文章编号: 1671-5896(2009)04-0389-07

入侵容忍综述

张云英, 努尔布力, 王程明, 姜 千, 胡 亮
(吉林大学 计算机科学与技术学院, 长春 130012)

摘要: 针对在大规模复杂网络环境下保证信息安全问题, 阐述了入侵容忍的概念和相关理论, 并对入侵容忍的发展现状、应用领域进行研究和分析, 最后讨论该领域当前存在的问题和未来的发展方向。研究结果表明, 入侵容忍作为第三代信息安全技术的核心, 能有效地预防、阻止入侵, 发展前景广阔。

关键词: 入侵容忍; 容错; 网络安全
中图分类号: TP3 **文献标识码:** A

Status of Intrusion Tolerance

ZHANG Yun-ying, NURBOL, WANG Cheng-ming, JIANG Qian, HU Liang
(College of Computer Science and Technology, Jilin University, Changchun 130012, China)

Abstract: In order to ensure the security of the information under the environment of complex network, intrusion tolerance is a good complement and the central issue of network security in recent years. The related theory of intrusion tolerance is illustrated, then the status and related application of intrusion tolerance are studied, at last the problems and future of intrusion tolerance are discussed. As the core of the 3rd generation information security, intrusion tolerance can prevent the intrusion effectively, it has a wide prospect.

Key words: intrusion-tolerance; fault-tolerance; network-security

引 言

在当今计算机软硬件及互联网快速发展的形式下, 网络病毒、网络攻击也在不断地变种、升级, 更加严重地威胁着企业及个人信息的安全。依靠传统的以保障、防护为主的安全策略及方法已经远不能满足信息安全的要求。入侵容忍[1]作为第三代信息安全技术, 改变传统的以隔离、防御、检测、响应和恢复为主的思想, 假定系统中存在一些受攻击点, 在系统的可容忍的限度内, 这些受攻击点并不会对系统的服务造成灾难性影响, 系统本身仍能保证最低质量的服务。其必要性在于: 在以第二代互联网为主要交互平台的网络环境中, 入侵容忍能保证服务端在适当降低服务效率的情况下, 不间断地为客户端服务, 这也是对服务端信誉的有利保证。入侵容忍并不是取代以往的安全策略及方法, 而是对他们的一个很好的补充, 应用入侵容忍技术, 能够提高系统的存活性, 将关键任务的服务维持在一个用户可接受的水平, 最终成为网络安全的最后一道防线。

入侵容忍技术是一门融合了密码技术和容错技术的新网络安全技术。当受保护系统的部分组件发生错误时, 能最低限度地维持整个系统关键信息和服务的完整性和可用性。其目标为[2]: 1) 保护系统的安全运行; 2) 保证服务的可用性; 3) 保证服务器上数据的秘密性; 4) 保证服务器上数据的真实性和

收稿日期: 2009-03-31
基金项目: 国家自然基金资助项目(60873235);教育部新世纪优秀人才支持计划基金资助项目(NCET-06-0300);吉林省科技支撑计划重点基金资助项目(20080318);吉林大学研究生"985工程"创新计划基金资助项目(20080244)
作者简介: 张云英(1984—),女,吉林省吉林市人,吉林大学硕士研究生,主要从事大规模网络入侵检测研究,(Tel) 86-13174463543 (E-mail) daying-21031225@163.com;胡亮(1968—),男,江苏句容人,吉林大学教授,博士生导师,主要从事网络与信息安全研究,(Tel) 86-431-85168277 (E-mail) hul@mail.jlu.edu.cn。

完整性。以上4个目标依次递进地增强对系统的保护功能。

笔者在对入侵容忍相关理论、发展现状及应用领域进行充分研究分析的基础上，讨论了当前入侵容忍仍然存在的问题以及其今后的发展方向。

1 入侵容忍相关

1.1 基础概念

1.1.1 入侵容忍概念

早在1982，国外就提出了入侵容忍相关概念，1985年Fraga和Powell[3]提出入侵容忍是“假定系统中存在一定数量未知的或未缓和的弱点，使得即使存在入侵、感染病毒，系统仍然能最低限度地继续提供服务。”入侵容忍概念的提出主要是源于故障模型[4]，该模型将一个计算机系统出现的故障归为两类：1）故意故障（Intentional Faults），主要是由攻击、病毒、蠕虫等引起的；2）非故意类故障（Non-Intentional Faults），主要是由代码错误、开发环境错误和配置错误等原因引起的。

