模型,其中入侵行为特征的判断采用有限状态自动机方法进行;给出了一种基于参数自适应的密码协议入侵容忍调整策略;性能测试表明了方案的有效性。

(8)提出了一种基于 Tornado 码的客户—服务器工作模式的分布式容忍入侵数据存储方案。通过构造编码后数据分块的 Hash 值级连,可实现 Byzantine

环境中存储数据的完整性保护;采用对称加密技术和分布式门限加密技术相结合的分布式存储系统保密方案,可在不对系统带来额外密钥管理负担的情况下实现对所存储数据的机密性保护;基于容忍入侵可信第三方模型的读/写句柄授权与认证机制,可在某些服务器被 Byzantine 攻击者成功控制时,保证客户接收到正确的句柄,并可防止非授权客户伪造句柄。

(9)针对现有技术在构建容忍入侵应用系统时存在的"头疼医头、脚疼医脚"、针对不同的业务类型要进行不同的个性化设计和开发的问题,研究了基于规范的容忍入侵中间件方法,并在一个开源的 J2EE 应用服务器 JBoss 中实现了对容忍入侵功能的支持,实现了用户应用的业务逻辑与容忍入侵等应用所依赖的非功能性服务分离。

本书是作者及所指导的研究生们近年来致力于容忍入侵方法与应用研究所取得成果的提炼和总结。第 6 章由王超完成,其余章节由郭渊博完成。本书可作为高等院校相关专业研究生和高年级本科生的教材或学习参考用书,也可供从事信息安全防护系统研究与研制人员参考使用。

在本书即将付梓之际,特别感谢我们博士期间共同的导师——西安电子科技大学计算机学院院长马建峰教授,我们在容忍入侵领域的研究都是在马老师的指导、关心和支持下取得的,马老师还仔细审阅了全书并提出了很多宝贵意见。还要感谢解放军信息工程大学副校长王亚弟教授和武汉大学张焕国教授,他们二位分别是本书第一作者的硕士导师和博士后指导老师,感谢他们多年如一日地指导、帮助和教诲。国防工业出版社电子信息图书事业部陈洁老师为本书的出版付出了很多辛苦的劳动,在此一并表示感谢。

容忍入侵是一个正在发展的研究领域,加之作者水平所限,书中难免有不足之处,敬请专家、读者批评指正。

目　录

第1章 绪 论

容忍入侵是一种融合了密码技术和容错技术的全新网络安全技术，它强调了即使系统的某些部分已经受到攻击者破坏或被攻击者成功控制，系统如何继续对外提供服务，并保证系统中关键数据的秘密性和完整性。显然，这种新型安全技术更符合当前信息可生存性的需求，是一种很有前途的安全防护手段。本章从分析现有网络安全防护技术的不足入手，讨论了容忍入侵技术出现的必然性；然后对容忍入侵的概念、现状和所存在问题进行了介绍。

1.1 容忍入侵技术的引入

网络安全技术大体经历了三个发展阶段：以“保护”为目的的第一代网络安全技术、以“保障”为目的的第二代网络安全技术和以“生存”为目的的第三代网络安全技术。

第一代网络安全技术通过划分明确的网络边界，利用各种保护和隔离的技术手段，如用户鉴别和认证、访问控制、权限管理以及信息加解密等技术，试图在网络边界上阻止非法入侵，达到信息安全的目的。第一代网络安全技术解决了很多安全问题，但并不是在所有情况下都有效：由于无法清晰地划分和控制网络边界，第一代网络安全技术对一些攻击行为如计算机病毒、用户身份冒用、系统漏洞攻击等就显得无能为力；传统的安全机制，如认证协议、数字签名和加密/解密等技术虽然在实现安全方面发挥了重要的作用，但是这些安全机制在实现网络系统的安全保护方面还是不够的，特别是对于诸如 DoS（Denial-of-Service）之类的攻击行为并不能发挥有效作用。在第一代安全技术中，通常假设系统中的一个或多个部件是安全的，即从未被攻击者所控制。显然，在安全关键的敏感应

用环境中,这种做法很不切合实际。无论保护措施有多严密,但由于针对安全关键信息系统的攻击手段和技术的不断发展,保护安全关键系统上的关键部件完全不受干扰、破坏或者入侵,几乎是不可能的。

