文章类型：论文|刊号（ISSN）：2972-4236(P) / 2972-4244(O)

基于计算机网络的安全通信机制探讨

任霄　王艳周
林州建筑职业技术学院
DOI:10.12238/acair.v3i1.11871

[摘　要] 伴随着互联网技术的迅速发展和信息时代的到来,计算机网络已经成为现代社会生活、工作的重要支撑。但是与此同时计算机网络安全问题日益凸显,各种网络攻击、信息泄露事件频发,这给个人和企业带来了严重的损失,使得安全通信机制成为了迫切需要解决的问题。基于此,本文将对计算机网络的安全通信机制进行探讨,分析其技术基础、应用场景以及实施与管理策略,期望为提高计算机网络安全通信水平提供理论支持。
[关键词] 计算机网络；安全通信机制；应用场景
中图分类号：G623.58　文献标识码：A

Discussion on secure communication mechanism based on computer network

Xiao Ren　Yanzhou Wang
Linzhou Polytechnic of Architecture

[Abstract] With the rapid development of Internet technology and the arrival of the information age, computer network has become an important support for modern social life and work. But at the same time, the problem of computer network security has become increasingly prominent, and various network attacks and information leakage incidents have occurred frequently, which has brought serious losses to individuals and enterprises. The secure communication mechanism has become an urgent problem to be solved. This paper will discuss the secure communication mechanism of computer network, analyze its technical basis, application scenarios, implementation and management strategies, and hope to provide theoretical support for improving the level of secure communication of computer network.
[Key words] computer network; Secure communication mechanism; Application scenario

引言

在数字化时代,信息已成为社会发展的重要驱动力。计算机网络作为信息传递的主要渠道,它承载着大量的个人隐私、商业秘密和国家机密。但是随着网络技术的飞速发展,计算机网络安全问题日益突出,安全通信成为保障信息安全的至关重要的一环。在信息技术日新月异的今天,探讨基于计算机网络的安全通信机制,以应对各种安全威胁,这已经成为我国信息化建设的一项紧迫任务。

1 计算机网络安全通信概述

1.1计算机网络安全通信的概念

计算机网络安全通信是指在网络环境中通过对信息进行加密、认证、完整性保护等手段,以确保信息在传输过程中不被窃取、篡改、伪造等恶意行为破坏,从而保证信息在传递过程中的安全性和可靠性。安全通信的目标是确保信息的机密性、完整性和可用性,使通信双方能够在安全的网络环境下进行有效沟通。计算机网络安全通信涉及到许多关键技术,这些技术包括加密算法、认证机制、安全协议等[1]。

1.2安全通信的重要性

安全通信在现代社会中具有极高的重要性,第一国家安全方面,计算机网络已经成为国家重要的基础设施,涉及国家安全、经济、科技等各个领域,确保计算机网络安全通信对于维护国家利益、保障国家安全具有重要意义。第二企业利益方面,企业内部网络承载着大量商业机密和敏感信息,一旦泄露将给企业带来严重的经济损失和信誉损害。基于安全通信机制,企业就可以保护内部信息的安全,确保业务顺利进行。第三公民个人信息安全方面,随着互联网的普及,越来越多的个人信息存储在网络环境中。计算机网络安全通信就可以保障公民个人信息的安全,避免因信息泄露导致的各种风险。第四计算机网络安全通信还关系到社会的和谐稳定,网络谣言、虚假信息等网络犯罪活动日益猖獗,而安全通信机制可以有效地打击网络犯罪,维护社会秩序。

2 安全通信机制的应用场景

2.1企业网络通信

企业网络通信是现代企业运作中不可或缺的一部分,涉及到企业内部各部门之间的信息传递、与合作伙伴的数据交换以及与客户的信息交流。在这个过程中数据的安全性至关重要,具体来说企业网络通信面临着黑客攻击、内部员工泄露、恶意软件等安全威胁。为了确保企业网络通信的安全,企业就需要采取一系列安全通信机制,比如加密技术、身份认证、访问控制等。基于这些技术可以有效防止数据被非法获取、篡改和破坏,确保企业信息的安全传输[6]。

2.2电子商务交易

电子商务交易作为现代社会的一种新型交易方式,已经成为人们日常生活的重要组成部分。在电子商务交易过程中涉及到用户个人信息、交易数据、支付信息等敏感信息的传输。这些信息一旦泄露或被篡改,不仅会导致用户财产损失,还可能引发信任危机。基于此电子商务交易需要采用安全通信机制,比如SSL/TLS协议、数字签名、双重身份认证等,以确保交易过程的安全性。这些机制可以防止中间人攻击、数据篡改、信息泄露等风险,保障电子商务交易的顺利进行。

2.3移动设备通信

由于移动设备的普及,移动设备通信已成为人们日常生活的重要组成部分,但是移动设备通信面临的安全威胁也日益严重。为了保障移动设备通信的安全性,以下几种安全通信机制被广泛应用:其一采用端到端加密技术,确保通信数据在传输过程中的安全性。其二运用身份认证机制,防止非法接入。除此通过实时监控移动设备的使用状况,发现并处理异常行为,降低安全风险[2]。

