信息与计算机通信网络安全技术探究

施　旭
国家管网集团天津液化天然气有限责任公司　天津　300452

摘　要：信息与计算机通信网络安全技术探究摘要：随着信息技术的飞速发展，计算机通信网络已经成为现代社会不可或缺的一部分。然而，网络安全问题也随之而来，给个人、企业和国家带来了巨大的损失。本文从网络安全的基本概念与原理、信息与计算机通信网络安全威胁分析和信息与计算机通信网络安全技术研究三个方面对信息与计算机通信网络安全技术进行探究。通过对加密技术、认证技术、防火墙技术、入侵检测与防御技术和安全审计与监控技术等安全技术的深入分析，旨在为构建和谐安全的网络环境贡献力量。

关键词：信息与计算机；通信网络；安全技术

引言：随着信息技术的不断发展和普及，计算机通信网络已经深入到人们生活的方方面面，极大地改变了人们的生活方式和社会形态。然而，随着网络规模的扩大和复杂性的增加，网络安全问题也日益突出，给个人、企业和国家带来了不可估量的损失。因此，对信息与计算机通信网络安全技术进行深入探究，提高网络安全防护能力，对于保障人们的合法权益和社会稳定具有重要意义。

1 网络安全的基本概念与原理

网络安全是指保护网络系统免受破坏、干扰和未经授权的访问，确保数据的完整性、可用性和保密性。随着互联网的普及和发展，网络安全问题日益严重，已经成为全球关注的焦点。网络安全的基本概念包括以下几个方面：（1）数据完整性：数据完整性是指数据在传输和存储过程中不被篡改、损坏或丢失的能力。保证数据完整性是网络安全的重要目标之一。（2）可用性：可用性是指网络服务在需要时能够正常运行，用户可以随时访问和使用。网络安全攻击可能导致网络服务中断，影响用户的正常使用。（3）保密性：保密性是指网络中的数据和信息只能被授权的用户访问，防止未经授权的访问和泄露。（4）认证与授权：认证是指确认用户身份的过程，授权是指赋予用户访问特定资源的权利。网络安全需要确保只有合法用户才能访问网络资源。（5）隐私保护：隐私保护是指保护用户的个人信息和隐私不被泄露、滥用或侵犯。网络安全需要采取措施保护用户的隐私权益。网络安全的原理主要包括以下几个方面：（1）加密技术：加密技术是通过变换数据的形式，使其在传输和存储过程中不易被破解和窃取。常见的加密技术有对称加密、非对称加密和哈希算法等。（2）防火墙技术：防火墙是一种用于保护内部网络免受外部网络攻击的安全设备。它可以对进出网络的数据包进行检查和过滤，阻止恶意流量进入内部网络。（3）入侵检测与防御：入侵检测技术是通过分析网络流量和行为，发现并阻止潜在的安全威胁。入侵防御技术则是通过采取主动措施，阻止攻击者对网络资源的非法访问和操作。（4）安全协议与标准：安全协议和标准是为了规范网络安全行为和技术而制定的一系列规则和约定。例如，SSL/TLS协议用于保护Web通信的安全，IPsec协议用于保护网络层通信的安全等。

2 信息与计算机通信网络安全威胁分析

随着信息技术的飞速发展，计算机通信网络已经成为现代社会不可或缺的一部分。然而，网络安全问题也随之而来，给个人、企业和国家带来了巨大的损失。首先，黑客攻击是网络安全的主要威胁之一。黑客通过技术手段，非法侵入他人的计算机系统，窃取、篡改或破坏数据，甚至控制整个网络。近年来，黑客攻击手段日益翻新，如钓鱼攻击、勒索软件、僵尸网络等，给网络安全带来了极大的挑战。其次，病毒和恶意软件也是网络安全的重要威胁。病毒和恶意软件可以通过电子邮件、下载文件、网页浏览等途径传播，感染计算机系统后，可能导致数据丢失、系统崩溃甚至泄露个人信息。为了防范病毒和恶意软件，用户需要定期更新操作系统和杀毒软件，提高安全意识。此外，网络钓鱼和社交工程也是网络安全不容忽视的威胁。网络钓鱼是指通过伪造网站、电子邮件等手段，诱使用户泄露个人信息的行为。社交工程则是通过人际交往技巧，骗取他人信任，进而获取敏感信息。为了防范这些威胁，用户需要提高警惕，不轻信陌生人的信息，谨慎填写个人信息。在企业层面，内部员工也可能导致网络安全风险。一些员工可能因为疏忽大意、误操作或者故意破坏，导致企业数

