信息化背景下计算机通信网络信息安全防护策略

杨　鹏

摘　要：随着信息技术的迅猛发展和广泛应用，计算机通信网络已成为现代社会不可或缺的基础设施。它承载着海量的数据传输、信息交流以及众多关键业务的运行，极大地促进了社会的信息化进程。然而，伴随着这一进程的是日益严峻的信息安全问题。计算机通信网络面临着来自各方面的威胁，如黑客攻击、病毒传播、数据泄露等，这些威胁不仅可能导致个人隐私的泄露，还可能对国家安全、社会稳定和经济发展造成重大影响。本文旨在探讨当前计算机通信网络面临的主要安全挑战，并提出相应的安全防护策略，以期为提升我国计算机通信网络的安全水平提供参考和借鉴。

关键词：信息化时代；计算机；通信网络；信息安全

引言

随着计算机网络飞速进步，它给人们的日常生活习惯和行为方式带来了根本性的巨大改变。信息科技与多项高级科技手段的有效融合，为社会的各行各业带来了飞速的现代化发展。随着网络平台上的信息通道变得越来越多元化和简化，我们频繁地看到网络安全的危险以及信息受到侵害的事件，从而使得信息泄露的威胁逐渐增强。虽然计算机网络的技术显著提高了交流、制造和工作的能力，但与此同时，它也带给我们信息安全的新问题和潜在风险。

一、计算机网络信息安全防护工作的重要意义

计算机网络信息安全防护的重要性是不可忽略的。信息化社会中，网络已经成为数据交换与信息存储的首要平台，覆盖了个人隐私，商业机密甚至国家安全数据等各类关键信息。网络信息安全防护不只是技术层面上的要求，也是维护社会秩序与经济稳定的主要基石。由于网络信息的多样性、易传播性等特点，当信息发生泄漏或者篡改时，可能会造成极其严重的后果。所以加强网络信息安全防护，保证信息内容完整与机密性对维护网络空间清朗，保护各利益相关方权益有着关键的实践意义。这一工作既是技术挑战也是事关社会全局的大事。

作者简介：杨鹏（1984.02——），男，汉族，北京海淀人，本科学历，主要从事计算机网络工程管理和项目运营管理工作。

二、信息化背景下计算机通信网络信息安全发展困境

（一）计算机网络高端技术人才缺失

目前计算机网络高端技术人才缺乏已经成为限制信息安全传输以及计算机通信网络保护的关键因素。伴随着信息化建设不断深化，相关行业对于高端人才需求越来越紧迫，特别是计算机通信网络信息安全方面，技能型人才匮乏现象日益突出。但现实的人才储备远没有达到这种需要，人才能力水平良莠不齐。其主要原因是很多企业利用网络信息资源谋求经济效益，却没有充分重视对信息网络的安全防护，缺少必要的投资与举措。这类企业通常都会忽略对计算机网络高端技术人才培养与引进工作，使得企业面对工业网络安全威胁越来越大而变得力不从心。另外，在互联网互联程度越来越高的情况下，计算机通信网络信息安全面临的威胁与日俱增。对还没有建立健全安全防护措施以及高端技术人才引进的公司而言，其面临接入认证、安全追溯、数据窃取等诸多安全风险，很难保障计算机通信网络信息安全。所以加强计算机网络高端技术人才培养与引进、提高企业信息安全防护意识与能力迫在眉睫。

（二）信息网络基础设施不完善

在信息化时代大潮中，很多行业与企业对于信息网络基础设施都有了更苛刻的要求，希望计算机通信网络系统能够表现出稳定、安全的工作状态与持续、高效地进行信息传播。据2022年9月的相关统计数据显示，中国的数据中心机架总规模已突破590万标准机架，服务器规模也接近2000万台大关。但在向网络强国迈进的道路上，必须面对一个实际的挑战，即信息网络基础设施

