计算机网络信息安全及防护策略研究

张春秀
海原县三河中学　宁夏　中卫　755200

摘　要：计算机网络信息安全面临多重挑战，包括系统脆弱性、外部攻击、用户误操作及技术监控不足。本文分析了网络钓鱼、入侵、数据截获、病毒传播及诈骗等威胁形式，并提出综合防护策略：加强漏洞扫描与风险评估，应用防火墙、数据加密及访问控制技术，部署入侵检测系统，隐藏IP并加密传输，同时提升用户安全意识与技能，以全面保障计算机网络信息安全。

关键词：计算机网络；信息安全；防护策略

引言：随着信息技术的迅猛发展，计算机网络已成为现代社会不可或缺的信息基础设施。然而，网络信息安全问题频发，给个人、企业乃至国家安全带来严重威胁。本文旨在深入探讨计算机网络信息安全的影响因素及主要威胁形式，提出有效的防护策略，以强化网络安全防护体系，减少安全事件的发生，保障信息的机密性、完整性和可用性，为网络环境的健康发展提供有力支持。

1 计算机网络信息安全的影响因素

1.1 网络系统本身的脆弱性

网络系统本身的脆弱性是信息安全的一大隐患。首先，开放式系统的特性使得数据和信息在传输和存储过程中容易受到攻击。开放式系统为了提供便捷的服务，往往牺牲了部分安全性，使得黑客可以利用系统漏洞进行攻击。其次，程序员在开发过程中可能会因为疏忽或技术水平有限，导致系统存在缺陷。这些缺陷可能被黑客利用，成为入侵系统的突破口。此外，TCP/IP协议作为互联网的基础协议，虽然具有开放性和灵活性的特点，但在安全性方面存在不足。协议本身缺乏足够的加密和身份验证机制，使得数据在传输过程中容易被窃取或篡改。

1.2 外部威胁因素

外部威胁因素也是影响计算机网络信息安全的重要因素。自然灾害如电磁泄漏、地震、雷电等可能对网络设备和线路造成物理损坏，导致网络中断或数据丢失。人为因素则更加复杂多变，包括黑客攻击、身份盗窃等恶意行为。黑客可以利用各种攻击手段，如DDoS攻击、SQL注入、钓鱼邮件等，来窃取敏感信息、破坏系统正常运行或进行勒索。身份盗窃则通过伪造身份或盗用他人账号，进行非法操作，给用户和企业带来巨大损失。此外，计算机病毒也是常见的外部威胁之一。病毒通过网络或存储设备传播，具有隐蔽性、传染性和破坏性，一旦感染病毒，系统可能面临崩溃、数据损坏等严重后果。

1.3 用户错误操作

用户错误操作也是导致网络安全问题的重要因素之一。许多用户在设置密码时过于简单或不设置密码，使得账户容易被破解。此外，个人信息和账号泄露也是常见的安全问题。一些用户在使用网络时不注意保护个人信息，如随意在社交媒体上发布个人信息、使用弱密码等，这些都可能成为黑客攻击的切入点。不安全的网络使用习惯也是导致网络安全问题的重要原因。例如，使用不安全的公共Wi-Fi、点击不明链接或下载来源不明的软件等，都可能导致系统感染病毒或泄露个人信息。

1.4 技术和监控手段的缺乏

技术和监控手段的缺乏也是影响网络安全的重要因素之一。缺乏有效的安全评估和监控机制，使得网络攻击难以及时发现和应对。一些企业和组织在网络安全方面投入不足，缺乏专业的安全团队和先进的技术手段来保障网络安全。此外，未及时更新系统和应用程序也可能导致漏洞被利用。系统和应用程序的更新往往包含安全修复和改进，但一些用户因为各种原因没有及时更新，从而增加了系统被攻击的风险。

2 计算机网络信息安全的主要威胁形式

2.1 网络钓鱼与钓鱼邮件

网络钓鱼是一种通过伪装成可信的实体，诱骗用户提供敏感信息（如密码、银行账户等）的网络欺诈行为。钓鱼邮件则是这种欺诈行为的主要手段之一。这些邮件通常包含虚假的链接或附件，一旦用户点击或下载，就可能暴露自己的个人信息给黑客。（1）虚假邮件和页面的欺骗性：钓鱼邮件和页面往往设计得与正规网站或邮件极为相似，甚至能够伪造发件人地址和邮箱账号，以迷惑用户。它们通常包含诱人的信息，如中奖通

知、账户异常等，诱使用户点击链接或输入敏感信息[1]。（2）获取用户账户和密码的方式：通过钓鱼邮件，黑客可以获取用户的账户和密码，进而控制用户的账户，进行非法操作或窃取资金。此外，一些钓鱼邮件还会诱导用户下载恶意软件，进一步危害用户的计算机系统。

