信息与计算机通信网络安全的技术探究

崔丽红
朝阳开放大学　辽宁　朝阳　122000

摘　要：信息与计算机通信网络安全技术是保护信息安全和网络稳定的关键，包括加密技术、认证技术、访问控制技术和安全审计与监控技术等。这些技术可以单独或组合使用，提供更全面和有效的安全保护。随着网络攻击技术的不断发展，安全技术也需要不断更新和升级，以应对新的威胁和挑战。因此，持续研究和开发新的安全技术是保护信息与计算机通信网络安全的重要手段。

关键词：信息；计算机通信；网络安全技术

引言：随着信息技术的飞速发展，信息与计算机通信网络已经成为人们生活和工作中不可或缺的一部分。然而，网络攻击技术的不断发展，也给信息安全和网络稳定带来了严重的威胁。因此，探究信息与计算机通信网络安全技术，保护信息安全和网络稳定，具有重要的理论意义和实践价值。

1 信息与计算机通信网络的重要性

信息与计算机通信网络在现代社会中扮演着极其重要的角色。它们不仅是人们获取与传递信息的关键工具，也是支持各种业务和服务的基础设施。然而，随着网络的普及和发展，网络安全问题也日益突出。保障信息与计算机通信网络的安全性成为一项至关重要的任务。信息与计算机通信网络扮演的角色十分关键。首先，它们成为人们获取信息的主要途径。无论是新闻、社交媒体、电子邮件还是搜索引擎，人们都依赖于互联网来获取他们所需的各种信息。这种便利的获取方式对于学习、工作和休闲都具有重要影响。其次，信息与计算机通信网络也是人们之间进行沟通交流的重要媒介。随着互联网的发展，电子邮件、即时通讯、社交媒体等工具成为人们与亲朋好友、同事与合作伙伴进行沟通的主要方式。无论时空距离如何，人们都可以通过网络与世界各地的人进行交流。信息与计算机通信网络也是商务活动的关键组成部分。电子商务的快速发展使得网上购物、在线支付和数字化营销成为现实。无论是大型跨国公司还是小型创业企业，他们都依赖着网络来进行业务活动。网络不仅提供了全球市场的机会，且使得商务活动更高效、更便利[1]。了保护信息与计算机通信网络的安全，各种安全技术得以应用。加密技术是保护信息传输的基本手段，它可以保证数据在传输过程中的机密性和完整性。通过使用对称加密算法和非对称加密算法，数据可以在发送和接收者之间加密和解密。数字签名和认证机制也能够确保数据的真实性和发送者身份的可靠性。此外，网络入侵检测与防御技术也是保护信息与计算机通信网络安全的重要手段。入侵检测系统可以监测和识别网络中的异常活动和攻击行为，从而及时采取相应的防御措施。防火墙、入侵检测系统和入侵防御系统的应用，可以有效地提高网络的安全性。另一种保护信息与计算机通信网络安全的技术是虚拟专用网络（VPN）。VPN通过在公共网络上创建私密通道的方式，为用户提供一个加密和安全的网络连接，以保护其信息的传输。它可以防止黑客和窃听者截获用户的数据，使得远程访问和通信更加安全可靠。只有确保了网络的安全，人们才能更加放心地使用网络进行各种活动，并推动数字化社会的发展。

2 信息与计算机通信网络安全体系结构

2.1 网络体系结构

信息与计算机通信网络安全体系结构是保护计算机通信网络免受攻击和数据泄露等威胁的重要手段。分层网络体系结构是一种将网络系统分为多个层次的网络体系结构。这些层次包括核心层、汇聚层和接入层，每个层次都有不同的功能和作用。核心层是网络体系结构的最上层，负责高速数据传输和网络控制。核心层的功能包括路由选择、数据传输、网络连接和流量控制等。汇聚层是网络体系结构的中间层，负责将接入层的数据汇总并传输到核心层。汇聚层的功能包括数据汇总、流量控制、路由选择和数据传输等。接入层是网络体系结构的最下层，负责将用户设备接入网络。接入层的功能包括用户认证、数据传输、网络安全和流量控制等。在分层网络体系结构中，每个层次都有不同的安全需求和保护措施。核心层需要防止未经授权的访问和数据泄露，因此需要进行严格的访问控制和加密传输。汇聚层需要防止流量溢出和拒绝服务攻击，因此需要进行流量控制和安全审计。接入层需要保护

