计算机领域关键威胁、防御技术与未来挑战的综合评述

董佳

嘉兴南洋职业技术学院，浙江嘉兴，314031；

摘要：随着信息技术的迅猛发展，计算机网络安全已成为保障国家安全、社会稳定和经济运行的重要组成部分。本文旨在系统分析当前计算机领域面临的主要安全威胁，包括人为攻击（如黑客攻击、社交工程攻击）、技术威胁（如恶意软件、分布式拒绝服务攻击）及组织级威胁（如高级持续性威胁、供应链攻击）。在此基础上，综述了常用的防御技术，如防火墙、入侵检测系统、加密技术和访问控制，并探讨了面向未来的防御技术，如人工智能、量子计算与生物识别技术的应用前景。最后，本文讨论了未来在技术与管理方面所面临的挑战，提出了加强加密算法研究、推动量子密码学发展、提高安全意识与培训等对策建议。研究表明，构建多层次、多维度的安全防护体系是应对日益复杂网络威胁的关键。

关键词：计算机网络安全；关键威胁；防御技术；人工智能；量子计算；安全管理；应急响应

DOI：10.64216/3080-1508.25.06.035

引言

本论文旨在全面梳理当前计算机领域面临的主要安全威胁，归纳主流防御技术的工作原理与应用场景，并前瞻性地分析未来技术演进带来的新挑战。通过综合评述，本文为学术界、产业界以及政策制定者提供了系统的参考框架，以促进网络安全技术的创新发展与管理体系的完善。具体而言，本文的研究目的包括：一是帮助从业者识别潜在风险，增强防护意识；二是推动新技术在网络安全领域的应用探索；三是为制定科学合理的网络安全战略提供理论支撑。总之，通过对计算机领域关键威胁、防御技术及其未来挑战的深入探讨，本文期望能够为建设更加稳健、可信的网络环境贡献智慧和力量。

1 计算机领域关键威胁分析

随着信息技术的广泛应用，计算机系统面临的威胁日益复杂多样。这些威胁不仅来自技术层面的漏洞，也涉及人为因素和组织性攻击。根据攻击主体、手段和目标的不同，可将当前计算机领域的关键威胁划分为人为威胁、技术威胁和组织威胁三大类。深入分析这些威胁的特征与机制，是构建有效防御体系的前提。

1.1 人为威胁

人为威胁主要指由个体或群体通过非技术或低技术手段，利用系统使用者的心理弱点或操作疏忽实施的攻击行为，具有隐蔽性强、成本低、成功率高的特点。

1.1.1 黑客攻击

黑客攻击是最广为人知的网络安全威胁之一，通常指未经授权的个人或组织利用技术手段非法访问、篡改、破坏或窃取信息系统中的数据。攻击方式包括端口扫描、暴力破解、SQL 注入、跨站脚本（XSS）、远程代码执行等。现代黑客攻击已从早期的“技术炫耀”演变为有组织、有目的的经济犯罪或网络间谍活动。攻击者往往具备较高的技术水平，能够长期潜伏于目标系统中，持续收集敏感信息或为后续攻击做准备。

1.1.2 社交工程攻击

社交工程（Social Engineering）是一种通过操纵人类心理而非技术漏洞来获取信息或权限的攻击方式。攻击者利用人们的信任、恐惧、好奇心或责任感，诱导其泄露密码、点击恶意链接或执行危险操作。常见的形式包括冒充上级领导要求转账、伪装 IT 支持人员索要账户信息、伪造紧急事件诱导用户配合等。由于此类攻击绕过了传统防火墙和杀毒软件的防护，防范难度较大，已成为许多重大数据泄露事件的“第一入口”。

1.2 技术威胁

技术威胁源于系统、软件或网络协议本身存在的漏洞或缺陷，攻击者通过技术手段加以利用，实现对系统的控制或破坏。

1.2.1 恶意软件与病毒

恶意软件（Malware）是指任何旨在干扰、破坏或未经授权访问计算机系统的程序，包括病毒、蠕虫、木马、勒索软件、间谍软件等。其中，勒索软件（Ransomware）近年来尤为猖獗，攻击者通过加密用户文件或锁定系统，迫使受害者支付赎金以恢复访问。例如，“Wa

nnaCry”勒索软件在 2017 年利用 Windows 系统的“永恒之蓝”漏洞，感染了全球数十万台计算机，造成巨大经济损失。恶意软件通常通过电子邮件附件、恶意网站或 U 盘传播，具有自我复制和隐蔽运行的能力。

