通信计算机信息安全问题及解决对策

沈　磊
上海华测导航技术股份有限公司　上海　201706

摘　要：通信计算机系统面临恶意软件、网络入侵、数据泄露及系统漏洞等多重威胁，导致信息安全防护难度剧增。本文从技术防御、数据保障、系统加固及人员管理四方面提出解决对策，并探讨新兴技术对信息安全的影响与未来防护理念创新，强调主动防御、零信任架构及协同合作的重要性，为构建安全、可信的通信计算机环境提供理论支撑。

关键词：通信计算机；信息安全；解决对策；发展趋势；协同合作

引言：在数字化时代，通信计算机系统深度融入社会各领域，支撑着经济、生活等方方面面运转。然而，信息安全问题如影随形，从恶意软件攻击到数据泄露风险，从系统漏洞到人员管理隐患，严重威胁系统稳定。解决信息安全问题迫在眉睫，需深入剖析问题并探寻有效对策，以保障通信计算机系统安全。

1 通信计算机信息安全面临的主要问题

1.1 网络攻击威胁

恶意软件攻击是信息安全领域的顽固难题。病毒、蠕虫、特洛伊木马等恶意软件借助多样传播途径侵入系统，电子邮件附件、恶意网站下载、未授权的移动存储设备使用，都能成为它们的“跳板”。这些恶意软件一旦成功潜入，便肆意破坏系统文件，干扰系统正常运转；还会偷偷窃取敏感信息，对用户造成难以预估的损失；同时大量占用系统资源，导致系统运行迟缓甚至瘫痪。更糟糕的是，恶意软件持续变异升级，不断突破检测和清除技术的防线，给信息安全防护工作增添巨大难度。网络入侵与攻击是黑客常用的手段。黑客利用系统漏洞、弱密码等薄弱点，精心策划入侵行动。一旦获取非法访问权限，就会对系统进行篡改、破坏，或盗取其中的数据。分布式拒绝服务（DDoS）攻击通过发送海量请求，无节制地占用网络带宽和系统资源，最终使服务陷入瘫痪状态，严重影响业务的正常开展。零日漏洞攻击凭借其隐蔽性和突发性，成为信息安全的重大威胁。零日漏洞指那些尚未被软件开发者察觉和修复的漏洞，攻击者利用这一特性发起隐蔽攻击，由于缺乏现成的防护方案，使得此类攻击极难防范。

1.2 数据安全风险

数据泄露风险贯穿存储与传输全流程。在存储阶段，数据库安全配置不当，或者存储设备意外丢失、被盗，都可能致使敏感信息泄露[1]。而在传输过程中，未加密传输的数据容易被拦截，中间人攻击更是能让数据被窃取或篡改。数据篡改与丢失带来的危害不容小觑。恶意篡改数据会干扰系统正常运行，误导业务决策，以财务数据、医疗记录等关键数据被篡改为例，可能引发一系列严重后果。硬件故障、软件错误、人为误操作等因素，都会导致数据丢失，进而带来各类损失。个人隐私数据在通信计算机系统的收集、存储和使用过程中，面临着泄露风险。企业商业机密数据在数据共享和合作时，也存在被泄露的挑战，如何保障机密数据安全成为一大难题。

1.3 系统自身漏洞与缺陷

软件漏洞广泛存在于操作系统、应用软件之中，缓冲区溢出漏洞、SQL注入漏洞等，都可能被攻击者利用。软件更新不及时会加剧漏洞风险，即便进行更新，也可能引入新的安全问题。通信计算机硬件设备同样存在安全隐患，芯片漏洞、硬件后门都可能被不法分子利用来窃取信息或破坏系统。硬件设备的兼容性和稳定性问题也不容忽视，一旦出现故障，可能导致数据丢失或系统崩溃。系统架构设计不合理带来诸多安全风险，缺乏有效的访问控制、身份认证机制不完善等问题较为突出。在分布式系统、云计算环境下，数据隔离、多租户安全等架构安全挑战也日益凸显。

1.4 人员安全意识与管理问题

部分员工对信息安全的重要性认识不足，安全防范意识薄弱，日常工作中随意点击不明链接、使用弱密码等行为屡见不鲜。用户在使用通信计算机服务时，不注重保护个人隐私信息，也容易被不法分子利用。内部人员违规操作也是信息安全的一大隐患。一些内部人员出于利益诱惑、报复心理等原因，实施窃取数据、破坏系统等行为。内部人员权限管理不当，容易造成权限滥用或越权访问，进一步加大信息安全风险。企业或组织若

缺乏完善的信息安全管理制度，就无法有效规范和约束人员行为与系统操作。安全培训和教育机制不健全，使得员工难以掌握最新安全知识和技能，难以应对复杂多变的信息安全威胁。