1.1.2 入侵容忍系统

传统的安全工作包括：阻止攻击的发生，不断解决系统存在的安全漏洞。但由于不断产生的未知攻击和已知攻击的不断变种，完全杜绝新安全漏洞是不可能的，所以入侵容忍系统（ITS: Intrusion Toler-anc-e System）非常必要。入侵容忍系统是指系统能在遭受一定入侵的情况下，通过采取一些必要的措施手段，以保证关键应用或关键服务能连续正确地工作。入侵容忍系统的功能主要包括：自我诊断能力、故障隔离能力和还原重构能力。

1.2 基础理论

1.2.1 实现机制

入侵容忍系统的主要实现机制有：安全通信机制、入侵检测机制、入侵遏制机制、错误处理机制和数据转移机制。安全通信机制是通过加密、认证、消息过滤等方法实现；入侵检测是对网络中潜在的或正在进行的攻击进行实时监测、响应。主要有异常检测和滥用检测两种检测方法，目前已经发展到分布式入侵检测阶段，可用来检测大规模网络环境下的协同攻击；入侵遏制是通过结构重构和冗余等方式达到进一步阻止入侵的目的；错误处理机制主要通过错误屏蔽的方法检测和恢复系统发生失效后的错误。

1.2.2 实现策略

入侵容忍系统的策略是指导入侵容忍系统的设计、并决定其运行效果的关键。它与入侵容忍的程度和可配置性有关。1）入侵容忍的程度。在应用系统受到入侵时，入侵容忍系统需要将应用系统保护到的程度。2）可配置性。在入侵容忍能力和代价上所进行的权衡，对一个已经实现的入侵容忍系统，要求在运行过程中，可根据管理员的意图，动态配置系统，调整入侵容忍的策略，以在入侵容忍收益与入侵容忍代价之间取得最佳的平衡。

1.2.3 实现方法

入侵容忍基本思想不是设法阻止错误，而是容忍错误、使系统维持生存，目前较广泛使用的两种入侵容忍途径包括攻击响应和攻击遮蔽[5]。1）攻击响应。当检测到系统局部失效或故障时，对系统当前危险状态进行估测，然后根据相应的策略调整系统结构，为系统重新分配资源（比如重装系统），继而使系统能继续服务。只要保证在系统更新时间间隔内，系统的局部失效或故障的数量小于拜占庭法则所能容忍的最大故障数量，并能及时移出恶意攻击或错误，对系统造成的不良影响即可。2）攻击遮蔽。利用容错技术原理，在系统设计之初，就设计足够充分的冗余、多表表决等，以保证各冗余部件之间具有复杂的关系和不同的结构。利用门限密码学、拜占庭法则等机制，通过定义每个部件之间的监控规则，遮蔽故障或攻击对系统的影响，进而再进行局部性的系统恢复，与前一种途径相比，这种途径增加了硬件开销和各部件之间的复杂度，但能减少恢复系统的时间开销，时间效率较高。

1.3　技术分类

1.3.1　基于被保护对象

一般按照被保护对象的不同,可将入侵容忍分为面向服务和面向数据。1)面向服务。对服务的入侵容忍,可解决系统在面临攻击的情况下,仍能为合法用户提供有效服务的问题。2)面向数据。对数据的入侵容忍,可面临攻击的情况下,保证数据的机密性和可用性。

1.3.2　基于功能需求

按照功能需求,入侵容忍可分为预防与检测和恢复与重构。1)预防与检测。包括 Firewall和 IDS在内的预防网络入侵的技术,还包括有防范意识的 (Intrusion Awared)系统结构、精确的功能描述方法、安全的协议、受保护的数据结构和完善的管理规则等。2)恢复与重构。强调系统受到一定程度的入侵后,如何发现入侵、排除干扰、继续提供服务和重构系统。

