入侵容忍技术及其实现

柴争义
(河南工业大学 信息科学与工程学院,河南 郑州 450007)

摘 要:入侵容忍是指系统在遭受攻击、故障或意外事故时,能够及时地完成其关键任务的能力,是目前网络安全领域的一种新技术。它突破了传统的网络安全技术从如何防止攻击的角度来进行安全保护的概念,从新的角度对网络安全问题进行研究,更能满足目前网络应用的现状。文中介绍了入侵容忍技术的起源、概念、特点、功能以及两种实现方法。

关键词:网络安全;可生存性;入侵容忍
中图分类号:TP309.08 **文献标识码**:A **文章编号**:1673-629X(2007)02-0223-03

Intrusion Tolerance Technology and Its Realization

CHAI Zheng-yi
(Department of Information Science and Technology, Henan University of Technology, Zhengzhou 450007, China)

Abstract: Intrusion tolerance refers that the system still can complete its key tasks when it suffers to the attacks, failure or the contingency. It is a kind of new technology on network security. It breaks through the traditional network security technology which focuses on prevent attacking. It studies the network from the new view and meets the network application better. Introduced the orgin, concepts, characteristic and two kinds of ways to realize it.

Key words: network security; survivability; intrusion tolerance

0 引 言

随着计算机网络的快速发展和广泛应用,各行各业对网络信息系统的依赖程度也越来越高。与此同时,网络安全事件也逐年上升,网络安全问题正成为人们关注的焦点。传统的网络安全技术主要是通过保护和检测手段来保障网络的安全,随着网络信息系统规模日益庞大,并朝着高度的分布式方向发展(即无边界系统),传统的安全技术日益显得力不从心。必须有新的安全理念来保证网络的安全性,这就是当前网络的可生存性技术,也是目前网络安全研究的新方向。而可生存性技术的核心就是入侵容忍技术。

1 入侵容忍技术的起源

1.1 信息保护技术

信息保护技术的关键思想是"防",主要采用加密、认证、安全分级、访问控制等办法来保证信息的安全。该技术的前提是假设能够明确地划分网络边界并能够在边界上阻止非法入侵。比如:通过口令阻止非法用户的访问;通过存取控制和权限管理让某些人看不到敏感信息;通过加密使别人无法读懂信息的内容等。由此可见,信息保护技术主要就是入侵阻止。该技术解决了很多安全问题。但是,并不是在所有情况下都能够清楚地划分并控制边界,保护措施也并不是在所有情况下都有效,再加上信息系统本身所固有的缺陷,使得信息保护难上加难。于是,出现了第二代信息安全技术——信息保障技术。

1.2 信息保障技术

信息保障技术的关键思想是"检",采用的主要技术有防火墙、IDS、边界控制、VPN、PKI 等。信息保障技术的基本假设是:如果挡不住敌人,但至少能发现敌人和敌人的破坏。比如,能够发现系统死机,发现有人扫描网络,发现网络流量异常等。通过发现,可以采取一定的响应措施。信息保障技术是以检测技术为核心,以恢复技术为后盾,融合了保护、检测、响应、恢复四大技术。但是,检测系统要发现全部的攻击是不可能的,完全准确地区分正确数据和攻击数据也是是不可能的。所以,信息保障系统并不能完全保障系统的安全。所以,在努力改进检测技术的同时,也在努力寻找新的技术途径。

收稿日期:2006-05-16
基金项目:河南省科技攻关项目(0524220044);河南工业大学重点资助项目(050216)
作者简介:柴争义(1976-),男,陕西渭南人,硕士,讲师,主要从事计算机网络、信息安全方面的研究工作。

1.3 信息可生存性技术

可生存性的主要思想可以总结为“容”,是一种增强免疫能力的技术。所谓生存技术就是系统在攻击、错误和突发事故的情况下、仍然可以及时地完成使命、为用户提供服务的能力。可生存技术是对传统的安全技术的突破,融合了传统网络安全技术中的冗灾、容侵、可靠性设计等技术。它以网络的实际情况为依据,假设网络中的任何一个节点都可能因为攻击、故障和意外事故等而失效。可生存性研究已经成为网络信息安全研究的新方向。入侵容忍被称为生存技术中的核心技术。

