计算机网络信息安全及其防护对策

靳会宇[1]　叶文晖[2]

1. 华为技术有限公司；2. 东莞城市学院在读大学生

摘　要：计算机网络信息安全是当今社会中备受关注的重要议题。本论文通过对信息安全的定义与重要性、计算机网络信息安全的基本概念以及面临的挑战进行概述，对常见的网络安全威胁类型、威胁产生原因、实例分析与案例研究进行深入分析，并提出了一系列计算机网络信息安全防护对策，包括密码学基础与加密技术、访问控制与身份认证、网络安全设备与防火墙技术、安全策略与管理、威胁检测与应急响应。这些对策将有助于提高计算机网络信息安全水平，保障网络系统的稳定运行。

关键词：信息安全；计算机网络；安全威胁；防护对策；网络安全设备

【DOI】10.12252/j.issn.2096-6261.2022.09.186

引言

随着计算机网络技术的迅速发展和广泛应用，计算机网络信息安全问题日益突显。信息安全是指对信息系统中的数据进行保护，防止其受到未经授权的访问、使用、披露、修改、破坏等不良行为的影响，保证信息的完整性、可用性和保密性。计算机网络信息安全涉及多个方面，包括数据传输、存储、处理等环节，面临着各种各样的安全威胁和挑战。因此，制定有效的信息安全防护对策，成为保障网络安全的关键所在。

一、计算机网络信息安全概述

1.信息安全的定义与重要性

信息安全是指保护信息系统中的数据不受未经授权的访问、使用、披露、修改、破坏等不良行为的影响，确保信息的完整性、可用性和保密性。这一概念涵盖了多个层面，包括技术、管理、政策等方面的要素。信息的完整性指信息在传输、存储、处理等环节中不被篡改或损坏，保证数据的准确性和完整性；可用性指信息在需要时能够及时、可靠地使用，确保系统的正常运行和服务的持续性；保密性则是指信息只能被授权的人或系统访问，不被未经授权的人获取或泄漏。

信息安全的重要性体现在多个方面。首先，对个人而言，信息安全保护个人隐私，防止个人信息被盗用、泄漏、滥用等，确保个人权益不受侵犯。其次，对组织而言，信息安全关乎企业机密、商业机密以及客户信息等重要资产的保护，可以防止竞争对手的窃取、破坏，维护企业声誉和市场竞争力。再者，对国家而言，信息安全涉及国家安全、国防安全、经济安全等重要领域，保护国家重要信息资产，维护国家稳定和发展。

信息安全在经济、政治、社会等各个领域都具有重要意义。在经济领域，信息安全能够促进电子商务、金融支付等业务的发展，增强经济运行的稳定性和可持续性；在政治领域，信息安全是国家治理和政府管理的基础，保障政府信息的安全和有效管理；在社会领域，信息安全涉及个人权益、社会秩序、公共服务等多个方面，直接关系到社会的和谐稳定和公民生活的质量。

2.计算机网络信息安全的基本概念

计算机网络信息安全是保护计算机网络中的数据和通信安全的重要概念。它涉及一系列技术和措施，旨在防止黑客攻击、病毒入侵、信息泄漏等安全威胁，确保网络的稳定运行和数据的安全传输。

首先，计算机网络信息安全强调数据的保护。数据是网络中的核心资产，包括用户的个人信息、企业的商业机密、政府的重要文件等。保护这些数据的安全性和完整性对于网络的正常运行至关重要。其次，通信安全是计算机网络信息安全的关键内容之一。网络通信涉及数据的传输过程，如何保证数据在传输过程中不被窃取、篡改或截获是网络安全的重要问题。加密技术是一种常见的手段，通过对数据进行加密和解密，保障数据在传输过程中的安全性。此外，身份验证和访问控制也是计算机网络信息安全的重要组成部分。身份验证确保网络用户的身份合法性，防止未经授权的访问；而访问控制则是对用户的权限进行管理和控制，确保用户只能访问其具备权限的资源和服务。

3.计算机网络信息安全面临的挑战

计算机网络信息安全面临着来自多个方面的挑战，这些挑战不断演变和加剧，给信息安全工作带来了巨大压力和挑战。

首先，网络攻击手段的日益多样化是信息安全面临的主要挑战之一。随着技术的发展，黑客、网络犯罪分子不断创新攻击手段，包括但不限于病毒、木马、钓鱼、勒索软件等，这些攻击手段既有直接侵入系统的技术手段，也有利用社会工程学手段诱骗用户的攻击手段，使得网络安全形势愈发严峻。其次，技术手段的不断更新也是信息安全面临的挑战之一。随着信息技术的

