网络安全协议在计算机通信技术中的应用研究

唐占文

（内蒙古中交信通网络科技有限公司 呼和浩特 010050）

摘 要 随着计算机网络技术的飞速发展，网络安全问题也越来越突出。因此，将网络安全协议应用于计算机通信领域是非常有必要的。文中在分析研究网络安全协议的基础上，讨论了它在计算机通信领域的应用。文中首先对网络安全协议的概念及分类进行了阐述，并对其在计算机通信领域的应用场景及功能进行了详细分析。最后，展望了计算机通信技术中网络安全协议的发展前景。

关键词： 网络安全协议；计算机通信技术；加密

中图分类号 TP393

Research on the Application of Network Security Protocol in Computer Communication Technology

TANG Zhanwen

（Inner Mongolia Zhongjiao Xintong Network Technology Co.，Ltd.，Hohhot 010050，China）

Abstract With the rapid development of computer network technology, network security issues have become increasingly prominent. Therefore, it is very necessary to apply network security protocols to the field of computer communication. Based on the analysis and research of network security protocols, this paper discusses their applications in the field of computer communication. This paper first elaborates on the concept and classification of network security protocols, and provides a detailed analysis of their application scenarios and functions in the field of computer communication. Finally, the development prospects of network security protocols in computer communication technology were discussed.

Key words Network Security Protocol，Computer communication technology，Encryption

0 引言

网络安全协议是计算机通信过程中为保证通信双方不被病毒、黑客等攻击或窃取而采用的一套规则和技术。将网络安全协议应用到计算机通信技术中，能有效地保证网络数据的完整性，保证信息在传输过程中不被泄漏或篡改。

1 网络安全协议的基本概念

1.1 网络安全协议的定义

网络安全协议是一种定义网络安全和隐私保护策略的框架和指南。它定义了网络管理员、设备和应用程序之间的安全通信方式，以确保网络的保密性、完整性和可用性。网络安全协议通常包括一组规则和指令，用于管理网络安全和隐私保护。这些规则和指令可以由管理员制定，也可以由设备或应用程序制定。例如，网络安全协议可以包括密码管理、入侵检测、防火墙策略、入侵防御等方面的内容，其可以保护网络的安全性和保密性，防止未经授权的访问、篡改和泄露信息，同时也可以防止恶意攻击和未经授权的访问。例如，网络安全协议可以帮助管理员控制进入网络的设备，监控系统运行状态，以及管理入侵防御系统等。此外，网络安全协议还可以帮助设备之间进行有效通信，确保数据的完整性和保密性。例如，网路安全协议可以帮助设备之间进行加密传输、数字签名、身份验证等操作，确保数据的完整性和保密性。网络安全协议是一种有效的工具，可以帮助管理员管理和保护网络的安全性。它涵盖了多种安全策略和指令，可以帮助设备之间进行有效通信、监控系统运行状态、管理入侵防御系统等[1]。

1.2 网络安全协议的分类

网络安全协议（Security Protocol）是保证网络系统安全而采取的一系列技术与策略，其可以按照不同的标准进行分类。网络安全协议按协议的类型可分为以下几类。（1）加密协议是一种保护数据保密性、完整性的技术.常用的加密协议有 AES，SSL，TLS 等。AES 是一种应用广泛、安全性高、能抵抗多种攻击的加密协议。SSL 是一种广泛使用的数据传输协议，能保证数据的保密性和完整性。TLS 协议是一种能保证数据在传输过程中完整性的安全通信协议。（2）认证协议是在网络设备或系统中保证用户身份的一种有效手段。常用的认证协议有 IKE，OCSP，IDEA 等。其中，IKE 是一种验证用户身份、验证用户权限的技术，OCSP 是

作者简介：唐占文（1975—），硕士，中级工程师，研究方向为移动通信技术。

一种验证数据完整性的技术，IDEA则是一种对发送者与接收者进行身份鉴别的技术。(3)访问控制协议(Access Control Protocol)是一种在网络环境下保护网络资源的有效方法。常用的存取控制协议有IPSec，ICMP等。IPSec是目前应用最广的一种访问控制协议，ICMP是一个标准的通信协议，用来验证主机是否正接受网络请求。(4)防毒协议是防止病毒和恶意软件等威胁的一种有效手段。常见的防毒软件有Adobe After Effect，Secure Business，SeaFile等。(5)审计监控协议是一种用于监控网络系统安全性和性能情况的技术，常见的审计监控软件有NTFS，FAT32等。NTFS是一种用于格式化文件系统文件和块，以便在不同设备之间共享和保护文件。FAT32是一种用于格式化文件系统文件和块，以便在不同设备之间共享和保护文件[2]。