2 入侵容忍技术概念

入侵容忍技术就是认同安全问题的不可避免性。针对安全问题,不再将消除或者防堵作为第一重点,而把目光投射到如何在攻击之下系统仍能保证不间断地正常运行这一点。譬如一个金融系统在遭到网络攻击的情况下,仍旧保持正常的交易,不致因系统的崩溃造成巨大的损失。这就是入侵容忍[1],也就是说,在存在攻击、错误或突发事件的情况下,系统仍然可以及时地完成它的使命。入侵容忍技术融合了数据容错、免疫理论、门限密码学、数据恢复技术、入侵检测等等相关理论和技术,在容侵数据库、容侵 CA 等方面有很多的研究。自然界存在各种病毒和细菌,由于人体具有一定的免疫性,抵制和瓦解了大约 90% 以上的进攻和入侵。换句话讲,由于人体的免疫性可以容忍大约 90% 以上的入侵,人体就是一个很好的容侵系统。参考生物的免疫特性,入侵容忍技术作为信息安全的一种全新思想,成为了国内外网络安全领域研究的新热点。

3 入侵容忍技术的特点和功能

无数的网络安全事件告诉人们,网络的安全仅依靠“堵”和“防”是不够的。入侵容忍技术就是基于这一思想,要求系统中任何单点的失效或故障不至于影响整个系统的运转。由于任何系统都可能被攻击者占领,因此,入侵容忍系统不相信任何单点设备。也就是说,任何单点发生故障不影响整个系统的运转。

入侵容忍可通过对权力分散及对技术上单点失效的预防,保证任何少数设备、任何局部网络、任何单一场点都不可能做出泄密或破坏系统的事情,任何设备、任何个人都不可能拥有特权。因而,入侵容忍技术同样能够有效地防止内部犯罪事件发生。

入侵容忍的宗旨就是如何在入侵发生的情况下,使系统仍能为合法用户提供预期的有效服务。因此,入侵容忍系统必须具有以下功能[2]:

(1)自我诊断能力。入侵容忍仍旧依赖检测或评估系统,称为入侵容忍的触发器,通过检测到局部系统的失效或估计到系统被攻击,然后调整系统结构,重新分配资源,从而达到继续服务的目的。

(2)故障隔离能力。如果诊断部分认为某种操作可能会严重影响后续的系统运作,隔离机制会将可疑的操作隔离到特殊区域。针对被隔离的数据和操作,当判决系统认为确实是攻击时,就将被隔离的操作删除掉。反之,就将这些隔离的内容融合到正确的系统中去。

(3)还原重构能力。具有容侵能力的系统必须修正所有被攻击影响到的数据,而又不能采用简单的回退恢复。系统必须保证未被感染的部分不被恢复,仅仅还原被感染的文件,让用户的大部分工作得以保留。

4 入侵容忍技术的实现方法

实现入侵容忍有两种方法[3]:一种是基于攻击响应,这也是比较容易想到的解决方案,通过改进检测系统,加快反应时间,从而将信息保障技术上升到一种在攻击发生的情况下能够继续工作的系统;另一种则被称为攻击遮蔽,是指攻击发生了以后,整个系统好像没什么影响。这两种实现方式各有优缺点。

4.1 基于攻击响应的入侵容忍实现方法

攻击响应的入侵容忍技术仍旧依赖检测或评估系统,或称为入侵容忍触发器系统。通过检测到局部系统的失效或估计到系统被攻击,然后调整系统结构,重新分配资源,从而达到继续服务的目的。攻击响应的入侵容忍系统一般都包括一个基于风险概念的入侵预测系统、一个具有很高正确率的入侵判决系统、一套系统资源控制系统和在线的修复管理程序。有些入侵容忍的体系中还包括隔离机制。当入侵检测系统预计某些活动可能是攻击时,就能调用资源的重新分配以减缓这种可能是攻击的操作。如果预测系统认为某种操作可能会严重影响后续的系统运作,则隔离机制会将这种可疑的操作隔离到其他区域。最后,到入侵判决系统作出正确的判决以后,修复管理程序再将攻击操作所导致的错误结果进行修补。针对被隔离的数据和操作,当判决系统认为确实是攻击时,就将被隔离的操作删除掉。当判定不是攻击时,就将这些隔离的结果融合到正确的系统中去。

由此可见,攻击响应的入侵容忍技术非常依赖于入侵判决系统。但目前的入侵检测系统拥有太高的误警率和太高的漏警率,从而无法担当入侵容忍触发器的重任。资源调整系统是入侵容忍系统中的重要环节。如何有效地调整资源,保证最大程度地限制被破