据泄露或系统瘫痪。因此，企业需要加强员工的网络安全培训，提高员工的安全意识。针对以上网络安全威胁，政府和企业应采取积极措施进行应对。政府应加强对网络安全的立法和监管，打击网络犯罪行为；企业应建立健全网络安全管理制度，投入更多资源进行安全防护；个人用户也应提高自身安全意识，养成良好的网络使用习惯[1]。

3 信息与计算机通信网络安全技术研究

3.1 加密技术是网络安全的基础

加密技术是网络安全的基础，它通过将原始数据转换为密文，使得未经授权的用户无法访问和理解这些数据。这种技术在保护敏感信息、防止数据泄露和确保网络通信安全方面发挥着至关重要的作用。对称加密技术是一种常见的加密方法，它使用相同的密钥进行加密和解密。这种方法的优点是加密速度快，因为加密和解密过程使用的是同一套算法和密钥。然而，对称加密技术的一个主要缺点是密钥管理复杂。由于每个用户都需要拥有一份密钥的副本，如果密钥丢失或被泄露，那么所有使用该密钥加密的数据都将变得不安全。此外，密钥的分发和管理也成为一个挑战。非对称加密技术则使用一对密钥，即公钥和私钥。公钥用于加密数据，而私钥用于解密数据。这种方法的优点是密钥管理简单，因为公钥可以公开分发，而私钥则安全地保存在用户手中。然而，非对称加密技术的加密速度较慢，因为它需要执行更复杂的数学运算。尽管如此，非对称加密技术在许多场景中仍然非常有用，特别是在需要安全地传输密钥的情况下。混合加密技术结合了对称加密和非对称加密的优点，以实现更高的安全性和效率。在这种技术中，首先使用对称加密算法（如AES）对数据进行快速加密，然后使用非对称加密算法（如RSA）对对称密钥进行加密。这样，即使非对称密钥被泄露，攻击者也无法解密原始数据，因为他们没有用于解密对称密钥的私钥。同时，对称加密的使用保证了加密速度。

3.2 认证技术是确保网络通信双方身份的重要手段

随着网络技术的发展，网络安全问题也日益突出。为了确保网络通信的安全，认证技术成为了一种重要的手段。首先，我们要了解的是数字证书。数字证书是一种基于公钥基础设施（PKI）的数字身份认证方式。它通过使用一对密钥，即公钥和私钥，来创建一个安全的环境。公钥用于加密信息，而私钥则用于解密信息。数字证书是由权威的第三方机构颁发的，可以有效地防止伪造和篡改，从而确保了网络通信的安全。其次，双因素认证也是一种有效的安全措施。双因素认证是指通过两种或多种不同的身份验证方式来确认用户身份。例如，用户可能需要输入密码，然后再接收到手机验证码。这种方式不仅提高了安全性，而且也增加了攻击者的难度，因为即使他们获取了用户的密码，也无法通过验证码验证[2]。最后，生物识别技术是近年来发展迅速的一种身份认证技术。这种技术通过分析个体的生理特征（如指纹、面部特征等）来进行身份认证。由于每个人的生理特征都是独一无二的，因此生物识别技术具有很高的安全性。同时，生物识别技术也具有便捷性，用户无需记住复杂的密码，只需要使用自己的生物特征就可以进行身份认证。

3.3 防火墙技术是网络安全的第一道防线

防火墙技术是网络安全的第一道防线，它的主要作用是对网络数据包进行检查，阻止未经授权的访问。传统防火墙主要通过对数据包的源地址、目的地址、端口等信息进行检查，以实现对网络流量的控制和保护。随着网络技术的发展，下一代防火墙（NGFW）应运而生。NGFW在传统防火墙的基础上，增加了对应用层协议的解析能力，可以实现更精细的流量控制。这意味着NGFW不仅可以对数据包的基本信息进行检查，还可以对应用层协议进行解析，从而更好地识别和阻止恶意流量。此外，NGFW还具有更高的性能和可扩展性，可以满足大型企业和数据中心的需求。虚拟防火墙是一种基于软件的防火墙技术，它可以在物理服务器上创建多个虚拟防火墙实例，实现对不同网络区域的隔离保护。虚拟防火墙具有灵活性高、部署快速、成本低廉等优点，适用于中小型企业和分支机构。通过虚拟防火墙，企业可以根据实际需求划分不同的网络区域，并对每个区域实施相应的安全策略，从而提高整体网络安全水平。