2 通信计算机信息安全解决对策

2.1 网络攻击防御技术

网络攻击防御技术是保障通信计算机系统稳定运行的基础环节。在恶意软件防护方面，部署并定期更新杀毒软件、防火墙等安全工具，能够有效识别和阻断常见的恶意程序入侵。这些工具不仅具备实时监测功能，还能对已知威胁进行快速响应。除此之外，行为分析与机器学习等新型检测技术的应用，使系统可以基于程序运行时的行为特征判断其是否具有潜在危害，从而显著提高防护系统的准确性与效率[2]。在网络入侵检测与防范方面，入侵检测系统（IDS）和入侵防御系统（IPS）作为核心组件，能够在流量层面持续监控网络活动，及时发现异常行为并采取隔离或阻断措施。加强网络边界防护，利用访问控制列表（ACL）、虚拟专用网络（VPN）等方式，限制非法用户的接入，有助于进一步加固网络安全防线。对于难以预测的零日漏洞攻击，建立漏洞监测与预警机制至关重要。通过跟踪各类安全情报来源，及时获取尚未公开的漏洞信息，并评估其可能造成的影响范围。在此基础上，采用虚拟化技术和沙箱环境，将可疑程序或关键服务隔离运行，即使遭受攻击，也能将其影响范围控制在有限区域内，降低系统整体风险。

2.2 数据安全保障措施

数据安全保障措施直接关系到信息的完整性、保密性和可用性。数据加密技术是保护敏感信息的重要手段之一，通过对存储和传输过程中的数据进行加密处理，可防止未经授权的访问者获取原始内容。常用的加密方式包括对称加密和非对称加密，前者适用于高效处理大量数据，后者则在密钥交换方面具有优势。无论采用哪种算法，密钥管理都必须受到严格管控，确保其生成、存储、分发和销毁各环节的安全性。除了加密之外，数据备份与恢复策略同样不可忽视。制定科学合理的备份计划，包括全量备份、增量备份和差异备份等多种形式，配合异地存储、云存储等技术手段，可以在遭遇硬件故障、人为失误或恶意破坏时迅速恢复业务运转，减少中断时间。隐私保护也是数据安全的重要组成部分，特别是在涉及个人身份信息和商业敏感数据的场景中，需采用数据脱敏、匿名化等技术手段，降低数据泄露后带来的潜在风险。实施严格的访问控制机制，依据用户角色和权限设定访问级别，能够有效防止越权操作，增强对敏感信息的保护力度。

2.3 系统安全加固与优化

系统安全加固与优化涵盖软件、硬件及架构设计等多个层面。在软件层面，漏洞修复和版本更新是最基本但至关重要的工作。开发人员应密切关注厂商发布的补丁信息，及时为操作系统和应用程序打上最新安全补丁，以消除已知漏洞带来的安全隐患。应建立漏洞扫描和评估机制，通过自动化工具定期检查系统状态，识别潜在弱点并加以修补。在硬件安全方面，选择经过验证的安全设备是基础要求，避免使用存在已知漏洞或被植入后门的硬件产品。对现有设备进行合理配置，例如设置强口令、启用安全启动、关闭不必要的端口和服务等，也能够有效提升系统的抗攻击能力。系统架构的设计对整体安全性有着深远影响，传统单体架构往往难以满足现代应用的扩展需求和安全挑战。建议采用分层架构或微服务架构，将系统划分为多个独立模块，便于管理和维护的同时，也有助于实现更细粒度的权限控制。在云计算和分布式环境中，应特别重视数据隔离与多租户访问控制，防止不同用户之间的资源交叉访问，确保数据的独立性和机密性。

2.4 人员安全意识提升与管理强化

人员安全意识的提升与管理制度的强化是信息安全保障中不可或缺的一环。尽管技术手段不断发展，但人为因素仍是许多安全事故的主要诱因。必须通过持续性的培训与教育活动，提高员工对信息安全的认知水平。企业应定期组织安全知识讲座、模拟演练等活动，帮助员工掌握基本的安全操作规范和应急处置方法。针对不同岗位和职责，提供定制化的培训内容，如面向开发人员开展安全编码实践课程，面向运维人员介绍系统加固技巧，有助于全面提升团队的安全素养。内部人员行为管理同样重要，应建立完善的权限分配机制，按照最小权限原则授予用户必要的访问权限，避免权限滥用[3]。同时加强对日常操作行为的审计和监督，利用日志记录和行为分析工具，及时发现异常操作并采取相应措施。为了保障信息安全工作的有序开展，还需制定健全的安全管理制度，明确各项流程和责任人，使安全管理有据可依。应建立信息安全应急响应机制，提前制定详细的应急预案，在突发安全事件发生时能够迅速启动响应流程，协调各方资源进行处置，最大限度地降低损失和影响。

