ISCCF

第十七届全国信息保密学术会议

（IS2007）

论 文 集

中国计算机学会信息保密专业委员会 编

金城出版社
GOLD WALL PRESS

ISCCF

第十七届全国信息保密学术会议
(IS2007)
论 文 集

中国计算机学会信息保密专业委员会 编

金城出版社
GOLD WALL PRESS

图书在版编目（CIP）数据

第十七届全国信息保密学术会议（IS2007）论文集/中国计算机学会信息保密专业委员会编. —北京：金城出版社，2007. 6

ISBN 978－7－80084－985－5

Ⅰ. 第… Ⅱ. 中… Ⅲ. 信息系统－安全技术－文集
Ⅳ. TP309. 53

中国版本图书馆 CIP 数据核字（2007）第 123789 号

第十七届全国信息保密学术会议(IS2007)论文集

作　　者　中国计算机学会信息保密专业委员会编
责任编辑　陆建伟
开　　本　787×1092 毫米　1/16
印　　张　25
字　　数　500 千字
版　　次　2007 年 8 月第 1 版　2007 年 8 月第 1 次印刷
印　　刷　北京金瀑印刷有限责任公司印刷
书　　号　ISBN 978－7－80084－985－5
定　　价　80.00 元

出版发行　金城出版社 北京市朝阳区和平街 11 区 37 号楼　邮编：100013
发 行 部　(010)84254364
编 辑 部　(010)64210080
总 编 室　(010)64228516
网　　址　http://www.jccb.com
电子邮箱　jinchengchuban@163.com
法律顾问　陈鹰律师事务所　(010)64970501

前　言

第十七届全国信息保密学术会议(IS2007)于二零零七年九月在湖北省襄樊市召开。经有关专家评审，从来自全国各科研开发单位、大专院校和管理部门的论文中选出六十篇编入此本《第十七届全国信息保密学术会议论文集》，供信息安全保密专业人员交流。

在此向热情为本次学术年会投稿的全体作者、为此论文集出版提供大力支持的专家、学者和湖北省国家保密局、沈阳东软软件股份有限公司、北京鼎普科技有限公司表示感谢。

中国计算机学会信息保密专业委员会

秘　书　组

二零零七年九月

目录

Contents

面向服务的层次化入侵容忍模型设计

刘红军[1] 黄遵国[2]
(1、2. 国防科学技术大学计算机学院，湖南长沙，410073)

摘 要： 提出了面向服务的层次化入侵容忍模型，将模型设计成五个层次，并细化了各个层次的设计。其中入侵防御层能灵活应用当前的安全工具，有很强的实用性，同时能根据网络环境和需要保护的信息动态调整安全策略，提高了系统的适应性；服务隔离层采用虚拟技术虚拟服务将请求与服务隔离，增强了系统的抗攻击性；关键服务层将需要保护的服务和信息独立出来，增强了保护的针对性；入侵诊断层引入数据融合和数据挖掘技术进行事件关联，提高了系统抵抗未知攻击的能力；最后应急响应层根据系统实时状况采取自适应的响应策略，并能评估响应效果从而学习调整响应策略，提高了响应的灵活性。

关键词： 入侵容忍；虚拟技术；应急响应

Layered Model Design of Intrusion Tolerance on Service

Liu Hong-jun[1] Huang Zun-guo[2]
(1、2. School of Computer Science, National University of Defense Technology, Changsha, Hunan 410073, China)

Abstract: This paper brings forward a five layered model of intrusion tolerance on service, and describes the layers in detail respectively. Among them, the intrusion prevention layer could flexibly use the current security tools to protect the system with higher availability. Mean-

while it can adjust the security policies according to the network environment and the protected information with higher adaptability. The services isolation layer adopts the virtual technology to simulate services so that the requests and the services are isolated and the ability of resisting attack is strengthened. The key service layer collects all the services and information that needs to protect, thus it enhances the pertinence of protecting. The intrusion diagnosis layer brings in the technologies of data fusing and data mining to associate security affairs, as a result it improves the ability to resist the unknown attack. Finally the layer of intrusion response not only takes self-adaptively policy to respond according to the system's real time situation, but also it can study and adjust the response policies by evaluating response effect, so that it increases the flexibility of response.