迅速发展，新的安全漏洞不断被发现，而黑客也在不断利用这些漏洞来入侵系统、窃取信息。对于网络管理员和安全专家而言，需要不断学习和更新安全知识，以应对不断变化的安全威胁。另外，人为因素引发的安全漏洞也是一个严重挑战。人为因素包括员工的疏忽大意、内部人员的恶意操作、社会工程学攻击等，这些因素可能会导致系统的安全漏洞和信息泄漏，给网络安全带来潜在风险。此外，网络安全威胁的隐蔽性和突发性也给信息安全工作带来了巨大挑战。许多安全威胁具有隐蔽性，往往在用户察觉之前就已经对系统造成了严重影响，而且有些攻击手段的突发性极强，难以预防和及时应对，使得网络安全防护工作变得更加困难。

二、计算机网络信息安全威胁分析

计算机网络信息安全面临着多种威胁类型，其中包括病毒、木马、僵尸网络、拒绝服务攻击（DDoS）、网络钓鱼和数据泄漏等。这些威胁对计算机网络的安全构成了严重威胁。例如，病毒是一种能够自我复制并传播的恶意软件，它可以破坏系统文件、窃取个人信息，甚至使整个网络系统瘫痪。木马则是一种潜伏在正常程序中的恶意代码，可用于远程控制系统、窃取敏感信息等恶意行为。僵尸网络是由大量被感染的计算机组成的网络，黑客可以通过控制这些僵尸计算机进行大规模的网络攻击，如DDoS攻击，使目标系统的服务不可用。网络钓鱼则是利用虚假网站或电子邮件等手段诱骗用户输入个人敏感信息，导致信息泄漏和财产损失。数据泄漏是指未经授权的信息披露或泄漏，可能导致个人隐私泄漏、商业机密外泄等严重后果。

这些威胁的产生原因包括技术漏洞、人为因素和社会工程学攻击等。技术漏洞是最主要的原因之一，黑客通过利用系统或应用程序中的漏洞来入侵系统，窃取信息或破坏系统功能。人为因素包括员工的疏忽大意、内部人员的恶意操作等，也可能导致系统的安全漏洞和信息泄漏。此外，社会工程学攻击是一种利用心理学和社会学原理诱导用户泄漏个人敏感信息的攻击方式，常见于网络钓鱼等手段中。

通过对历史上发生的网络安全事件进行实例分析和案例研究，可以更深入地了解网络安全威胁的性质、影响和应对方法。

三、计算机网络信息安全防护对策

1 密码学基础与加密技术

密码学基础与加密技术是保障信息安全的重要手段，其核心目标是确保信息在传输和存储过程中不被未经授权的访问者所获取或篡改。加密技术通过对数据进行转换或处理，使其变得难以理解或解读，从而保护信息的机密性、完整性和可用性。

首先，加密技术通过使用密钥将原始数据转换为密文，只有拥有正确密钥的接收者才能解密并获取原始数据。对称加密算法使用相同的密钥进行加密和解密，而非对称加密算法使用一对密钥，即公钥和私钥，其中公钥用于加密，私钥用于解密。这种加密技术广泛应用于网络通信和数据存储中，如SSL/TLS协议用于保护网站通信，PGP用于加密电子邮件等。其次，数字签名是一种用于验证数据完整性和认证发送者身份的技术。数字签名结合了非对称加密和哈希函数，发送者使用私钥对数据进行签名，接收者使用发送者的公钥验证签名的有效性，从而确保数据的真实性和完整性。数字签名常用于网络通信中，如HTTPS协议中的数字证书用于验证网站的身份。此外，身份认证是确保通信双方身份合法性的重要环节。常见的身份认证方法包括密码认证、生物特征识别、智能卡等。密码认证是最常见的身份验证方式，用户通过输入正确的用户名和密码来验证身份，但其安全性受到密码强度和管理的影响。生物特征识别技术利用个体生物特征（如指纹、虹膜等）进行身份认证，具有较高的安全性和便利性。

2.访问控制与身份认证

访问控制与身份认证是保障网络安全的重要措施，它们旨在确保只有经过授权的用户能够访问系统资源，并根据其权限执行相应操作，防止未经授权的访问和潜在的安全威胁。

首先，身份认证是确认用户身份的过程，确保用户是其声称的那个人。常见的身份认证方式包括密码认证、生物特征识别、智能卡等。密码认证是最常见的方式，用户通过提供用户名和密码来验证其身份。生物特征识别利用个体生物特征（如指纹、虹膜等）进行身份认证，具有较高的安全性和便利性。智能卡则是一种集成了加密芯片的身份认证设备，可以存储用户的数字证书和私钥，提供更安全的身份认证方式。其次，访问控制是根据用户身份和权限对其访问系统资源的行为进行控制和管理。访问控制可以分为两种类型：基于角色的访问控制（RBAC）和基于策略的访问控制（ABAC）。RBAC通过将用户分配到不同的角色，并为每个角色分配相应的权限来实现访问控制。ABAC则根据用户的属性、资源的属性和环境条件来动态确定访问策略。除了RBAC和ABAC，访问控制还包括访问控制列表（ACL）和强制访问控制（MAC）等机制。

