文章类型：论文|刊号（ISSN）：2737-4505(P) / 2737-4513(O)

网络通信中数据信息安全保障技术探究

周挺挺
中国电信股份有限公司绍兴分公司
DOI:10.12238/etd.v5i3.7802

[摘　要] 在互联网技术的普及下,社会生活和生产对网络通信的依赖度越来越高,但由于网络的虚拟性、开放性,网络通信的弊端也越来越明显,如数据流失、数据篡改、数据窃取等,使得广大民众的核心利益受到巨大威胁。基于此,本文将从网络通信中数据信息安全的重要性出发,简单分析了网络通信中的信息安全威胁和常见的一些数据信息安全保障技术,包括数据加密技术、数字签名技术、防火墙技术、入侵检测技术、网络安全管理技术、访问控制和安全审计等,希望能为相关人士提供一些有益的参考。
[关键词] 网络通信；数据信息；安全保障
中图分类号：TN711　文献标识码：A

Exploration of Data Information Security Technology in Network Communication

Tingting Zhou
China Telecom Shaoxing Branch

[Abstract] With the popularization of Internet technology, social life and production have become more and more dependent on network communication. However, due to the virtuality and openness of the network, the drawbacks of network communication have become more and more obvious, such as data loss, data tampering, data theft, etc., making the core interests of the majority of the people a huge threat. Based on this, this article will start from the importance of data information security in network communication, and briefly analyze the information security threats and common data information security protection technologies in network communication, including data encryption technology, digital signature technology, firewall technology, intrusion detection technology, network security management technology, access control and security audit, etc., hoping to provide some useful references for relevant personnel.
[Key words] network communication; Data information; Security measures

引言

当前,网络通信已经成为民众生活的重要组成部分,对推动现代社会的发展起到了关键作用。但另一方面,由于网络的虚拟性和开放性,使得一些不法分子有了可乘之机,如利用病毒攻击他人的网络系统、窃取机密信息等,不仅影响了网络通信的可持续发展,也给他人造成了巨大的损失,甚至威胁国家安全。因此,在未来的发展中,相关技术人员需要深刻认识到保障数据信息安全的重要性,并基于对常见安全威胁的分析,不断优化和创新数据信息安全保障技术,进而切实维护国家和民众的核心利益。

1 网络通信中数据信息安全的重要性

随着网络通信在各领域的广泛应用,保障数据信息安全变得十分重要,其重要性主要体现在以下几方面：第一,保障国家安全。在国家的发展中,一些重要领域可能面临黑客的攻击,如外部势力通过网络攻击手段窃取我国军事力量的部署情况、重要基础设施的位置等,一旦国家机密外泄,将会严重威胁国家安全。因此,就要提高数据信息安全保障意识,并通过科学的管理措施和技术手段进行防范。第二,保障个人隐私安全。当前,人们使用网络通信的频次越来越高,而其中就涉及个人的隐私信息,如姓名、家庭住址、银行账户等,假如这些个人隐私被不法分子窃取,将造成个人财产损失,甚至受到人身安全威胁。第三,保障企业商业机密安全。在企业办公实现无纸化、信息化的情况下,企业的很多机密信息都被保存在网络管理系统之中,假如在网络通信中被不法分子窃取或受到病毒攻击,很可能造成机密信息的丢失和外泄,给企业的正常运转造成影响,严重的话将造成巨大经济损失。此外,如果客户信息被外泄,企业还将面临法律制裁和巨额赔偿。所以,保障数据信息安全对企业的长远发展具有重要意义。第四,保障公共安全。水利、电力等重要基础设施的运行目前都比较依赖于网络,但在提高运行效率和减少工作量的情况下,也面临一定的安全威胁,如黑客通过网络攻击电力基础设施系统,造成大面积的停电事故,这不仅影

响民众的正常生活,还会造成社会恐慌,后果十分严重。所以,在日常管理中需要重视数据信息安全保障技术的应用,以确保公共安全[1]。第五,保障网络社会稳定。网络通信目前已成为人们生活中不可或缺的一部分,假如受到安全威胁,必然影响人们的生活,所以加强数据信息安全保障有助于确保网络社会的稳定。

2 网络通信中的信息安全威胁分析

2.1网络虚拟性引发的安全问题

在互联网技术的发展中,人们经常听到的一句话是“网络是一把双刃剑”,这是因为它虽然给人们的生活带来了许多便利,如检索信息方便、数据存储量大等,但同时也有一定的弊端,如许多网络资源都是公开的,其质量参差不齐,甚至有一些网络资源的可靠性与真实性存在很大问题,如有的不良居心之人将病毒伪装成正常网络文件,假如人们没有仔细辨别就打开它,个人隐私很可能遭到外泄。究其原因,主要是由于网络具有虚拟性与开放性的特征,使得不法分子或不良居心之人有了可乘之机,通过网络复制、窃取或篡改他人的机密信息,以获取不当利益。例如,在2022年南昌市的一家网络公司就被不法分子长期监听窃取重要信息,损失高达700万人民币。