2.2 网络入侵

网络入侵是指黑客利用技术手段，未经授权地访问、控制和操纵目标系统的行为。网络入侵通常伴随着系统漏洞的利用和多种攻击手段的应用。（1）寻找和利用系统漏洞：黑客会利用系统或软件的漏洞，通过暴力破解、SQL注入等手段，绕过安全机制，进入目标系统。（2）攻击目标系统的各种方式：一旦进入系统，黑客可能会进行各种恶意操作，如篡改数据、植入恶意软件、窃取敏感信息等。这些行为不仅危害用户数据安全，还可能影响系统的正常运行。

2.3 数据截获

数据截获是指黑客通过截获和解密数据包，获取敏感信息的行为。这种威胁形式在网络通信中尤为常见。（1）通过截获和解密数据包获取敏感信息：黑客可以在数据传输过程中，通过拦截数据包并解密其内容，获取用户的敏感信息，如银行交易信息、个人身份信息等。（2）使用明文传输密码和数据的风险：一些系统在设计中可能采用明文传输密码和数据的方式，这使得黑客可以更容易地截获并解析这些数据。为了避免这种风险，应采用加密传输技术，确保数据在传输过程中的安全性。

2.4 网络病毒

网络病毒是一种具有传染性和破坏性的计算机程序，它可以通过网络或存储设备传播，感染用户的计算机系统。（1）病毒的传播和扩散方式：网络病毒通常通过邮件、恶意网站、共享文件等方式传播。一旦感染病毒，用户的计算机系统可能会受到各种恶意操作的影响，如数据破坏、系统瘫痪等。（2）病毒对系统运行和数据的影响：病毒会占用系统资源，降低系统性能，甚至导致系统崩溃。同时，病毒还可能窃取或篡改用户的数据，给用户带来重大损失。

2.5 网络诈骗

网络诈骗是指通过网络手段，欺骗用户钱财或敏感信息的犯罪行为。这种威胁形式往往伴随着各种骗术的应用。（1）各种骗术欺骗用户钱财或敏感信息：网络诈骗的形式多种多样，如假冒客服、中奖诈骗、网络购物诈骗等。这些诈骗手段往往利用用户的贪念或疏忽，诱使用户上当受骗。（2）安装反诈骗插件的必要性：为了防范网络诈骗，用户应提高警惕，不轻易相信陌生人的信息。同时，安装反诈骗插件也是有效防范手段之一。这些插件可以识别并阻止恶意网站的访问，保护用户的财产安全和个人信息安全。

3 计算机网络信息安全的防护策略

3.1 漏洞扫描与风险评估

（1）对重要网络设备进行定期漏洞扫描：网络设备，如路由器、交换机、服务器等，是网络的核心组成部分。这些设备一旦存在漏洞，就可能成为黑客攻击的突破口。因此，定期对这些设备进行漏洞扫描，及时发现并修复漏洞，是确保网络安全的关键。（2）及时更新和修复漏洞：随着技术的发展，新的漏洞不断被发现。为了确保网络安全，需要及时更新和修复已知漏洞。这包括安装最新的安全补丁、更新操作系统和应用程序等。同时，还应建立漏洞管理机制，跟踪漏洞的修复进度，确保所有漏洞得到及时修复[2]。

3.2 安全技术应用

3.2.1 防火墙技术

（1）防火墙种类及作用：防火墙是一种网络安全设备或程序，它位于网络的不同区域之间，通过检查进出网络的数据包，防止未经授权的访问和数据泄露。防火墙可以分为硬件防火墙和软件防火墙两种。硬件防火墙通常是独立的硬件设备，而软件防火墙则运行在操作系统上。（2）防火墙的典型体系结构：防火墙的典型体系结构包括包过滤防火墙、代理服务器防火墙和状态检测防火墙等。包过滤防火墙通过检查数据包的头部信息，决定是否允许数据包通过。代理服务器防火墙则作为内外网络之间的中介，替用户处理外部网络的请求和响应。状态检测防火墙则结合了包过滤和代理服务器的优点，能够检测网络会话的状态，提供更精细的访问控制。

3.2.2 数据加密技术

（1）对称加密与公开密钥加密：数据加密技术是保护数据安全的重要手段。对称加密和公开密钥加密是两种常用的加密方式。对称加密使用相同的密钥进行加密和解密，速度快但密钥管理复杂。公开密钥加密则使用一对公钥和私钥，公钥用于加密，私钥用于解密，安全性更高但速度较慢。（2）数字签名、报文摘要、SSL和SET协议：数字签名是一种用于验证数据完整性和身份真实性的技术。报文摘要则通过对数据进行摘要处理，生成一个固定长度的哈希值，用于检测数据是否被篡改。SSL和SET协议是两种用于保障网络通信安全的协议。SSL协议主要用于Web浏览器和服务器之间的安全通信，而SET协议则用于电子商务中的安全支付[3]。