Key words: intrusion tolerant; virtual technology; emergency respond

引言

“入侵容忍”最早出现在1982年，但相关研究工作是最近几年才兴起的，成为了网络安全技术发展的新方向。入侵容忍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。其目标是保证即使系统的某些部分或部件由于攻击而受到破坏，或者被恶意攻击者操控时，该系统仍能够触发一些防止这些入侵造成系统安全失效的机制，从而能够对外继续维护正常运行（可能是以降级的方式），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中的最后一道防线。

入侵容忍的主要研究内容有三点：第一是专注于研究对服务产生威胁的事件的入侵触发器，第二是研究如何将容错理论研究中的优秀成果应用到入侵容忍理论，第三是利用研究所得的容侵理论和技术构建一个新的网络安全信息系统。由于网络中的信息交换大多是通过服务来实现的，本文就从层次方面提出并设计了面向服务的入侵容忍系统模型，它能较好地满足可用性、完整性、可控性和自适应性的要求。

1 相关研究

近几年来，以美国DARPA的OASIS计划和NSF一系列计划以及欧盟MAFTIA高级研究计划资助为主体，国外学术界对容忍入侵的相关问题展开了大量研究，取得了许多丰富的成果。

在入侵容忍系统方面，研究了特别是基于门限密码、秘密共享的容忍入侵系统实现和运行中的一些细节问题，如 Internet 等异步结构模型中容忍入侵方法的实现问题，包括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 系统协商问等，以及抗自适应攻击的门限密码方案、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。同时还研究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、入侵遏制和错误处理等手段和机制，构建“纵深防御”的容忍入侵安全防线[1]。

在国内也开始了这方面的思考和研究。其中，彭文灵、王丽娜等提出了基于角色访问控制的入侵容忍机制研究[2]；伍忠东、谢维信等提出了一种安全增强的基于椭圆曲线可验证门限签名方案[3]；刘海蛟、荆继武等提出了一种入侵容忍的资料库[4]；崔竞松、彭文灵等分别提出了一种并行容忍入侵系统研究模型[5]和基于秘密共享方法的容忍入侵软件系统模型[6]；朱建明、史庭俊等提出了基于秘密共享的多代理容忍入侵系统模型以及容忍入侵的数据库系统模型等[7]；王超和马建峰对三种类型的容忍入侵系统，即资源冗余、完全信息冗余和部分信息冗余的容忍入侵系统，采用随机 Petri 网模型进行了系统服务的可用性分析[8]。

当前的这些研究中，大多只是应用入侵容忍的思想来解决某个问题，另一些则是基于某种技术来建立入侵容忍系统框架，但是却没有从全局的角度将入侵容忍系统层次化并具体细化各个层次模块。本文正是从这个角度来设计入侵容忍模型，这对整体设计容侵系统和具体细化实现各个子模块有重要的指导意义。

2 入侵容忍模型的建立

随着互联网上入侵活动愈演愈烈，建立所谓“完全安全”系统仅在理论上存在可能性，在实践中根本无法实现或者说是不可行。防御－检测－容侵的多层次安全体系[7]是一种比较理想的系统安全解决之道，但现阶段真正具有实用价值的入侵容忍系统还未出现。因此，入侵容忍系统就必须将多种安全技术通过合理的技术手段有机地结合起来构建纵深防御，使它们互相配合、相互依托、互相促进。

2.1 模型的系统结构

入侵容忍就是对各种各样的网络入侵行为进行处理，如果不对这些入侵行为做出相应的处理，可能会导致系统的某些安全特性受损。入侵容忍处理包括响应、清除、恢复和屏蔽四个过程。要完成这些过程，容忍系统必须具有以下几个基本功能模块[9]：服务监视模块，服务代理模块，系统控制模块，分析模块，策略执行模块和系统备份模块。Dr. Carl[10]等认为入侵容忍系统的组成构件应包括入侵防止、入侵检测、入侵遮蔽、破坏检测、恢复和响应。针对网络服务，本模型将这些模块综合简化成五层，包含入侵防御层、服务隔离层、关键服务层、入侵诊断层和应急响应层。具体模型架构见图 1：