第二代网络安全技术以检测技术为核心,以恢复技术为后盾,融合了保护、检测、响应、恢复四大技术。众所周知,攻击 + 脆弱性 = 入侵。第二代安全技术也正是从防止脆弱性和抗攻击两个方面展开的。防止脆弱性的方法主要是在系统配置或使用之前进行严格测试,试图指出并修正系统部件中存在的脆弱点;或者根据系统配置之后所发现的针对系统的成功入侵,对系统加补丁。尽管这种方法在处理许多攻击时都很有效,然而经验表明,大多数应用系统中仍然存在着相当数量的脆弱点,特别是对于网络化的分布式系统,由于其部件间可能的复杂交互,脆弱点的防止会变得尤其困难。

入侵检测系统(IDS)主要通过对网络流量或主机运行状态的检测来发现对系统资源的非授权访问与破坏行为,并对各种恶意入侵做出响应。在对付针对信息系统的安全威胁方面,入侵检测系统起到了非常重要的作用,然而也有自己的缺陷,如通常只关注一些已知的和定义好的攻击,而且在性能上存在着高误报率、漏报率、不精确的报告、攻击和检测之间的时间延迟等问题。另一方面,即使恶意攻击能够被检测出来,系统管理员仍要面临两大难题:一是如何确定入侵所引起的破坏;二是如何将系统恢复到安全状态。由于入侵者一般都会在入侵后修改系统日志文件,擦去入侵的痕迹,使得确定入侵所引起破坏的位置更为困难。而系统恢复需要有干净的备份,还要重新初始化系统、从备份中恢复信息等操作。此外,诊断的困难性也增加了恢复的困难性,而恢复本身通常需要较长的时间才能完成,这无疑也会降低系统的可用性,甚至可能引起安全备份与入侵发生期间所建立数据的不一致。

防火墙尽管可以较有效地抵御网络外部的入侵攻击,但对于来自网络内部的攻击却显得无能为力。对于信息系统而言,一个存在缺陷的安全措施在系统工作过程中不可能非常有效和可靠地提供安全保护。更危险的是,这样的系统会给人们造成一个“安全”的错觉。显然,将这样的系统用于安全关键的场合,会造成十分严重的后果。

第三代网络安全技术是一种信息“可生存技术”,Carnegie Mellon 大学的学者给这种“可生存技术”下了一个定义:所谓“可生存技术”,就是系统在攻击、故障和意外事故已发生的情况下,在限定时间内完成使命的能力。它假设不能完全正确地检测对系统的入侵行为,当入侵和故障突然发生时,能够利用“容忍”

技术来解决系统的“可生存”问题,以确保信息系统的保密性、完整性、真实性、可用性和不可否认性等特性。当前,在实现系统的可生存性防护方面,容错技术,特别是远地备份技术和 Byzantine 容错技术等,都发挥了很大的作用。

然而,容错技术不能解决全部的信息可生存问题:

(1)并不是所有的破坏都是由故障和意外导致的,例如攻击者的有意攻击,而容错理论并不是针对攻击专门设计的。

(2)并不是所有攻击都表现为信息和系统的破坏,例如关键性数据的篡改等,只要这种攻击本身不构成一种显式的错误,容错就无法解决问题。

(3)部件故障是随机发生的,而攻击却是有预谋的,这比随机故障更难预防。

(4)最重要的是,单纯的备份使得攻击者的攻击点从备份前的一台主机变成多台主机,这不仅不能增强系统中敏感数据的安全性,相反倒增加了攻击者成功的机会。

容忍入侵是一种融合了密码技术和容错技术的全新网络安全技术,它强调了系统的某些部分即使已经受到攻击者破坏或被攻击者成功控制时,系统如何继续对外提供服务,并保证系统中关键数据的秘密性和完整性。显然,这种新型安全技术更符合当前信息可生存性的需求,是一种很有前途的安全防护手段。

与传统网络安全方法的思路不同,容忍入侵的概念承认系统中脆弱点的存在,并假定随着时间的发展,其中某些脆弱点可能会被入侵者利用。其设计目标就是使得系统在受到攻击时,即使系统的某些部分或部件已经受到破坏,或者被恶意攻击者操控,系统仍能够触发一些防止这些入侵或破坏造成系统安全失效的机制,从而仍然能够对外继续维护正常运行(可能是以降级的模式),提供核心或系统的基本服务,以保证系统的基本功能。由于这种方法在考虑对系统可用性保护的同时,还考虑了对系统数据和服务的机密性与完整性等安全属性的保护,因此能够达到防患于未然的目的,被称作是系统安全防护的最后一道防线。