2.2操作系统的网络信息安全问题

计算机的操作系统涵盖了多项内容,如外联设备管理、中央处理器管理、内存管理等,假如操作系统不够稳定,将会对网络通信的质量和安全产生直接性的影响。目前,网络通信中主要使用TCP/IP协议,但因为其存在一定的漏洞,容易被不法分子窃取隐私信息或篡改重要信息。以FTP作为例子来讲,在安装程序的时候会有可执行文件,由于其都是人为编写,假如编写中存在漏洞,便可能被不法分子利用,使得文件传输期间被窃取、监听,继而引起网络安全问题。此外,后门程序通常是为了便于对操作系统的后期调试与修改而设置,一般不被安全监管系统管控,所以它如果被不法分子利用,将会导致网络通信中的数据信息安全受到威胁。最后则是因为操作人员对系统的安全方法机制不了解、操作水平不高,从而导致信息外泄,如随意点开网络上的不明链接[2]。

2.3网络病毒引发的信息安全问题

随着互联网技术的快速发展,网络病毒也得到了一定的发展,呈现出隐蔽性、多样性和智能化等特征。相比传统网络病毒而言,新型的网络病毒不仅具有更强的攻击力,其攻击范围也比较广,一旦相关主体没有数据信息安全保障意识和采取有效防范措施,极有可能遭受网络病毒的攻击,从而造成经济损失。例如,邮件病毒是依托电子邮件进行传播,假如人们在使用电子邮件的过程中没有注意鉴别其真伪,或者计算机上没有应用数据信息安全保障技术,将会被网络病毒攻击,由此造成一定的损失。还有人们熟知的木马病毒,它作为一种后门程序,可以实现对目标计算机的远程控制,从而窃取机密信息。

3 网络通信中数据信息安全保障技术

3.1数据加密技术

数据加密技术指的是将原始数据进行加密,只有通过相应的密钥才能读取,这样就能确保网络通信中原始数据不会被其他人窃取或篡改。从目前数据加密技术的应用情况来看,主要有非对称加密和对称加密两种方式,前者使用需要用到一对密钥,包括用于解密数据的私钥和可以公开公发的公钥,其特点是加密强度高,但加密速度相对较慢。常见的非对称加密算法有ECC、DSA与RSA等;后者则是使用一个密钥,用于对数据的加密和解密,所以它的特点是加密速度快,针对需要加密大量数据的应用场景比较合适,如数据库加密、文件加密等。常见的对称加密算法有3DES、DES和AES等。两种数据加密方式的优缺点都比较明显,如对称加密在密钥的管理与分发上存在隐患,容易出现密钥泄露的问题,一旦密钥被不良居心之人获取,将会引发数据信息安全问题。而非对称加密虽然在密钥管理与分发上更加安全,但它的计算相对复杂,针对大量原始数据的加密需要耗费更多时间和精力。为此,在实际应用中可以采取混合加密的策略,即将两种数据加密方式进行有机结合,以提高其适用性。

3.2数字签名技术

在保证数据信息的真实性、所有权和完整性方面,数字签名技术的应用不可忽视。简单来讲,数字签名好比现实生活中手写签名,以用于表明数据信息的来源和信息完整性。但与手写签名相比,数字签名更加安全,功能更强。该技术的应用原理是先用哈希函数计算一个消息摘要,一旦在网络通信中原始数据被修改都会引起哈希值的变化。之后,原始数据的发送方通过密钥对其进行加密,生成数字签名。接收方在收到数据信息后,需要通过对方提供的公钥对数字签名进行解密,然后将所得哈希值对自己计算得到的哈希值进行对比,以判断数据信息是否被篡改。目前,数字签名技术在许多场景都有应用,如电子合同的签署中使用数字签名技术,可以确保合同具有法律效力;在电子邮件的发送中使用数字签名技术,保证了电子邮件的可信度与真实性;在金融交易中使用数字签名技术,有助于防止抵赖和欺诈[3]。

3.3防火墙技术

作为当前网络通信中常见的一种数据信息安全保障技术,防火墙技术主要是基于相关的软件与硬件设备,在公共网与专用网、外部网与内部网之间形成一道保护屏障,如此在网络通信中就可以阻挡一些外部攻击。与此同时,内部网络的数据信息在流出时也需要经过防火墙,此时防火墙可以通过对数据信息的监测,避免内部信息的外泄。随着科学技术的不断发展,传统的防火墙技术得到了进一步完善,如将其与入侵防御系统、深度包检测等进行结合,提高了防火墙的灵活性与安全性,从而更好保障数据信息的安全。关于防火墙技术的应用场景,常见的有企业网络边界保护,其目的是帮助企业过滤病毒传播、黑客攻击等,使企业的数据安全得到保障。再如,学校为了保护职工和学生的隐私,使用防火墙技术用于执行访问控制。

