第一图书网, tushu007.com

<<基于随机博弈模型的网络安全分 >

图书基本信息

书名：<<基于随机博弈模型的网络安全分析与评价>>

13位ISBN编号：9787302268758

10位ISBN编号：7302268754

出版时间：2011-12

出版时间：清华大学出版社

作者：林闯，王元卓，汪洋 著

页数：277

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：http://www.tushu007.com

内容概要

本书全面论述了随机博弈模型的相关知识，以及如何应用其对具体网络安全问题进行分析与评价。
第1章至第4章介绍了基础模型理论和相关知识，包括概率论、随机模型、排队模型、随机petri网模型以及博弈与随机博弈的相关知识；第5、6章阐述了网络安全模型分析框架及网络攻击模型与评价技术，给出了基于模型的网络安全分析的一般框架；第7章讨论了基于随机模型的dos攻击及邮件攻击问题的模型及安全分析；第8章介绍了基于博弈模型的无线网络路由机制、信任评估以及节点合作信任激励方面的模型和应用分析；第9章给出了随机博弈网模型的具体应用，包括企业网机密性与完整性分析、企业网防御机制的分析、电子商务的安全分析、网上银行的安全分析等。

本书可用作计算机、通信、信息等专业的教材或教学参考书，也可供这些专业的研究人员和工程技术人员阅读。

书籍目录

《基于随机博弈模型的网络安全分析与评价》
第1部分 基础理论
第1章 概率论与随机过程
1.1 概率论
1.1.1 概率的定义
1.1.2 条件概率和独立性
1.1.3 贝叶斯定理
1.2 随机过程
1.2.1 随机变量
1.2.2 随机过程
1.2.3 马尔可夫链
参考文献
第2章 排队模型与随机petri网
2.1 排队模型
2.1.1 排队的基本形式
2.1.2 排队分析
2.2 随机petri网
2.2.1 petri网模型概述
2.2.2 时间变迁
2.2.3 随机petri网(spn)
.2.2.4 广义随机petri网(gspn)
2.2.5 随机回报网
2.2.6 随机petri网与排队论
2.2.7 随机高级petri网
参考文献
第3章 博弈与随机博弈
3.1 博弈
3.1.1 博弈论基础
3.1.2 纳什均衡
3.1.3 拍卖理论
3.1.4 合作博弈
3.2 随机博弈
3.2.1 随机博弈基础
3.2.2 马尔可夫均衡
参考文献
第4章 随机博弈网
4.1 基本概念与性质
4.2 模型建立方法
4.2.1 基本模型方法
4.2.2 竞争博弈典型模型方法
4.2.3 合作博弈典型模型方法
4.3 效用描述方法
4.4 均衡策略计算方法
4.4.1 基于层次化矩阵的计算方法
4.4.2 基于非线性规划的计算方法

4.5 层次化分析方法
4.6 基于随机博弈网的安全性评价
参考文献
第2部分 网络安全模型与评价方法
第5章 网络安全问题概述
5.1 网络安全威胁
5.1.1 网络服务安全
5.1.2 业务流程安全
5.2 网络攻击行为
5.2.1 侦查攻击
5.2.2 会话攻击
5.2.3 权限提升攻击
5.2.4 针对机密性的攻击
5.2.5 针对完整性的攻击
5.2.6 拒绝服务攻击
5.2.7 命令植入攻击
5.2.8 服务过程攻击
5.3 防御措施
5.3.1 模式验证
5.3.2 模式硬化
5.3.3 强制web服务安全性策略
5.3.4 soap消息处理
5.3.5 web服务安全性
5.4 网络安全中的博弈问题
参考文献
第6章 网络安全模型与评价
6.1 网络安全性评价概述
6.2 网络安全性评价指标
6.2.1 安全性指标的定义及数学表示
6.2.2 安全性指标的计算
6.3 网络安全性评价模型
6.3.1 网络安全问题的分类
6.3.2 网络安全性评价模型分类
6.3.3 网络安全性评价整体模型
6.4 网络攻击模型分类
6.4.1 攻击者模型
6.4.2 攻击行为模型
6.5 网络攻击模型方法
6.5.1 攻击树和攻击图
6.5.2 特权图
6.5.3 模型检测
6.5.4 基于状态的随机模型
6.5.5 基于模型的高级随机模型
6.6 网络可生存性分析
参考文献
第3部分 随机博弈模型在网络安全分析评价中的
第7章 基于排队模型的网络安全分析