2 网络安全协议在计算机通信技术中的应用

2.1 信息加密技术

网络安全协议是计算机通信领域为了保证信息的安全传输而建立的一套协议。在这些协议中，信息加密技术非常重要。该技术能将信息加密，使之不易被人读懂，其是一种有效的手段，能防止信息在传输过程中被窃取和篡改。网络安全协议将信息加密技术应用于计算机通信技术，具体包括以下几个方面。(1)数据加密。在数据传输过程中，将原始数据进行加密处理，使其难以被他人读取和理解。例如，在网络通信中，可以使用对称密钥算法对数据进行加密处理。(2)数字签名。指在传输过程中，利用一定的算法来验证原始数据的真实性与完整性，其是一种有效的防御攻击手段。(3)防火墙。防火墙是用来保护计算机网络安全，防止外部攻击的一种技术。防火墙可通过设置不同的规则与策略对外部攻击进行拦截。(4)访问控制。其能利用某种算法来限制用户的访问权限，从而保护用户的隐私和数据的安全性。例如，用户身份验证机制可用于网络通信，以限制用户对某些敏感信息的访问。(5)加密算法。指利用一种算法来处理原始数据，使它很难被其他人读懂。采用加密技术、防火墙等技术，提高了信息传输的安全可靠性，能有效地防止数据被窃取、篡改等攻击[3]。

2.2 数字签名技术

数字签名是对数据进行加密的一种技术，它能保证数据的保密性和完整性。数字签名技术可应用于计算机通信中，具体包括以下几个方面。(1)身份验证。数字签名技术能用来确认资料的来源与真伪。如果数据来自非法渠道，则不可信任。数字签名是一种利用密码学原理对数据进行认证的技术，以保证数据的保密性和完整性。(2)消息摘要。数字签名技术也可应用在消息摘要中，使数据更容易了解。消息摘要技术能将原始数据分解成较小的部分，以便理解与解释。它能验证消息，以保证消息的保密性和完整性。(3)完整性检验。数位签章技术可以用来检查资料是否被窜改。这一点可以利用密码学的原理，如RSA算法、椭圆曲线加密等。如果数据经过修改，则无法再对其进行验证。(4)匿名。数位签章技术也可被用来保护资料的保密性与完整性。该算法既能保证数据的保密性，又能有效地防止数据被篡改或伪造。(5)不可否认性。数字签名技术可用于非抵赖性，以确保资料不受窜改或否认。数字签名是一种非常有效的网络安全协议，它能有效地保护数据的保密性和完整性，被广泛地应用于计算机通信领域[4]。

2.3 认证技术

网络安全协议在计算机通信中起着重要的作用，它能保护通信双方的信息安全与隐私。在网络安全协议中，认证技术能保证通信双方的身份是真实可信的，并能防止未经授权的访问与通信。常用的端对端身份验证方法有SSH，TCP/IP，TLS等。其中，SSH算法应用最为广泛，它采用对称加密与不对称加密两种方式，既能保证数据的保密性，又能保证数据的完整性。IP是另一种应用广泛的端对端认证方式，它利用IP协议向接收者发送数据包，然后在接收者处解密。TLS是一种更加安全的端对端认证方式，它采用不对称加密算法来保证数据的保密性和完整性。SSL/TLS(SSL/TLS)是一种广泛使用的安全协议，它能保证Web应用与客户端应用在数据传输时不受篡改或泄漏。网络安全协议的应用，保证了通信双方真实可信的身份、可靠的通信链路以及良好的网络环境。此外，该协议还能防止各种恶意攻击、窃听、篡改等行为，保护通信双方的信息不被泄漏或破坏。

2.4 数据完整性验证技术

本文介绍了一种新型的基于网络的数据完整性认证方法。数据加密能防止未授权用户对数据进行访问，身份认证能保证通信双方身份的真实性，数字签名能保证通信双方所传递的信息是真实可信的。数据完整性验证是网络安全协议的重要组成部分。在网络安全协议中，采用加密算法、认证算法和数字签名等方法，实现了数据的完整性验证。以Windows为例，网络安全协议通常使用对称加密算法对数据进行完整性验证。对称加密算法在保证信息安全的前提下，可以防止非授权用户获取信息，但同时也存在密钥泄漏和破解等安全性问题。为保证网络安全协议中数据的完整性与安全性，可采取如下措施。(1)加密算法。资料加密确保资料不会被未授权使用者存取。DES是一种常用的加密算法，它能保证信息在传输过程中的安全。(2)认证算法能保证通信双方的身份认证。常用的认证算法有SSH，SSL等，其都能保证通信双方的身份鉴别。(3)数字签名能保证通信双方所传递的信息是真实、可靠的。目前常用的数字签名技术有HASH，ECC等，它们能保证信息在传输过程中不可被篡改和篡改。(4)在网络安全协议中，安全协议是保证数据完整、安全的重要方法。安全协议一般包括网络访问控制、身份鉴别、数据加密、数字签名等。例如，