1.3.3　基于实现技术

入侵容忍基于实现技术可分为 3大类。1)基于冗余与适应性的入侵容忍。研究冗余与适应性的入侵容忍算法和入侵容忍构建方法,如拜占庭法则系统。2)基于门限密钥共享体制的入侵容忍。主要研究密钥管理 (包括共享秘密的产生、分配与更新)、门限秘密共享体制的设计、组件间交互的协议分析设计与验证、多方计算、重构过程、系统恢复与系统评估等工作。在入侵容忍中,假设各参与方是不安全的,不能独自恢复秘密,而传统系统则相反,认为参与各方是安全的。3)基于系统重配的入侵容忍。主要研究当系统组件产生入侵触发信息后,对系统组件进行重新配置的策略和方法,进而建立能对大规模、异步的分布式系统进行主动或反应性重新配置的安全、自动框架。

2　发展现状

2.1　研究现状

国外对入侵容忍的研究较国内要早约 20年。90年代初期,国外已经开发了具有容忍功能的分布式计算系统,主要研究计划包括由美国国防部 (Darpa)资助的 OASIS(The Organically Assured and Survivable Information Systems)计划、ITSP (Intrusion Tolerant System Program)计划、OASIS Dem/Val (Demonstration and Validation)计划和由欧洲 IST (Information Society Technologies)开启的 MATFIA (Malicious and Accidental-Fault Tolerance for Internet Applications)计划。

其中 OASIS包括近 30个研究项目,研究内容涉及在组件具有潜在安全漏洞的基础上建立 ITS、构造低成本的 IT机制、开发评估和验证 IT机制的方法等。其中著名的项目如下。

1) ITUA (Intrusion Tolerance by Unpredictability and Adaptation)。该项目的主要研究通过监视系统的状态,发现基于多阶段的协同故意攻击,并开发具有适应此类攻击的算法和软件工具,利用不可预言和适应性,开发一个中间件协助应用程序对确定的攻击类型进行容忍。项目的创新点是开发了能容忍故意攻击和多阶段攻击系统 (其中攻击类型可以是同一时间发生在不同地方的攻击),通过适应性解决攻击对系统资源造成的影响,在应用程序和基础程序资源之间采用中间件的形式进行控制,使用不可预见的适应性达到识别故意攻击目的。

2) SITAR (A Scalable Intrusion Tolerant Architecture for Distributed Service)[6]。该项目主要研究开发了能容忍动态错误的通用模型 (其中错误类型可以是在任意时间内发生的完全不可预测的错误),并在此基础上开发了一个可入侵容忍 Web服务器系统。SITAR[7]创新点在于利用动态配置策略,重新配置入侵容忍模型,使用基于模型和基于测量的方法估测框架的安全性,并可进行成本效益的权衡性学习。

3) WRAITS (Workshop on Recent Advances on Intrusion-Tolerant Systems)。从 2007年开始,入侵容忍系统发展研讨会研究内容包括:入侵容忍、分布式信任、关键基础设施的安全、主动恢复[8]、多样性和非独立性、生存系统、拜占庭错误容忍[9]、安全控制和嵌入式系统,基于虚拟化的容错[10]和入侵、分布式环境中虚拟化的使用安全、弹性虚拟化技术、基于虚拟技术的可信计算基的实施[11]、基于 TV的可靠系统的适应性、形式化虚拟验证和操作系统[12,13]等。

2.2 应用领域

目前，入侵容忍已深入到计算机所能涉及的各个领域，作为受保护系统的最后一道屏障，入侵容忍发挥着至关重要的作用。

2.2.1 入侵检测系统

在复杂网络环境下，越来越多的入侵及攻击是通过跨越多个终端或工作站协同发生的，因此在这种情况下，单一的入侵检测则往往显得束手无策。基于入侵容忍的入侵检测系统的提出，克服了以往的入侵检测系统对无法有效识别分布式协同攻击以及在入侵后无法提供恢复系统线索的弊端，通过将入侵容忍及入侵检测的有效结合，能及时预测、发现复杂攻击，并在容忍攻击的情况下，保证系统能最低限度地提供关键性服务，边服务边修复系统。DBSL (Distributed Bayesian Structure Learning) 入侵容忍入侵检测系统[14,15]是目前研究的热点，该系统框架是通过将机器学习、贝叶斯网络、入侵检测与入侵容忍的有机结合，建立一个全局的贝叶斯网络[16]，利用删除概率较低路径的思想，达到提高入侵检测效率，降低误报率、漏报率，进而较少系统全面崩溃概率的目地。