3.2.3 访问控制

（1）访问控制模型和安全策略：访问控制是限制用户访问网络资源的一种方法。常见的访问控制模型包括自主访问控制、强制访问控制和基于角色的访问控制。自主访问控制允许用户根据自己的意愿设置对其他资源的访问权限；强制访问控制则根据预定义的安全策略对用户和资源进行分类，并限制它们之间的交互；基于角色的访问控制则通过将权限分配给角色，再将角色分配给用户，实现更细粒度的访问控制。（2）自主访问、强制访问、基于角色的访问控制：这些访问控制模型各有优缺点，适用于不同的应用场景。例如，自主访问控制适合用于小型网络环境，而基于角色的访问控制则更适合大型企业和组织。

3.2.4 防御病毒技术

（1）安装杀毒软件并定期更新：杀毒软件是防御病毒的重要工具。通过安装杀毒软件并定期更新病毒库，可以及时发现并清除计算机系统中的病毒。（2）避免从未知来源下载和打开文件：许多病毒通过下载和打开未知来源的文件传播。因此，用户应避免从不明网站或不可信的人那里下载文件，也不要随意打开来自陌生人的邮件或消息中的附件。

3.3 入侵检测系统

（1）入侵测试概述及分类：入侵测试是通过模拟攻击行为，测试网络系统的安全性和防御能力的过程。它可以分为白盒测试和黑盒测试两种。白盒测试是在了解系统内部结构和代码的情况下进行的，旨在发现潜在的漏洞和弱点。黑盒测试则是在不了解系统内部细节的情况下进行的，旨在评估系统对外部攻击的防御能力。（2）入侵检测技术的应用和改进：入侵检测系统可以应用于各种网络环境，如企业网络、数据中心和云环境等。它们通过收集和分析网络流量、系统日志和异常行为等信息，发现潜在的攻击行为。为了提高入侵检测的准确性和效率，可以采用基于机器学习和人工智能的技术来优化检测算法和模式匹配。此外，还可以将入侵检测系统与防火墙、数据加密和访问控制等安全技术相结合，形成更加完善的网络防御体系。

3.4 隐藏IP地址和加密传输

（1）代理服务器在隐藏IP地址中的作用：代理服务器是一种充当网络中介的服务器，可以隐藏用户的真实IP地址。当用户使用代理服务器访问网络时，代理服务器会代替用户与目标服务器进行通信，并将结果返回给用户。这样，黑客就无法直接获取用户的真实IP地址，从而增加了网络通信的安全性[4]。（2）加密传输方式及协议（如HTTPS）：加密传输是通过使用加密协议和技术来保护网络通信的安全。HTTPS是一种常用的加密传输协议，它结合了HTTP协议和SSL/TLS加密技术，提供安全的Web浏览和数据传输服务。通过使用HTTPS协议，可以确保用户在浏览网页、进行在线购物或提交敏感信息时，数据能够在传输过程中得到加密保护，防止被黑客窃取或篡改。

3.5 用户安全意识与技能培训

（1）定期进行安全培训和宣传：企业应定期组织员工进行网络安全培训，提高员工对网络安全的认识和理解。培训内容可以包括网络安全基础知识、常见网络攻击方式和防范方法、安全操作规范等。同时，还可以利用企业内刊、宣传栏等渠道进行网络安全宣传，增强员工的安全意识和责任感。（2）提升用户安全防护意识和技能：除了企业内部的培训外，用户自身也应注重提升安全防护意识和技能。例如，定期修改密码、不随意点击陌生链接或下载未知来源的文件、安装可靠的安全软件等。此外，用户还应了解并熟悉常见的网络攻击方式和手段，以便在遭遇攻击时能够及时采取措施进行应对。

结束语

综上所述，计算机网络信息安全是一项复杂而系统的工程，涉及技术、管理、法律等多个层面。面对日益严峻的安全挑战，我们必须不断更新防护理念和技术手段，构建多层次、立体化的安全防护体系。同时，加强用户安全教育，提升全社会的信息安全意识至关重要。未来，随着技术的不断进步，我们期待更加智能、高效的防护策略不断涌现，共同守护计算机网络信息安全的底线，为数字化转型和信息安全保驾护航。

参考文献

[1]龙振华.大数据时代计算机网络信息安全及防护策略.[J]中国管理信息化,2022,(06):61-62.

[2]马遥.大数据时代计算机网络信息安全与防护研究.[J]科技风,2020,(09):82-83.

[3]官节福.大数据时代计算机网络信息安全及防护策略研究.[J]计算机产品与流通,2019,(06):47-48.

[4]董伟.计算机网络信息安全和防护策略[J].电子技术与软件工程,2019,(16):197-198.