入侵容忍技术现状与发展*)

张险峰 张 峰 秦志光 刘锦德

(电子科技大学计算机学院 IBM 技术中心 成都 610054)

摘 要 入侵容忍技术是美国提出的第三代安全的核心。入侵容忍是一种主动防护能力,当受保护系统的部分组件受到攻击时,入侵容忍旨在能维持整个系统关键信息和服务的完整性、机密性和可用性。本文介绍了入侵容忍技术的理论基础,包括系统故障模型、入侵容忍机制和入侵容忍策略;通过将入侵容忍同入侵检测、容错技术对比,研究了入侵容忍的应用特征;从应用类型、研究层次和领域问题对入侵容忍研究工作进行了分类;通过介绍 OASIS 计划支持的几个典型项目总结了入侵容忍研究工作现状;对该技术的未来发展进行了分析。

关键词 入侵容忍系统,门限密码体制,故障模型,错误恢复,群通信系统

Intrusion Tolerance Technology—Survey and Direction

ZHANG Xian-Feng ZHENG Feng QIN Zhi-Guang LIU Jin-De

(IBM Technology Center, School of Computer Science and Engineering, UESTC, Chengdu 610054)

Abstract Intrusion tolerance technology(ITT)is the core of "the 3rd Generation Security(3GS)". When some components of the protected system are attacked, ITT aims to maintain the integrity, confidentiality and availability of the critcal data and services provided by the whole system. This paper introduces the theoretical background, mechanisms and strategies of ITT. By comparison of ITT with intrusion detection and fault tolerance technology, the application characteristics are described. Some typical projects supported by OASIS program are briefly investigated to present the research state of the art of ITT. The paper ends with the perspectives of ITT and authors' next work.

Keywords Intrusion tolerant system, Threshold cryptography, Fault model, Error recovery, Group communication system

1 引言

第一代安全系统依靠密码学、可信的计算基础、认证、访问控制等技术来抵御入侵行为。第二代安全涉及到运用边界控制器(如防火墙)、IDS(Intrusion Detection System,入侵检测系统)、PKI(Public Key Infrastructure,公钥基础设施)等技术来弥补普遍存在的防卫漏洞[1]。因此,传统上的安全工作可归结为两个方面:(1)阻止攻击的发生;(2)不断解决系统存在的安全漏洞。

由于不可能预知所有未知形式的攻击,也不可能完全杜绝新安全漏洞的存在,导致一些攻击取得成功,所以有必要研发即使遭到攻击仍能运转的系统。入侵容忍系统允许系统存在一定程度的安全漏洞,并且假设一些针对系统组件的攻击能够取得成功。在面对攻击的情况下,入侵容忍系统不是想办法阻止每一次单个入侵,而是设计触发阻止使系统失效发生的入侵行为的机制,从而能够以可测的概率保证系统的安全和可操作性。

入侵容忍概念早在 1985 年由 J. Fraga 和 D. Powell 提出来[2],Deswarte、Blain 和 Fabre 在 1991 年开发了一个具有入侵容忍功能的分布式计算系统[3],但相关研究工作的兴起则是在最近几年才开始的。目前,美国国防高级研究项目署(DARPA)启动了一个新的研究和开发方向,名为"The 3rd Generation Security(3GS)[1]",主要研究入侵容忍技术,包括系统在面临攻击的情况下保持系统幸存性和弹性(自动恢复)的能力,以及对这些能力进行评估的手段。另外,欧洲和我国的一些科研单位也在开展这方面的研究工作[4~6]。

本文主要介绍入侵容忍的理论基础及其应用特征;对相关的研究工作和研究现状进行总结;详细介绍了几个典型项目;最后对该领域未来的发展方向进行分析。

2 理论基础

2.1 系统故障模型

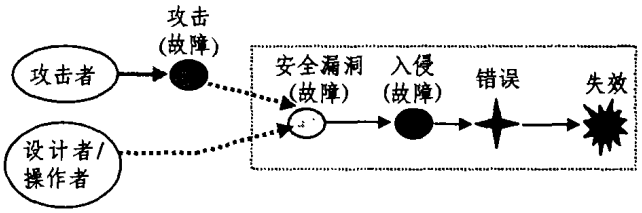

图 1 AVI 系统故障模型

在面临攻击的情况下,一个系统或系统组件被成功入侵的原因主要有两个:(1)安全漏洞,本质上是需求、规范、设计或配置方面存在的缺陷,如不安全的口令、使得堆栈溢出的编码故障等,安全漏洞是系统被入侵的内部原因;(2)攻击者的攻击,这是系统被入侵的外部原因,是攻击者针对安全漏洞的恶意操作,如端口扫描、DOS 攻击等方法。攻击者对系统或系统组件的一次成功入侵,能够使系统状态产生错误(error),进而会引起系统的失效(failure)。为了把传统容错技术用到入侵容忍上面来,可把任何攻击者的攻击、入侵和系统组件的安全漏洞抽象成故障系统故障(fault)。一个系统从面临攻击到系统失效的过程中,通常会出现以下事件序列:故障(fault)-错误(error)-失效(failure)。为了推理用于建立阻止和容忍入侵的机制,有必要对系统故障进行建模。在实践中,常