3.4入侵检测技术

入侵检测技术,顾名思义就是用于检测恶意入侵行为、黑客攻击等的技术手段,以确保数据信息的安全性。常见的入侵检测

技术有主机入侵检测与网络入侵检测，前者是通过对主机系统的行为进行监控，及时识别网络中的恶意行为，如进程控制、用户操作、文件更改等。在此基础上，主机入侵检测可以通过采取有效的措施抵御攻击行为。后者则是基于对网络流量的检测，识别相关的攻击行为，如恶意代码的传播、漏洞利用和端口扫描等。入侵检测技术在现实中的应用也非常多，如有的企业会通过部署入侵网络系统，监控和及时解决潜在的攻击行为；在电力、水利事业的发展中，关键基础设施的保护中也会用到该技术，以防御对相关控制系统的恶意攻击[4]。

3.5网络安全管理技术

网络安全管理技术一般用于对网络中的安全漏洞与安全事件进行管控，其主要涵盖安全培训、安全策略与安全管理系统。安全培训指的是通过对相关管理人员、用户和IT人员进行网络安全意识的培训，使其可以正确识别常见的安全威胁，如社交媒体陷阱、钓鱼邮件等。同时，要对相关技术人员进行技能培训，包括如何应对网络攻击、如何配置安全设备、如何维护安全设备等。安全策略则是制定科学完善的安全标准与法规要求，约束各种网络活动必须严格按照其进行开展，一般涵盖访问控制、数据分类与保护和加密标准等。还有为了避免数据丢失或损坏引起的重大损失，需要制定相应的数据备份计划，特别是对关键数据要进行定期备份，以便在遇到数据丢失或损坏时可以拿出来进行数据恢复，保证业务运转顺利。安全管理系统则是基于安全管理平台、网络监控攻击等，监控用户活动、网络流量、网络设备，及时识别潜在威胁，此时系统将会自动触发响应措施，有效抵御网络中的安全威胁。

3.6访问控制

访问控制是指对应用程序与网络系统进行访问，用于管控访问权限的一种技术手段。在网络通信中，该技术的应用主要是对访问者的身份进行验证，如果访问者具有访问的权限便能进入网络系统与应用程序，反之将会被阻止访问，对避免信息外泄和黑客入侵具有重要作用。目前访问控制主要涉及三个方面的内容，即身份验证、授权和审计。首先，身份验证就是对访问者使用的用户名及密码进行验证，确定其是否具有访问权限；授权则是根据相应的访问规则，对用户授予相应的访问权限，如修改、读取等；审计则是对访问者的所有访问活动进行监控，一旦出现异常行为将会被及时制止。目前，访问控制在很多领域中都有应用，特别是敏感领域，如军事、政府、企业内网等，以确保敏感信息或重要数据信息的安全[5]。

3.7安全审计

安全审计是指用于对网络中安全事件进行发现与分析的技术，该技术的有效应用可以帮助网络安全管理人员及时发现网络或系统中的安全漏洞、异常事件，并将其详细记录下来，以用于对网络安全问题的解决，继而保证数据信息的安全。从实际应用来看，安全审计主要涉及三个步骤，第一步就是对网络通信中的安全事件进行记录，如权限更改、登录尝试、系统配置变动等；第二步是对日志记录进行审查和分析，以判断是否存在潜在的安全威胁；第三步是形成报告，为安全管理团队或上级管理者提供科学依据，以及时采取有效防控措施保障数据信息的安全。与其他数据信息安全保障技术类似，安全审计也有诸多的应用场景，如企业内部安全、政府机构等。

4 结束语

近年来，网络通信中的数据信息安全问题越来越常见，对国家、企业和个人都造成了巨大损失，如何保障网络通信中的数据信息安全问题理应引起社会各界的广泛关注。本文通过对网络通信中数据信息安全的重要性和面临的安全威胁进行分析，深入探讨了一些行之有效的数据信息安全保障技术，如数据加密技术、入侵检测技术、防火墙技术和数字签名技术等。不同主体可以根据自身的数据信息安全保障需求选择合适的技术予以应用，以确保网络通信中数据信息的安全。

[参考文献]

[1]陈克通.网络通信中的数据信息安全保障技术研究[J].网络安全技术与应用,2024,(02):56-57.

[2]祝鑫.网络通信中的数据信息安全保障技术分析[J].电子质量,2023,(12):65-68.

[3]王洪波.网络通信中的数据信息安全保障技术研究[J].中国新通信,2023,25(02):110-112.

[4]王玉.网络通信中的数据信息安全保障技术策略探讨[J].中国新技术新产品,2022,(22):131-133.

[5]刘贵强.网络通信中的数据信息安全保障技术分析[J].现代传输,2022,(05):49-52.