<<容忍入侵方法与应用>>

图书基本信息

书名：<<容忍入侵方法与应用>>

13位ISBN编号：9787118067767

10位ISBN编号：7118067768

出版时间：2010-5

出版时间：国防工业出版社

作者：郭渊博，王超 著

页数：244

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（2007AA01 Z405）”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人侵模型，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，给出了一种容忍人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，讨论了容忍人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。

<<容忍入侵方法与应用>>

内容概要

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码的客户一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。

<<容忍入侵方法与应用>>

书籍目录

章节摘录

插图：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。

编辑推荐

《容忍入侵方法与应用》主要内容：面向服务的容忍入侵模型。
秘密共享协议研究。
容忍入侵的可信第三方系统设计及其规格说明。
容忍入侵的入侵响应模型研究与设计。
容忍入侵的系统安全性评估方法。
容忍入侵的自适应重配置安全通信模型与设计。
容忍入侵的密码协议自适应安全运行防护。
容忍入侵的数据存储方案。
容忍入侵的应用服务器中间件结构设计与实现。

<<容忍入侵方法与应用>>

版权说明