*)本课题得到国家 863 课题(编号:2002AA142040)资助。张险峰 博士生,研究方向为信息和网络安全。张 峰 博士生,研究方向为信息和网络安全。秦志光 教授,博导,研究方向为信息和网络安全、电子商务。刘锦德 教授,博导,研究方向为开放系统及其安全、中间件技术。

用的故障模型是AVI混合故障模型(Attack, Vulnerability, Intrusion composite fault model)[7],见图1。

由图1可见,故障是引起系统产生错误的原因,错误是故障在系统状态方面的表现,而失效是一个错误在系统为用户提供服务时的表现,即系统不能为用户提供预期的服务。为了实现入侵容忍,防止系统失效,可以对事件链的各个环节进行阻断,见图2:

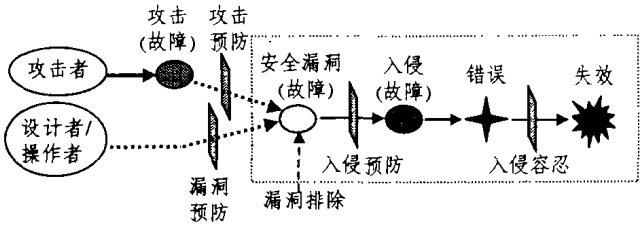

图2 阻止系统失效的AVI系统故障模型

由图2可见,综合应用多种安全技术可以防止系统失效,这些安全技术包括:(1)攻击预防:包括信息过滤、禁止JavaScript等可能含有恶意的脚本、对入侵进行预测等技术;(2)漏洞预防:包括完善的软件开发、预防配置和操作中的故障;(3)漏洞排除:针对程序堆栈溢出的编码错误、弱口令、未加保护的TCP/IP端口等漏洞,采用漏洞排除方法,从数量和严重程度上减少安全漏洞的存在,然而要完全排除系统安全漏洞并不现实。(4)入侵预防:针对已知形式的攻击,采取防火墙、入侵检测系统、认证和加密等手段,可以对这些攻击进行预防和阻止;(5)入侵容忍:作为阻止系统失效发生的最后一道防线,入侵容忍意味着能检测到入侵引起的系统错误,并采用相应机制进行错误处理。

2.2 入侵容忍机制

入侵容忍技术从本质上讲是一种使系统保持幸存性(Survivability)的技术。根据安全需求,一个入侵容忍系统应达到以下目标:(1)能够阻止和预防攻击的发生;(2)能够检测攻击和评估攻击造成的破坏;(3)在遭受到攻击后,能够维护和恢复关键数据、关键服务或完全服务。

入侵容忍系统目标的实现,需要一定的安全机制来保证,主要有以下机制:

1. 安全通信机制 在网络环境里,为了保证通信者之间安全可靠的通信,预防和阻止攻击者窃听、伪装和拒绝服务等攻击,安全通信机制是必需的。入侵容忍的安全通信机制通常采用加密、认证、消息过滤和经典的容错通信等技术。

2. 入侵检测机制 入侵检测通过监控并分析计算机系统或网络上发生的事件,对可能发生的攻击、入侵和系统存在的安全漏洞进行检测和响应。入侵检测通过和漏洞分析、攻击预报技术结合,能预测错误的发生、找出造成攻击或带来安全漏洞的原因。入侵检测也可结合审计机制,记录系统的行为和安全事件,对产生的安全问题及原因进行后验分析。

3. 入侵遏制机制 通过资源冗余和设计的多样性增加攻击者入侵的难度和成本,还可通过安全分隔、结构重配等措施来隔离已遭破坏的组件,限制入侵,阻止入侵的进一步扩散。

4. 错误处理机制 错误处理旨在阻止产生灾难性失效,具体包括错误检测和错误恢复。

错误检测包括完整性检测和日志审计等。错误检测的目的在于:(1)限制错误的进一步传播;(2)触发错误恢复机制;(3)触发故障处理机制,以阻止错误的发生。

错误恢复机制的目的在于使系统从入侵所造成的错误状态中恢复过来,以维护或恢复关键数据、关键服务甚至是完全服务。错误恢复机制包括:(1)前向恢复(Forward recovery):系统向前继续执行到一个状态,该状态保证提供正确的服务;(2)后向恢复(Backward recovery):系统回到以前被认为是正确的状态并重新运行;(3)错误屏蔽(Error masking):系统地应用冗余来屏蔽错误以提供正确的服务,主要保障机制包括:组件冗余、门限密码学、系统投票操作、拜占庭协商和交互一致性等。