Windows系统的安全性协议一般都是通过SSL/TLS来实现的;在Windows 2000系统中,一般使用SSH/TLS来实现安全协议。在计算机通信技术中,数据完整性验证技术是保障数据安全性和完整性的重要手段之一,可以根据实际情况选择不同的加密算法、认证算法、数字签名等技术,以实现数据完整性验证,从而保证数据的安全性和完整性。

2.5 网络监控和攻击防御技术

网络监测与攻击防御技术是计算机通信技术中的重要内容。计算机通信技术利用网络监测技术,能有效地监控并抵御来自外部的诸如木马病毒、蠕虫病毒等攻击。同时,利用IDS技术,计算机通信技术能发现网络中存在的安全漏洞与威胁,从而采取相应的防御措施。在设计与实现网络安全协议时,需综合考虑多方面的因素。首先,要保证网络通信的保密性与完整性,这就要求使用加密技术对数据进行保密保护。其次,应避免利用漏洞实施攻击与入侵。攻击者往往利用系统或软件的弱点实施攻击,因此必须采取相应的防范措施。此外,还应防止黑客利用这些漏洞实施攻击与入侵,因此必须采取安全保护措施以保证网络通信的安全可靠。因此,本文提出了一种基于网络安全的网络安全协议。只有不断地将网络安全协议应用于计算机通信技术,才能使网络免受攻击与入侵[5]。

3 网络安全协议在计算机通信技术中的应用方法分析

3.1 基于VPN技术的网络安全协议应用方法分析

VPN是一种利用隧道技术建立不同网络间安全连接的安全协议,其具有强大的加密、认证功能,被广泛地应用于网络安全领域。虚拟专用网的安全协议是虚拟专用网的一项重要功能,相对于传统的加密方式,虚拟专用网采用了更加先进的加密算法以及更加复杂的协议,能更好地保护用户的隐私和安全。VPN技术的应用需从安全、高效、可靠3个方面进行考虑。利用VPN技术实现网络安全协议的方法如下。(1)加密算法选择。不同的加密算法对数据安全性的影响是不一样的。因此,在选择VPN技术时,必须兼顾安全与高效的数据加密算法。(2)认证机制。VPN技术采用了多种认证机制,如IPSec,SSL,TLS等。这些身份验证机制能保证数据传输的保密性与完整性。(3)密钥管理。VPN技术需要管理密钥,包括公用密匙,私人密匙,对称密匙等。采用不同的金钥管理机制,可确保在传送过程中,资料不会被盗用或篡改。(4)安全性审计。VPN技术要求对数据进行安全性审计,以防止数据在传输过程中被篡改和窃取。通过对VPN技术的分析,提出了一种新的解决方案,即加密技术和回放技术。(5)分布式部署。VPN技术能把数据传送给多个节点,由各节点对其进行身份验证、加密。基于VPN技术的网络安全协议应用应从安全、高效、可靠3个角度出发,通过不同的加密算法与认证机制来保护数据的隐私性与安全性。同时,为了保证数据在传输过程中不被窃取、篡改,需要从密钥管理、安全性审计等多个方面进行综合考虑与设计[6]。

3.2 基于防火墙技术的网络安全协议应用方法分析

防火墙技术是为抵御外部威胁而设计的一项技术,它能监控网络流量,过滤掉不安全的数据流。网路安全协定是定义电脑通信与分享资讯的规范程式集合,这类协议一般包括加密,认证,防火墙等。网络安全协议在防火墙技术中占有重要地位,使用网络安全协议的常用方法如下[7]。(1)加密封包。防火墙技术可利用密码技术防止数据包被非法存取。如果数据包不经过加密,则会被传送到目标地址,这样就会造成数据被窃听或截取。(2)认证。防火墙技术能通过多种认证方式来确保网络的安全。例如,数字证书或电子签名都可以被用来验证用户的身份。这些方法能有效地防止未授权用户对重要信息及资源进行访问。(3)过滤通信。防火墙技术能有效地过滤掉不安全的数据流,从而保证网络的安全。例如,它能限制外部站点或应用,从而阻止恶意攻击或信息泄漏。(4)使用防火墙规则。防火墙技术还可利用防火墙规则,以确保网络的安全。这些规则通常都有一定的限制性,如只允许被授权的用户访问某些资源或服务。(5)监控与反应。防火墙技术能监控并响应恶意攻击或威胁,它包括监测系统的运行状态,检测攻击并采取相应措施等[8]。

