信息与计算机通信网络安全技术探究

梁荣欣
上海市政工程设计研究总院（集团）有限公司　上海　200092

摘　要：本文先概述了网络安全的基本概念，接着详细分析了其面临的威胁，包括网络攻击手段和类型、内部威胁及人为失误。重点阐述了多种网络安全技术，如加密技术、防火墙技术、入侵检测与防御系统、虚拟专用网络、访问控制技术和安全审计技术，并论述了网络安全管理方面的安全策略制定与实施以及人员安全意识培训。通过对这些方面的研究，为提升信息与计算机通信网络的安全性提供了全面的理论支持和实践指导。

关键词：建筑施工；安全管理；防范措施

引言：在当今数字化的时代，信息与计算机通信网络已成为社会运转的重要基石。然而，随着网络的普及和应用的深化，网络安全问题日益凸显。从个人隐私泄露到企业关键数据被盗，从网络欺诈到大规模的网络攻击，网络安全威胁无所不在，给个人、企业乃至国家带来了巨大的损失和潜在风险。因此，深入探究信息与计算机通信网络安全技术，加强网络安全管理，具有极其重要的现实意义和紧迫性。

1 信息与计算机通信网络安全概述

信息与计算机通信网络安全至关重要，它主要指保护计算机系统上的数据在未经用户许可的情况下不被他人或计算机系统窃取。同时，要确保计算机系统正常运行，防止被监听。

计算机通信网络是将若干具有独立功能的计算机通过通信设备及传输媒体相互连接，在通信软件支持下实现信息传输与交换的系统。网络安全的目的是使网络系统不受任何威胁与侵害，能正常实现资源共享功能。这需要保证网络的硬件、软件正常运行，以及数据信息交换的安全。网络安全涵盖多个方面，具有多个重要特性。保密性确保信息不被非授权访问，即使非授权用户获取信息也无法理解其内容；完整性维护信息的一致性，保证信息在生成、传输、存储和使用过程中不被篡改；可用性保障信息资源随时可提供服务，授权用户能够随时访问所需信息；不可抵赖性使信息交互过程中的参与者不能否认曾经完成的操作或承诺；真实性要求信息中涉及的事务客观存在，信息的各个要素真实齐全，来源真实可靠；可控性意味着对信息的传播及内容具备控制能力，可控制用户的信息流向，并进行审查；可审查性则是在出现安全问题时提供依据与手段。

网络安全的发展历史悠久。早期计算机网络初步建立时，安全问题主要集中在实体防护和软件正常运行上[1]。随着密码学的兴起，特别是公钥密码学的发明，网络通信安全性得到极大提高。然而，罗伯特·莫里斯设计的蠕虫程序利用unix系统安全漏洞造成大量计算机瘫痪，引发了对网络安全的广泛关注。进入21世纪，网络用户激增，网络安全问题变得复杂严峻。例如，icloud泄露事件暴露了云存储服务的安全漏洞，mirai僵尸网络攻击揭示了物联网设备的安全隐患。

2 信息与计算机通信网络安全面临的威胁

2.1 网络攻击手段和类型

（1）截获：攻击者通过窃听等方式获取网络中传输的通信内容，但不影响网络通信。这种攻击类似于流量分析，攻击者只观察和分析协议数据单元，以窃取其中的数据信息。（2）中断：旨在中断他人的网络通信，使目标无法进行正常的数据传输。（3）篡改：对网络上传输的报文或分组信息进行修改，也被称为更改报文流。例如，篡改网站数据或交易信息，可能导致严重的后果。（4）伪造：制造虚假的报文信息并在网络中传递，以欺骗接收方或干扰正常的网络操作。（5）恶意软件：包括病毒、蠕虫、木马、逻辑炸弹等。病毒可以传染其他程序，通过自我复制破坏目标程序；蠕虫通过网络传播并消耗系统资源，可能导致设备宕机；木马主要用于与外部沟通，如盗号木马、远程控制木马等；逻辑炸弹则在特定条件下启动执行特定程序。（6）分布式拒绝服务攻击（DDoS）：攻击者利用大量被控制的设备（僵尸网络）向目标服务器发送海量请求，使其无法正常处理合法用户的请求，导致服务瘫痪。这种攻击也被称为网络带宽攻击或连通性攻击。（7）SQL注入：针对SQL数据库的攻击方式。攻击者利用网页上未正确设置权限的HTML表单执行恶意的SQL查询，从而创建、读取、修改或删除数据库中的数据。（8）中间人攻击（MITM）：攻击者拦截双方之间的通信，试图监视、窃取个人信息

