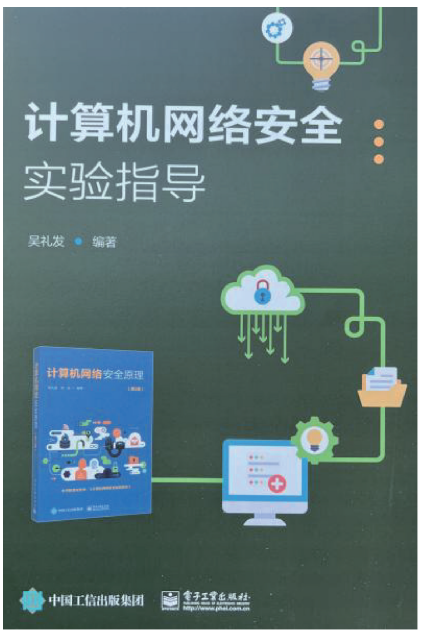
计算机网络安全技术发展趋势
——评《计算机网络安全实验指导》

计算机网络已成为信息社会不可或缺的基础设施,广泛渗透于并支撑着社会经济的各个领域。然而,伴随着网络的广泛应用,网络安全问题也日益凸显,成为制约信息技术产业健康发展的重要因素。网络攻击手段不断翻新,威胁类型日益复杂多样,给国家安全、社会稳定和个人隐私带来了前所未有的挑战。基于此,了解和掌握计算机网络安全技术的发展趋势,不仅具有重要的现实意义,也是保障国家安全、促进经济社会发展的重要基础。

计算机网络安全技术作为应对网络威胁的关键手段,其发展直接关系到网络空间的安全稳定。《计算机网络安全实验指导》是一本针对计算机网络安全原理的实验指导书,涵盖了计算机网络安全的基础理论及其实践操作。全书分为 14 个知识单元,设计了 21 个实验项目,内容全面具体,可帮助读者深入理解和掌握计算机网络安全原理。每个试验项目都详细列出了实验目的、内容、要求及环境,并提供了试验示例,便于读者构建试验环境并进行操作。书中所使用的工具软件均为可公开获取的免费软件,方便读者下载和使用。全书结构清晰,逻辑严密,为读者构建了一个完整的计算机网络安全试验框架。每章内容均围绕核心试验展开,既有理论深度,又注重实践应用,具有广泛的适用范围,在网络安全教育和实践中具有重要价值。



书名:计算机网络安全实验指导
编者:吴礼发
出版社:电子工业出版社
ISBN:9787121397790
出版时间:2020 年 10 月
定价:59 元

编者指出,在计算机网络安全领域,人工智能与自动化技术的深度融合正成为不可逆转的发展趋势。随着大数据、机器学习等技术的不断成熟,人工智能在网络安全中的应用范围日益广泛,其智能化、自动化的特点为网络安全防护带来革命性的变化。人工智能通过机器学习算法,自动学习网络流量的特征,识别异常行为模式,从而实现对未知威胁的实时检测和预警,既提高了检测的准确性和时效性,还大大减轻了安全人员的工作负担。一旦检测到潜在威胁,人工智能系统就能够迅速启动预设的应急响应流程,自动隔离受感染设备、阻断攻击路径、收集攻击证据等,有效遏制威胁的扩散。生成式人工智能在网络安全领域的应用也初显成效,以 Microsoft Security Copilot 为代表的安全解决方案,能够利用大型语言模型的强大表达能力和专用安全模型的专业知识,对复杂多变的网络安全环境进行深度理解和智能决策,生成适合的防御措施和修复方案,并自动执行或辅助专业人员完成相关任务。

笔者认为,面对日益复杂的网络安全威胁,构建多层次、多维度的安全防护体系已成为计算机网络安全技术发展的必然选择,通过综合运用多种技术手段和管理措施,形成全方位、立体化的安全防护网,可有效抵御各类网络攻击和威胁。传统网络安全防护往往侧重于某一层面或某一环节,难以形成有效的整体防护,而多层次防护则强调从网络边界、主机系统、应用层面等多个层次入手,实施全方位的安全防护。例如在网络边界部署防火墙、入侵检测系统等设备,对进出网络的数据流进行过滤和监控;在主机系统层面安装防病毒软件、配置安全策略等,防止恶意软件的入侵和扩散;在应用层面则采用加密技术、身份认证等手段,保障数据传输和访问的安全性。除了技术手段外,安全防护体系还需要综合考虑管理、法律、教育等多个维度。在管理方面,建立健全的安全管理制度和流程,明确安全责任和义务,加强安全培训和演练等;在法律方面,完善相关法律法规体系,加大对网络犯罪的打击力度;在教育方面则普及网络安全知识提高公众的网络安全意识等。此外,随着新技术新应用的不断涌现,如区块链、量子加密等,亦将为安全防护体系注入新的活力。区块链技术以其去中心化、不可篡改的特点,为数据安全和隐私保护提供了新的解决方案;量子加密技术则以其超强的加密能力,为数据传输提供了更加安全的保障。

综上,在信息化浪潮的推动下,计算机网络安全性直接关系到国家稳定、经济发展和个人隐私。面对不断演变的网络威胁,计算机网络安全技术的发展显得尤为关键。从基础密码学到前沿人工智能,再到多层次防护体系的构建,见证了网络安全防护手段的全面升级与革新。展望未来,网络安全领域将持续探索与创新,融合更多前沿科技,如量子计算、边缘计算等,以应对复杂多变的网络攻击,构建一个更加协同、高效的网络安全防护生态。

(庄渊/新加坡阿米提全球学院)