3 通信计算机信息安全未来发展趋势与展望

3.1 新兴技术对信息安全的影响

人工智能与机器学习为信息安全带来革新与挑战。

在恶意软件检测中，这些技术可通过分析程序行为模式，快速识别未知威胁；在入侵预测方面，利用历史数据建模能预判攻击趋势；安全态势感知场景下，实时处理海量数据助力掌握全局风险。但技术本身存在被滥用风险，对抗样本攻击可欺骗机器学习模型，使恶意程序绕过检测。物联网设备爆发式增长带来复杂安全局面。设备数量庞大、协议多样且更新滞后，导致漏洞长期存在，大量接入设备也增加数据隐私泄露风险。不过这也推动技术创新，安全芯片嵌入设备提供硬件级防护，区块链技术通过分布式账本保障数据传输不可篡改，为物联网安全开辟新路径。量子计算凭借超强算力冲击传统加密体系。其原理基于量子叠加与纠缠特性，能大幅缩短破解传统加密算法的时间。为应对威胁，量子密钥分发利用量子态特性实现绝对安全的密钥传输，后量子密码算法研究也在探索抗量子攻击的加密方案。

3.2 信息安全防护理念与模式的创新

信息安全防护正从被动应对转向主动防御。威胁情报驱动的防御模式，通过收集、分析全球范围内的攻击信息，提前识别潜在威胁；诱捕系统通过设置虚假目标，吸引攻击者暴露手段与意图，为防御提供依据。动态安全防护体系根据实时安全态势，自动调整防火墙规则、入侵检测策略等，实现防护策略与攻击变化的同步更新，增强系统自适应能力。零信任架构颠覆传统网络安全观念。其核心遵循“默认不信任，始终要验证”原则，无论用户位于内网或外网，每次访问资源都需经过严格身份认证与权限校验。在远程访问场景中，零信任架构通过多因素认证、设备健康检查等机制，确保接入安全；在云环境下，对数据访问进行细粒度管控，防止权限滥用与数据泄露，显著提升系统安全性[4]。协同安全与生态共建成为信息安全发展新方向。企业、组织、机构间共享安全威胁情报与防护经验，打破信息孤岛，形成安全合力。产业链上下游企业紧密合作，从芯片设计、操作系统开发到应用软件部署，全链条嵌入安全机制。信息安全生态系统通过技术共享、标准统一，推动行业整体安全水平提升，共同抵御复杂网络威胁。

3.3 对未来通信计算机信息安全发展的展望

随着数字化进程不断加快，通信计算机系统在各行各业中的作用日益关键，信息安全的重要性也愈加凸显。未来的安全发展将呈现出技术与理念并重的趋势。一方面，人工智能、物联网、量子计算等新兴技术的广泛应用，将持续推动安全防护手段的升级，也为攻击方式带来了新的不确定性，促使信息安全体系必须具备更强的前瞻性和适应性。另一方面，传统的静态防御模式已无法应对日益复杂的威胁环境，主动防御、动态响应和零信任架构将成为主流，推动安全机制向智能化、精细化方向演进。与此同时，单一组织或企业难以独立应对大规模、高强度的安全挑战，跨行业、跨领域的协同合作愈发重要。通过建立统一标准、共享威胁情报、联动应急响应，构建开放、协作的信息安全生态体系，将有效提升整体防护能力。未来的信息安全不仅是技术层面的较量，更是管理理念、制度建设和合作机制的综合体现。只有不断优化技术手段、创新防护思路、加强多方协作，才能为通信计算机系统的持续稳定运行提供坚实保障。

结束语

通信计算机信息安全问题错综复杂，需从技术、管理等多维度综合施策。随着新兴技术发展，信息安全挑战与机遇并存。未来，唯有持续创新防护理念与模式，强化多方协同合作，构建完善信息安全生态体系，才能有效应对不断变化的安全威胁，为通信计算机系统安全稳定运行筑牢根基。

参考文献

[1]沈毅.云计算背景下计算机安全问题及对策分析[J].上海轻工业,2024,(03):111-113.

[2]魏涛.大数据背景下计算机网络信息安全风险和解决对策研究[J].软件,2022,43(11):120-122.

[3]陈哲,周荣.计算机应用中大数据信息安全问题及解决对策[J].计算机产品与流通,2024(11):159-161.

[4]魏翠萍.计算机应用中网络信息安全问题及解决对策[J].重庆电力高等专科学校学报,2024,29(4):22-26.