3 安全通信机制的实施与管理

3.1制定安全策略与规范

3.1.1安全通信机制的应用与实施需要根据实际情况来制定出相应的策略与规范,这样一来才能够确保整个安全通信机制能够正常运行。而在具体的实施过程中其必须要符合一定的规范,这是由于不同的策略与规范会影响到计算机网络的安全。通常情况下安全通信机制在实际应用中主要包括了信息发送、信息接收、信息存储、信息管理四个部分。在实际应用中主要是通过网络的传输来实现信息的发送与接收,而在整个过程中如果没有相关的规范,那么就会出现安全隐患问题。基于该点而言必须制定出相应的规范来加强对计算机网络的管理,从根本上解决安全通信机制中存在的问题。

3.1.2为了加强计算机网络的安全,就要制定出相应的策略与规范。其中安全策略是对安全通信机制中信息传递过程的规范,计算机网络中的信息传递可以分为两种形式,即信息发送与信息接收。在信息发送的过程中必须要遵循一定的通信协议,其中包括了相关的安全规则,通过制定规范来确保通信过程中存在安全隐患问题时能够及时解决。而在信息接收的过程中主要包括了接收程序与接收内容两个部分,在具体应用过程中需要对数据信息进行分类与筛选,如此一来才能够有效地避免在接收过程中出现数据丢失问题[7]。

3.2建立安全管理体系

3.2.1建立完善的安全管理体系需要从多个方面进行考虑,具体要从以下几个方面展开：第一在网络安全通信机制中需要建立完善的管理体系,以此更好地发挥安全通信机制的作用。第二在建立安全管理体系时要对安全通信机制进行全面的分析,了解其结构以及作用。第三在计算机网络系统运行过程中需要对其进行全面的管理和维护,以此更好地保障计算机网络系统的运行。第四在计算机网络系统运行过程中要对其进行有效的监测和分析,及时发现其存在的问题并进行修复。

3.2.2在计算机网络安全通信机制中需要对网络安全进行有效的管理,只有建立完善的管理体系才能够更好地发挥安全通信机制的作用。基于该点而言在建立安全管理体系时需要对计算机网络安全进行全面的管理,要对计算机网络的系统、设备、人员等方面进行有效的管理,以此更好地保障网络安全。同时在建立完善的安全管理体系时需要对计算机网络系统进行全面的分析和研究,找出系统中存在的漏洞和问题,然后对这些问题进行处理和修复。除此在计算机网络系统运行过程中需要加强对计算机网络系统运行情况的监测和分析,如此一来才能够及时发现安全问题并进行处理[3]。

3.3监测与评估安全性能

3.3.1计算机网络通信系统在实际运行中会出现各种安全问题,为了保障计算机网络通信的安全,就需要对其进行监测与评估,以发现问题并解决问题。在计算机网络通信系统中存在着多种安全隐患,比如非法用户入侵、系统漏洞等。在计算机网络通信系统中一些黑客、病毒等会利用漏洞入侵计算机网络,对其进行破坏和攻击。非法用户入侵是一种非常常见的情况,如果不能及时发现和解决问题,就会威胁到计算机网络通信的安全性。对于非法用户入侵事件就可以采用入侵检测技术进行检测和识别,入侵检测技术可对入侵的数据进行分析和处理,并根据处理结果采取相应的防护措施。

3.3.2为保证计算机网络通信的安全性,就需要对计算机网络安全性能进行监测与评估,在安全通信机制中监控是一种很重要的方式。计算机网络通信系统的监控工作,需要通过对安全通信机制的监测,并对其进行评估。具体来说,其一在监控过程中要对系统的各项指标进行分析,并建立一套完整的评估体系。其二在评估过程中应该结合计算机网络通信系统实际运行情况,并结合其相关标准进行评估。基于对计算机网络安全通信机制进行监测与评估,能及时发现其存在的问题,然后将问题反馈给技术人员,并根据相应的标准制定解决方案[8]。

3.4安全审计与监控

3.4.1网络安全审计系统主要包括两个方面,分别是数据采集和数据分析。数据采集主要是对网络中的资源使用情况进行记录,通过这些信息可以判断网络中是否存在违规行为,还可以对网络安全事件进行分析,从而做出响应。数据分析则是通过对网络中的数据进行分析,从而了解网络系统的运行状态以

及系统是否存在安全隐患。在安全审计与监控中主要的工作包括：对用户活动和网络资源使用情况进行记录；对用户的操作行为进行分析；通过对网络事件的记录来判断网络系统是否出现问题；根据审计结果做出响应；根据安全评估结果对系统进行更新等。

