# 计算机网络工程的安全问题及其解决措施研究

刘彦凯

（兰州博文科技学院，甘肃 兰州 730101）

摘要：现阶段，计算机网络广泛应用于人类的生产和活动中，随之而来的安全问题也备受关注，操作系统存在安全风险、计算机病毒感染风险、不法入侵与外来攻击等问题层出不穷，如何采取有效措施增强计算机网络的安全性已经成为摆在我们面前的一项重大课题。维护网络安全刻不容缓，研究计算机网络工程的安全问题与解决措施更是具有重大意义，对此笔者总结了以下几点问题和对策，以维护计算机网络工程安全，使人们的生产和活动更加便捷。

关键词：计算机；网络工程；安全问题；解决对策

随着计算机网络技术的应用普及，其在长时间的使用过程中显露出诸多安全问题，在带给人们快捷和便利的同时，也带来了诸多负面影响，如病毒入侵所致的文件丢失、资料丢失；数据传输过程中遭到拦截而部分损坏；黑客攻击所致的系统瘫痪或软件瘫痪等。这就对人们的生产和活动造成了一定困扰，更可能有事业单位、企业单位面临商业层面的困境。因此，研究计算机网络工程的安全问题和解决对策具有重要现实意义。

## 一、计算机网络工程的安全概念阐述

如今，计算机早已走进了千万家庭，构建出了一个信息联通的巨大网络，笼罩着生存在互联网环境下的每一个人。因此，计算机网络工程安全、信息安全绝不是个人的事情，而是公共的、集体的，是我们要合力解决的重要问题。我们不仅要管理计算机硬件设备，还要控制相关软件、存储空间等的数据与材料，力求通过多样化的保护手段使其不受外界干扰，甚至是不受更改与损毁等等。站在最受信息安全问题影响的商业客户角度来说，他们的个人资料、业务往来、财务数据等属于“财产”，因此也必须保证信息在传输过程中不被泄露或篡改。尤其在网络病毒、网络黑客愈演愈烈的态势下，我们更要增强对计算机网络工程安全的重视程度，力求通过新理念、新技术等增强网络防护级别，力求更多使用计算机的人群养成良好上机习惯，保证互联网关系的纯洁性、互联网环境的整洁干净。

## 二、计算机网络工程的安全问题分析

### （一）操作系统的安全问题

实际上，保障计算机网络工程安全的前提是其计算机具备安全操作系统，但当前计算机和信息化发展迅速，信息网络连接更是无处不在，特别是计算机网络安全操作系统已经实现了网络操作。一般来说，存在 RDP 漏洞、VM 漏洞、UPNP 漏洞等多种安全漏洞时，计算机网络工程安全系统自然出现问题，漏洞被利用也会对计算机造成打击，以至于从操作系统处突破安全防线，对用户网络使用环境造成威胁。

### （二）计算机病毒感染风险

计算机病毒指的是人为编制程序，而计算机运行这一程序时能够自动拷贝或者有修改的拷贝到其他程序中，进而可能对计算机整体运行造成故障，甚至是计算机瘫痪、软件瘫痪等。计算机病毒的传播途径多种多样，常见的有收发邮件、插入不安全移动硬盘或 u 盘、安装程序时遇到病毒等等。这些病毒有着极强的传染性，目前广为传播的活性病毒就有一万四千多种，而且这一数量还在成倍增加，已经成为威胁计算机网络工程安全的重要因素之一。

### （三）不法入侵与外来攻击

1. 传输协议攻击

由于部分传输协议在制定时就存在漏洞，一些攻击者就可能利用这些漏洞进行恶意请求或恶意攻击，进而可能导致目标系统无法正常运行，甚至是系统性的崩溃。SYNFlood 攻击就属于传输协议攻击的一种，专针对 TCP/IP 协议里的“三次握手”漏洞进行攻击。无独有偶，ICMPF1ood 攻击可以通过大量垃圾数据包发送耗尽接收端资源，进而导致系统的崩溃或瘫痪。

2. 伪装技术攻击

伪装技术攻击的主要方法是对 IP 地址、DNS 解析地址、路由条目等进行伪造，致使服务器无法识别或响应，进而导致其网关地址相同、数据包无法转发，相应的会使某一网段处于瘫痪或崩溃状态。

3. 攻击服务端口

由于部分计算机应用软件在设计时针对指针函数与边界条件考虑不周全，实际执行过程中可能出现地址空间安全漏洞，进而可能导致服务端口受到攻击瘫痪。例如，应用软件可能无法对部分报文或请求处理或执行，进而可能导致应用软件无法正常运行，直接造成软件系统的瘫痪和崩溃。常见的 OOB 攻击就是最典型的例子，其主要针对 Windows 系统的 TCP 端口 139 随机发送数据，进而可能导致整个 CPU 始终处于工作状态。