由于错误检测方法不可靠或有较大的延迟,从而会影响错误恢复的有效性,因此,错误屏蔽是优先考虑的机制。

2.3 入侵容忍策略

入侵容忍应用的建立必须结合入侵容忍策略,即当系统面临入侵时,系统采取何种策略来容忍入侵,避免系统失效的发生。入侵容忍策略来自于经典的容错和安全策略的融合,策略以操作类型、性能、可得到的技术等因素为条件,在衡量入侵的成本和受保护系统的价值的基础上制订。一旦入侵容忍策略定义好了,就可根据确定的入侵容忍机制设计入侵容忍系统。具体而言,入侵容忍策略包括以下几个方面:

1. 故障避免和容错 故障避免策略指在系统设计、配置和操作过程中尽可能排除故障发生的策略,由于要完全排除系统组件的安全漏洞并不现实,而且通过容错的方法来抵消系统故障的负面影响往往比故障避免更经济,因此,在设计入侵容忍系统时,应将故障避免和容错策略折衷考虑。在一些特殊情况下,对于至关重要的系统,故障避免是追求的目标。

2. 机密性操作 当策略目标是保持数据的机密时,入侵容忍要求在部分未授权数据泄露的情况下,不揭示任何有用的信息。入侵容忍系统的机密性操作服务可以通过错误屏蔽机制来实现,错误屏蔽有多种方法,如门限密码体制[8]或法团(Quorum)方案[10]。

3. 可重配操作 可重配操作策略是指在系统遭受攻击时,系统根据组件或子系统的受破坏程度来评估入侵者成功的程度,进而对系统资源或服务进行重新配置的策略。可重配操作基于入侵检测技术,在检测到系统组件错误时能够自动用正确的组件来替代错误组件,或者用适当的配置来代替不适当的配置。可重配操作策略用于处理面向可用性或完整性服务,比如事务数据库、Web服务等。由于可重配策略需要对资源或服务进行重配,系统提供的服务可能临时无效而造成一些性能上的降级。

4. 可恢复操作 对于一个系统,假设:(1)使它失效至少需要时间 t_f;(2)系统至多需要时间 t_r 从失效状态恢复到正常状态,而且时间 t_r 对于应用者而言可以接收;(3)系统崩溃也不会产生不正确的计算;(4)对于一次给定的攻击,其攻击持续时间为 t_c,并且有 $t_c < t_f + t_r$。如果系统满足以上四个假设,则其遭受攻击并失效时,系统可采用可恢复操作来恢复正常。在分布式环境里,可恢复操作需要借助安全的协商协议来实现。

5. 防失败 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。这种策略常用于任务至关重要的系统,是其他策略的补充。

3 应用特征

当一些节点和通信链路受到攻击时,入侵容忍旨在维持关键信息和服务的完整性、机密性和可用性,并以一种及时的方式恢复被入侵的信息或服务。

入侵容忍系统的设计需要结合入侵阻止和入侵检测技术,但是,入侵容忍是一种主动防护能力,不是阻止和检测。入侵阻止和入侵检测是一种反应能力,前者通过静态布署防火

墙、防病毒软件和其它防御措施来阻止已知漏洞的利用；后者是一种检测入侵和报警的机制，其工作应集中在发现攻击者意图和攻击手段上。因此，入侵容忍主要以入侵产生的结果作为出发点，重视检查当前行为是否偏离了预期的行为，而不是建立在识别具体攻击的基础上，所以，入侵容忍适用于安全漏洞未知和新攻击存在的场合。

容错和入侵容忍都是使系统在异常情况下能连续提供可接受的服务，所以，一些关键的容错机制能用于入侵容忍，这些容错机制包括：(1)冗余的复制、多样性和重配置等；(2)冗余组件的独立性(设计的多样性)，比如，通过采用不同操作系统，减少通用模式安全漏洞的概率和通用模式攻击的概率。容错技术的错误检测、破坏程度评估、错误恢复、错误处理和连续服务几个阶段，也可作为设计和执行一个入侵容忍系统的参考。