2.2.2 Web服务器系统

在开放性网络中，由于没有绝对安全的办法能为Web服务器[17]建立一个安全的屏障，因此将入侵容忍应用于Web服务器系统中，可大大提高服务器在开放性网络中的可靠性和可用性，其中著名的系统框架为SITAR。

2.2.3 CA (Certificate Authority) 认证

CA认证[18]主要应用于电子政务、电子商务之间信任关系的建立，以及信息的安全传输。保证CA私钥安全是CA安全的核心，如果攻击者入侵了CA，则很有可能获得CA私钥，因此需要保证即使一台或多台CA设备遭到攻击或无法正常工作时，仍然能保证整体PKI (Public Key Infrastructure) 的正常工作，各电子政务、电子商务之间的信任关系不会被轻易破坏[19]，所传输的重要敏感数据不会轻易被劫持、篡改等[20]。在CA认证中主要运用RSA公钥算法和 (t, n) 秘钥共享思想保护CA私钥的安全，目前已经提出了一种基于椭圆曲线[21]可验证门限数字签名的在线CA安全增强方案，结合门限体制、可验证秘密共享体制以及主动秘密共享方案。

2.2.4 网络取证系统

网络取证技术作为一个新兴的交叉学科，密切关系着人们在网络生活方式下的权益和利益。目前的大部分网络取证技术都是以取证系统的可靠性为前提，而当网络状态可信度无法保证时，人们所获得的各种证据可信度也随之大大降低。最早用于取证的是DS技术，融合了入侵容忍技术的系统能在很大程度上保证系统的可靠性。因为入侵容忍的设计思想就是假定在系统中存在一定数量的不可靠结点。NFS (Network Forensic System Based on Intrusion Tolerance)[22]是一种基于入侵容忍的网络取证系统，NFS结合了入侵容忍系统SITAR框架和Agent技术，利用系统错误检测、冗余资源和投票算法等方法，在很大程度上提高了被取证系统的可用性、可靠性和可信任性；而且根据不同的系统状态，可获取不同程度的证据；根据这些不同的状态，可以定位犯罪的性质和严重程度。因此将入侵容忍应用于网络取证技术中，对电子法庭的实现与发展，都具有深远的意义。

2.2.5 数据库

入侵容忍在数据库[23]中的应用，主要是针对事务级数据库[24]。一般采用的方法是在控制阶段增加更新日志目录、采用过量控制，并将解控阶段分3个步骤完成：1) 系统解除控制那些实际没有受到破坏的对象；2) 取消恶意事务的操作；3) 修复受破坏对象。

2.2.6 文件系统

利用客户端硬盘剩余空间重复存储网络中的文件[25]，并通过加密技术将文件加密，分布地存储到网络其他客户端的硬盘中[26]。用户在使用该文件时，系统会自动地寻找该文件并进行组装。此方法可确保当系统中有少数客户端的硬盘数据受损时，通过相关的分布算法，能恢复局部结点的数据，不至于对系统数据的可用性造成威胁。

2.2.7 卫星星载

卫星星载测试方面,已经完成了卫星星载计算机软件单粒子反转容错能力的测试仪及测试;卫星星载系统开发方面,开发了基于相应系统的星载的计算机实时、容错分布式系统软件。一方面能保证缩短卫星设计周期,降低卫星设计成本;另一方面保证了在不增加硬件的条件下,能实施恢复正常状态。

随着入侵容忍研究的不断深入,国家科技部也正在进行高端容错计算机项目的研究,用于开发承担关键商用高端容错计算机系统 (如银行的储蓄业务系统,汇兑结算系统,银联信用卡交易结算系统,证券的交易系统和报价系统,电信领域的通讯网网管系统等)。

3 存在的问题

虽然入侵容忍已经发展成为一个成熟的方向,得到了国内外网络安全业界人士的普遍的认可和关注,但在理论和技术方面仍然存在一些问题,尚未达到入侵容忍所被期待的程度,主要从以下几个方面进行讨论。