1.2.2 零日漏洞利用

零日漏洞（Zero-day Vulnerability）是指尚未被软件厂商发现或未发布补丁的安全漏洞。攻击者在漏洞公开前就已掌握其利用方法，可在系统毫无防备的情况下实施入侵。由于防御方无法提前部署防护措施，零日攻击具有极高的成功率和破坏力。例如，Stuxnet 病毒利用多个零日漏洞攻击伊朗核设施的工业控制系统，造成物理设备损坏。零日漏洞通常价格昂贵，多被国家级黑客组织或高级犯罪团伙使用，是 APT 攻击中的关键武器。

1.3 组织威胁

组织威胁是指由具备高度资源、技术和组织能力的团体发起的复杂、长期、多阶段的网络攻击，通常针对政府、军工、金融、能源等关键基础设施。

1.3.1 APT 攻击

高级持续性威胁（Advanced Persistent Threat，APT）是由高资源背景组织（如国家级黑客团队）发起的长期、隐蔽、定向的网络攻击。APT 攻击通常结合多种技术手段（如钓鱼邮件、零日漏洞、横向移动），分阶段渗透目标网络，潜伏数月甚至数年，持续窃取情报或破坏系统。其特点是高度定制化、低频率活动、强反检测能力。典型的 APT 攻击包括“震网”（Stuxnet）、“方程式组织”（Equation Group）等，目标多为国家机密或核心技术。

1.3.2 供应链攻击

供应链攻击（Supply Chain Attack）通过在软件开发、分发或更新环节植入恶意代码，实现“一击多杀”。攻击者不直接攻击最终目标，而是攻击其依赖的第三方供应商，利用信任关系将恶意程序传播至大量客户系统。2020 年的“SolarWinds”事件是供应链攻击的典型案例：攻击者在该公司网络监控软件的更新包中植入后门，导致美国多个联邦机构和大型企业被渗透。此类攻击影响范围广、追溯困难、修复成本高，已成为当前最具破坏力的网络威胁之一。

综上所述，计算机领域的安全威胁呈现出多样化、复杂化和组织化的发展趋势。从个体黑客到国家级 APT 组织，从简单病毒到精密供应链攻击，防御体系必须不断演进，才能有效应对日益严峻的网络安全挑战。

2 防御技术综述

面对日益复杂和多样化的网络安全威胁，防御技术不断发展演进，形成了从基础防护到智能响应、从被动拦截到主动预测的多层次安全体系。根据技术成熟度和应用广度，可将当前的防御技术划分为常用防御技术和面向未来的新兴防御技术两大类。

2.1 常用防御技术

2.1.1 防火墙

防火墙（Firewall）是网络安全的第一道防线，部署在网络边界或关键节点，用于监控和控制进出网络的数据流量。根据工作原理，防火墙可分为包过滤防火墙、状态检测防火墙和应用层防火墙。现代防火墙支持深度包检测（DPI），能够识别应用协议（如 HTTP、FTP、DNS），并基于预设安全策略阻止恶意流量。防火墙通过限制未授权访问、隔离内部网络与外部环境，有效防止外部攻击者直接渗透内网。

2.1.2 加密技术

加密技术是保障数据机密性、完整性和不可否认性的核心技术。对称加密算法（如 AES）使用相同密钥进行加解密，适用于大数据量传输；非对称加密算法（如 RSA、ECC）使用公钥和私钥配对，常用于密钥交换和数字签名。SSL/TLS 协议广泛应用于网页通信（HTTPS）、电子邮件和即时通讯中，确保数据在传输过程中不被窃听或篡改。此外，端到端加密（E2EE）技术在即时通讯和云存储服务中日益普及，进一步提升了用户隐私保护水平。

2.1.3 访问控制与认证

访问控制通过权限管理机制，限制用户对系统资源的操作范围，防止越权访问。常见的模型包括自主访问控制（DAC）、强制访问控制（MAC）和基于角色的访问控制（RBAC）。多因素认证（Multi-Factor Authentication, MFA）则通过结合“你知道的”（密码）、“你拥有的”（手机令牌、U 盾）和“你具有的”（指纹、人脸）三种认证方式，显著提升账户安全性。MFA 已成为防范密码泄露、钓鱼攻击的有效手段，广泛应用于金融、政务和企业系统中。