1.2 容忍入侵的基本概念与现状

从某种意义上讲,入侵可以看做一种蓄意故障,这种故障将引起系统部件的某种错误,使得系统进入某种错误状态,从而引起系统中数据和服务的机密性、完整性以及可用性等安全属性的失败,即攻击 + 漏洞 = 入侵→错误(故障)→失

败。因此从本质上讲,容忍入侵方法可看做一个容忍和避免故障、以及实现安全的问题,其对入侵的检测和响应类似于容错系统中对于系统故障的诊断与处理。

容忍入侵主要考虑的是在入侵存在的情况下系统的生存能力。它总是假定系统存在一些已知的和未知的脆弱点,并且这些脆弱点总是可为攻击者所利用。其主要思想就是利用分布式系统中的硬件或者软件容错技术屏蔽任何入侵或者攻击对系统功能的影响,保证系统关键功能的安全性和连续性。因此,在容忍入侵机制的保护下,即使入侵活动成功发生,系统也可为用户提供所需的基本服务。

根据系统或者信息可生存性的假设,任何系统部件都可能遭到入侵。在容忍入侵模型中,假定入侵总是会引起系统部件发生故障。故障的表现是系统功能或服务的错误,其中,可能的故障模式有以下几种:

(1)停止工作:系统部件不可用(崩溃或拒绝服务等)。

(2)对称故障:例如,对数据存储部件的攻击使得该部件产生无效或者恶意的信息。

(3)Byzantine 故障:部件表现出任意行为(包括正常行为,可由攻击者选择)。

其中,出现 Byzantine 故障的系统部件的行为是不可预测的,因此最难以处理。

容忍入侵关注的焦点不再是所构建的系统是否充分安全、入侵活动发生与否、发生的具体原因或实施入侵时所采用的具体方法等,而是关注入侵对系统功能的影响。其对入侵的处理就是屏蔽,并在入侵对系统造成更大影响之前消除其危害并恢复系统。这就好比建立起了一道类似于人体免疫系统的屏障,其作用在于保证系统在具有安全风险威胁的环境中,依然能够最大限度地保障系统的基本功能。在遭到攻击时减少损失,保证系统生存。虽然理论上无法完全预防系统受到破坏,但是一旦系统被攻击,则在攻击对系统性能造成很大危害之前能够尽早发觉,并采取相应的防护和补救措施。

图 1-1 表示的是具有容忍入侵防线的系统安全防护过程。其中图 1-1(a)表示系统具有许多潜在的脆弱点;图 1-1(b)表示通过使用安全工程或形式化方法避免了某些脆弱点(安全专用系统);图 1-1(c)表示通过系统测试、分析等方法消除了一些已知脆弱点;图 1-1(d)表示通过入侵检测等防护技术检测并阻塞掉一些已知脆弱点;图 1-1(e)表示通过容忍入侵手段,对经过上述安全措施之后系统尚存的脆弱点进行屏蔽后的结果。从该图中,可以看出容忍入侵

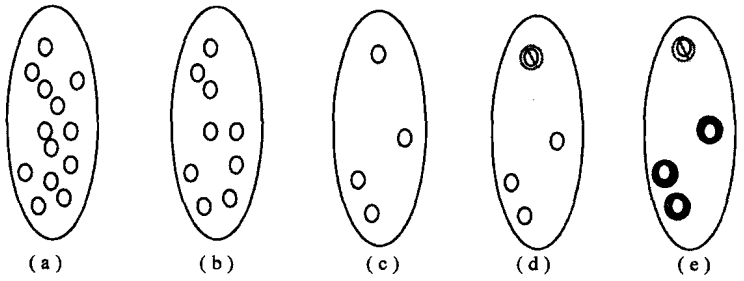

图1－1 具有容忍入侵防线的系统安全防护过程

方法在系统防护中的作用。

国际上容忍入侵相关的研究工作始于20世纪80年代中后期。Dobson和Randell在1986年的一篇论文中提出了利用不安全并且不可靠的部件来构建安全可靠的系统的方法[1]，这实际上是容忍入侵的思想雏形；Fraga和Powell在其论文中正式提到了容忍入侵(intrusion tolerance)的术语并一直被延用至今[2]；其后，Deswarte、Blain和Fabre等人提出了基于分割+分散(fragmentation-scattering technique)的方法实现容忍入侵的思路[3]。在此之后，容忍入侵的思想一直没有得到业内人士太多关注。直到20世纪90年代后期，随着分布式密码学研究的深入，特别是秘密共享和门限密码学方面研究的逐渐成熟与完善，再加上分布式网络应用系统的大量涌现，容忍入侵的理论、方法与应用又开始进入人们视野，开始活跃并且逐渐成为信息安全业内人士关注的一个焦点。