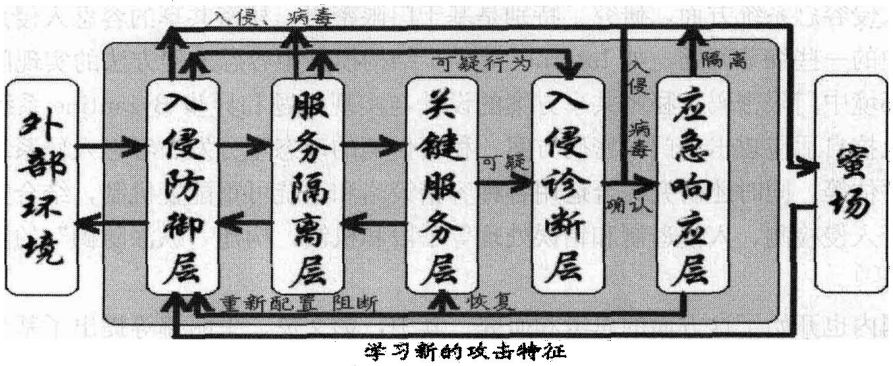

图 1　基于层次的入侵容忍模型

2.2　系统工作原理

整个系统结合已有的安全工具并采用其他安全技术形成了功能相对完备的安全体系。入侵防御层是主机防御的最前线，它负责与外部环境进行交互。该防御层包含了现有的安全工具，如防火墙、防病毒系统等，并对信息初步过滤和根据安全规则阻断攻击。同时它将确认的攻击重定向到蜜场中进行隔离、收集和分析攻击特征，将可疑的攻击行为发送到入侵诊断层对可疑行为进行确认。

服务隔离层采用虚拟技术虚拟服务，在请求和服务间提供了一个隔离带。这个隔离带可以虚拟在不同系统中提供该服务，这就为攻击者提供了错误的扫描信息，提高了抗攻击性，同时入侵者攻击服务就会首先攻击这个虚拟服务层，从而可以将确认的攻击重定向到蜜场，将可疑的攻击行为发送到入侵诊断层进行确认。

关键服务层负责将系统中需要保护的服务和信息集中起来进行管理，同时对外提供服务。该层对用户请求的应答消息将经过服务隔离层的转化后同用户进行交互。

入侵诊断层对可疑的消息序列进行结构分析、功能分析、行为分析等深入分析，通过特征匹配、异常分析等多种模式分析方法对安全事件进行判断，同时采用数据融合、数据挖掘等技术实现预警，提高安全事件的准确性，确认是不是攻击行为，为是否采取应急响应措施提供依据。

应急响应层是系统安全的最后一条防线。它首先对攻击进行风险评估，然后根据威胁的等级执行相应的响应策略，在结束后还可以对响应效果进行评估学习，从而动态的调整响应策略。它还需要同其他安全工具进行协同，如用防火墙对某个连接进行阻断，用杀毒系统进行杀毒等，同时还要根据危害的严重程度对服务采取不同的恢复措施以保证服务的连续性。

蜜场[11]负责集中收集各个服务器的安全威胁。它采用蜜罐技术，将所有的蜜罐均部署在蜜场中，而在服务器中设置一系列的重定向器，若检测到当前的网络数据流是黑客攻击所发起时，通过重定向器将这些流量重定向到蜜场中的某台蜜罐主机上，由蜜场中部署的一系列数据捕获和数据分析工具对黑客攻击行为进行收集和分析，并进一步的监控和研究入侵者的行为，并可以提供对入侵过程的安全审计、离线恢复和取证分析等功能，必要时还可以提供攻击现场的自我保护和隔离功能，从而保护真正服务器的安

全，提高网络的整体安全防护性能。最后它将分析出来的新攻击特征更新到入侵防御层，调整策略，形成了自适应学习过程。

3 模块的具体设计

3.1 入侵防御层模块设计

入侵防御层将访问控制、透明代理、漏洞攻击防御、邮件病毒过滤集为一体，提供整体的立体式网络安全防护。它灵活采用了当前的网络安全工具，可以全面防御常见网络攻击行为的能力，对经过防御系统的所有数据包进行协议解码，对基于操作系统漏洞、协议漏洞和程序漏洞的攻击或者病毒，进行有效防御。具体设计框架见图 2：

