关于计算机网络中数据的保密与安全探讨

范绍恒
（华南农业大学珠江学院，广东 广州 510900）

摘 要：随着当前过经济水平的不断提升，人民生活质量与日俱增。电脑与互联网已经成为了普通家庭不可或缺的重要分子。它不仅是人们认识和了解世界的重要途径，同时也无时无刻不在对各行各业的发展起着重要的影响。与此同时，网络安全问题也开始受到人们的高度关注，网络发展依旧受其制约。目前针对用户信息泄露等信息安全事件层出不穷，因此确保计算机网络中数据的安全性已然成为当前社会亟待解决的一项重要问题。因此，有必要对此问题展开深入研究，从而进一步提升网络数据的保密与安全，让计算机网络得以发挥出更大的作用。本文就此展开讨论，希望能够为相关的工作人员提供一些参考和帮助。

关键词：计算机网络；数据保密；数据安全
【DOI】10.12231/j.issn.1000-8772.2020.26.192

1 引言

在如今网络化的时代，计算机网络技术广泛应用于人们的日常工作和生活中，成为人们不可或缺的必备工具，人们对于网络的依赖性愈发强烈。网络的作用非常大，不仅可将资料上传到云端进行储存，还可进行资金转账。当然，互联网的系统性和开放性的不断提升虽然为社会大众的工作、生活都带来了前所未有的便利，并促进了经济发展，但其风险也不容小视，病毒、黑客的入侵就是经常发生的现象，结果是造成用户大量数据资料丢失，经济方面的损失问题也已屡见不鲜。因此，人们在大量使用网络的同时也应该强化网络安全监督，做好计算机网络数据的保密与安全防范举措，以此让我国的网络环境得到更好地净化，让人们能够更加安心的使用这一工具。

2 计算机网络中数据的保密与安全相关概述

对于计算机网络中数据的保密与安全而言，其含义主要包括计算机网络系统的安全与数据保护、信息保密两个方面。前者强调网络系统硬件、软件及系统中的数据不因偶然或恶意因素被而泄露、破坏或更改。后者则是对系统中信息资源的存取、修改、扩散和其它使用权限予以有效控制，从而避免其受到攻击。

3 计算机网络中数据所面临的主要风险

3.1 病毒入侵带来的威胁

计算机病毒一直以来都是互联网中极具威胁性的危险因素。计算机病毒一般体现为一段恶意代码、一个恶意软件或者插件等，并通过计算机网络或者其他信息载体进行传播。计算机病毒一般都具有较强的隐蔽性，使用者一般都是在病毒已经对计算机及网络系统造成了一定破坏、数据资料发生了泄露之后，才意识到病毒的入侵及破坏。如果计算机病毒通过伪装而未能被杀毒软件所识别和杀灭，则使用者一般很难对其主动发现和清除。一旦一台计算机染毒，往往与其相关的计算机也极易染上病毒，继而遭受病毒的入侵和破坏。

3.2 黑客的攻击

黑客攻击也是迄今为止最具广泛性且危害程度最大的一类威胁。其主要有两种攻击方式：其一是网络攻击，即通过各种途径来损害网络数据及信息。其二是网络侦查，即不破坏网络的有效性能，但是却通过多种不正当手段获取其重要的信息。网络攻击的主要手段包含：拒绝服务攻击、欺骗攻击、通过协同工具进行攻击、对移动设备的攻击、电子邮件攻击等等。

4 计算机网络中数据保密与安全问题防范的主要技术分析

4.1 防火墙技术

防火墙技术是目前网络安全应用非常普遍的一种技术，应用原理主要是采用将网络区域隔离为多个区块，赋予各个区块的不同系统访问控制权限，从而管理各个权限等级区块之间的数据包交互。它对在各个区块之间通信的数据包依照一定的安全规则来进行过滤，由此判断区块之间的交互是否被响应，同时监听整个网络的联通情况。现在防火墙技术能够在相当大的程度上确保网络数据安全，但是依然存在显著的无法解决的缺陷：内网对内网的恶意攻击，部署在 DMZ 里面的应用服务器攻击，利用网络协议漏洞的恶意攻击，配置规则漏洞级及服务器系统漏洞等。

4.2 计算机加密技术

计算机加密技术的原理就是对于储存在计算机系统中的信息资源采用各种技术手段加密，从而令其即使被盗取也难以读取信息的原貌。因原信息经过加密之后就需要解密才具有实用价值，未经解密只是一堆杂乱的原码。计算机加密技术也是计算机信息的一道严密的防线。但随着软件技术发展，很多加密技术都能够被破解，有时已经无法满足目前计算机信息保护的需要。因此，加密技术也需要不断进行完善，以适应各类网络病毒及计算机安全维护的需要。

4.3 密钥管理数据加密与数字签名技术

网络数据加密技术的核心工作原理在于基于用户的许可，通过产生、分配、保存与销毁等环节以完成对信息的加密工作。通过密钥进行数据加密时，可选的密钥种类诸多，磁卡、磁盘、半导体这些都是比较常见的存储器形式。由于其能在产生、分配等环境上对信息进行保密，密钥管理数据加密技术目前来说应用比较广泛，在信息安全保护方面有很大优势，相较于密钥的复杂性，数字签名技术更为方便快捷，只需于相关文件中链接专属于自己的数字签名就可以将其打开。数字签名技术是基于在网络中所产生一系列钥匙串与数据相互配对实现的。因此只有掌握钥匙串的用户本人方可成功打开数据。但这意味着如果“钥匙串”丢失或其他安全用户需要使用数据时会较为麻烦。

5 结束语

综上所述，伴随着社会经济的快速发展，信息技术所涉及的应用范围不断扩大，网络已经成为了人们生活的一部分，网络安全维护也受到了企事业单位及个人的高度重视。相关的保密与安全问题防范技术自然也得到了广泛的应用，且有向世界各个领域延伸的趋势。当然，当前我们在维护网络数据安全方面仍存在很多问题，比如检测技术有效性偏低、灵活性不够等，这些因素极大降低了网络数据与信息安全维护能力。鉴于此，必须要构建起更加系统完善的计算机网络数据与信息管理系统，从而更加全方位且高效地监测控制网络安全问题。

参考文献

[1]贾书影.网络信息保密技术研究[J].科技创新导报，2020(07).
[2]王芳.网络信息保密技术探究[J].网络安全技术与应用，2017(04).
[3]鄢渼心，张娟.网络信息保密技术探究[J].信息与电脑(理论版)，2018(05).