3.3 基于身份验证技术的网络安全协议应用方法分析

网络安全协议是保证网络数据安全的一种重要方法。其中,以认证为基础的网络安全协议被广泛采用。该方法为用户提供了认证服务,保证了用户在网络上传输的数据的合法性、可信性和完整性。基于身份认证的网络安全协议通常采用生物识别、密码算法等多种技术来保证数据的安全传输,这些方法主要通过对用户的身份进行验证,如指纹识别,人脸识别等。另外,为了保证数据传输的保密性和完整性,采用了加密算法。在以身份认证为基础的网络安全协议中,安全协议起着重要的作用。在网络传输过程中,采用安全的协议来保证数据不会被篡改、盗用、伪造等,常见的安全性协议有IPSec,SSLVPN等。基于认证技术的网络安全协议在实际应用中具有广阔的应用前景。例如,在金融业,认证技术可以被用来进行身份认证,交易验证等;在医疗领域,可将身份认证技术应用于健康数据的采集和传输;在工业领域,认证技术被用来控制数据的隐私性和数据的完整性。合理运用这些技术,可提高网络数据传输的安全性与可靠性,保证数据不会被篡改、盗用、伪造等,从而保障网络环境的安全[9]。

4 结语

随着计算机通信技术的飞速发展,网络安全协议被越来越多地应用于计算机通信领域。采用网络安全协议,能

有效地保证计算机通信系统的安全可靠，防范信息泄漏与攻击。同时，网络安全协议能提高计算机通信系统的性能、效率以及用户体验。

参考文献

[1] 刘鹏宇，郭家鑫.网络安全协议在计算机通信技术中的作用分析[J].信息记录材料，2024，25(11)：225-227.

[2] 陈洁，吴全，王子豪.网络安全协议在计算机通信技术中的运用分析[J].信息与电脑(理论版)，2024，36(1)：171-173.

[3] 青松.网络安全协议在计算机通信技术中的作用[C]//中国管理科学研究院教育科学研究所.2022电脑校园网络论坛论文集.山东理工大学计算机科学与技术学院，2022：3.

[4] 景青山.网络安全协议在计算机通信技术中的作用研究[J].无线互联科技，2022，19(8)：28-29.

[5] 刘碧微.网络安全协议在计算机通信技术中的作用分析[J].信息记录材料，2021，22(11)：77-78.

[6] 洪浩.网络安全协议在计算机通信技术中的作用与意义[J].科技传播，2019，11(4)：164-165.

[7] 杨荔琼，黄陵.网络安全协议在计算机通信技术中的应用[J].电子技术与软件工程，2018(18)：194.

[8] 李伟.网络安全协议在计算机通信技术当中的作用与意义分析[J].信息与电脑(理论版)，2018(15)：187-188.

(上接第131页)

输加密模式，避免敏感医疗数据明文传输，保证患者隐私数据的机密性和完整性。(5)构建层次化区域网络，对医疗物联网进行安全监控。按照医疗服务需求，构建层次化区域网络，安装区域间、内外网防火墙、入侵检测系统，从而对通信网络进行安全监控，及时发现异常行为。(6)在应用层设置高级的访问控制机制。医疗物联网的应用层面向用户，容易成为黑客入侵的入口，需在应用层采用高级的访问控制方式来保护系统，可采用指纹、虹膜或人脸识别等安全性较高的访问控制方式。(7)部署病毒防火墙，定期进行病毒扫描。各个层面的漏洞容易被入侵者利用来传播病毒或恶意代码，需部署病毒防火墙，并定期进行病毒扫描，及时发现并清除病毒、木马等恶意代码，保护系统安全。(8)定期进行人员安全培训，提高人员安全意识。人员操作错误或受社会工程学攻击情况在系统内部时有发生，因此应定期对系统人员进行安全教育培训，提高人员安全意识，避免因为人员安全问题而对医疗物联网造成损害。

4 结语

当前，医疗物联网物理终端和应用系统增长迅猛，医疗物联网蕴含丰富的病患敏感数据，系统运行中断影响着患者生命安全，导致医疗物联网的应用价值备受攻击者关注，医疗物联网面临着巨大的安全挑战。本文分析了医疗物联网的分层体系结构、各层次面临的安全风险，针对这些安全风险提出了相应的安全控制措施，旨在提高医疗物联网安全，为保护医疗数据安全和保证医疗系统服务持续性提供参考方案。

参考文献

[1] 曹阳.基于物联网的智慧医院医疗设备管理体系的构建与应用[J].中国医疗器械信息，2024，30(7)：148-150.

[2] 李丹，张美琴，唐诗.基于物联网的远程医疗在老年健康管理中的应用研究进展[J].医学信息学杂志，2022，43(9)：47-53.

[3] 李志勇，彭雄俊，李鹏伟，等.身联网+医疗健康及其相关医学装备安全风险应对[J].中国医学装备，2021，18(12)：144-152.

[4] 万振，邱丹，刘元喆，等.国内医疗物联网技术发展及应用现状[J].医疗卫生装备，2020，41(11)：82-86，102.

[5] 董圆.医院无线网络建设策略探析[J].网络安全技术与应用，2023(11)：84-86.