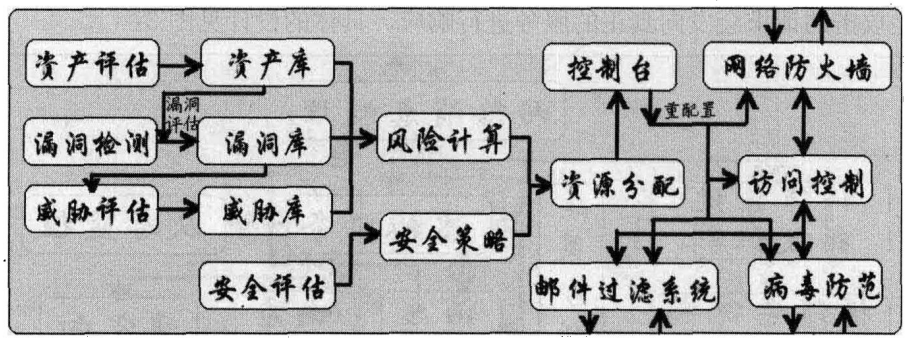

图 2 入侵防御层模块设计

防火墙作为第一道关口，负责控制进入网络的访问控制，以防止不可预测的、潜在破坏的非法入侵。它通过监测、限制、修改跨越防火墙的数据流，尽可能地对外屏蔽网络内部地结构、信息和运行情况，以此来实现内部网络地安全保护。

病毒防范模块通过病毒预警技术、已知与未知病毒识别技术、病毒动态滤杀技术等技术从网络体系的安全性、网络协议的安全性、操作系统的安全性等多个方面加强对计算机病毒的识别、预警以及防治能力，形成基于网络的病毒防治体系。访问控制模块负责判别访问者的标识信息或权限来决定其是否能访问某项资源。

资产评估模块识别并评估关键的信息资产，如数据库及数据文件、系统文件、用户手册、培训材料、操作或支持程序、连续性计划、后备安排和文档信息等，还包括各种服务，如 WWW、SMTP、POP3、FTP、Telnet、DNS、呼叫中心、内部文件服务、网络连接、网络隔离保护、网络管理等等。然后考虑资产的机密性、完整性和可用性等安全属性，采用定性、定量和半定量三种赋值方法，对资产赋值评估后形成一个资产库。

漏洞检测模块非常详细地扫描系统内的安全漏洞，然后进行漏洞评估，就是对每项资产具有的安全漏洞进行分析，对漏洞被利用的难易程度赋值。漏洞评估后形成一个漏洞库，包括漏洞级别及相应解决方案。威胁评估是对资产潜在威胁和可能入侵给出全面的分析，潜在威胁主要是根据每项资产的安全漏洞而引发的安全威胁。通过对威胁发生的可能性和造成后果的严重性来对威胁进行高、中、低三个等级的赋值。通过分析，形

成一个威胁库。风险计算模块利用资产价值、漏洞严重性、威胁可能性以及措施有效性等多个取值计算风险值，通过风险计算，可以形成风险库。然后结合安全评估模块对整个系统进行评估给出的安全策略分配资源，对风险高的威胁，提前对相关事件给予更多的关注和分配更多的资源。这样当相关事件出现时，事件的响应就会更有效。控制台模块根据分析的策略对各种安全工具的规则进行重新配置，保持与新的威胁和新的发展同步，从而保持系统安全的动态性。

3.2 服务隔离层模块设计

服务隔离层模块采用虚拟技术对关键服务进行模拟，同时虚拟出操作系统环境，从而保护真正操作系统中的真实服务。由于虚拟服务会根据用户的请求伪造相应的数据包进行响应，从而可以发现攻击并对其进行跟踪，并将攻击重定向到蜜场收集相应数据。如果不是攻击的请求会发向真正的服务进行响应。具体的设计见图 3：

