浅谈计算机网络安全技术在网络安全维护中的应用

胡海涛
苏州江南航天机电工业有限公司　江苏　苏州　215000

摘　要：计算机网络安全技术在网络安全维护中扮演着关键角色。面对日益复杂的网络攻击手段，如勒索病毒、DDoS攻击等，防火墙、入侵检测与防御系统、数据传输加密、防病毒及VPN技术应运而生。这些技术通过监控网络流量、识别并防御潜在威胁、确保数据安全和提供远程访问安全通道，共同构建了全面的网络安全防护体系，有效维护了网络环境的稳定和数据的机密性。

关键词：计算机网络安全技术；网络安全维护；应用

引言：随着互联网技术的飞速发展，网络安全问题日益凸显，成为制约信息化进程的关键因素。计算机网络安全技术作为保障网络安全的重要手段，通过构建多层次、立体化的防御体系，有效应对各类网络攻击和威胁。本文旨在探讨网络安全技术的最新进展及其在网络安全维护中的具体应用，以期为提升网络防护能力、保障信息安全提供参考和借鉴。

1 网络安全现状分析

1.1 网络攻击手段多样化

网络攻击手段已经远远超出了传统的病毒、木马和钓鱼攻击。这些传统手段虽然依然存在并持续演化，但新兴的攻击方式更加复杂和隐蔽。勒索病毒便是一种典型的新兴攻击手段，它通过加密受害者的数据并要求支付赎金以换取解密密钥，给个人和企业带来了巨大的经济损失。此外，DDoS攻击（分布式拒绝服务攻击）通过控制大量计算机或网络设备向目标发送大量无用的数据包，使其无法提供正常服务。高级持续性威胁（APT）则是一种更为隐蔽和持久的攻击方式，攻击者通常具有明确的目标和计划，并会长期潜伏在受害者的系统中，窃取敏感信息或破坏系统。

1.2 网络攻击目标的广泛性

网络攻击的目标不再局限于大型机构，小型企业和个人家庭也频繁成为受害者。随着物联网（IoT）技术的普及，智能设备的安全性问题日益突出，许多IoT设备在设计时并未充分考虑安全性，缺乏足够的保护措施，使得它们成为黑客攻击的理想目标。此外，远程办公和智能家居的普及也增加了网络攻击的风险，恶意软件可能通过这些设备传播，对整个网络环境构成威胁。

1.3 网络安全意识的淡薄

尽管网络安全问题日益严重，但许多用户在网络安全方面的意识依然淡薄。这表现在密码策略的忽视、防病毒软件的不当使用以及数据备份的不足等方面。许多用户仍然使用简单或重复的密码，甚至将个人密码公开，这使得他们的账户和系统容易受到攻击。同时，一些用户对于防病毒软件的使用也存在误区，如不及时更新病毒库或关闭实时防护功能，从而降低了系统的安全性。在数据备份方面，许多用户缺乏定期备份数据的意识，导致在数据丢失或损坏时无法恢复[1]。

1.4 法律法规的不完善

我国在网络安全法律法规方面取得了一定的进展，但仍存在许多挑战。随着网络技术的快速发展和网络环境的日益复杂，现有的法律法规难以全面覆盖所有网络安全问题。此外，一些法律法规的执行力度和监管机制也存在不足，导致一些网络安全违法行为得不到有效遏制。同时，我国在网络安全方面的国际合作也尚待加强，以共同应对跨国网络安全威胁。

2 计算机网络安全技术

2.1 防火墙技术

防火墙是网络安全的第一道屏障，通过制定和执行安全策略，监控并控制进出网络的流量。（1）包过滤型与应用型防火墙。包过滤型防火墙。基于预定义的规则，检查每个数据包的头信息，如源地址、目标地址、端口号等，决定是否允许数据包通过。这种防火墙简单高效，但无法检查应用层的数据内容，对复杂攻击（如应用层攻击）防护能力有限。应用型防火墙。也称为代理服务器防火墙，工作在应用层，能够深入解析协议内容，根据应用层的上下文做出访问控制决策。它不仅检查数据包头，还分析应用层数据，提供更高水平的安全防护。然而，由于需要对每个请求进行深度解析，应用型防火墙的性能开销较大。（2）防火墙在网络安全中的作用及限制。防火墙的主要作用是保护内部网络免受外部攻击，控制进出网络的数据流，提供基本的访问控制

和安全策略执行。然而，防火墙并非万能，其局限性包括：无法防御内部威胁、无法识别所有类型的攻击（尤其是针对应用层的复杂攻击）、以及配置错误可能导致的安全漏洞。因此，防火墙应与其他安全设备和技术结合使用，形成多层防御体系。