或凭据，或者改变通信内容。在端到端加密不普及的情况下，这种攻击较为常见。（9）DNS隧道：攻击者将恶意软件插入或“隧道化”到DNS查询中，创建大多数防火墙难以检测到的持久通信通道，从而实现对目标的持续访问。

2.2 内部威胁和人为失误

在信息与计算机通信网络中，系统漏洞和软件缺陷是网络安全的重大隐患。

（1）操作系统漏洞是其中一个关键问题。不同的操作系统，如Windows、Linux等，都可能存在各种漏洞。这些漏洞可能源于设计上的疏忽、代码编写的错误或者对新出现的威胁未能及时预见。例如，某些操作系统在处理内存分配时可能出现错误，使得攻击者能够通过特定的操作获取系统的控制权。（2）应用软件漏洞同样不可小觑。无论是办公软件、浏览器还是各类专业应用程序，都可能存在安全漏洞。以常见的浏览器为例，其插件机制或者脚本解释器中的漏洞可能被黑客利用，执行恶意代码，从而窃取用户的隐私信息或控制用户的计算机。（3）未及时更新补丁是导致系统漏洞和软件缺陷被利用的重要原因之一。补丁通常是软件开发者针对已发现的漏洞和缺陷推出的修复程序。然而，由于用户缺乏对更新的重视，或者因为更新过程可能带来的不便，许多用户未能及时安装补丁。这就给了攻击者可乘之机，他们可以利用这些已知但未修复的漏洞发起攻击。

3 信息与计算机通信网络安全技术

3.1 加密技术

加密技术是保护信息机密性和完整性的基石。它通过对明文进行特定的数学变换，将其转换为难以理解的密文，只有拥有正确密钥的合法接收者才能将密文还原为明文。见下图1-1信息加密技术。

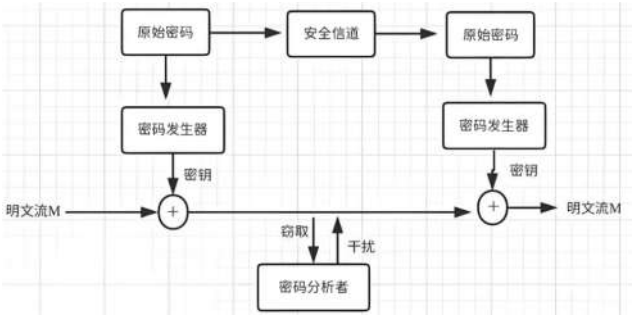

图1 信息加密技术

（1）对称加密算法：如AES（高级加密标准），使用相同的密钥进行加密和解密。这种算法的优点是加密和解密速度快，效率高，适用于大量数据的快速处理。

（2）非对称加密算法，以RSA为代表，使用一对密钥：公钥和私钥。公钥可以公开，用于加密信息；私钥则由所有者秘密保存，用于解密。（速度慢，但保证了秘钥安全）见下图1-2所示：

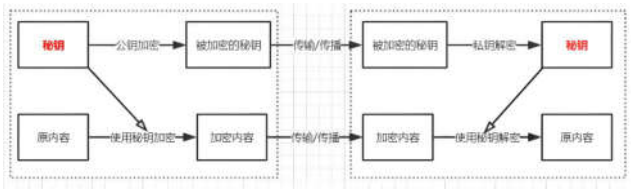

图2 对称加密算法和非对称加密算法

3.2 防火墙技术

防火墙是位于内部网络和外部网络之间的一道屏障，用于控制进出网络的流量。

防火墙主要有包过滤防火墙、状态检测防火墙和应用层网关防火墙等类型[2]。包过滤防火墙基于数据包的源地址、目的地址、端口号等信息进行过滤，决定是否允许数据包通过。它的配置相对简单，但无法识别数据包的上下文信息，可能会误判一些合法流量。状态检测防火墙不仅检查数据包的头部信息，还跟踪连接的状态。它能够识别更复杂的网络通信模式，提供更精确的访问控制。应用层网关防火墙可以深入到应用层，对特定的应用协议进行分析和控制。例如，它可以阻止不符合规定的HTTP请求或FTP操作。

3.3 入侵检测与防御系统

入侵检测系统（IDS）用于监测网络或系统中是否存在异常活动或潜在的入侵行为。IDS的原理主要包括基于特征的检测和基于异常的检测。基于特征的检测依赖于已知的攻击模式和特征库，能够快速识别常见的攻击；基于异常的检测则通过建立正常的行为模型，检测偏离正常模式的活动。IDS可以分为基于主机的IDS和基于网络的IDS。基于主机的IDS主要监控单个主机的系统活动和日志，能够检测针对该主机的攻击；基于网络的IDS则分析网络流量，能够发现整个网络中的入侵迹象。入侵防御系统（IPS）是在IDS的基础上发展而来，不仅能够检测入侵行为，还能实时采取措施阻止攻击。IPS的特点包括实时响应、主动防御和深度检测。它能够在攻击造成实质性损害之前进行拦截，有效降低安全风险。