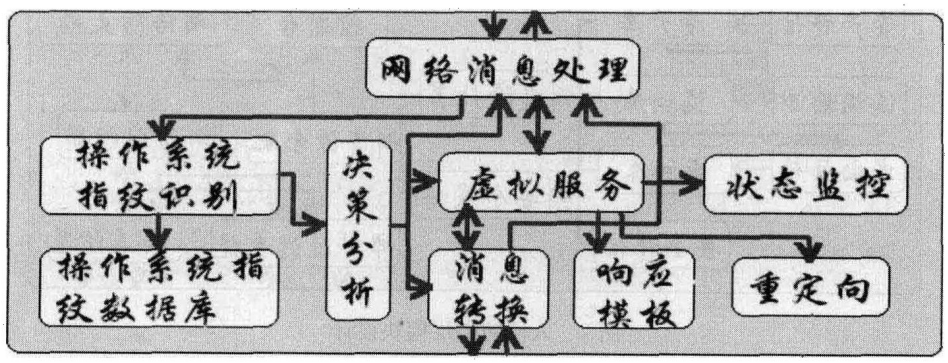

图 3 服务隔离层模块设计

网络消息处理模块负责采集本局域网内其他主机发出的数据包、外部网络发往虚拟服务的数据包以及与外部网络进行交互；操作系统指纹识别模块通过查询指纹数据库分析网络中存在的主机的操作系统类型，并将这些分析的结果定期发送给决策分析模块。

决策分析模块通过分析现有的网络状况，决定将虚拟服务配置成什么样的操作系统，并将配置结果分别通知网络消息处理模块、虚拟服务模块和消息转换模块。虚拟服务模块模拟操作系统、服务进程、协议，它调用状态监控模块监视用户可疑行为，如果发现为攻击，它将调用响应模块创建相应的欺骗包代替真实的网络服务对访问请求进行响应，并将该攻击定向到蜜场；否则它通过消息转换模块将请求发向真正服务，并将服务应答消息发给请求用户。

状态监控模块实时对可疑行为在虚拟环境内部的操作进行监视，防止可疑行为在该系统内肆意破坏，防止真正的入侵者利用该系统对其他系统进行攻击，并将真正的攻击重定向到蜜场进行数据捕获、数据分析和数据控制。如果用户请求不是攻击就将其发送给真正的服务进行应答。这样就能够在遭受攻击的同时还能继续提供服务，因为受攻击的只是虚拟服务。消息转换模块负责将消息格式在虚拟的操作系统和真实的操作系统之间进行转换。

重定向模块的主要功能是按照特定的入侵转移策略将异常网络通信转发至蜜场中进

行监测。在重定向模块的设计和实现过程中，如何在重定向操作发生后尽可能地避免引起入侵者怀疑的问题，是设计需要解决的一个关键问题，李之棠[18]等设计和实现了基于终端（应用层重定向器）的透明通信转发机制用来很好的解决了这个关键问题。

3.3 入侵诊断层模块设计

网络设备、安全设备、应用系统每天都会产生海量的安全事件，这些事件报警中存在着大量的误报，同时对未知病毒、未知网络攻击、未知系统攻击等问题存在漏报，而且对多个安全系统的日志不能进行自动实时审计，这样使得很多安全事件不能及时发现。入侵诊断层模块就专门针对这些问题判断可疑行为和事件是不是攻击，同时应用数据挖掘等技术寻找新的攻击进行预警。具体的设计见图 4：

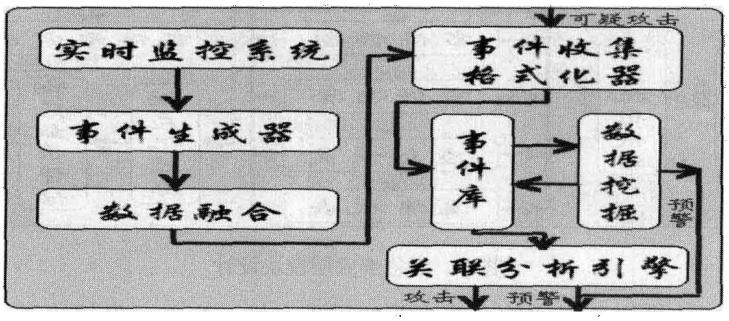

图 4 入侵诊断层模块设计

实时监控系统负责监视信息有没有被修改，操作有无异常，例如一张消费卡刚在上海消费，几乎同时又在北京消费，或者这时间差小于飞机飞过两城市的时间，则这种操作就是异常的，数据是可疑的。又比如，一张卡一般每次只花很少的钱，突然一次花很多的钱；一个商家平常周一只有 10 万营业额，突然本周一上午就超过 50 万，等等。然后将这些异常操作传给事件生成器。事件生成器模块主要是产生原始事件，并把这些事件基于安全策略、入侵检测系统的探头等进行预过滤。

