

计算机网络安全技术发展趋势探索

——评《计算机网络管理与安全技术研究》

在信息化高速发展的今天,计算机网络安全已成为国家安全、经济发展和社会稳定的重要组成部分。随着新一代信息技术与经济社会发展各领域的深度融合,网络安全技术在维护国家安全、支撑产业转型、服务社会发展、保护公众利益等方面的重要作用愈加凸显。然而,网络攻击、数据泄漏等安全事件频发,使得网络安全成为全球关注的焦点。在这样的背景下,计算机网络安全技术的发展趋势成为业界和学术界共同关心的话题。

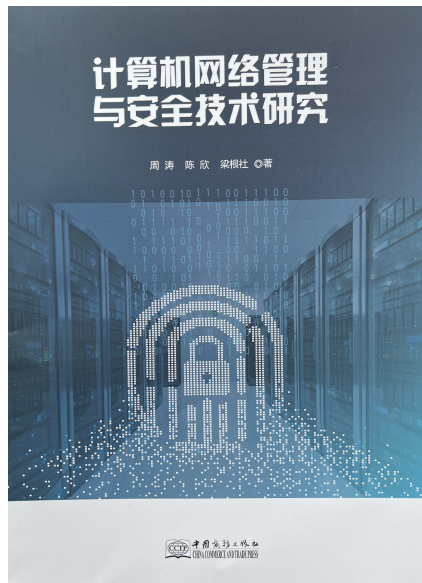
网络安全关系到个人、企业、国家乃至整个社会的经济发展与安全。《计算机网络管理与安全技术研究》一书结合近期新的网络管理与安全技术成果、方法和实际应用,深入阐述了计算机网络管理与安全技术方面的内容。全书共分为12章。第1章介绍了网络管理的基本概念、基本功能、标准和对象。第2章讲解了数据链路层的基本理论和功能。第3章分享了网络层的相关内容。第4章深入剖析了网络管理的基础架构、模式和基本协议等。第5章探讨了远程网络监视的基本理论、管理信息库以及应用等。第6章阐述了网段规划与管理,包括IP地址分配、域名管理以及VLAN管理等。第7章讲述了网络监控管理的重要性、软件工具以及故障管理的方法等。第8章全面介绍了网络安全的基础知识、安全服务和机制、安全策略以及管理等。第9章深入探究了对称密码体制、非对称密码体制以及数字证书等密码技术。第10章论述了信息隐藏技术的理论和应用,如数字水印等。第11章阐解了防火墙的基本概念、体系结构以及主要技术等。第12章探讨了病毒理论、木马技术以及网络病毒的危害和防治方法。

作者指出,网络管理具有配置管理、性能管理、故障管理、安全管理和计费管理等基本功能。网络管理体系有集中式、分布式和层次式等不同的管理模式,网络协议在网络管理中起着重要的作用。网络监控可使用各种监控软件和工具来实时监测网络状态、性能以及流量等。防火墙技术、密码技术、信息隐藏技术以及病毒防治等关键技术可为网络安全提供有力的保障,帮助网络管理员有效应对各种网络安全威胁。

笔者认为,技术的快速发展使得网络安全形势日益复杂,传统的安全防护技术越来越难满足现代网络对安全的需求。许多企业仍然依赖于防火墙和杀毒软件等基础设施,这些措施通常无法抵御复杂的攻击手段。因此,有必要探索网络安全技术的发展趋势,找到更加全面和先进的技术来满足现实需求。随着新技术的日益涌现和法治环境的逐渐完善,计算机网络安全技术的发展主要呈现以下一些趋势。①人工智能(AI)赋能网络安全,带来技术革新。近年来,AI技术在众多领域的深入应用,为网络安全带来了新的变革。AI技术能够实现对复杂多变网络安全环境的深度理解和智能决策,生成适合的防御措施和修复方案。未来,随着大语言模型与多模态技术的加速融合,生成式人工智能将在威胁检测与响应、自动化安全防护与修复、实时威胁情报与预测等方面发挥更大作用。这标志着智能化安全技术将成为计算机网络安全领域的重要发展趋势。②隐私计算技术提供技术保障。在数据要素加速开放共享的新形势下,隐私计算正成为支撑数据要素流通的核心技术。隐私计算技术在确保数据不泄漏、限定数据处理目的方面具有原生优势。随着数据安全法的落地实施和公众提高隐私保护意识,隐私计算技术将在计算机网络安全领域得到更广泛的应用,为数据安全提供有力的技术保障。③内生安全防御架构的兴起。传统边界防御架构难以有效应对日益复杂的网络安全威胁。因此,向内生安全防御架构转变成为计算机网络安全领域的重要趋势。内生安全防御架构强调,在系统设计上天然具有对攻击的识别和防御能力,从而实现对网络安全的全面保障。这一转变将推动计算机网络安全技术向更加智能化、自适应的方向发展。④供应链安全管理的加强。随着关键信息基础设施安全保护条例、网络安全审查办法等相关法律法规的制定和施行,对供应链安全提出更高标准的规定与要求。未来,计算机网络安全技术将更加重视供应链安全管理的加强,通过技术手段实现对供应链各环节的安全监控和风险防范。

综上,计算机网络安全技术的发展趋势呈现出智能化、隐私保护、内生安全防御、供应链安全管理不断加强以及法律法规更加完善等多重特点。这些趋势将推动计算机网络安全技术不断向前发展,为数字化时代网络安全提供有力的技术支撑和保障。

(刘瓔川/唐山幼儿师范高等专科学校/副教授;殷建艳/唐山幼儿师范高等专科学校/副教授)



书名:计算机网络管理与安全技术
研究

作者:周涛,陈欣,梁根社

出版社:中国商务出版社

ISBN:9787510342042

出版时间:2023年7月

定价:50元