3.4.2安全审计与监控主要是对网络资源的使用、用户活动和网络事件进行记录和分析。主要的功能是对网络的使用情况进行审计，审计信息主要包括：用户权限、用户活动、活动时间、活动内容等，基于这些信息可以对用户的操作和网络使用行为进行记录，从而判断网络系统是否存在违规行为。在网络安全事件发生后，还可以通过审计记录来判断网络中发生了什么问题。除此监控功能是安全审计和监控的目的之一，安全审计是对整个网络系统进行全面的评估，主要包括对系统自身性能和服务质量的评估，而监控则是在系统出现问题时做出响应[4]。

3.5应急响应计划

3.5.1在计算机网络安全通信机制的实施过程中，其应对突发事件的能力也是十分重要的，只有在发生突发事件时能够及时处理才能够有效保证计算机网络安全通信机制的正常运行。基于该点而言就需要对应急响应计划进行制定，其一在该计划中需要对应急响应机制进行明确，并且能够针对突发事件对其进行有效的处理。其二在计算机网络安全通信机制中需要对应急响应计划中的人员与物资进行明确，以便能够提高应急响应计划的执行效率。除此还需要对应急响应计划中所需设备进行明确，以便能够在发生突发事件时能够及时处理。

3.5.2在计算机网络安全通信机制的实施与管理过程中需要对应急响应计划进行制定，以确保在发生突发事件时能够及时处理。同时需要对应急响应计划进行不断地完善，并对其进行不断的优化。在计算机网络安全通信机制的实施与管理过程中相关部门需要不断地对其进行完善与优化，以确保在实际应用过程中能够充分发挥出该机制的优势与作用，如此一来才能够有效提高计算机网络安全通信机制的应用效果[9]。

3.6持续改进与优化

3.6.1安全通信机制实施过程中要根据实际情况对其进行不断改进和优化，安全通信机制的实施与管理过程中要对其不断进行优化和改进，主要是为了解决目前计算机网络安全通信机制实施过程中存在的问题，提高计算机网络安全通信机制实施效果。具体来说，其一在计算机网络安全通信机制实施过程中要根据实际情况对其进行不断优化和改进。其二在计算机网络安全通信机制实施过程中要对其不断进行优化和改进，一方面可以根据实际情况对计算机网络安全通信机制实施过程中的制度、流程等进行优化，另一方面可以对计算机网络安全通信机制实施过程中的管理、监督等进行优化[5]。

3.6.2在整个计算机网络安全通信机制实施过程中要对其不断进行优化和改进，在计算机网络安全通信机制实施过程中，会有很多不确定因素和不稳定的因素，这些不确定因素会对计算机网络安全通信机制实施造成干扰。针对这些不确定因素和不稳定因素，就要在计算机网络安全通信机制实施过程中不断进行优化和改进。优化和改进主要包括以下几个方面：第一对计算机网络安全通信机制实施过程中所使用的技术、设备、工具等进行优化，对其进行升级。第二对计算机网络安全通信机制实施过程中的制度、流程等进行优化。第三对计算机网络安全通信机制实施过程中的管理、监督等进行优化[10]。

4 总结

计算机网络安全通信是保障信息安全的关键环节，它涉及到加密技术、认证技术等多个方面。在信息时代背景下网络安全通信面临着前所未有的挑战，基于本文的探讨，我们认识到计算机网络安全通信的重要性，了解了其技术基础和应用场景。在实施安全通信机制的过程中企业需要制定安全策略与规范，建立安全管理体系，以应对不断变化的网络安全威胁。未来随着技术的不断发展，网络安全通信将更加完善，进一步为我国信息安全和经济社会发展提供有力保障。

[参考文献]

[1]任伟嘉.关于计算机网络通信协议安全性与系统验证的分析[J].电子测试,2022,36(22):134-136.

[2]豆增学.基于网络安全维护的计算机网络安全技术应用研究[J].信息与电脑,2023,35(12):201-203.

[3]吕海坤.基于数据加密技术的计算机网络通信安全研究[J].户外装备,2023(1):237.

[4]梁建强.计算机网络通信安全中关于数据加密技术的运用探讨[J].信息化建设,2016(8):68-69.

[5]钱建波,于正永,蒋愚劼,等.一种基于无线通信系统的计算机网络安全管理方法:CN202310249768.1[P].CN116248403A[2024-10-30].

[6]杨冬.基于数据加密技术的计算机网络通信安全防御研究[J].电子通信与计算机科学,2023,5(3).

[7]回文静,张学军.新形势下计算机通信网络安全防护策略[J].工程技术(文摘版),2022(15).

[8]孙中波.计算机网络通信安全问题与防范策略探讨[J].数字化用户,2017,23(51):111.

[9]虞凤娟.基于数据加密技术的计算机网络通信安全设计[J].信息与电脑,2023,35(18):181-183.

[10]陈中凯.数据加密技术在计算机网络通信安全中的应用探讨[J].电脑爱好者(校园版),2023(11):1-3.

作者简介：

任霄(1988--),女,汉族,河南省安阳市人,本科,中级,计算机网络技术专业。