4. 木马病毒攻击

木马的隐蔽性较强，其也是黑客常用的攻击工具之一，一旦计算机运行过程中被植入木马，黑客完全可以控制主机，从而成为隐蔽的用户进行一系列操作。一般情况下，黑客多用木马程序收集账号、密码、口令的关键信息，以此为计算机用户造成各式各样的威胁与困扰。

## 三、计算机网络工程安全的现状

### （一）信息管理能力比较弱

信息管理能力是针对个人提出的，而管理能力的好坏也在一定程度上决定着个人的信息受保护程度。除需要更安全、更高效的技术外，个人的信息管理能力也不容忽视，甚至是要重视和培养，才能够有效将不安全因素所隔绝。但目前，绝大多数在网络上冲浪、学习、工作的人并没有养成良好信息保护观念，甚至不会刻意用各类手段保护自己的计算机或个人信息。加之并没有一个绝对健康的互联网环境，在管理制度、管理方式等方面存在缺乏，自然无法保证更多人的计算机处于安全状态，而这也将为不法分子“钻空子”留下缺口。

### （二）网络安全管理的缺失

现代化网络环境下，各类信息纷繁复杂，在一家企业中也很难单独设立网络管理部门，即使有专门的网络管理人员负责这一板块，也往往由其他部门的领导人员负责。这就容易导致管理决策、管理制度实施不畅，进而引发计算机网络工程安全问题而造成不良影响。就笔者个人经验而言，对网络安全管理缺乏系统认识和学习的话，难以真正对症下药和因势利导，更难以实现信息安全管理。这不仅仅是人们对于计算机网络工程管理的不重视，也是对其不了解、不作为的最直接体现，同时也不利于个人或企业、

组织等的计算机网络工程安全、稳定和长效发展。

**四、计算机网络工程安全的解决措施**

（一）提高用户安全意识和能力

当今社会，每一位计算机用户都应当提高自身安全意识、安全能力，以此来保护自己的上网安全与权益。假如每个工作单位、每个互联网用户都有着较强的安全意识，那要比任何计算机网络安全措施、策略、操作等更加有效，因此必须从源头处深入问题、解决问题，也就是提高计算机用户的安全意识和能力。依托互联网运营的工作单位有必要组织和开展网络安全知识宣传工作，让每一位公司员工都认识和了解计算机网络工程的安全问题，让其懂得计算机病毒、黑客攻击等的危害。久而久之，相关工作人员才能够形成良好上网习惯，不随便下载，不使用不了解的 u 盘、移动硬盘、软件等，不浏览风险网页，防止计算机网络系统受到攻击或木马、病毒的入侵。

笔者认为，政府方面应当加强对计算机网络工程的监管，完善监管条例和处罚措施，避免执法过程中受到多种因素干扰。而落实到个人处也应当严于律己、严格遵守监管条例，做到对系统文件、可执行文件与数据的保护，做到不适用来历不明的程序或数据，做到不适用软盘进行系统引导。在此基础上，计算机用户还要避免浏览风险网站和接受不明电子邮件，避免从外部自动接收病毒。计算机网络工程的安全绝非个人之事，其也代表着互联网环境的纯洁性与专业性，加强政府监管、加强公司宣传、加强个人防护能够从根本上优化上网路径，保证计算机的正常生产和运营，保证恶意攻击被扼杀在摇篮中。

（二）采取有效加密与保护措施

针对重要的数据和信息，计算机用户应当采取加密保护措施，防止自身账号、密码、口令等关键信息遭他人窃取或修改。当数据转化为加密文件后，其防护系数自然增加，能够增加窃取者、攻击者的执行难度，其在无密钥的情况下难以对数据进行还原，也在一定程度上保障了个人信息的安全性，保证了个人隐私不受损害。其中，密钥主要指信息的发送与接收方使用相同标准对数据进行加密或解密，虽能够快速操作完成，但密钥管理相对容易泄露而埋下安全隐患。因此就需要通信双方保持上网环境的干净，做到交换密钥安全、对数据加密安全操作、虽报文同时发送和接受。在此概念下，非对称加密主要指的是加、解密操作通过一对密钥分别实现，能够加强保护措施的有效性、保密性。非对称加密主要分为两个部分，共同由甲方生成、保管、发放，公钥能够配合公开使用，针对公开指令或业务进行放行，而私钥为甲方私发给乙方，并由乙方对接使用，能够增强互联网使用的针对性与个性化。这样的方式能够有效加强信息保密程度，进而能够实现数据安全与计算机网络安全。