容侵和容错系统毕竟有所区别，在入侵容忍中很好地结合容错技术并不容易，这是因为：(1)容错技术在设计和执行阶段对可能发生的偶然和恶意的错误都已预先考虑，对一些能预料到的错误行为可做一些合理的假设。入侵行为从动机上都是恶意的，从形式上很难预料；(2)入侵行为通常是由系统组件外部攻击引起的，传统的容错系统很少考虑这方面行为；(3)目前的容错技术主要处理已有的软硬件模块错误故障，它们的错误模式相对容易定义，然而面对攻击的分布式服务环境的每一个组件都包含很复杂的功能，定义错误模式更为困难；(4)系统攻击是有意的、系统的和可重复的，单纯的容错冗余将使错误存在于所有的复件里，入侵者基于相同攻击可系统攻击所有的备用组件，从而不能提供入侵容忍；同样，简单的容错重配使得系统为了应对无数相似的攻击而不断地进行重配，从而系统变得不稳定甚至不能提供服务。

4 研究工作分类

入侵容忍技术涉及的问题众多而广泛，下面从应用类型、研究层次、研究问题等方面对该领域的研究工作做综合的分类介绍。

4.1 应用类型

在实际应用中，入侵容忍应用可根据被保护的对象分为以下两类：

1. *对服务的入侵容忍* 主要研究系统在面临攻击的情况下，仍能为预期的合法用户提供有效服务的方法和机制。目前具有入侵容忍的服务有：入侵容忍的交易服务[5]、入侵容忍的 CA(Certificate Authority)认证服务[6,8,10]、入侵容忍 Web 服务[8]和入侵容忍的网络基础设施服务[9]等。对服务的入侵容忍策略常用故障避免策略和可重配策略，对服务的入侵容忍机制常用安全通信机制、入侵检测和遏制机制、错误处理机制。

2. *对数据的入侵容忍* 主要研究系统面临攻击的情况下如何保证数据的机密性和可用性。目前涉及的数据类别主要是入侵容忍的文件系统[2,3]和入侵容忍的数据库系统[11]。对数据的入侵容忍策略常用可重配策略和机密性操作策略，对数据的入侵容忍机制常用安全通信机制、入侵检测机制和错误处理机制。

4.2 研究层次

按照网络和应用体系分层的思想，入侵容忍的研究在物理层之上分为以下几个层次：

1. *网络和传输层* 研究针对网络基础设施(即路由器、域名服务器等)的入侵容忍方法，以提供网络环境下安全和可靠的路由、域名解析服务[9,12]。

2. *中件间系统* 研究基于中间件的入侵容忍解决方案，帮助应用程序在面临攻击的情况下能够幸存，包括：异构的入侵容忍 CORBA 系统[13]；能对系统的可用性和质量进行感知和反应的中间件技术；在恶意环境下，用于入侵容忍服务复制的中间件体系结构[15]；结合系统症状，在变化的环境和操作条件下能提供自适应的和攻击者无法预测系统反应的中间件技术[16]。

3. *高级服务和设施* 研究面向特殊类型应用的入侵容忍服务和设施，包括：用于网络上认证服务的 CA[6,8,10]；入侵容忍的 PKI[17]等。

4. *应用解决方案* 研究基于入侵容忍的特定应用，包括：容错和容侵的文件系统[2]、能够提供高安全性和可用性的入侵容忍 Web 应用[8]、能提供完整性和可用性的入侵容忍数据库应用[11]等。

4.3 领域问题

目前，入侵容忍领域所研究的问题可分为以下几类：

1. *构建方法*

(1)基于软件的入侵容忍。这方面工作主要研究入侵容忍的中间件系统[13~16]、入侵容忍的软件体系结构[18]、对软件系统的安全属性进行建模和量化的方法[19]。

(2)基于硬件的入侵容忍。在分布式系统环境中，用于容忍任意故障的分布式算法在资源和时间上开销很大，为了提高效率，采用具有增强的失效控制模式的硬件有助于建立更高的可信度，从而实现更为高效的入侵容忍系统。目前，这方面工作主要研究硬件组件的冗余配置[20]。

2. *实现原理*

(1)基于门限密码体制的入侵容忍。主要研究密钥管理(包括共享秘密的产生、分配和更新)、门限方案的设计、组件间交互的协议分析设计与验证、多方计算、重构过程、系统恢复、系统评估等工作[6,8,10,21]。

(2)基于冗余和适应性的入侵容忍。研究基于冗余和适应性的入侵容忍算法[14]和入侵容忍系统构建方法[22]。

(3)基于系统重配的入侵容忍。研究工作包括：当系统组件产生入侵触发信息后，对系统组件的功能和性能进行重新配置的策略和方法[23]；能够对大规模、异步的分布式系统进行主动或反应性重新配置的安全、自动的框架[24]。

