

# 浅析计算机网络安全防范与措施

毕哲睿

西安外事学院 陕西省西安市 046100

**摘要:** 现如今,信息和通讯的飞速发展导致人们对计算机极其依赖,无论是在生活方面还是在工作方面,计算机所扮演的角色都十分重要,是人们生活必要的一部分,对工作和生活中的关键点都有着极大的影响作用。然而,在工作和生活中对计算机频繁使用同时也引发了很多网络安全问题。本文主要以计算机网络安全的影响因素作为切入点进行深入分析,发现当下计算机网络安全需要改进的地方,对网络安全中频繁发生的攻击方式进行了系统的整理和归纳,并提出合理有效的防范措施。

**关键词:** 通讯; 计算机; 网络安全

## 1 影响计算机网络安全的主要因素

根据当前计算机网络安全所面临的各种风险来看,导致网络出现风险的因素主要有以下几个:第一个是网络的开放特性;第二个是网络操作系统存在很多漏洞;第三个是网络资源具有共享性;第四个是网络系统设计仍然存在一定的不足;最后一个黑客的恶意攻击等。具体表现为以下几个方面:

### 1.1 互联网络的不安全性

存在于网络系统当中的安全隐患主要有两种:第一种是网络结构设备;第二种是网络系统自身所携带的不足。现如今,集线型和星型是大多数人使用的网络结构,这些混合型结构都表现为多种结构混为一体。由于设备会因为自身技术方面的问题而受到一定的制约,因此都会将或大或小的安全隐患携带到计算机网络系统上。此外,网络系统本来就存在着一定的不足,网络技术的好处有两点:一个是开放性;另一个是资源共享性。由于互联网络是一个非常庞大的体系,具有全球性复杂交错的特点,因此它的优点也是它的缺点,非常容易受到攻击。计算机网络协议原本就有很多的不安全因素,比如说我们常见的欺骗攻击以及数据截取等。

### 1.2 操作系统存在的安全问题

作为一个支撑软件,操作系统能够使程序或者其他运用系统处于正常运行环境。其能够提供大量的管理功能,主要是对系统当中的软件以及硬件资源进行有效的管理。操作系统软件本身所存在的不安全性以及在对系统进行开发的时候,由于不够周密谨慎而遗留的一些破绽,都有可能在未来对网络安全造成威胁。

操作系统所包含的管理很多,例如内存、CPU 以及外设等,所有的管理都会或多或少的对一些模块或程序

有所牵连,若这些程序出现任何问题,例如内存管理,通过外部网络而传入的连接,恰巧与有问题的模块连接了起来,最终会导致的结果就是计算机系统会彻底崩溃。因此,黑客通常就是会对操作系统的不完善下手,做出一系列的供给,从而使计算机系统,尤其是服务器完全陷入瘫痪。

除此以外,创建进程也是操作系统不安全的一个非常重要的原因。首先它能够支持进程的远程创建以及激活;其次它还能够支持被创建进程继承创建的权利。正是由于满足了这些条件,远端服务器上才很有可能被安装上“间谍”软件。如果通过补丁的方式将间谍软件渗透到合法的用户上,尤其是拥有特权的用户,那么整个系统进程以及作业监视程序就都没有办法对黑客或间谍软件等进行有效的监控。

## 2 网络常见的攻击方式

### 2.1 间谍软件

间谍软件,实际上就是通过计算机来进行信息的搜集整合,同时在未经计算机用户准许的情况下,把信息传送给第三方,主要包括以下几种:第一种是监视击键;第二种是对机密信息进行搜集;第三种是搜取邮箱地址;最后一种是对浏览习惯进行跟踪。除此以外,间谍软件还存在一个副产品,受到其影响之后网络性能会大大折损,系统速度会变得越来越慢,使得整个商业进程都受到干预。

### 2.2 混合攻击

混合攻击,顾名思义将各种各样的攻击方式集合起来,它们将蠕虫等多种恶意代码汇聚起来,专门寻找服务器或者互联网的漏洞,对其进行猛烈且迅速的攻击,

使其受到极大的破坏。

### 2.3 绕道攻击

网关级别的安全防护并不能满足电脑的绝对安全，其还是会受到源于 CD 以及 USB 等设备上的恶意软件攻击。相同的道理，如果员工的电脑在办公室以外的地方被操作，那么也就无法保证绝对安全。如果你的电脑存在于无线热点区域里，那么电脑的有关通讯就很有可能会被窃听者或者是 AP 盗用者进行拦截。若你所使用的电脑因为没有使用完备的客户端安全防护措施而受到以上所提到的攻击，那么我们就将该种情况叫做“绕道攻击”。

### 2.4 强盗 AP

强盗 AP 并非 IT 部门所有，同时也不是由 IT 部门按照公司安全策略来实施的。我们将强盗 AP 视为主要的网络安全风险导入源头，其能够准许并未得到授权的人监听网络通讯，更为严重的是可以尝试将风险注入，如果有强盗 AP 连接到网络上，那么仅仅通过一些简单的操作，例如将 Wi-Fi 适配器插入到 USB 端口中等，没有获得授权的用户就能够在公司以外对你的网络进行访问。

### 2.5 网页及浏览器攻击

网页漏洞攻击实际上就是借助 Web 服务器来对安全防护进行一系列的破坏，例如 Sunday 的 Java Web 服务器等。

### 2.6 蠕虫及病毒

蠕虫就是对现有计算机程序所存在的病毒进行感染，其在计算机安全威胁病毒当中十分普遍。通常都会隐藏在文档以及表格当中，传播途径通常为电子邮件，蠕虫的传播实际上就是借助网络传播自己。如果电脑受到了蠕虫或者病毒的感染，那么别的系统也就很有可能受到感染，现有的系统也很有可能就会遭到严重的破坏。