坏区域的扩大是该类入侵容忍系统所要研究的。已有的许多设备可以作为资源调整系统的基础,如具有带宽调整功能的防火墙就可以将被怀疑的攻击 IP 地址的带宽限制在一定的范围内,从而保证其他用户的正常通信。通过重新定向的技术可以把可疑的操作导向到一个隔离区域从而保护系统的正常运转[4]。修补系统是该类型入侵容忍技术中的一个难点。一旦最后的判决认为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,不能称此系统为入侵容忍,只能被称为是简单的恢复。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,这才是入侵容忍的宗旨。如何跟踪每个可疑的操作,如何备份就成为这个体系中的重要内容。许多入侵容忍的系统就基于这样的结构,如 ITDB 数据库系统、Internet 的服务保护系统等[5]。这样的入侵容忍不需要重新设计系统结构,系统的操作和连接界面也可以保持与原有的一样。

4.2　基于攻击遮蔽的入侵容忍实现方法

攻击遮蔽的方法就是一开始就重新设计整个系统,以保证攻击发生后对系统没有太大的影响[6]。该方法的原理可以用古老的容错技术进行说明。比如,在设计时就制造足够的冗余,以保证当部分系统被攻击时,整个系统仍旧能够正常工作。当然,入侵容忍的冗余并不是简单的容错中的冗余,入侵容忍的冗余技术应该保证各冗余部件之间具有复杂的关系,并具有不一样的结构。类似双机备份这样的技术没有办法构成入侵容忍的结构,因为攻击者攻克第一个服务器,他也就能够攻克第二个服务器。当需要机密性服务时,双机备份也不行,因为攻入一个系统就能够得到所有的信息。多方安全计算的技术、门槛密码技术、Byzantine 协议技术等成为入侵容忍技术的理论基础。这些理论都具有同样一个基本假设,就是计算环境是不可信的。要设计一种结构,使可信的部分系统能够在不可信的环境中安全地合作,才能完成系统的使命。“n 个个体中的 t 个个体参与合作就能够完成某种密码计算,而少于 t 个个体即使合作也无法完成这种密码计算”,这就是门槛密码学的一个简单解释。这就是说,只要少于 t 个个体被攻击者控制了,只要还拥有多于 t 个个体,就能完成这种计算而攻击者不能完成。Byzantine 容错主要针对随机错误发生,当错误发生时,只要满足一定的条件,整个系统仍旧能够得出正确的结果。

5　结　论

随着网络和计算机的迅速发展,传统的安全方案已经不能解决全部的安全问题。一个基本的事实就是没有人能够保证一个系统能够抵制任何攻击、故障和事故。入侵容忍这一新技术,不仅仅是阻止攻击者,更重要的是在攻击、故障或事故已经发生的情况下,能保证关键功能继续执行,关键系统能够持续地提供服务。入侵容忍技术是理解风险分析最好的一种技术,因为它不仅放弃了过去绝对安全的假设,其实现机制也是针对系统使命来进行,而不是致力于完善和保护工具本身。不过,入侵容忍技术并不能替代第一代和第二代安全技术。过去的安全技术以有效性和相对更低的成本优势,仍旧具有广泛的应用前景。各种新的保护、检测、响应和恢复技术对整个信息网络的发展具有重要的意义,并具有非常巨大的发展空间。入侵容忍技术,作为一种新的安全技术将在关键的信息系统中发挥重要作用。

参考文献:

[1] Westmark V R. A Definition for Information System Survivability[C] // In: Proceeding of the 37th Hawaii Internal Conference on System Sciences (HICSS '04), Truck 9. Washington: IEEE Computer Society Press, 2004.

[2] Linger R C, Mead N R, Lipson H F. Requirements Definition for Survivable Network Systems[R]. [s. l.]: System Design Laboratory, SRI International Press, 2002.

[3] Mead N R, Ellison R J, Linger R C, et al. Survivable Network Analysis Method[C] // In: Intrusion Tolerant Systems Joint PI Meeting Presentation. Washington: IEEE Computer Society Press, 2004.

[4] Linger R C, Lipson H F, McHugh J, et al. Life-Cycle Models for Survivable Systems[R]. Sledge TECHNICAL REPORT CMU/SEI-2002-TR-026 ESC-TR-2002-026. Washington: IEEE Computer Society Press, 2002.

[5] 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, 19(2): 119-123.

[6] 荆继武,冯登国. 一种入侵容忍的 CA 方案[J]. 软件学报. 2002, 13(8): 1417-1422.