2.2 面向未来的防御技术

2.2.1 人工智能与机器学习

人工智能（AI）与机器学习（ML）正深刻改变网络安全防御模式。传统基于规则的检测方法难以应对新型、变种攻击，而 AI 可通过训练模型自动学习正常行为模式，识别异常流量或恶意活动。例如，基于深度学习的异常检测系统可发现零日攻击、APT 潜伏行为；自然语言处理（NLP）可用于分析日志、邮件内容，识别钓鱼或内部威胁。此外，AI 还可用于自动化漏洞扫描、威胁情报分析和安全事件响应，提升整体防御效率与智能化水平。

2.2.2 生物识别技术

生物识别技术通过采集和比对个体的生理或行为特征（如指纹、虹膜、面部、声纹、步态）进行身份认证，具有唯一性、不易伪造的优点。与传统密码相比，生物识别提升了认证的便捷性与安全性。现代系统普遍结合活体检测技术（Liveness Detection），防止照片、视频或 3D 模型欺骗。未来，行为生物识别（如键盘敲击节奏、鼠标移动轨迹）将实现持续身份验证，进一步增强系统对异常登录行为的识别能力。

综上所述，网络安全防御技术正从静态、被动的防护模式，向动态、智能、主动的综合防御体系演进。传统技术仍发挥基础作用，而人工智能、量子安全和生物识别等新兴技术则为应对未来挑战提供了新的解决方案。构建“技术+数据+流程”深度融合的智能安全体系，将成为保障数字时代网络安全的关键路径。

3 未来挑战分析

随着信息技术的持续演进和网络空间的不断扩展，网络安全面临的挑战日益复杂和严峻。这些挑战不仅体现在技术层面的攻防对抗升级，也反映在组织管理、人员意识和应急机制等软性能力的不足。总体来看，未来网络安全的发展将面临来自技术与管理两个维度的多重压力。

3.1 技术挑战

3.1.1 加密算法破解

加密技术是保障数据机密性和完整性的基石，但随着计算能力的提升，传统加密算法的安全性正受到威胁。例如，RSA、ECC 等广泛使用的公钥加密算法依赖于大数分解或离散对数难题的计算复杂性，而量子计算的发展可能在未来十年内通过 Shor 算法高效破解这些数学难题。即使在经典计算环境下，密码分析技术的进步和侧信道攻击（Side-channel Attacks）的出现，也使得部分弱加密实现面临被破解的风险，亟需推动更安全的加密标准和实现方式。

3.1.2 云计算与物联网安全

云计算和物联网（IoT）的普及极大提升了信息系统的灵活性和智能化水平，但也带来了新的安全风险。在云计算环境中，多租户架构可能导致数据隔离失效，虚拟机逃逸、API 滥用、配置错误等问题频发，且云服务的复杂性增加了安全监控和溯源难度。而在物联网领域，设备数量庞大、硬件资源受限、固件更新困难，使其成为攻击者理想的“跳板”。大量 IoT 设备缺乏基本的安全防护机制，易被劫持用于 DDoS 攻击或作为内网渗透的入口。此外，边缘计算与 5G 网络的融合进一步扩大了攻击面，对安全架构提出了更高要求。

3.2 管理挑战

3.2.1 安全意识与培训

尽管技术防御手段不断升级，但人为因素仍是安全链条中最薄弱的环节。员工缺乏基本的网络安全知识，容易成为钓鱼邮件、社交工程攻击的受害者。许多数据泄露事件源于内部人员的误操作或安全意识淡薄。因此，如何建立常态化的安全培训机制，提升全员的安全素养，成为组织面临的重要课题。未来需要将安全教育纳入员工入职培训和绩效考核体系，并通过模拟演练、案例教学等方式增强实际应对能力。

3.2.2 安全策略与规范制定

许多组织在安全管理上存在“重技术、轻制度”的倾向，缺乏统一、系统、可执行的安全策略和操作规范。安全政策往往流于形式，未能覆盖数据分类、访问控制、日志审计、第三方管理等关键环节。此外，随着合规要求（如《网络安全法》《数据安全法》《个人信息保护法》）的日益严格，组织需建立符合国家标准和行业规范的安全管理体系（如 ISO/IEC 27001、等级保护制度），并定期进行风险评估和合规审计，确保安全措施落地见效。