## 3 计算机网络安全的主要防御策略

对于计算机网络安全风险隐患，首先要做的就是对计算机网络安全防范进行不断的强化，一方面需要全面采用网络安全技术以及防范手段，另一方面还要强化网络法规制定，从而使得计算机安全保护能够更加彻底。在对计算机网络安全进行讨论的时候，主要从以下几点介入：

首先，不要把不知源头的软件或程序下载到电脑上。在平时使用计算机的时候，要频繁的对系统补丁进行更新，这样是为了避免病毒入侵，若出现感染病毒的情况，一定要及时下载查杀软件。此外，下载的软件一定不要出自非官方网站，这些软件很有可能就是病毒的载体，严重的话就会导致计算机的资料消失，因此在下载软件

的时候一定要挑选拥有良好信誉的网站。

其次，要对电子邮件的攻击进行防范。我们经常会收到一些不知出处的邮件，对于这些邮件一定要保持谨慎，最好不要打开阅读，因为很有可能是病毒携带体。如今病毒依附邮件的传播手段十分频繁，我们很有可能就会在不知情的時候受到攻击。电子邮件攻击通常表现为电子邮件的轰炸，实际上就是借助非法的 IP 将大量的垃圾邮件发送到某个邮箱号上，使得邮箱走上瘫痪。除此以外还有电子邮件欺骗，这些攻击人员通常为扮演成管理者，用指令的方式将病毒种到用户的电脑当中。目前有很多病毒过滤软件都可以对这类病毒进行效果不错的拦截。

此外，要对浏览器进行安全设置。浏览器也是经常被网络病毒侵害的一个部分。Cookie，实际上就是在进行浏览的时候，会被部分网站在硬盘里加以属于，它们会对用户的特定信息进行相关记录，所以当用户重新返回到原先页面上的时候，信息就很有可能会被重复使用。所以，若想在使用浏览器的时候能够保障安全就需要对安全级别进行合理的设置，将 Cookie 关掉。

最后，要对自己的 IP 地址进行全面的保护。在网络安全协议当中，始终都会有一个唯一的 IP 地址存在。一般来说，IP 地址不管是对自己还是对别人都处于隐藏状态。然而在进行网络聊天的时候，由于聊天信息的传递必须要对 IP 地址进行捆绑，所以在这个时候很容易将 IP 地址泄露出去，恰好成为黑客的作案辅助。所以，在平常使用计算机的时候一定要主要良好习惯的养成，尽可能的减少个人信息泄露，避免损失。

## 4 结论

总的来说，计算机网络信息安全与防范并非易事，反之，其是一个综合且长久的课题，所牵涉的方面也非常广泛，例如技术以及管理等。其一方面有计算机系统本身就存在的许多安全问题，另一方面也涉及到了物理和逻辑等问题。尽管如今有很多产品都在网络信息安全中得到了一定的使用，例如我们所熟知的防火墙等，然而还是无法彻底解决黑客入侵的问题。在对计算机网络信息进行全面的安全防护时应该非常谨慎，尽可能的避免黑客等入侵的情况发生，使网络信息能保持安全和完整。同时，要对信息系统的脆弱性以及各种威胁多加关注，通过有效的安全策略进行风险的规避，这对于信息系统的安全保障非常关键。在对网络信息进行安全防范的时候需要对新技术的使用大力关注，在最快的时间内对自身的防御系统进行有效的优化升级。

现如今，网络技术发展的越来越迅速，网络资源具有一定的共享性和开放性，因此更要对其所携带的安全

隐患加以关注。为了能够使信息的安全保障能力得到不断的强化,对国家安全以及稳定等进行有效的维护,将科学的计算机网络防范体系构建出来非常必要,使计算机网络安全风险降到最低,使计算机网络安全技术得到不断的提升,将科学技术以及理论基础等提供到安全的网络环境当中。

### 参考文献:

- [1] 王晓燕. 大数据时代计算机网络安全及防范措施探讨 [J]. 技术与市场, 2020, 27(10): 108+110.
- [2] 李静燕. 计算机网络安全中数据加密技术的应用研究 [J]. 科技创新与应用, 2020(28): 173-174.
- [3] 刘磊. 计算机网络中大数据与人工智能技术的应用 [J]. 计算机产品与流通, 2020(11): 69+140.
- [4] 朱剑平, 刘迁. 计算机网络安全防护体系建设分析 [J]. 计算机产品与流通, 2020(11): 83.
- [5] 张天明. 探讨计算机网络安全 [J]. 计算机产品与流通, 2020(11): 90.
- [6] 张健. 互联网时代下的计算机网络系统的安全集成研究与发展 [J]. 计算机产品与流通, 2020(11): 93.
- [7] 周海玉. 浅谈计算机网络安全中数据安全加密技术的应用 [J]. 计算机产品与流通, 2020(11): 95.
- [8] 热依汗古丽·胡达拜迪. 计算机网络应用安全问题及策略关键研究 [J]. 计算机产品与流通, 2020(11): 110.
- [9] 刘洪亮, 杨志茹. 大数据时代计算机网络安全技术探讨 [J]. 电子测试, 2020(18): 137-138.
- [10] 范骐嘉. 常见网络安全问题和应对方案的研究 [J]. 电子制作, 2020(18): 82-83+58.