（三）注意病毒防护技术的应用

注意病毒防护技术的应用尤其重要，其是避免病毒攻击的有效方法，更能够隔绝部分病毒实现网络安全管理。对未知病毒的查杀基于虚拟执行技术而生成，能够与虚拟技术、人工智能联动，能够确保准确对未知病毒进行查杀。智能引擎能够利用扫码优势弥补不足之处，能够确保扫码病毒不会因为病毒增大而对速度造成严重影响，也能够发挥出特征码的扫描优势。压缩智能还原技术能够保证文件还原、数据还原，那么多余的部分自然为病毒程序，也就暴露了敌方目标，能够轻松实现病毒消杀。现阶段，病毒免疫这项技术也日渐成熟，主要根据控制自主访问和设置磁盘禁写保护区病毒完成免疫功能，能够有效抵御部分病毒攻击。嵌入式杀毒也是有效的病毒防护技术，其主要是应用对象的自我保护，能够通过操作系统或者应用程序的内部接口完成消杀。

对于计算机系统，使用防火墙、防毒墙技术是有效的病毒防护措施，能够实现对病毒的物理隔绝，也能够通过各类技术手段查杀病毒。通常来说还需要使用过滤、应用网关、状态检测等多种手段才能够配合完成。以过滤技术为例，其就能够对数据流中的数据包进行辨别检查，在分析源地址、目标地址、包端口的基础上判定数据是否合格、是否通过检测。一旦数据不合法，能够自然拦截和消杀，然而却对于允许连接的计算机病毒数据流不起作用。在此基础上，防毒墙技术能够有效隔绝病毒，在网络入口处发现病毒过滤功能，进而能够在网关处实现查毒操作，从而避免有效避免了 worm、BOT 等病毒的进一步扩散。其中，网络管理员还能够对分组安全策略进行重新定义，以此实现网络流向的过滤。

（四）加强入侵检测技术的应用

入侵检测技术也是计算机网络工程安全运行的好帮手，其在实际应用过程中能够发挥积极意义，从源头处抑制入侵、安全防护，实现对计算机网络工程安全水平的有效提升。网络入侵检测的体系结构通常由三部分组成，分别为 Agent、Console 以及 Manager。其中，Agent 的作用是对网段内的数据包进行监视，精准查找出相关数据并发放至管理器；Console 主要负责搜集代理处信息，将攻击数据外显并发送至管理器；Manager 主要响应配置攻击警告信息，将最终的攻击警告发送至控制台，进而通过报警和防护系统配合有效驱逐入侵攻击行为。入侵检测技术的工作模式基于网段部署多个入侵检测代理，也就需要按照各部分实际情况连接和处理。如果网段内的连接方式为总线式，那么就需要把代理与集线器中的某个端口相连接；如果网段内的连接方式为交换机，那么只拥有一个代理对子网进行监听很难实现连接和处理，反而可以将交换机核心芯片中用于调试的部分与入侵检测端口相连接，能够获取关键数据而实现有效检测。以对主机的入侵检测为例，会将检测重点设置在主机上，从而对本主机的系统进行详细分析、详细筛查，如有可疑会采取针对性措施。而入侵检测技术的应用当以实际数据为主，避免流于形式，避免数据不到位引起的安全问题，以针对性解决网络安全问题。

**五、结语**

总而言之，科学技术在进步和发展，计算机网络工程的安全问题也不容忽视，相关工作者应当切实分析现存的安全问题，努力研究对策、解决问题，维护计算机网络工程安全的同时发挥其社会功能，维护社会稳定和经济繁荣发展。计算机网络工程安全问题需要在技术层面、管理层面、信息层面不断加强和提高，也就需要长久的维护和努力，才能够确保计算机网络工程的长久安全与效能发挥。

**参考文献：**

[1] 刘森 . 数据加密技术在计算机网络安全中的运用策略——评《计算机网络安全与管理》[J]. 热带作物学报，2021，42（12）：3735.

[2] 曹书槐，黄崇争 . 计算机软件工程安全问题及其对策探讨 [J]. 科技创新导报，2019，16（30）：105-106.

[3] 段峻 . 基于云计算技术的计算机网络安全储存系统设计及开发 [J]. 电子设计工程，2019，27（09）：115-118.

[4] 代连奇，谭洪旭，袁帅，任利峰 . 计算机网络工程安全策略与防护病毒 [J]. 产业与科技论坛，2019，18（01）：55-56.

作者简介：刘彦凯（1968-），男，汉，甘肃省兰州市人，工程师，研究方向：软件工程。