薄弱。这一短板从某种程度上弱化了计算机通信网络的信息安全问题。具体而言，虽然我国信息网络技术一些方面有明显进步，比如量子计算、5G技术等已经进入世界前列，但是工业软件方面、在芯片和数据库这些核心领域上，我们离世界先进水平还有着不可忽视的距离。这就意味着，我们还没有建立起完全独立研发，坚实可靠的核心技术体系。

三、信息化背景下强化计算机网络信息安全防护的有效措施

（一）加强隐蔽信道的权限差异化设置

对于隐蔽信道功能研究而言，有必要对应用层协议中隐蔽信道有关问题进行深入探讨，同时构造出相应分级模型以便综合评价。应用层是隐蔽信道建设的核心区，在其顺利建成后对信息进行封闭管理。客户机发送请求后，信息响应模块会做出快速反应，从而达到信息畅通沟通的目的。

为了保证具体安全防护标准的实现，隐蔽信道建立时需要基于统一资源标识符。同时建立分级模型对隐蔽信道风险评估非常关键。当安全等级不同时，需要有相应的防护措施，需要按照权限差异化准确分配才能达到有效保障安全。

权限的差异化分配，是保障系统安全至关重要的一环。合理分配权限可以阻止非法权限入侵。系统内重要信息可依据不同用户角色差异化分配权限。这就使得不同层次的用户只能够获取并调用自己权限下的消息。另外，差异化权限分配具有自动修复功能，在数据信息被破坏或者丢失情况下系统可以自动修复以保证信息完整安全。

（二）加强计算机用户管理

为了增强计算机网络信息的安全性，我们必须从用户的角度出发，强化对用户身份的验证与管理，同时提高用户登录时的账号保护机制，从而确保数据存储的安全性。身份认证技术在此扮演着至关重要的角色，它为用户在网络环境中的合法权益提供了坚实的保障。通过建立计算机与用户之间牢固的绑定关系，我们能够实现高效的信息安全防护。此外，通过科学控制访问权限，我们可以确保用户后续登录操作的合法性，有效遏制不法分子冒充用户、盗取信息的恶意行为。

身份认证主要采取三种方式：生物识别、口令输入和动态密码认证。为了进一步提升用户信息数据的安全性，我们推荐采用两种认证方式相结合的方法来完成身份认证过程。这样的双重验证机制能够大大提高用户账户的安全性，确保用户数据不被非法获取或滥用。

（三）应用多样化的加密技术

加密技术是确保计算机网络系统安全与稳定的核心手段，以身份验证技术为例，它要求用户在登录系统时提供独特的身份验证信息，这通常是密码、生物特征识别或是动态令牌等，确保只有授权用户能够访问系统资源，据相关统计数据显示，采用多重身份验证技术的系统，其遭受非法入侵的风险可降低60%以上。在实际应用中，加密技术不仅限于用户登录环节，还应贯穿于整个数据传输与存储过程。例如，对于金融交易系统而言，每一笔交易数据在传输前都应经过高强度的加密处理，确保即使数据在传输过程中被截获，攻击者也无法解析其真实内容，据金融安全机构报告指出，采用256位高级加密标准的金融交易数据，在现有计算技术下，几乎无法被破解。

此外，系统内部的风险识别模块同样重要，它能够通过对网络流量、用户行为等信息的实时监控与分析，及时发现异常行为并发出预警。据网络安全研究中心的数据显示，配备了智能风险识别模块的系统，能够在发生安全事件后的平均5分钟内作出响应，大大降低了潜在损失。

结束语

总之，为了保障网络信息安全就需要站在计算机用户角度，不仅要加强用户管理，还要全面提高用户安全防护意识。与此同时，需要采用多样化技术手段来强化计算机系统安全等级。另外，在国家层面上还应该积极健全相关法律法规，从而为网络信息安全的实现提供扎实的法制保障。这样，才能更加有效应对网络安全的挑战，确保数据安全和完整。

参考文献

[1]颜清华.信息化背景下网络安全漏洞与防范措施分析[J].信息与电脑（理论版），2019（12）：217-218.

[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]龙震岳，魏理豪，梁哲恒，等.计算机网络信息安全防护策略及评估算法探究[J].现代电子技术，2015，38（23）：89-93.