2.2 入侵检测与防御系统

入侵检测与防御系统是网络安全的第二层防线，通过实时监测网络流量和系统日志，发现并响应潜在的入侵行为。（1）IDS的监测功能与IPS的防御功能。IDS：主要功能是监测网络活动，通过分析网络流量、系统日志等数据源，识别异常行为或潜在的攻击模式。IDS可以生成警报、记录事件或触发其他响应机制，但本身不直接阻断攻击。IPS：在IDS的基础上增加了主动防御功能，能够实时检测并自动阻断恶意流量。IPS不仅提供监测和警报功能，还能直接干预网络流量，阻止攻击者进一步渗透。（2）实时响应与事件处理。IDS/IPS系统能够实时监测网络中的异常情况，并迅速做出响应。这包括自动生成警报、触发预设的安全策略、记录详细的事件日志以及与其他安全系统集成，实现协同防御。通过自动化的事件处理流程，可以显著降低人工干预的成本，提高响应速度和准确性[2]。

2.3 数据传输加密技术

数据传输加密技术是确保数据在传输过程中不被窃听、篡改或泄露的重要手段。（1）对称加密与非对称加密。对称加密。使用相同的密钥进行加密和解密，高效且易于实现，但密钥管理复杂，需要在通信双方之间安全地共享密钥。非对称加密。使用一对公钥和私钥，公钥用于加密数据，私钥用于解密。这种加密方式解决了密钥管理的难题，但加密和解密过程相对较慢。（2）数字签名与认证技术。数字签名用于确保数据的完整性和来源的真实性。通过哈希函数生成数据的唯一摘要，并使用私钥对摘要进行加密，生成数字签名。接收方使用公钥验证数字签名，确保数据在传输过程中未被篡改。认证技术则用于验证通信双方的身份，防止中间人攻击。

2.4 防病毒技术

防病毒技术是保护计算机免受恶意软件（如病毒、蠕虫、木马等）感染的关键。（1）预防、检测、消除病毒的技术手段。预防。通过实时监控文件操作、网络流量等行为，阻止恶意软件的入侵。检测。利用病毒特征库进行匹配检测，识别已知的恶意软件。同时，也采用行为分析等技术，识别未知恶意软件的行为模式。消除。一旦发现恶意软件，防病毒软件将采取措施隔离、删除或修复受感染的文件。（2）病毒库的更新与防护策略。防病毒软件需要不断更新病毒库，以应对新出现的恶意软件。同时，采取多层防护策略，如实时扫描、定期全盘扫描、邮件过滤等，提高防护能力。此外，用户教育也是防病毒策略的重要组成部分，提醒用户避免打开未知来源的邮件和文件。

2.5 虚拟专用网络（VPN）技术

虚拟专用网络（VPN）技术通过构建安全的加密通道，实现远程用户与内部网络之间的安全通信。（1）隧道技术、加解密技术、身份认证技术。隧道技术。将原始数据包封装在加密的隧道中传输，确保数据在公共网络上传输时的安全性。加解密技术。使用加密算法对隧道内的数据进行加密和解密，确保数据的机密性。身份认证技术。通过数字证书、用户名/密码、生物识别等方式验证用户的身份，防止未经授权的访问。（2）VPN在远程办公中的应用。随着远程办公的普及，VPN成为连接远程员工与内部网络的关键技术。通过VPN，远程员工可以像在办公室一样访问内部资源，如文件服务器、数据库等。同时，VPN提供的安全隧道和身份认证机制，确保了远程通信的机密性和完整性。这对于保护敏感数据和遵守数据保护法规至关重要。此外，VPN还提供了灵活的远程访问控制策略，允许企业根据业务需求调整访问权限。

3 计算机网络安全技术在网络安全维护中的应用

3.1 防火墙技术在网络安全入口的核心应用

防火墙是网络安全的第一道屏障，其主要功能是监控并控制进出网络的流量，以防止潜在的网络威胁。（1）设置安全规则，筛选恶意流量。防火墙通过预设的安全规则，能够智能地筛选网络流量，只允许符合规则的流量通过。这些规则基于源地址、目标地址、端口号等多种条件，能够有效地阻止恶意流量，如DDoS攻击、端口扫描、恶意软件等。同时，防火墙还能够根据网络环境和安全策略的变化，动态调整安全规则，以适应新的威胁形势。（2）保护内部网络免受外部攻击。防火墙通过隐藏内部网络结构、限制访问权限等方式，降低了内部网络遭受外部攻击的风险。它像一道坚实的屏障，将内部网络与外部潜在的威胁隔离开来。此外，防火墙还支持NAT（网络地址转换）和端口转发功能，使得外部用户只能通过特定的端口和地址访问内部网络资源，进一步增强了内部网络的安全性。