在美国国防部高级研究计划署(DARPA)的OASIS(Organically Assured and Survivable Information System)计划支持下，Stanford大学的ITTC项目(Intrusion Tolerance via Threshold Cryptography)首开基于门限密码的容忍入侵技术研究之先河。其后，美国Cornell大学在NSF(美国自然科学基金)资助下相继推出了基于秘密共享方法的容忍入侵在线证书权威服务COCA[4]以及强健的秘密数据分布服务CODEX[5]。

除了美国DARPA和NSF计划在容忍入侵研究领域进行了大量资助以外，欧盟的MAFTIA高级研究计划也有部分相关资助。就目前的研究现状而言，无论是在算法研究还是模型研究方面，容忍入侵方法的研究在10年多的时间里已取得了许多重要的研究成果，但在整体理论和所涉及的各个环节中都仍有一些问题尚待突破，且完善或功能完整的原型系统或产品开发尚不多，距离实用化尚有一段距离。由于该领域的理论研究至今仍缺少系统化的成果，因此想要给出

系统的现状分析和趋势分析比较困难。根据我们的理解，可将该领域的理论研究划分为以下几个方面：基于门限密码/秘密共享的系统容忍入侵防护方法、基于 COTS 构件的容忍入侵系统构建方法、容忍入侵系统中的相关算法或协议研究、“纵深防御”的容忍入侵安全防御方法等。

(1)基于门限密码/秘密共享的系统容忍入侵防护，特别是对特定服务和数据，如 CA、口令认证服务、密钥交换服务、文件服务、DNS 服务、路由服务与重要数据保护服务等的容忍入侵保护，包括相应的协议设计及性能评估等。

(2)使用监控、接受测试以及冗余等容错手段，实现基于 COTS 构件的容忍入侵应用系统，如容忍入侵的 Web 服务器系统和数据库管理系统等，并实现基于模型的容忍入侵系统运行过程描述。

(3)容忍入侵系统，实现和运行中的一些细节问题研究，如 Internet 等异步模型中容忍入侵方法的实现问题，异步环境中门限密码/秘密共享方案的设计与实现问题和异步 Byzantine 系统协商问题，以及秘密份额的动态重分发、容忍入侵系统的定量或定性评估等。

(4)综合运用各种容错策略和系统可重配置机制，结合安全通信以及基于入侵检测、入侵遏制、错误处理、损坏评估和可信恢复等手段和机制，构建“纵深防御”的容忍入侵安全防线。例如，Pennsylvania 州立大学的 ITDB 项目的目的就是通过多阶段的容忍入侵实现纵深防御功能，开发出能够容忍入侵的数据库管理系统(DBMS)。其主要思路就是综合事务级的入侵检测、入侵隔离、多阶段损坏定位和限制以及自稳定性等技术或手段，达到容忍入侵的目的。由美国 BBN 公司、Illinois 大学、Maryland 大学和波音公司共同承担的研究项目 ITUA 旨在通过一种先进的冗余管理技术和动态资源分配技术，针对有计划的攻击或按部就班的攻击产生一种对攻击者而言无法预测的资源调配和复杂的响应，使攻击者很难进行攻击计划或协作下一步的攻击。但 ITUA 的不足之处在于只能够针对有计划或按部就班的攻击，无法防御未定义的攻击或现有攻击的变种，且没有关注系统的机密性等安全属性。

在实用系统开发和应用方面，国际也出现了一些针对特定应用系统的容忍入侵产品或原型，这些系统普遍使用了基于门限密码学(秘密共享)或复制冗余的容侵防护策略。在无线安全领域，容忍入侵方法也已经发挥了重要的作用，例如在 Ad hoc 和无线传感器网络安全防护体系中普遍应用的分布式容忍入侵 CA 系统，以及容忍入侵的路由技术等。

国内的研究者也较早关注了容忍入侵的研究方向。近几年来，中国科学院