3.4 入侵检测与防御技术是网络安全的重要组成部分

入侵检测与防御技术是网络安全的重要组成部分，它们在保护网络系统免受恶意攻击和破坏方面发挥着关键作用。这些技术通过实时监控网络流量、分析异常行为和自动阻断攻击，为企业和个人提供了强大的安全保障。入侵检测系统（IDS）是一种用于监控网络流量并识别潜在威胁的安全设备。它通过收集和分析网络数据包，以确定是否存在任何异常或可疑活动。IDS可以分为基于网络的IDS（NIDS）和基于主机的IDS（HIDS）。NIDS部署在网络的关键节点上，监视整个网络的流量；而HIDS则安装在单个主机上，监视该主机的活动。IDS的主要功能包括：1)实时监控网络流量，以便及时发现异常行为；2)分析网络数据包，以识别潜在的攻击特征；3)生成警报，通知管理员有关潜在威胁的信息；4)提供日

志记录功能，以便进行事后分析和取证[3]。入侵防御系统（IPS）是一种集成了IDS功能的设备，除了检测潜在威胁外，还具备自动阻断攻击的能力。IPS可以根据预先设定的规则和策略，对检测到的攻击行为进行实时响应，从而阻止恶意流量进入内部网络。IPS的主要优势在于其主动防御能力，可以有效减少网络受到攻击的风险。安全事件管理系统（SIEM）是一种集中管理和分析安全事件的系统，可以帮助企业及时发现和应对安全威胁。SIEM通过收集来自各种安全设备的日志和警报信息，对这些数据进行统一分析和处理，以便快速识别和解决安全问题。SIEM的主要功能包括：1)集中管理多个安全设备的数据；2)对收集到的数据进行实时分析和关联；3)生成详细的安全报告和可视化图表；4)提供自动化的威胁响应和处置功能；5)支持与其他安全系统集成，实现全面的安全防护。

3.5 安全审计与监控技术是网络安全的有力保障

随着网络技术的发展，网络攻击的手段也在不断升级，这对网络安全提出了更高的要求。为了应对这些挑战，我们需要采取一系列的措施来保障网络安全。其中，安全审计与监控技术是网络安全的有力保障。首先，日志分析是一种重要的安全审计技术。日志文件是系统和应用程序运行过程中生成的记录，它记录了系统和应用程序的各种操作信息。通过对日志文件的分析，我们可以发现系统中的异常行为和潜在威胁。例如，如果一个用户在短时间内连续进行了多次登录尝试，那么这可能是一种恶意登录尝试，需要立即进行处理。通过日志分析，我们可以及时发现这些异常行为，从而防止潜在的安全威胁。其次，流量分析也是一种有效的安全监控技术。网络流量是网络中传输的数据量，通过对网络流量的深入分析，我们可以识别出恶意活动和攻击模式。例如，如果一个网络中的某个节点的流量突然增大，那么这可能是一种DDoS攻击的迹象。通过流量分析，我们可以及时发现这些恶意活动，从而采取相应的防御措施。最后，行为分析是一种基于用户行为的安全监控技术。通过对用户的行为模式进行分析，我们可以发现异常行为和潜在威胁。例如，如果一个用户在短时间内频繁地访问一些不常见的网站，那么这可能是一种恶意行为，需要立即进行处理。通过行为分析，我们可以及时发现这些异常行为，从而防止潜在的安全威胁。

结束语

信息与计算机通信网络安全技术是当今社会的关键问题，随着科技的不断发展，网络安全问题日益严重。本文从基本概念、常见威胁、加密技术、认证技术、防火墙技术、入侵检测与防御技术以及安全审计与监控技术等方面进行了详细阐述。虽然这些技术为保障网络安全提供了有力支撑，但仍然需要我们继续关注和研究新的安全技术，以应对不断变化的网络安全威胁。让我们共同努力，为构建一个更加安全、开放、高效的计算与通信网络环境贡献力量。

参考文献

[1]刘博舒.计算机安全技术在企业信息管理中的应用[J].现代工业经济和信息化,2022,12(11):93-95.

[2]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(29):11-13.

[3]田杰.安全技术在计算机软件开发中的应用分析[J].中国新通信,2021,23(23):127-128.