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

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

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。