综合身份认证和访问控制可构建一个完善的安全体

系，确保系统只允许合法用户在授权范围内进行操作，提高系统的安全性和可信度。然而，为了确保访问控制和身份认证的有效性，还需要定期审计和监控系统的访问活动，及时发现并应对潜在的安全威胁。同时，教育用户加强安全意识，如定期更改密码、不随意泄漏个人信息等，也是确保网络安全的重要措施之一。

3.网络安全设备与防火墙技术

网络安全设备是保护计算机网络免受未经授权访问、攻击和其他安全威胁的关键组成部分。其中，防火墙、入侵检测系统（IDS）、入侵防御系统（IPS）等设备在网络安全中发挥着重要作用。

首先，防火墙是一种网络安全设备，用于监控和控制进出网络的流量，根据预先设定的安全策略，阻止不符合规定的流量通过。防火墙可以分为软件防火墙和硬件防火墙两种类型。软件防火墙安装在计算机上，通过过滤和检查数据包来实现网络安全保护；而硬件防火墙则是一种独立的设备，通常部署在网络边界上，对进出的流量进行检查和过滤，提供更高效的安全保护。其次，入侵检测系统（IDS）和入侵防御系统（IPS）是用于检测和防止网络攻击的设备。IDS负责监视网络流量和系统活动，检测可能的安全事件或攻击行为，并生成警报通知管理员。而IPS则不仅具有IDS的功能，还能够对检测到的恶意流量进行实时响应，阻止攻击并修复系统漏洞，从而提高网络安全的响应速度和效率。这些网络安全设备可以配合使用，构建多层次的安全防护体系，有效防止网络攻击和威胁。

4.安全策略与管理

建立健全的安全策略和管理体系对于保障网络安全至关重要。安全策略是组织内部规定的关于信息安全的方针和目标，而安全管理则是指实施这些策略的具体措施和流程，以确保网络系统免受各种安全威胁的侵害。

首先，制定安全政策是安全管理的第一步。安全政策应该明确规定组织对信息资产的价值和保护要求，以及员工在处理信息时应遵循的规则和标准。这些政策可以涉及访问控制、数据备份、密码管理、网络使用等方面，旨在建立起一个全面、系统的安全管理框架。其次，安全培训是提高员工安全意识和技能的重要途径。通过定期的安全培训，员工可以了解到最新的安全威胁和防范措施，学习如何安全地使用系统和应用程序，并掌握应急响应和事件处理的技能。这有助于减少员工的安全风险，提高组织的整体安全水平。此外，安全审计和监控是确保安全策略有效执行的重要手段。通过对系统和网络流量、日志文件、访问记录等进行持续监控和分析，及时发现异常活动和安全事件，对安全措施和政策进行评估和改进，提高组织的安全性和应对能力。

5.威胁检测与应急响应

建立威胁检测系统和应急响应机制是保障网络安全的重要措施，其目的在于及时发现并应对各种网络安全威胁，确保网络系统的稳定运行。这些防护对策相互配合、相互促进，共同构建起完善的网络安全防护体系。

首先，威胁检测系统是用于监控和识别网络中的安全威胁和攻击行为的设备或软件。它可以包括入侵检测系统（IDS）、入侵防御系统（IPS）、网络流量分析工具等。这些系统通过分析网络流量、检测异常活动和恶意行为，发现可能存在的安全威胁，并生成相应的警报或日志，以提醒管理员及时采取措施应对。其次，应急响应机制是针对发现的安全威胁和事件制定的应对措施和流程。它包括预先制定的应急响应计划、指定的应急响应团队以及相应的应急响应流程。当发生安全事件时，应急响应团队可以根据预先制定的计划和流程，快速响应并采取措施，最大限度地减少安全事件对系统和业务的影响。威胁检测系统和应急响应机制之间相互配合、相互促进，共同构建起完善的网络安全防护体系。威胁检测系统通过监控和识别安全威胁，为应急响应提供及时的警报和信息，使得应急响应团队能够迅速作出反应。而应急响应机制则通过预先制定的计划和流程，保证在发生安全事件时能够迅速、有效地应对，最大限度地减少损失和影响。

结束语

计算机网络信息安全问题是一个复杂而严峻的挑战，需要各方的共同努力和有效的应对措施。本文从信息安全的重要性、计算机网络信息安全的基本概念、面临的挑战等方面进行了概述，深入分析了常见的网络安全威胁类型、威胁产生原因，并提出了一系列针对性的防护对策，这些对策的实施将有助于提高计算机网络信息安全水平，保障网络系统的稳定运行，推动信息社会的健康发展。在未来的工作中，我们还需不断学习和总结经验，加强国际合作，共同应对网络安全挑战，共建和谐安全的网络空间。

参考文献

[1]大数据时代计算机网络信息安全探讨[J].许青林.自动化应用，2022（12）

[2]信息化背景下计算机网络信息安全防护策略分析[J].潘天昊.信息与电脑（理论版），2022（20）

[3]新环境下的计算机网络信息安全及其防火墙技术应用分析[J].吴红.网络安全技术与应用，2022（07）