<<网络用户行为的安全可信分析与控制>>

图书基本信息

书名：<<网络用户行为的安全可信分析与控制>>

13位ISBN编号：9787512107014

10位ISBN编号：7512107013

出版时间：2011-8

出版时间：北京交通大学出版社

作者：田立勤

页数：158

内容概要

《网络用户行为的安全可信分析与控制》主要论述：新型网络中有关用户行为安全可信的分析与控制问题，共10章。
第1章主要讲述云计算等新型网络及其对用户行为安全可信需求。
第2章主要讲述用户行为信任评估中有关行为证据的预处理问题。
第3章主要讲述单次用户行为信任的评估问题，重点讲述了基于层次分析法（AHP）的用户行为信任评估方法。
第4章主要讲述长期用户行为信任评估问题，重点讲述了基于滑动窗口的长期行为信任评估机制。
第5章主要讲述服务提供者之间如何在共享用户行为信任信息的基础上评估用户行为信任。
第6章主要讲述用户行为信任预测问题，重点讲述了基于贝叶斯网络的多条件用户行为信任预测机制。
第7、8章主要讲述用户行为的控制问题，包括基于信任预测的用户行为博弈控制机制和基于用户行为信任的动态角色访问控制机制。
为了使本书的知识系统完整，第9章讲述了传统的用户身份认证机制，第10章对照传统的用户身份认证机制讲述用户行为认证问题。

<<网络用户行为的安全可信分析与控制>>

书籍目录

章节摘录

版权页：插图：1.3.2 可信网络的体系结构互联网在设计之初对安全问题考虑不足，是产生当前网络众多脆弱性的一个重要因素。
然而目前的许多网络安全设计很少触及网络体系的核心内容，大多是单一的防御、单一的信息安全和打补丁附加的机制，遵从“堵漏洞、作高墙、防外攻”的建设样式，以共享信息资源为中心、在外围对非法用户和越权访问进行封堵，以达到防止外部攻击的目的。
在攻击方式出现复合交织的趋势下，当前安全系统将变得越来越臃肿，严重地降低了网络性能，甚至破坏了系统设计开放性、简单性的原则。
因此基于这些附加的、被动防御的安全机制上的网络安全是不可信的，从体系结构设计的角度减少系统脆弱性并提供系统的安全服务尤为重要。
尽管在开放式系统互联参考模型扩展部分增加了有关安全体系结构的描述，但只给出了一个概念性的框架，很不完善。
网络安全已不再仅局限于信息的可用性、完整性和机密性，服务的安全将被作为一个整体属性为用户所感知的趋势日益凸现，这需要重新考虑网络体系设计，整合多种安全技术并使其在多层面上相互协同运作。
一方面，作为补丁而附加到网络系统上的传统安全机制，由于单个安全技术或者安全产品的功能和性能都有其局限性，只能满足特定的安全需求，如入侵检测不能对抗蠕虫病毒，防病毒软件不能对抗拒绝服务攻击，而防火墙对病毒攻击和木马攻击也无能为力。
此外，安全系统自身在设计、实施和管理各个环节上也不可避免地存在着脆弱性，严重威胁这些防御设施功效的发挥。
另一方面，网络安全研究的理念已经从被动防御转向了积极防御，不再局限于在共享信息外围部署安全防御，而需要从访问源端的开始进行安全分析，尽可能地将不信任的访问操作控制在源端。
因此，十分需要为网络提供可信的体系结构，避免出现类似传统附加性安全机制的弊端。
可信网络体系结构研究必须充分认识到网络的复杂异构性，从系统的角度保障安全服务的一致性。

编辑推荐

《网络用户行为的安全可信分析与控制》是由北京交通大学出版社出版的。

版权说明