3.1 密码学

目前普遍采用状态机复制结合自适应更新的方法,该方法主要是通过检测系统正常状态是否发生改变达到对系统进行感知的目的。但很多情况下,在系统状态尚未发生改变时,入侵或攻击已经发生了,这就很有可能导致某些关键性的子系统已经无法正常工作。目前的自适应入侵容忍系统仅限于门限密码、共享密码方案,对如何配置系统和参数的动态调整等问题,都有待于进一步深入研究。

3.2 策略模型

目前入侵容忍普遍采用拜占庭容忍模型来定位当前系统所能容忍的错误数量,但拜占庭容忍模型本身并没有考虑系统的保密性,并且在容错与容侵领域的度量标准是不同的。由于人为因素的存在,导致在容错上所满足的数学分布模型,在容侵领域是不能用简单的概率模型表示的,即不满足随机性。

3.3 可信检测器

作为一个群组,保证入侵容忍系统各组件之间的可靠通信非常必要[27]。可信检测器能保证每个部件的可信任性,即该组件没有被入侵或出现故障。因此使整个入侵检测系统对可信检测器的依赖程度非常高,如果触发可疑事件过早,可能将过多正常的组件误报为可疑组件;如果在确定了入侵后触发可疑事件,又会造成入侵的扩散。因此对可信检测器的设计也是入侵容忍亟待解决的一个问题。

4 入侵容忍展望

经过短短十几年的发展,入侵容忍已取得了一些显著的成果。但随着黑客入侵手段,计算机软硬件,互联网络及安全技术的不断发展,人们对入侵容忍在各个领域的发展及应用也有了更高的要求和需求。

4.1 航天事业

在恶劣的空间环境中,卫星对系统的可靠性要求非常高。单纯的采用冗余,会导致卫星体积、质量和功耗的增加。因此找到一种既可缩短开发周期又节省开发成本的容错算法是非常必要的。

4.2 电子商务

目前,电子商务在我国取得了巨大的发展,阿里巴巴、慧聪等一大批电子商务网站的运营模式成功地深入我国各大中小企业,并将继续引领经济危机下的中小型企业冲出国际环境下各种困境的重围。目前的网络攻击都致力于使特定的应用程序无法工作,大多数的系统都有一个主要的程序以保护系统软硬件、网络、操作系统等基础设施。将入侵容忍技术应用电子商务中,一改以往的通过访问控制保证系统信息安全的概念,使在发生网络攻击、系统故障的情况下,应用程序仍然可以在有限时间内,最低限度地提供服务,增强系统的安全性和可用性。

4.3 高端服务器

目前,国内高端容错服务器基本上都被国外垄断,在付出高昂成本及运营附加费用的同时,诸如银

行、汇兑结算系统、证券交易系统等涉及国家信息安全的领域，如果长期由国外垄断，一旦这些敏感信息泄漏，将对国家将造成重大损失。因此开发具有自主知识产权的容错高端服务器，具有重大意义。

4.4 高端电子取证

随着网络的不断发展，作为新兴的犯罪手段，网络犯罪已经不容忽视。电子取证就是在形式诉讼中针对网络犯罪进行调查、收集、提取证据的过程。将电子取证技术与入侵容忍技术相结合，构建一个具有容忍入侵的取证系统，根据系统的不同状态进行取证，可大大减少证据的存储量。

4.5 云计算

2008年最热门的话题就是云计算，与网格计算不同，网格强调的是连接，而云计算对计算资源中心的控制能力要比网格计算强得多，此外可以实现对资源的动态分配和动态切割功能。但今天的云计算还没有充分被用户认可，主要是因为现有的产品和服务仍然存在不稳定和不可信等问题，对数据的一致性及容灾备份等，都是亟待解决的问题。因此将入侵容忍理念应用到云计算的未来发展中，完善云计算，提高系统的可靠性和安全性势在必行。

5 结 语

入侵容忍技术虽然是一门新兴的安全领域技术，但已经成为网络安全整体机构框架中不可缺少的一个重要组成部分，作为信息安全领域的最后一道防线，可在系统发生错误、故障或受到攻击时，在有限的时间内保证系统最低限度地提供服务。将入侵容忍技术与多种安全技术相结合，可有效地预防或阻止入侵，降低系统瘫痪带来的损失，发展前景非常广阔。

参考文献:

[1] PAL P, WEBBER F, SCHANTZ R E, et al. Intrusion Tolerant Systems [C] //Proceedings of the IEEE Information Survivability Workshop (ISW-2000). Boston, Massachusetts: [s. n.], 2000: 24-26.