3. *体系结构* 对入侵容忍体系结构的研究主要包括：入侵容忍体系结构的概念和设计问题[7]、自适应入侵容忍服务器的体系结构[20]、能够提供高可用性和完整性的入侵容忍体系结构[25]。

4. *入侵容忍协议* 入侵容忍协议设计是入侵容忍群通信系统的重要组成部分。群通信系统是一组通过网络互连协同操作的进程(或主机)，入侵容忍群通信系统是当部分进程(或主机)被入侵时，能够容忍任意形式的故障，连续提供正确结果的群通信系统。在入侵容忍群通信系统里，入侵容忍协议旨在阻止攻击，提供安全可靠和有序的消息传送和群成员资格服务(group membership service)[26]。目前，这方面研究主要包括：安全可靠的入侵容忍群通信协议[12,26,27]、用于入侵容忍群通信系统的群成员资格协议(group membership protocol)[28,29]。

5. *分析方法* 信息系统的安全以前被认为是定性的属性，然而，只有对安全进行合理量化和评估，才能更好地对安全风险、需求和策略进行平衡，从而在保证安全的同时，节省成本。这方面主要研究：提供群通信系统入侵容忍所需成本的量化方法[30]、入侵容忍的概率验证方法[31]、运用状态转换模型刻划入侵容忍系统[32]、入侵容忍系统的安全建模和量化问题[33]等。

5 研究现状

目前，DARPA 正资助实施 OASIS(Organically Assured

and Survivable Information System，有机保证和可幸存的信息系统)计划[1]，该计划旨在研究入侵和攻击的方法，由近 30 个项目组成。OASIS 的研究目标包括：(1)基于潜在具有安全漏洞的组件来建立入侵容忍系统；(2)描述节省成本的入侵容忍机制；(3)开发评估和验证入侵容忍机制的方法。

2000 年 1 月，欧洲启动了 MAFTIA(Malicious and Accidental Fault Tolerance for Internet Applications，用于因特网应用的恶意和意外故障容忍)研究项目，以期系统地研究容忍模型，建立大规模可靠的分布式应用[4]，MAFTIA 的主要研究成果包括：(1)定义了用于弥补可靠性(dependability)和安全性(security)差异的入侵容忍结构化框架和概念模型；(2)开发了一组建立入侵容忍系统的机制和协议，包括：一组模块化和可伸缩的安全群通信中间件协议；大规模分布式的入侵检测系统体系结构，该结构具有入侵容忍属性；入侵容忍的分布式认证服务。(3)提出了针对 MAFTIA 中间件部分组件的形式化验证和评估方法。另外，我国从 2001 年启动并开展了一些有关入侵容忍的研究[5,6]。

下面，简单介绍 OASIS 计划支持的几个典型项目：

1. SITAR[23]

Duke 大学开展了 SITAR(Scalable Intrusion Tolerance Architecture，可伸缩的入侵容忍体系结构)项目。其目标是：(1)研究容错和入侵的关系，开发入侵容忍模型，定义初始的体系结构；(2)折衷考虑分析和仿真方法，实现一个原型系统，通过实验评估原型系统。

SITAR 主要应用了可重配操作策略和错误处理策略，采用了入侵检测机制、入侵遏制机制。具体而言，系统中代理服务器模块运用资源冗余和设计多样性设计，每个系统组件含有入侵检测模块。系统在面临入侵时能够对安全策略、系统资源和服务进行重新配置，保证系统的安全和服务的连续性。

2. ITTC[8]

Stanford 大学开展的 ITTC(Intrusion Tolerance via Threshold Cryptography，基于门限密码学的入侵容忍)项目主要研究基于 RSA 的门限密码体制，进而建立入侵容忍的 Web 安全和 CA 应用。ITTC 项目主要应用容错策略、可重配操作策略和机密性操作策略，采用安全通信机制、入侵检测机制、入侵遏制机制和错误处理机制。通过将秘密钥分成若干共享影子分别保存在不同的服务器上，ITTC 系统能确保一部分系统组件被攻破后并不泄露敏感的安全信息，在应用过程中，不进行秘密钥的重建。