用户隐私和防止恶意攻击，因此需要进行用户认证和网络安全管理等。通过分层网络体系结构的设计和应用，可以有效地提高网络的安全性和可靠性，防止未经授权的访问和数据泄露等威胁。

2.2 安全协议体系结构

信息与计算机通信网络安全体系结构是一个复杂的系统，它包括了多个层次和组件。其中，安全协议体系结构是一个重要的组成部分，它定义了在网络通信中用于保护数据完整性、机密性和可用性的协议。安全协议体系结构通常由以下几个层次组成：物理层、数据链路层、网络层、传输层和应用层。每个层次都有其特定的功能和责任，例如物理层负责传输比特流，而应用层则负责处理应用程序之间的通信。在安全协议体系结构中，常用的安全协议包括SSL/TLS、IPsec、SSH等。这些协议都采用了不同的加密算法和技术来保护数据的安全性。例如，SSL/TLS协议采用了非对称加密算法来保证数据的机密性，而IPsec协议则采用了隧道模式来保护数据在公共网络上的传输安全。这些组件可以帮助用户验证对方的身份，并确保只有授权的用户才能访问受保护的资源。信息与计算机通信网络安全体系结构是一个复杂而重要的系统，它需要采用多种技术和方法来保护数据的安全性。安全协议体系结构作为其中的一个重要组成部分，为用户提供了一种可靠的方式来保护网络通信的安全。

2.3 安全管理体系结构

信息与计算机通信网络安全体系结构以及安全管理体系结构是保障网络安全的重要手段。在信息化社会，计算机网络已经成为人们生活和工作的重要组成部分，而网络安全的威胁也日益增加。为了保护网络信息安全，我们需要建立一套完整的网络安全体系结构和安全管理体系结构。信息与计算机通信网络安全体系结构主要包括物理层安全、网络层安全、系统层安全、应用层安全和安全管理。物理层安全主要是指通信线路的安全、物理设备的安全和机房的安全等；网络层安全主要是指网络设备的安全，如防火墙、入侵检测系统等；系统层安全主要是指操作系统的安全，包括文件保护、访问控制等；应用层安全主要是指应用软件的安全，如安全协议、加密算法等；而安全管理则是整个网络安全体系结构的核心，它包括安全策略、安全管理机构、安全人员、安全培训等[2]。安全管理体系结构主要包括安全策略、组织结构、人员管理、安全技术和安全管理。安全策略是企业制定的一系列安全规定和措施，用于指导企业的安全管理工作；组织结构是指企业内部的安全管理部门，包括安全管理机构、安全人员等；人员管理是指对安全人员进行培训、考核和激励等管理活动；安全技术是指用于保障网络安全的各种技术手段，如加密技术、防火墙技术、入侵检测技术等；而安全管理则是整个安全管理体系结构的核心，它包括安全策略的制定、实施和监督等。只有建立完善的网络安全体系结构和安全管理体系结构，才能有效地保障计算机网络的安全。

3 信息与计算机通信网络安全技术分类

3.1 加密技术

信息与计算机通信网络安全技术中的加密技术是保障信息安全的核心手段之一。加密技术通过对数据进行加密处理，使得未经授权的人员无法获取敏感信息的真实内容，从而保障数据的机密性和完整性。加密技术可以分为对称加密和非对称加密两类。对称加密技术是指加密和解密使用相同的密钥，这种方法具有较高的安全性，但密钥管理较为困难。非对称加密技术是指加密和解密使用不同的密钥，其中公钥用于加密，私钥用于解密，这种方法具有较高的安全性，且密钥管理较为方便。在实际应用中，加密技术可以应用于数据传输、身份认证、数字签名等领域。例如，SSL/TLS协议中的对称加密算法可以保障Web浏览器和服务器之间通信的数据机密性和完整性；数字签名技术可以用于验证文件的真实性和完整性；公钥基础设施（PKI）可以用于管理数字证书和密钥，保障网络的安全性和可靠性。加密技术在信息与计算机通信网络安全技术中具有重要的作用，可以有效地保护数据的机密性和完整性，防止未经授权的访问和数据泄露等威胁。