数据融合模块将监控系统产生的数据进行分析处理与汇总，判断可能发生的入侵事件。它分析多个安全事件，从中发现单个安全事件无法确定的攻击，以进一步核实发现的攻击，并为决策支持系统提供入侵报警信息，以提高报警的准确性。

事件收集格式化器模块将对各种格式的原始消息进行过滤和正则化，对不同级别的告警进行整合，形成统一格式的消息，并把结果存入事件库中。事件库主要是存储经过格式化的标准消息、系统状态和一些告警信息。数据挖掘模块对事件库中的大量安全事件进行过滤、转换和组织成信息集，并用这些信息发现从前没有发现的隐藏的入侵模式，从而能够预测新的攻击，达到预警的目的。

关联分析引擎模块通过建立一个上下文环境，对复杂的消息序列进行结构分析、功能分析、行为分析等深入分析，通过特征匹配、异常分析等多种模式分析方法对安全事件进行判断，通过一定措施降低误报/漏报率，从而准确找出有危害的安全事件。这样就很好地解决了各个安全事件孤立、相互之间无法形成很好的合成关联问题，通过关联流量监控（网络病毒）、服务器运行状态监控（主机病毒）、完整性检测（主机病毒）结

合分析，快速定位真实问题。

3.4 应急响应层模块设计

应急响应层模块能够及时地采取响应措施阻止攻击的延续以减少攻击成功的机会和降低系统的损失。它自动进行响应决策并及时地对攻击做出响应，响应方式也应当能随着攻击的进行不断地调整，从而保护系统的安全。具体的设计框架见图 5：

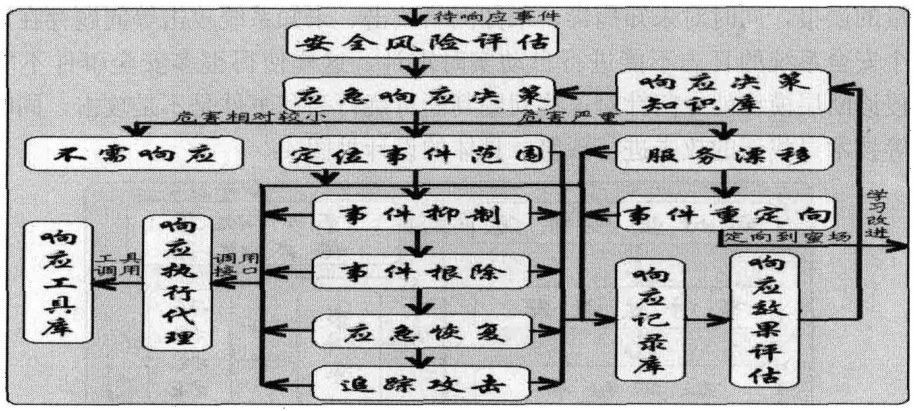

图 5 应急响应层模块设计

安全风险评估模块负责评估系统当前的可生存性。当前已经提出了一些定性分析的方法，如 SNA（Survivable Network Analysis）[12]方法通过定义系统能力和结构、分析攻击场景和系统组件的易损性从而评价可生存性，但该方法只能定性地给出对系统抵抗、识别、恢复等方面能力和策略的描述，不能获得定量的、精确的评估。为实现对可生存性的量化分析，一些研究者试图将系统的生存模型加以形式化描述[13]，通过定义系统的服务状态、环境状态，将系统被攻击和破坏表示为系统状态的变换，并在状态转移时引入概率等量化指标，如攻击成功概率、服务被满足的概率等，从而分析出系统在遭受攻击和破坏后保障基本服务的能力。此外，针对特定的攻击或故障类型，则可以选择相应的性能参数来评估系统的生存能力。例如衡量网络层故障恢复的指标通常采用恢复时间、带宽使用率；而分析抗 DoS 等攻击的技术则要考察攻击成功率等。

应急响应决策模块根据响应决策知识库，决定对检测出的安全事件做出何种响应。它是入侵响应模块的核心，根据检测出的攻击及相应的一些属性（如可信度等），决定对当前攻击做出什么响应。当前已有多种技术被提出并应用，Wenke Lee 在他的论文[14]中提出成本敏感模型作为响应决策的基础，使入侵响应系统满足合理性要求；Christopher 和 Robert[15]介绍了意图识别技术在入侵响应中的应用，从而增强了入侵响应系统的实时性和合理性；Curtis[16]介绍了他们开发的入侵响应系统 AAIRS，该系统能够满足自适应性要求。