3. COCA[13]

COCA 是 Cornell 大学研发的认证中心，为局域网和 Internet 提供容错和安全在线认证服务。它主要运用可重配操作策略、错误处理策略，采用入侵检测和错误处理机制。在 COCA 中，签名私钥以秘密共享的方式分别存储在总数为 $3t+1$(t 为整数)个共享服务器上，系统采用门限密码算法签发证书，当系统中至多 t 个服务器出故障或被入侵时，并不影响系统的可用性和安全。另外，COCA 项目提出了将拜占庭法团系统(Quorum system)和主动恢复密钥相结合的方法，以获得可靠性和主动安全。

4. ITUA[14]

ITUA(Intrusion Tolerance by Unpredictable Adaptation)项目由 DARPA 资助，BBN Technologies，Illinois 大学，Maryland 大学，和 Boeing Corporation 联合研发。针对预先计划的、协同的、可能导致系统灾难性失效的攻击，该项目的目标是开发能够容忍这类攻击的算法和软件工具。该项目主要运用容错策略，采用入侵检测、入侵遏制和错误处理等容忍机制，开发自适应的、能感知和反应系统可用性和服务质量的中间件技术，使系统具有适应性和不可预知性，帮助应用程序在面临攻击的情况下能容忍攻击造成的影响。

6 未来发展与展望

目前，对入侵容忍的研究取得了一些成果。网络基础设施和基本协议方面考虑安全属性(SNMP，IPV6)等。随着入侵手段和安全技术的发展，我们认为在入侵容忍的未来发展中有以下几个方面值得重视。

1. 入侵预警机制。要彻底杜绝网络入侵行为是不可能的，我们应该研究一种安全机制，在入侵发生或入侵造成严重后果前对可疑行为进行预警。由于攻击者经过一个大规模网络进行入侵通常需要按一定步骤、花费一定时间来实施，我们有可能通过对网络数据的实时收集和分析，同时结合系统安全漏洞分析来监控识别入侵企图，进行入侵预警，并进而采取主动防范措施。入侵预警机制是入侵容忍机制的重要补充。

2. 高效门限密码体制的应用。由于门限密码体制能够灵活产生、安全存储和发放密钥，为开发一个安全、高效和经济的入侵容忍系统提供了新的技术手段，同时在部分系统组件已被攻破的情况下仍能保护系统中用于加密、认证和访问控制等目的的秘密信息，所以基于高效门限密码体制的入侵容忍应用值得关注。

3. 系统进化。可进化的入侵容忍系统、结合入侵检测和自动恢复机制的入侵容忍技术值得研究。

4. 进一步的工作。鉴于椭圆曲线加密算法(ECC)在安全性和执行效率方面的独特优点，我们将重点研究基于 ECC 的门限加解密体制、门限签名体制，在此基础上，研究能提供完整性、可用性和机密性服务的入侵容忍系统。

参考文献

1 http://www.darpa.mil/ipto/programs/oasis/techprogram.htm, 2003
2 Fraga J, Powell D. A fault-and intrusion-tolerant file system. In: Proc. of the 3rd Intl. Conf. on Computer Security, 1985. 203～218
3 Deswarte Y, Blain L, Fabre J-C. Intrusion tolerance in distributed computing systems. In: Proc. of the 1991 IEEE Symposium on Research in Security and Privacy, 1991. 110～121
4 Powell D, Stroud R. Conceptual Model and Architecture of MAFTIA, MAFTIA Deliverable D21, Project MAFTIA IST-1999-11583, Jan. 2003, Research Report, RZ 3377, IBM Zurich Research Laboratory. http://www.newcastle.research.ec.org/maftia/deliverables/D21.pdf
5 荆继武，周天阳. Internet 上的入侵容忍服务技术. 中国科学院研究生院学报，2001，19(2)：119～123
6 荆继武，冯登国. 一种入侵容忍的 CA 方案. 软件学报，2002，13(8)：1417～1422
7 Verissimo P E, Neves N F, Correia M P. Intrusion Tolerant Architecture: Concepts and Design. http://www.di.fc.ul.pt/tech-reports/03-5.pdf, 2003
8 Malkin M, Wu T, Boneh D. Building Intrusion Tolerance Applications. DARPA Information Survivability Conference & Exposition - Volume 1, Hilton Head, South Carolina, Jan. 2000
9 Cheung S. An Intrusion Tolerance Approach for Protecting Network Infrastructure. Dissertations. University of California at Davis http://seclab.cs.ucdavis.edu/papers/Dissertations/S.Cheungdissertation.PDF, 2003
10 Zhou Lidong. Towards Fault-tolerant and Secure On-line Services. Dissertation. http://www.cs.cornell.edu/home/ldzhou/thesis.pdf, 2001
11 Luenam P, Liu P. The Design of an Adaptive Intrusion Tolerant Database System
12 Lung L C, Correia M, Neves N F, et al. A Simple Intrusion-Tolerant Reliable Multicast Protocol Using the TTCB. http://www.di.fc.ul.pt/～nuno/PAPERS/SBRC03.pdf, 2003
13 Sames D, Matt B, Niebuhr B, et al. Developing a Heterogeneous Intrusion Tolerant CORBA System. In: Proc. of the Intl. Conf. on Dependable Systems and Networks (DSN'02)
14 Cukier M, Lyons J, Pandey P, et al. Intrusion Tolerance Approaches in ITUA. http://www.dist-systems.bbn.com/papers/2001/ICDSN/01CUK01.pdf, 2001
15 Ezhilchelvan P. A Middleware Architecture for Intrusion Tolerant Service Replication. http://www.cs.ncl.ac.uk/research/pubs/inproceedings/papers/577.pdf, 2003

