计算机网络安全现状与对策研究

刘　淼　郑晰元

（中国网络安全审查技术与认证中心，北京 朝阳区 100020）

摘要：当前，计算机网络安全问题已经成为我们生活中需要关注的重点问题，计算机涉及我们日常生活的方方面面，一旦计算机内信息被泄露，就可能给用户造成巨大损失，历史上发生过许多由于计算机病毒入侵导致系统瘫痪和信息被泄露的事件，都造成了巨大的社会损失，因此保护计算机网络安全是现代生活中的一项重点工程。本文针对计算机网络系统存在的安全性问题，从目前的网络安全隐患和解决措施等方面进行探讨，希望可以提高计算机用户对网络安全的认识。

关键词：网络安全；安全隐患；对策

一、目前计算机网络的安全隐患

当前，计算机网络安全主要分为两方面内容：网络信息安全和计算机设备安全。信息安全主要指计算机内保存的信息不被泄露，计算机设备安全是指计算机设备正常运转。

（一）计算机操作者安全意识不高导致信息泄露和计算机设备瘫痪

计算机用户对网络安全不重视，人为泄露信息，可能导致信息被人拦截、获取。计算机软件会定期对系统漏洞进行修补，但系统提示有安装补丁包时，计算机用户不重视，可能导致系统被有心人攻击，给用户造成损失。电脑不定期杀毒也可能导致计算机系统被病毒入侵，从而影响计算机使用。再者，如果用户不重视保护自己的账号和密码，随意借于他人或者在外部电脑上登录，也会导致信息泄露问题。

（二）人为的恶意攻击

人为的恶意攻击是目前网络安全问题面临的最大的隐患。人为恶意攻击又分两种，一种是主动攻击，另一种是被动攻击。主动攻击不仅破坏信息，而且可能会造成计算机系统的瘫痪。被动攻击是在悄无声息中拦截、获取用户信息。这两种攻击都会严重危害网络安全。

（三）计算机软件的漏洞和“后门”泄露导致系统被恶意程序入侵

网络软件往往存在各种漏洞，攻击软件的漏洞是黑客入侵他人系统最常用的方式，所以软件公司会定期对软件做维护升级，增加补丁包，提高软件的安全性。软件系统的“后门”是为了方便编程人员测试、更改、升级系统而存在的，因此后门是软件系统的秘密通道，如果被外部人员发现可能会进行软件入侵。

二、网络安全问题的应对策略

（一）增强计算机用户网络安全意识

当前社会环境下，增强公民网络安全意识极其重要。网络公司应该加强网络信息安全的义务宣传教育，增强公民保护信息安全的意识，让公民了解维护网络信息安全有哪些途径。保护自己的网络安全首先要保护自己的用户名和密码，不把这些信息轻易泄露出去。其次，定期对计算机进行杀毒，消灭恶意程序，重视软件补丁包的安装提示，修补软件漏洞。

（二）访问控制安全

访问控制是指通过验证、识别用户来保护信息安全。用户访问时，系统确认其身份后才允许登陆，从而达到保护用户信息的目的。访问控制主要有口令、访问权限、网络安全检测、审计和跟踪等方式。口令是指用户注册系统时，系统检查其登录名和口令的合法性，从而防止恶意入侵。口令是网络安全最外层的防线。访问权限设置主要应用在共享文档、共享设备上，通过设置网络资源的操作权限，保护信息、资源只被内部人员使用，以此保护信息安全。网络安全监视也被称为“网管”，即检测整个网络的运行状态并处理各种临时事件。网络监视的目的在于找出网络系统中的安全隐患，例如查找网络故障点、阻止网络 IP 非法进入以及控制网络访问等。网络资审计和跟踪指记录、反馈、分析网络资源的使用权限、网络故障等。

（三）数据传输安全

传输安全是指保护数据在传输过程中不被截取和破坏。保护数据传输安全主要有加密和数字签名、防火墙技术、使用摘要算法认证、PKI 认证、VPN 技术保护等方式。加密与数字签名是数据接受者验证数据发送者是否正确的一种方法，主要通过加密算法和验证协议实现。防火墙提示是用户在网络使用过程中经常遇到的网络安全保护手段，防火墙设置在不同网络和网络安全域之间，通过对跨越防火墙的数据流进行检测、限制来保护用户的网络安全，它可以检测到网络内外部运行状态和结构，是一种应用比较广泛的网络安全技术。PKI 即公开密钥体系，这种认证体系综合了摘要算法、数字签名等技术，安全系数比较高，常用在电子邮件、应用服务器访问、防火墙认证等方面。VPN 技术是使分布在各个地方的专用网络在公共网络上实现安全通信的技术，它提供一种安全的双向通信，采用复杂算法加密信息，保证传输数据不被窃听和破坏。

三、结语

网络信息技术已经渗透到我们生活的方方面面，并且网络信息系统具有一定的脆弱性，容易受到非法入侵和破坏，因此保护计算机网络安全是现在生活中一项非常重要的事情，目前已经有比较完善的信息加密技术，但计算机用户在使用过程中还是要重视网络安全问题，保护个人信息，其次，软件开发公司也要不断完善信息系统，对信息系统进行定期维护和升级，及时修补漏洞，保护用户的网络安全。网络安全问题的保护一方面要加强用户身份认证，使用口令、访问权限设置等技术认证信息使用者身份，保护用户信息安全；另一方面要加强数据传输中的安全，通过认证信息发送者身份、加密数据等方式保护信息数据在传输过程中不被窃听和解密，确保信息的安全传输。

参考文献：

[1] 曾国凡 . 计算机网络安全的现状及对策 [J]. 通讯世界，2015（23）：69.

[2] 李丽 . 我国互联网信息安全现状及对策研究 [J]. 信息与电脑（理论版），2015（23）：157-158.

[3] 潘谈 . 计算机网络安全现状分析与防范对策分析 [J]. 黑龙江科技信息，2014（36）：151.