定位事件范围模块负责定位这些攻击所造成的破坏的范围。一旦最后确认某个操作确实是攻击，系统必须修正所有被该攻击影响到的数据而又不要采用简单的回退恢复。为了达到入侵容忍的目的，系统必须保证未被感染的部分不被恢复。这样，修复系统首先必须搞清楚哪些数据或系统受到影响变“坏了”；其次，就是把这些“坏了”的设备

或数据进行正确的修复。比如，一个病毒进入系统感染了5个文件，而用户此时又修改了10个重要的文件，而10个中只有2个感染了病毒，此时，必须要定位到哪些文件被感染了，如果不能很好地定位，而采用简单的恢复技术，则用户的10个文件就都会被恢复到原始状态，这就不是入侵容忍，而仅仅是简单的恢复。如果能够仅仅恢复被感染的文件，而让用户的大部分工作得以保留，这才是入侵容忍。

事件抑制模块负责控制事件的影响范围，隔离并抑制突发事件。它可能采用的抑制策略有：关闭所有的系统，从网络上断开相关系统，修改防火墙和路由器的过滤规则，封锁或删除被攻破的登录账号，提高系统或网络的监控级别，设置陷阱，关闭服务，反击攻击者的系统等。在事件被抑制后，事件根除模块通过对有关恶意代码或行为的分析结果，找出事件的根源并彻底清除。

应急恢复模块负责将所有被攻破的系统和网络设备彻底还原到它们正常的任务状态，维持最基本的服务。如果攻击者获得了超级用户的访问权限，一次完整的恢复应该强制性的修改所有的口令。传统的方法是采用磁盘镜像、数据备份技术，以提高系统的可靠性。为提高系统遭受毁灭性破坏后的恢复能力，采用的技术还包括网络结构的冗余容错和动态切换、计算机网络系统恢复技术、计算机远程恢复技术和计算机网络自修复技术。

服务漂移模块根据分析评估模块评估系统当前的生存性，当系统负载过重、服务响应缓慢，或者有些关键基本服务不能迅速修复，或者检测到连接到本系统请求相比以前很少时就需要采取主动漂移机制[17]将服务转移到其他服务器上继续进行。当攻击者成功入侵系统的部分组件时，系统功能或性能受到破坏，当系统不能再容忍故障发生的情况下，系统有可能发展到潜在的不安全状态。此时，有必要提供紧急措施（如停止系统的运行）以避免系统受到不期望的破坏，并将攻击重定向到蜜场收集数据。

响应执行代理模块提供调用接口来调用响应工具集中的响应程序。响应记录库负责对多步骤地响应执行过程进行管理并记录生成的响应。响应效果评估模块根据响应记录库中执行记录评估响应效果，和过去的执行经验进行关联，根据环境的改变对响应动作进行适应性的调整。这样就使得应急响应模块具有了动态适应性。

4 模型分析

网络和主机的安全关系正如辩证法中的整体与局部的关系，网络越安全，各个主机也就越安全，反之，各个主机是构成网络的基石，它们的生存能力越强，抗攻击时间越长，就会使网络有充足的时间来从容应对各种攻击。所以，建立层次的入侵容忍模型是十分必要的。

本模型创新性地将入侵容忍系统分为五大层次，构筑了功能较为安全的纵深防御体系。它能灵活的应用现有的安全工具，具有很强的实用性，同时它能动态地根据环境和需要保护的信息改变安全策略，有较好的自适应性。

模型引入了虚拟服务的概念虚拟出提供关键服务的平台，它隔离了客户请求和实际服务的直接连接，起到了隐藏真正服务的目的，同时对客户请求进行监视。客户的请求

通过虚拟层转送到服务层提供服务，如果该请求是攻击时，就会被虚拟层发现并且被重定向到蜜场中收集数据，虚拟服务会创建欺骗包应答攻击者，反之则由真实服务提供应答。这样就可以在遭受攻击的情况下提供正常服务，提高了服务的抗攻击性。