(下转第 27 页)

5 Goldman R, McHugh J, Widom J. From Semi-structured Data to XML: Migrating the Lore Data Model and Query Language. http://citeseer. nj. nec. com/cache/papers/cs/24625/http: zSzzSzxml. coverpages. orgzSzLore-WebDB99. pdf/goldman99from. pdf.

6 Maruyama K, Uehara K. Mining Association Rules from Semi-structured Data. www. ai. cs. scitec. kobe-u. ac. jp/report/maru-199912. pdf

7 Papakonstantinou Y, Garcia-Molina H, Widom J. Object exchange across heterogeneous information sources. In: Proc. of the Eleventh Intl. Conf. on Data Engineering, Taipei, Taiwan, Mar. 1995. 251～260

8 Prof. Dan Suciu. Managing XML and Semistructured Data: lecture 2 : XML. http://www. cs. washington. edu/homes/suciu/COURSES/590DS/02xmlsyntax. htm. Spring 2001

9 Bourret R. XML and Databases. http://www. rpbourret. com/xml/XMLAndDatabases. htm. July, 2003

10 Braga D, Campi A, Klemettinen M, Lanzi P L. Mining association rules from xml data. In: Proc. of the 41h Intl. Conf. on Data Warehousing and knowledge discovery(DaWak 2002)Sep. Aixen-Provence, France, 2002. accepted.

11 Braga D, et al. Discovering interesting information in xml data with association rules:[Technical Report 2002-15]. Dipartimento di Elettronica e Informazione-Politecnico di Milano, 2002

12 Bragal D, et al. A Tool for Extracting XML Association Rules. In: Proc. of the 14th IEEE Intl. Conf. on Tools with Artificial Intelligence(ICTAI'02)2002

13 Meo R, Psaila G, Ceri S. A new sql-like operator for mining association rules. In VLDB'96, Mumbai(Bombay), India, 1996. 122～133

14 World Wide Web Consortium. XQuery 1. 0: An XML Query Language(W3C Working Draft). http://www. w3c. org/TR/2001/WD-xquery-20011220, DEC. 200

15 World Wide Web Consortium. XML Path Language(XPath)Version 1. 0(W3C Recommendation). http://www. w3c. org/tr/xpath/, Nov. 1999

16 Nestorov S, Ullman J, Wiener J, Chawathe S. Representative Objects: Concise Representations of Semi-structured Hierarchal Data. In: Proc. of 13th Intl. Conf. on Data Engineering, 1997. 79～90

17 Wang K, Liu H. Schema discovery for semi-structured data. In: Intl. Conf. on Knowledge Discovery and Data Mining, Newport Beach, Aug. 1997. 271～274

18 Wang K, Liu H. Discovering Typical Structures of Documents: A Road Map Approach. In: Proc. of 21st Annual Intl. ACM SIGIR Conf. on Research and Development in Information, 1998. 146～154

19 Agrawal R, Imielinski T, Swami A. Mining association rules between sets of items in large databases. In: Proc. of the ACM SIGMOD Conf. on Management of data, 1993. 207～216

20 Cong G, Yi L, Liu B, Wang K. Discovering Frequent Substructures from Hierarchical Semi-structured Data. www. siam. org/meetings/sdm02/proceedings/sdm02-11. pdf.