7.1 拒绝服务攻击模型和安全分析
7.1.1 拒绝服务攻击概述
7.1.2 拒绝服务攻击的排队模型
7.1.3 模型求解
7.1.4 安全性评价指标与数值算例
7.2 邮件攻击模型和安全分析
7.2.1 邮件攻击概述
7.2.2 邮件系统攻击模型
7.2.3 邮件攻击的排队分析
7.2.4 模型求解
7.2.5 安全性评价指标
7.2.6 数值算例
参考文献
第8章 基于博弈模型的网络安全分析
8.1 基于非合作博弈的无线网络路由机制
8.1.1 基于信任度的机制
8.1.2 基于非合作博弈的激励机制
8.1.3 基于网络编码的优化
8.1.4 节点共谋
8.1.5 研究挑战与未来展望
8.2 基于博弈的信任评估模型
8.2.1 移动自组织网络环境下的信任评估
8.2.2 基于博弈的信任评估模型
8.2.3 信任度计算
8.2.4 信任关系的建立
8.2.5 实验分析
8.3 基于二阶段拍卖的信任激励机制
8.3.1 移动自组织网络环境下的信任激励机制
8.3.2 基于拍卖的信任评估
8.3.3 基于二阶段拍卖的节点合作信任激励机制
8.3.4 激励效能分析
参考文献
第9章 基于随机博弈网模型的网络安全分析
9.1 企业网机密性与完整性分析
9.1.1 问题描述
9.1.2 攻击防御行为
9.1.3 分角色模型
9.1.4 组合模型及机密性、完整性分析
9.2 企业网防御机制分析
9.2.1 问题描述
9.2.2 防御机制
9.2.3 基于攻—防结构的sgn模型
9.2.4 组合模型及防御机制分析
9.3 电子商务的安全分析
9.3.1 问题描述
9.3.2 攻击防御行为
9.3.3 分角色模型及攻击成功率分析

9.4 网上银行的安全分析
9.4.1 问题描述
9.4.2 分角色模型
9.4.3 层次化模型化简及安全性分析
参考文献
索引

章节摘录

版权页： 插图： 系统安全性评价模型可划分为几个子模型：系统行为模型，攻击者模型，系统脆弱性模型；系统行为模型中，还可进一步建立容侵机制子模型和系统负载子模型。
在安全性评价模型上，建立安全测度，由安全性指标表现系统的安全性能。
图6.3.2中的箭头标明了各部分之间的交互作用。
各自模型之间联系表明了子模型评价要重点涉及的关系主要存在如下3种：（1）系统脆弱性与攻击者之间的关系：系统脆弱性与攻击者对其的探寻和利用之间的匹配；（2）系统行为与攻击者之间的关系：系统随机故障与人为攻击的区分和组合；（3）系统行为与脆弱性之间的关系：系统行为和故障对脆弱性的影响。
在建立清晰的网络系统子模型的基础上，将子模型进行组合分析，可以获得全面的系统行为模型，从而评价系统的安全性能。
虽然上述子模型涵盖的内容和侧重点各不相同，但是它们的模型对象都是与安全相关的系统行为和状态。
因此，可以考虑将它们归结到一个统一的安全模型。
从方法论的意义上讲，在上述安全性分析框架中，系统描述可以使用经典可信赖性分析中的随机方法。
然而，人为攻击的刻画还没有确定的方法，这将是一个充满挑战的课题，本章下面两节将就此给出详细讨论。
6.4网络攻击模型分类 建立适用的攻击模型要满足两方面的要求。
首先，模型要有恰当的抽象程度，这依赖于攻击模型的类别、目的和应用范畴。
对于一个给定的目标系统，确定模型恰当的抽象程度取决于很多因素，例如，系统自身行为特点、安全性评价指标等。
其次，模型包括系统和攻击者行为中的关键点，例如，因攻击行为可能改变的模型的相关状态以及可能影响攻击行为的系统的相关状态。
攻击是攻击者对系统进行的有特定目的的行为，有可能造成系统的安全破坏。
目前，新的攻击方法和手段不断出现，且具有随机性、多样性、隐蔽性和传播性，因此对攻击模型的刻画绝非易事。
从网络安全性评价的角度出发，描述攻击行为需要考虑如下3个特点：（1）攻击是含有人为意图的行为，人们观察到的安全事件可能表现出随机性，但存在隐蔽的依赖关系；（2）攻击者具有学习能力和决策能力，同时，攻击者的知识和经验也是攻击中的重要因素；（3）攻击是攻击者与网络系统进行交互的行为，攻击者要寻找系统可利用的漏洞和脆弱性，并在攻击的同时受到网络系统防火墙等安全措施的影响。

编辑推荐

《基于随机博弈模型的网络安全分析与评价》主要以排队论、随机Petri网、博弈论以及随机博弈网为模型基础，深入地探讨网络安全威胁的模型方法，并结合具体应用对网络中的典型安全问题进行建模、分析与量化评价。
书中绝大部分内容取材于我们近期在国际、国内一流学术期刊和会议上发表的论文，全面、系统地展示了很多新的研究成果和进展。
《基于随机博弈模型的网络安全分析与评价》可用作计算机、通信、信息等专业的教材或教学参考书，也可供这些专业的研究人员和工程技术人员阅读。

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:http://www.tushu007.com