[2] PAULO ESTEVES VERISSIMO, NUNO FERREIRA NEVES, MIGUEL PUPO CORREIA. Intrusion-Tolerant Architectures: Concepts and Design [C] //Architecting Dependable Systems. [S. l.]: Springer-Verlag, 2003: 3-36.

[3] MICHAEL E WHITMAN, HERBERT J MATTORD. 信息安全原理 [M]. 第2版. 北京: 清华大学出版社, 2006.
MICHAEL E WHITMAN, HERBERT J MATTORD. Principles of Information Security [M]. 2nd. Beijing: Tsinghua University Press, 2006.

[4] JAYNARAYAN H LALA. Intrusion Tolerant Systems [C] //Presentation on 2000 Pacific Rim International Symposium on Dependable Computing. Los Angeles, California: [s. n.], 2000: 3.

[5] PAULO SOUSA, ALYSSON NEVES BESSANI, MIGUEL CORREIA, et al. Resilient Intrusion Tolerance through Proactive and Reactive Recovery [C] //Proceedings of the 13th IEEE Pacific Rim International Symposium on Dependable Computing. Washington, DC, USA: IEEE Computer Society, 2007: 373-380.

[6] DR FEIYI WANG, GONG FENGMIN, SARGOR C. SITAR: A Scalable Intrusion Tolerant Architecture for Distributed Services [C] //Proceedings of 2nd Annual IEEE Systems, Man, and Cybernetics Information Assurance Workshop. New York: IEEE Press, 2001: 1-8.

[7] DAZHI WANG, BHARAT B MADAN, KISHOR S TRIVEDI. Security Analysis of SITAR Intrusion Tolerance System [C] //Proceedings of the 2003 ACM Workshop on Survivable and Self-Regenerative Systems: in Association with 10th ACM Conference on Computer and Communications Security 2003. New York, NY, USA: ACM, 2003: 23-32.

[8] WANG Xi, GUO Zhen-yu, LIU Xue-zeng, et al. Hang Analysis: Fighting Responsiveness Bugs [C] //Proceedings of the 3rd ACM SIGOPS/European Conference on Computer Systems 2008. New York, NY, USA: ACM, 2008: 177-190.

[9] ALYSSON NEVES BESSANI, EDUARDO PELISON ALCHIERI, MIGUEL CORREIA, et al. DepSpace: A Byzantine Fault-Tolerant Coordination Service [C] //Proceedings of the 3rd ACM SIGOPS/European Conference on Computer Systems 2008. New York, NY, USA: ACM, 2008: 163-176.

[10] DUTCH T MEYER, GITIKA AGGARWAL, BRENDAN CULLY, et al. Parallax: Virtual Disks for Virtual Machines [C] //Proceedings of the 3rd ACM SIGOPS/European Conference on Computer Systems 2008. New York, NY, USA: ACM, 2008: 41-54.

[11] CARSTEN WEINHOLD, HERMANN HARTIG. VPFS: Building a Virtual Private File System with a Small Trusted Computing Base [J]. ACM SIGOPS Operating Systems Review, 2008, 42 (4): 81-93.

[12] YOSHIHISA ABE, HIROSHI YAMADA, KENJI KONO. Enforcing Appropriate Process Execution for Exploiting Idle Resources from Outside Operating Systems [C] //Proceedings of the 3rd ACM SIGOPS/European Conference on Computer Sys-