3.2 认证技术

认证技术通过对用户或设备进行身份验证，确保其合法性和可信度，从而防止未经授权的访问和攻击。常见的认证技术包括用户名/密码认证、数字证书认证和生物特征认证等。用户名/密码认证是最常见的一种认证方式，但容易被猜测或破解；数字证书认证通过验证用户的公钥和私钥来确认身份，具有较高的安全性；生物特征认证通过采集用户的生物特征信息，如指纹、虹膜等，进行身份验证，具有更高的安全性。在实际应用中，认证技术可以应用于登录、授权、会话管理等领域。例如，在SSH协议中，用户登录时需要提供公钥和私钥来进行身份验证；在Web应用程序中，用户登录后可以获得一个会话令牌，用于后续的请求和访问控制。认证技术在信息与计算机通信网络安全技术中具有重要的作用，可以有效地确认用户或设备的身份，防止未经授权的访问和攻击。同时，认证技术还可以结合其他安全技

术，如加密技术、访问控制等，提供更全面和可靠的安全保护。

3.3 访问控制技术

信息与计算机通信网络安全技术是保障网络安全的重要手段，访问控制技术则是其中的一种关键措施。它能够限制对系统资源的访问，确保只有经过授权的用户和设备才能访问特定的资源，从而有效避免信息泄露和非法操作等安全风险。访问控制技术主要包括身份认证、访问授权和访问审计三个方面。身份认证是指确认用户身份的过程，通常采用密码、指纹、智能卡等方式进行身份验证，以确保只有合法用户才能访问系统资源。访问授权是指根据用户的角色和权限设置，限制用户对系统资源的访问范围。访问审计则是对用户的访问行为进行监控和记录，以便于事后追溯和分析。在实际应用中，访问控制技术通常采用多层次的防护策略，包括网络层、应用层和操作系统层等。网络层的访问控制主要包括防火墙、入侵检测和流量控制等，用于防止非法用户进入网络和控制网络中的数据流量。应用层的访问控制则包括身份认证、授权和审计等功能，用于确保应用程序的安全性和可靠性。操作系统层的访问控制则包括用户认证、文件权限和访问控制列表等，用于保护操作系统和文件系统的安全。访问控制技术是信息与计算机通信网络安全技术的重要组成部分，它能够有效保障系统资源的安全性和可靠性，避免信息泄露和非法操作等安全风险。随着网络技术的不断发展和应用，访问控制技术也将不断演进和完善，为网络安全提供更加有力的支持。

3.4 安全审计与监控技术

信息与计算机通信网络安全技术中的安全审计与监控技术是保障信息安全的重要手段之一。安全审计与监控技术通过对系统中的操作和行为进行记录和监控，及时发现和处理安全事件，并提供相应的告警和报告。常见的安全审计与监控技术包括日志审计、入侵检测/防御、异常行为检测、完整性监控等[3]。日志审计通过对系统中的日志进行分析和处理，发现异常操作和行为；入侵检测/防御可以实时检测网络流量，发现并阻止入侵行为；异常行为检测可以监测系统的运行状态和行为，发现异常操作和行为；完整性监控可以监测系统的文件、数据和配置等，确保其完整性和一致性。在实际应用中，安全审计与监控技术可以应用于操作系统、数据库、网络设备、应用程序等领域。例如，在操作系统中，日志审计可以监控系统登录、注销、文件访问等操作；在数据库中，日志审计可以监控数据库的访问、修改和删除等操作；在网络设备中，入侵检测/防御可以实时监测网络流量，发现并阻止网络攻击等。安全审计与监控技术在信息与计算机通信网络安全技术中具有重要的作用，可以有效地发现和处理安全事件，提供及时告警和报告，帮助组织及时采取相应的措施，保障系统的安全性和可靠性。

结语

信息与计算机通信网络安全技术探究是一个不断发展的领域，需要我们时刻保持警惕。随着网络技术的不断进步和网络攻击的不断增加，我们需要不断学习和研究新的安全技术来保护我们的信息和通信。只有综合运用各种手段，才能有效地应对网络安全威胁，确保信息与计算机通信网络的安全运行。

参考文献

[1]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.

[2]李霞.计算机安全技术及防护措施在图书馆管理中的应用[J].计算机与网络,2021,47(02):50-51.

[3]丁勇.安全技术在计算机软件开发中的应用研究——评《计算机安全技术》[J].现代雷达,2021,43(01):95.