在入侵针断层中引入了数据融合和数据挖掘技术将各个安全事件深入关联分析，寻找发现新的或隐藏的入侵模式，为抵抗各种层出不穷的新攻击提供了保障。

在应急响应层中引入三种应急决策技术根据入侵危害等级进行自适应响应，实现了响应的灵活性、自适应性和及时性。同时还引入破坏检测技术精确定位破坏范围，使得系统进行精确恢复。通过引入服务漂移机制在系统不能提供正常的服务后，将服务主动漂移到其他活动服务节点上，保证了服务的连续性和可用性。最后还可以对响应效果进行评估，根据响应经验动态调整响应策略，提高响应的自适应性和有效性。

5 结束语

入侵容忍是信息安全领域前沿的研究课题，有着广阔的应用空间，其研究结果可广泛用于安全关键的网络化应用系统及网络基础设施的容忍入侵安全防护中。然而从其目前国内外研究现状来看，还远未达到实用化的程度。本文从层次方面对入侵容忍系统建立了模型，并描述各模块之间的相互关系，详细介绍了各个模块的具体设计，最后分析了模型的特性，为以后具体系统地构建提供了框架。本文中描述的系统仍旧是一个设计，需要进一步地完善和实现。

参 考 文 献

[1] Jiwu Jing, Peng Liu, Dengguo Feng, et al. ARECA: a highly attack resilient certification authority. ACM workshop on Survivable and self-regenerative systems. 2003.

[2] 彭文灵，王丽娜，张焕国，傅建明．基于角色访问控制的入侵容忍机制研究．《电子学报》. Vol. 33 No. 1 Jan. 2005.

[3] 伍忠东，谢维信，喻建平．一种安全增强的基于椭圆曲线可验证门限签名方案．《计算机研究与发展》. ISSN 100021239/ CN 1121777/ TP 42 (4): 705～710 , 2005.

[4] 刘海蛟，荆继武，林锵，杜皎．一种入侵容忍的资料库．《中国科学院研究生院学报》. Vol. 23 January No. 1 2006.

[5] 崔竞松，王丽娜，张焕国，傅建明．一种并行容侵系统研究模型-RC 模型．《计算机学报》. 2004, 27 (4): 500～506

[6] Peng Wen-ling, Wang Li-na, et al. Buiding Intrusion Tolerant Software System. Wuhan University Journal of Natural Science. 2005, 1: 47～50.

[7] 朱建明，史庭俊，马建峰．基于多代理的容忍入侵体系结构［J］．《计算机工程与应用》. 2003, 39 (11): 19～22.

[8] Chao Wang, Jin-Feng Ma. Availability Analysis and Comparison of Different Intrusion-Tolerant Systems. Advanced Workshop on Content Computing, LNCS, 2004.

[9] 郭大伟，安宁．入侵容忍系统设计．《计算机工程与应用》. 2005, Vol. 41 No. 29.

[10] Dr. Carl E. Landwehr Research Direction in Intrusion Tolerant Systems IFIP WG 10.4 42nd Meeting. June 29, 2002.

[11] L. Spitzner "Honeypot Farms," 2003/08/13. Available from http: //www. securityfocous. com/infocous/1720.

[12] Robert J. Ellison, Richard C. Linger, Thomas Longstaff, and Nancy R. Mead. Survivable Network System Analysis. A Case Study, IEEE Software. Vol. 16 No. 4, July/August 1999: pp. 70～77.

[13] John C. Knight, Elisabeth A. Strunk, and Kevin J. Sullivan. Towards a Rigorous Definition of Information System Survivability. Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX'03).

[14] Wenke Lee. Toward Cost-Sensitive Modeling for Intrusion Detection and Response. Journal of Computer Security, Volume 10, Issues 1/2, 2002.

[15] Christopher W. Geib, Robert P. Goldman. Plan Recognition in Intrusion Detection Systems. IEEE. 2001.

[16] Curtis Curtis A. Carver. A Methodology for Using Intelligent Agents to provide Automated Intrusion Response. Proceedings of the IEEE Systems. 2000.

[17] 黄遵国．面向生存能力的应急响应与事故恢复技术研究．国防科技大学博士学位论文，2003，11.

[18] 李之棠，徐晓丹．动态蜜罐技术分析与设计．《华中科技大学学报（自然科学版）》．Vol. 33 No. 2 Feb. 2005.