tems 2008. New York, NY, USA: ACM, 2008: 27-40.
[13]PETROS EFSTATHOPOULOS, EDDIE KOHLER. Manageable Fine-Grained Information Flow [J]. Operating Systems Review, 2008, 42 (4): 301-314.
[14]杨义先, 钮心忻. 入侵检测理论与技术 [M]. 北京: 高等教育出版社, 2006.
YANG Yi-xian, NIU Xin-xin. The Theory and Technology of Intrusion Detection [M]. Beijing: Higher Education Press, 2006.
[15]DACIER M. Design of an Intrusion Tolerant Intrusion Detection System (verion 4.3) [DB/OL]. [2002-08-09]. http://research.cs.ncl.ac.uk/cabernet/www.laas.research.ec.org/maftia/deliverables/D10.pdf.
[16]秦华旺, 戴跃伟, 王执铨. 基于贝叶斯网络的入侵容忍系统 [J]. 计算机科学, 2008, 35 (7): 78-80.
QIN Hua-wang, DAI Yue-wei, WANG Zhi-quan. Intrusion Tolerant System Based on Bayesian Networks [J]. Computer Science, 2008, 35 (7): 78-80.
[17]荆继武, 周天阳. Internet上的入侵容忍服务技术 [J]. 中国科学院研究生院学报, 2001, 18 (2): 119-123.
JING Ji-wu, ZHOU Tian-yang. An Intrusion Tolerant Services on Internet [J]. Journal of Graduate School of the Chinese Academy of Science, 2001, 18 (2): 119-123.
[18]徐秋亮. 改进门限 RSA数字签名体制 [J]. 计算机学报, 2000, 23 (5): 449-453.
XU Qiu-liang. A Modified Threshold RSA Digital Signature Scheme [J]. Chinese Journal of Computers, 2000, 23 (5): 449-453.
[19]袁巍, 张云英, 胡亮, 等. Rijndael算法的结构归纳与攻击分析 [J]. 吉林大学学报: 信息科学版, 2008, 26 (5): 487-493.
YUAN Wei, ZHANG Yun-ying, HU Liang, et al. Structure Cryptanalysis of Rijndael Algorithm [J]. Journal of Jilin University: Information Science Edition, 2008, 26 (5): 487-493.
[20]黄建华, 宋国新. 入侵容忍技术在身份认证系统中的应用 [J]. 华东理工大学学报: 自然科学版, 2005, 31 (3): 350-353.
HUANG Jian-hua, SONG Guo-xin. Application of Intrusion Tolerant Techniques to Authentication System [J]. Journal of East China University of Science and Technology: Natural Science Edition, 2005, 31 (3): 350-353.
[21]肖立国, 钟诚, 陈国良. 基于椭圆曲线密码体制的动态秘密共享方案 [J]. 微电子学与计算机, 2002, 19 (1): 30-31, 35.
XIAO Li-guo, ZHONG Cheng, CHEN Guo-liang. Dynamic Secret Sharing Scheme Based on Ellipse Curve Cryptosystem [J]. Microelectronics & Computer, 2002, 19 (1): 30-31, 35.
[22]张有东, 江波, 王建东. 基于入侵容忍的网络取证系统设计 [J]. 计算机工程, 2007, 33 (19): 161-163.
ZHANG You-dong, JIANG Bo, WANG Jian-dong. Design of Network Forensic System Based on Intrusion Tolerance [J]. Computer Engineering, 2007, 33 (19): 161-163.
[23]朱建明, 马建峰. 基于容忍入侵的数据库安全体系结构 [J]. 西安电子科技大学学报: 自然科学版, 2003, 30 (1): 85-89.
ZHU Jian-ming, MA Jian-feng. Intrusion-Tolerant Based Architecture for Database System Security [J]. Journal of Xidian University: Natrual Science Edition, 2003, 30 (1): 85-89.
[24]陈伟鹤, 殷新春, 谢立. 数据库管理系统的入侵容忍技术研究进展 [J]. 计算机科学, 2004, 31 (4): 14-18.
CHEN Wei-he, YIN Xin-chun, XIE Li. The State of the Art of Database Intrusion Tolerance Research [J]. Computer Science, 2004, 31 (4): 14-18.
[25]FRAGA J S, POWELL D. A Fault and Intrusion-Tolerant File System [C]//Proceedings of the 3rd International Conference on Computer Security, IFIP/SEC85. Oakland CA: [s.n.], 1985: 203-218.
[26]DOUCEUR R J, HOWELL J. Byzantine Fault Isolation in the Farsite Distributed File System [DB/OL]. [2009-03-10]. http://iptps06.cs.ucsb.edu/papers/Douceur-BFI.pdf.
[27]RAMASAMY H V, CUKIER M, SANDERS W H. Formal Specification and Verification of a Group Membership Protocol for an Intrusion-Tolerant Group Communication System [C]//Foundations of Intrusion Tolerant Systems. [S.l.]: IEEE Computer Society Press, 2003: 251-260.

(责任编辑: 刘俏亮)