3.4 虚拟专用网络（VPN）

VPN技术通过在公共网络上建立加密的通信隧道，实现安全的远程访问和数据传输。VPN的技术原理基于隧道协议，如IPsec和SSL/TLS。它将原始数据包封装在新的数据包中，并进行加密，通过公共网络传输到目的地后再进行解封装和解密。VPN的应用场景广泛。企业可以利用VPN让员工远程安全地访问企业内部网络资

源，实现移动办公；不同分支机构之间可以通过VPN构建安全的私有网络，进行数据共享和通信；个人用户在使用公共无线网络时，也可以通过VPN保护隐私和数据安全。

3.5 访问控制技术

访问控制技术用于确定谁可以访问哪些资源以及可以进行何种操作。身份认证是访问控制的第一步，常见的方法包括用户名/密码、智能卡、生物识别等。多因素认证结合多种认证方式，大大提高了身份认证的安全性。授权和访问权限管理根据用户的身份和角色，分配相应的访问权限。例如，管理员可能拥有对系统的完全控制权，而普通用户可能只能读取和修改部分文件。

3.6 安全审计技术

安全审计的目的包括监测系统活动、发现违规行为、评估安全策略的有效性等。其流程通常包括数据采集，从系统日志、网络流量、用户操作等多个来源收集信息；数据存储，将采集到的数据安全地保存；数据分析，运用统计分析、模式识别等技术挖掘有价值的信息；报告生成，向管理员提供审计结果和建议。通过对上述网络安全技术的综合应用和有效管理，可以构建一个相对安全的信息与计算机通信网络环境，保护敏感信息，防范各种网络威胁。

4 信息与计算机通信网络安全管理

4.1 安全策略的制定和实施

安全策略是信息与计算机通信网络安全管理的基础和指导方针。制定安全策略时，需要全面考虑组织的业务需求、风险承受能力以及法律法规的要求。首先，要明确网络的访问控制策略，规定谁可以访问哪些资源，以及在什么条件下可以访问。例如，对于敏感数据，只有特定的授权人员在特定的时间段内可以访问。其次，制定数据保护策略，包括数据的加密、备份和恢复机制，以确保数据的机密性、完整性和可用性。此外，还应制定设备管理策略，规范计算机、服务器、移动设备等的使用和维护。实施安全策略需要强有力的技术手段和管理措施。技术方面，通过防火墙、入侵检测系统、加密技术等保障策略的执行。管理上，建立监督机制，定期审查策略的执行情况，对违反策略的行为进行严肃处理。随着业务的发展和技术的更新，安全策略也需要不断地评估和调整，以适应新的安全威胁和环境变化[3]。

4.2 人员安全意识培训

人员是信息与计算机通信网络安全中最关键也是最薄弱的环节。即使拥有最先进的技术防护措施，如果人员缺乏安全意识，也容易导致安全漏洞的出现。因此，开展人员安全意识培训至关重要。培训内容应涵盖网络安全的基本知识，如常见的网络攻击手段、个人信息保护方法、密码设置的原则等[4]。同时要让员工了解组织的安全策略和相关规章制度，明白自己在网络安全中的责任和义务。通过实际案例分析，让员工直观地认识到网络安全事故的危害和后果，提高他们的警惕性。此外，还应培训员工如何识别和应对钓鱼邮件、社交工程攻击等常见的安全威胁，培养他们良好的网络使用习惯。定期进行安全意识的考核和强化培训，确保员工始终保持较高的安全意识水平，从而形成一道坚实的人为防线，降低因人为因素导致的网络安全风险。

结束语：总之，信息与计算机通信网络安全是一个复杂且不断变化的领域。我们虽然在网络安全技术和管理方面取得了一定的成果，但面对层出不穷的新威胁和挑战，仍需持续投入研究和创新。未来，应进一步加强技术研发，提高安全策略的适应性和有效性，同时不断提升人员的安全意识，形成全方位、多层次的网络安全防护体系，以保障信息与计算机通信网络的稳定、可靠和安全，为社会的发展和进步提供坚实的支撑。

参考文献

[1]赵广磊,牛俊朋.基于计算机网络技术的计算机网络信息安全及其防护策略分析[J].科学与信息化,2022(3):49-50.

[2]李长挺.信息化背景下计算机网络信息安全防护策略[J].电子世界,2022(1):146-147.

[3]邹佳彬.基于计算机网络技术的计算机网络信息安全及其防护策略[J].数字技术与应用,2021,39(11):225-227.