综上所述，未来网络安全的挑战是全方位、系统性的。技术层面需应对量子计算、云原生安全、AI 对抗等前沿问题，管理层面则需补齐意识、制度和响应能力的短板。唯有构建“技术+管理+人才”三位一体的综合防御体系，才能在日益复杂的网络威胁环境中实现可持续的安全防护。

4 对策与建议

面对日益复杂严峻的网络安全形势，必须从技术与管理两个维度协同发力，构建科学、系统、可持续的安全防护体系。针对前文分析的各类威胁与挑战，提出以下对策与建议。

4.1 技术层面

4.1.1 加强加密算法研究

为应对传统加密算法可能被破解的风险，应加大对高强度、抗攻击能力强的新型加密算法的研究与应用推广。重点支持国产密码算法（如 SM2、SM3、SM4、SM9）在政务、金融、能源等关键领域的部署，提升自主可控能力。同时，积极参与国际密码标准制定，推动轻量级加密算法在物联网设备中的应用，确保资源受限环境下的数据安全。

4.1.2 人工智能在网络安全中的应用

积极推动人工智能与网络安全深度融合，发展智能威胁检测、自动化响应和预测性防御能力。鼓励开发基于机器学习的异常行为分析系统，用于识别 APT 攻击、内部威胁和零日漏洞利用。建设网络安全知识图谱和威胁情报平台，提升 AI 模型的可解释性与实战能力。同时，应加强对 AI 自身安全的研究，防范对抗样本、模型窃取等新型攻击，确保 AI 系统本身的可信与鲁棒。

4.2 管理层面

4.2.1 提高安全意识与培训

将网络安全意识教育纳入组织文化建设的重要内容，建立覆盖全员、分层分类的安全培训机制。针对普通员工开展基础防护知识培训（如识别钓鱼邮件、设置强密码）；针对技术人员进行攻防实战训练；针对管理层强化风险责任意识。定期组织模拟攻击演练（如钓鱼测试、应急演练），检验培训效果，形成“人人懂安全、人人守安全”的良好氛围。

4.2.2 建立完善的安全策略与规范

组织应依据国家法律法规和行业标准，制定全面、可操作的信息安全管理制度。明确数据分类分级、访问控制、日志审计、第三方管理、漏洞管理等关键环节的操作规范。推行“零信任”安全架构，实施“最小权限原则”和“持续验证机制”。定期开展安全合规审查与风险评估，及时发现并整改安全隐患，确保安全策略落地执行。

综上所述，应对未来网络安全挑战，必须坚持“技管结合、预防为主、综合治理”的原则，既要加强前沿技术攻关，提升主动防御能力，也要完善管理体系，夯实组织保障基础，从而构建全方位、多层次、动态演进的网络安全防护体系，为数字化社会的健康发展保驾护航。

5 结论

计算机领域的安全威胁正呈现出多样化、复杂化和组织化的发展趋势，从传统病毒到高级持续性威胁，防御体系面临前所未有的挑战。本文系统分析了当前主要安全威胁，综述了防火墙、加密技术、人工智能等多层次防御手段，并指出未来在量子计算、云计算与安全管理等方面的新挑战。研究表明，单一技术无法应对日益演进的攻击手段，必须构建“技术+管理”协同的综合防护体系。建议从加强后量子密码研究、推动 AI 安全应用、提升人员安全意识、完善应急响应机制等方面综合施策。唯有坚持技术创新与管理优化并重，才能有效提升网络安全整体水平，为数字社会的稳定运行提供坚实保障。

参考文献

[1]李桂海,刘勇强,罗栋焕.基于智能免疫的计算机网络安全防御技术演进与体系构建研究[J].轻工科技,2025,41(04):130-132.

[2]苗佳.基于大数据时代的网络安全风险与应对策略探究[J].信息记录材料,2025,26(07):200-202.DOI:10.16009/j.cnki.cn13-1295/tq.2025.07.076.

[3]冯有学.计算机网络安全中的问题与对策分析[J].集成电路应用,2025,42(04):87-89.DOI:10.19339/j.issn.1674-2583.2025.04.030.

[4]吕犇.基于人工智能技术的计算机网络安全防御系统的设计[J].网络安全和信息化,2025,(04):101-103.

[5]王旭阳.计算机网络信息安全及加密技术[J].数字通信世界,2025,(02):18-20.

作者简介：董佳（1997.10-）男;汉;浙江海盐;本科;实习研究员;研究方向：网络安全、信息安全、数据安全、人工智能。