3.2 入侵检测与防御系统在实时监测中的核心应用

入侵检测与防御系统（IDS/IPS）能够实时监测网络流量和系统活动，及时发现并阻止恶意活动。（1）监控网络流量与系统活动。IDS/IPS系统通过部署在网络的

关键位置，能够实时捕获网络流量和系统日志，并进行深入分析。通过智能算法和模式匹配技术，系统能够识别出网络中的异常行为，如未经授权的访问、恶意软件传播、数据泄露等。这些异常行为一旦被检测到，系统会立即触发警报，并向网络安全团队报告[3]。（2）及时发现与阻止恶意活动。对于IPS系统而言，它们不仅能够发现恶意活动，还能自动采取防御措施，如阻断恶意流量、隔离受感染设备等。这种主动防御的能力，使得IPS系统能够在威胁造成实际损害之前，就将其扼杀在摇篮中。同时，IDS/IPS系统还能够与防火墙、加密技术等其他安全设备联动，形成更加完善的防御体系。

3.3 加密与身份验证技术在数据传输中的核心应用

加密与身份验证技术是保护数据在传输过程中机密性和完整性的重要手段。（1）保护数据的机密性和完整性。加密技术能够将数据转换为难以解读的密文形式，确保数据在传输过程中的机密性。即使攻击者截获了传输中的数据，也无法轻易解密其内容。同时，身份验证技术能够确保数据只能由合法的接收者接收和读取，防止数据被冒名顶替的接收者窃取或篡改。这两种技术共同作用，为数据传输提供了全面的安全保障。（2）防止数据被窃取和篡改。加密和身份验证技术的应用，使得数据在传输过程中更加安全。即使攻击者试图窃取或篡改数据，也会因为无法破解加密或伪造身份验证信息而失败。这种强大的安全保障能力，使得数据在传输过程中更加可靠和可信。

3.4 安全套接层（SSL）和传输层安全（TLS）协议在通信安全中的核心应用

SSL和TLS协议是保障网络通信安全的重要标准。（1）加密和认证网络连接。SSL和TLS协议通过为客户端和服务器之间的通信提供加密和身份验证机制，确保了网络连接的机密性和完整性。这些协议使用公钥和私钥进行加密和解密操作，并通过数字证书验证通信双方的身份。通过这些机制，SSL和TLS协议能够有效地防止中间人攻击和数据窃取。（2）防止中间人攻击和数据窃取。中间人攻击是一种常见的网络攻击方式，攻击者通过拦截并篡改客户端和服务器之间的通信数据，来窃取敏感信息或破坏通信过程。SSL和TLS协议通过为通信双方建立加密通道，并使用数字证书进行身份验证，确保了只有合法的接收者才能接收和读取数据。这样，即使攻击者试图拦截并篡改通信数据，也会因为无法破解加密或伪造数字证书而失败[4]。

3.5 漏洞扫描与漏洞修补在安全管理中的应用

漏洞扫描与修补是保障系统和应用程序安全的重要环节。（1）检测和修补系统与应用程序中的潜在漏洞。漏洞扫描工具能够自动扫描系统和应用程序中的潜在漏洞，包括配置错误、代码缺陷等。这些工具通过模拟攻击行为或分析系统配置和代码结构，来发现可能的安全隐患。一旦发现漏洞，网络安全团队就可以及时采取措施进行修补，从而降低系统遭受攻击的风险。（2）降低系统遭受攻击的风险。通过定期进行漏洞扫描和修补工作，网络安全团队能够及时发现并修复系统中的安全隐患。这不仅可以减少系统遭受攻击的可能性，还能够提高系统的整体安全性和稳定性。同时，漏洞扫描和修补工作也是符合最佳安全实践的重要步骤之一，有助于企业提升网络安全管理水平并满足法规要求。

结束语

综上所述，计算机网络安全技术在网络安全维护中发挥着不可替代的作用。随着技术的不断进步，我们需要不断更新和完善安全防护体系，以应对日益复杂的网络威胁。同时，加强用户的安全教育和意识提升也是至关重要的。只有全社会共同努力，形成合力，才能确保网络环境的安全稳定，为信息化发展保驾护航。未来，我们期待更加先进、高效的网络安全技术不断涌现。

参考文献

[1]袁懿弘.网络安全维护中计算机安全技术分析[J].科技视界,2022,(02):31-32.

[2]巨贝贝.计算机网络安全技术在网络维护中的应用[J].无线互联科技,2022,(17):160-161.

[3]邢云隆.基于网络安全维护的计算机网络安全技术应用探讨[J].科技创新与应用,2022,(15):189-190.

[4]冯江杉.网络安全技术在网络安全维护中的应用研究[J].网络安全技术与应用,2022,(09):94-95.