21 Asai T, Abe K, Kawasoe S, Arimura H, Sakamoto H, Arikawa S. Efficient Substructure Discovery from Large Semi-structured Data. In: Proc. the 2nd SIAM Int'l Conf on data mining (SDM2002). 2002. 158～174

22 Zaki M J. Efficiently Mining Frequent Trees in a Forest, Computer Science Department, Rensselaer Ploytechnic Institute: [PRI-TR01-7-2001]. 2001. http://www. cs. rpi. edu/～ zaki/PS/TR01-7. ps. gz

23 Singh L, Scheuermann P, Chen B. Generating association rules from semi-structured documents using an extended concept hierarchy. In CIKM, 1997. 193～200

24 Singh L, Chen B, Haight R, Scheuermann P, Aoki K. A Robust System Architecture for Mining Semi-structured Data. In: Proc. of 13th Intl. Conf. on Data Engineering, 1997. 79～90

25 Xin Y, Ju S. Mining Conditional Hybrid-dimension Association Rule on the basis of Multi-dimension Transaction Database. In: The Second Intl. Conf. on Machine Learning and Cybernetics the IEEE Systems, Man and Cybernetics Technical Committee on Cybernetics, Xi-an, China, Aug. 2003

26 Taniguchi K, Sakamoto H, Arimura H, Shimozono S, Arikawa S. Mining Semi-Structured Data by Path Expressions. In: Proc. The 4th Int'l Conf. on Discovery Science, LNAI 2226, 2001. 387～388

27 Shimozono S, Arimura H, Arikawa S. Efficient discovery of optimal word-association patterns in large text databases. New Generation Computing, 2000, 18: 49～60

(上接第22页)

16 Pal P P, Webber F, Schantz R E, et al. Intrusion Tolerant Systems. IEEE Information Survivability Workshop(ISW-2000)

17 Wang Xunhua. Intrusion- Tolerant Password-Enabled PKI. http://middleware. internet2. edu/pki03/presentations/secondpki. pdf, 2003

18 Stavridou V, Dutertre B, Riemenschneider R A, et al. Intrusion Tolerant Software Architectures. In: Proc. of the DARPA Information survivability Conference and Exposition(DISCEXII'01)

19 Madan B B, Goseva-Popstojanova K, Vaidyanathan K, Trivedi K S. Modeling and quantification of security attributes of software systems. In: Proc. Int. Conf. DSN, (IPDS stream), volume 2, 2002. 505～514

20 Valdes A, Almgren M, Cheung S, et al. An Adaptive Intrusion-Tolerant Server Architecture. http://www. sdl. sri. com/users/valdes/DIT_arch. pdf, 2002

21 Cachin C, Poritz J A. Secure Intrusion-tolerant Replication on the Internet. In: Proc. of the Intl. Conf. on Dependable Systems and Networks(DSN'02)

22 Hiltunen M A, Schlichting R D, Ugarte C A. Building Survivable Services Using Redundancy and Adaptation. IEEE transactions on computers, 2003, 52(2): 181～194

23 Wang F, Gong F, Sargor G, et al. SITAR: A Scalable Intrusion Tolerance Architecture for Distributed Server. IEEE SMC Information Assurance Workshop' 01

24 Wolf A L, Heimbigner D, Bend J K. Don't Break: Using Reconfiguration to Achieve Survivability. IEEE Information Survivability Workshop(ISW-2000)

25 Valdes A, Almgren M, Cheung S, et al. Dependable Intrusion Tolerance: Technology Demo. In: Proc. of the DARPA Information Survivability Conference and Exposition(DISCEX'03)

26 Kihlstorm K P, Moser L E, Melliar-Smith P M. The SecureRing Group Communication System. ACM transactions on Information and System Security, 2001, 4(4): 371～406

27 Dutertre B, Sa ï di H, Stavridou V. Intrusion-Tolerant Group Management in Enclaves. DSN'01

28 Reiter M. A Secure Group Membership Protocol. In: Proc. of the IEEE Symposium on Research in Security and Privacy, 1994. 176～189

29 Ramasamy H V. Group Membership Protocol for an Intrusion Tolerant Group Communication System: [MS thsis]. University of Illinois at Urbana-Champaign, 2002

30 Ramasamy H V, Pandey P, et al. Quantifying the Cost of Providing Intrusion Tolerance in Group Communication System. In: Proc. of the Intl. Conf. on Dependable Systems and Networks (DSN'02)

31 Sanders W H, Cukier M, Webber F, Pal P, et al. Probabilistic Validation of Intrusion Tolerance. http://www. dist-systems. bbn. com/papers/2002/SAN/02SAN02. pdf, 2002

32 Goseva-Popstojanova K, Wang Feiyi, Wang Rong, et al. Characterizing Intrusion Tolerant Systems Using A State Transition Model. (DISCEXII'01). http://panda. ece. utk. edu/～fwang2/papers/darpa00. pdf, 2002

33 Madan B B, Trivedi K S. Security modeling and quantification of intrusion tolerant system. http://srel. ee. duke. edu/PAPERS/Madan-FA2002240. pdf, 2002