网络安全防范与思考

（黄刚 河南科技学院 河南新乡市 453000[[1]](#footnote-1)）

摘要：随着科学技术的高速发展，计算机网络已经成为新时期知识经济社会运行的必要条件和社会的基础设施。本文针对现代网络威胁，对网络的各种安全隐患进行归纳分析，并针对各种不安全因素提出相应的防范措施。

关键词：计算机网络;信息安全;防火墙;防护措施;

1网络不安全因素

网络的不安全因素从总体上看主要来自于三个方面：第一是自然因素。自然因素指的是一些意外事故，如发生地震、海啸，毁坏陆上和海底电缆等，这种因素是不可预见的也很难防范。第二是人为因素，即人为的入侵和破坏，如恶意切割电缆、光缆，黑客攻击等。第三是网络本身存在的安全缺陷，如系统的安全漏洞不断增加等。

由于网络自身存在安全隐患而导致的网络不安全因素主要有：网络操作系统的脆弱性、TCP/IP协议的安全缺陷、数据库管理系统安全的脆弱性、计算机病毒等。目前人为攻击和网络本身的缺陷是导致网络不安全的主要因素。

2计算机网络防范的主要措施

2.1计算机网络安全的防火墙技术

计算机网络安全是指利用网络管理控制和技术措施，保证在一个网络环境里，信息数据的保密性、完整性和可用性受到保护。网络安全防护的根本目的，就是防止计算机网络存储和传输的信息被非法使用、破坏和篡改。

目前主要的网络安全技术有：网络安全技术研究加密、防火墙、入侵检测与防御、VPN和系统隔离等技术。其中防火墙技术是一种行之有效的，对网络攻击进行主动防御和防范，保障计算机网络安全的常用技术和重要手段。

2.2访问与控制策略

对合法用户进行认证可以防止非法用户获得对公司信息系统的访问，使用认证机制可以防止合法用户访问他们无权查看的信息。访问控制策略其任务是保证网络资源不被非法使用和非法访问。各种网络安全策略必须相互配合才能真正起到保护作用，它也是维护网络系统安全、保护网络资源的重要手段，访问控制是保证网络安全最重要的核心策略之一。

(1)入网访问控制。入网访问控制是网络访问的第一层安全机制。控制哪些用户能够登录到服务器并获准使用网络资源，控制用户登录入网的位置、限制用户登录入网的时间、限制用户入网的主机数量。当交费网络的用户登录时，如果系统发现“资费”用尽，还应能对用户的操作进行限制。用户的入网访问控制通常分为三步执行：用户名的识别与验证;用户口令的识别与验证;用户账户的默认权限检查。

(2)权限控制。权限控制是针对在网络中出现的非法操作而实施的一种安全保护措施。用户和用户组被给予一定的权限。网络控制着能够通过设置，指定访问用户和用户组可以访问哪些服务器和计算机，可以在服务器或计算机上操控哪些程序，访问哪些目录、子目录、文件和其他资源，设定用户对可以访问的文件、目录、设备能够执行何种操作。

(3)属性安全控制。访问控制策略还应该允许网络管理员在系统一级对文件、目录等指定访问属性。本策略允许将设定的访问属性与网络服务器的文件、目录和网络设备联系起来。属性安全策略在操作权限安全策略的基础上，提供更进一步的网络安全保障。当用文件、目录和网络设备时，网络系统管理员应给文件、目录等指定访问属性。属性安全控制可以将给定的属性与网络服务器的文件、目录和网络设备联系起来。属性安全在权限安全的基础上提供更进一步的安全性。网络上的资源都应预先标出一组安全属性。用户对网络资源的访问权限对应一张访问控制表，用以表明用户对网络资源的访问能力，网络的属性可以保护重要的目录和文件，防止用户对目录和文件的误删除、执行修改、显示等。

(4)网络服务器安全控制。网络系统允许在服务器控制台上执行一系列操作。用户通过控制台可以加载和卸载系统模块，可以安装和删除软件。网络服务器的安全控制包括可以设置口令锁定服务器控制台，以防止非法用户修改系统、删除重要信息或破坏数据。系统应该提供服务器登录限制、非法访问者检测等功能。

(5)网络监测和锁定控制。网络管理员应能够对网络实施监控。网络服务器应对用户访问网络资源的情况进行记录。对于非法的网络访问，服务器应以图形、文字或声音等形式报警，引起网络管理员的注意。对于不法分子试图进入网络的活动，网络服务器应能够自动记录这种活动的次数，当次数达到设定数值，该用户账户将被自动锁定。

2.3安全基石---防火墙

防火墙是网络访问控制设备，用于拒绝除了明确允许通过之外的所有通信数据，它不同于只会确定网络信息传输方向的简单路由器，而是在网络传输通过相关的访问站点时对其实施一整套访问策略的一个或一组系统。防火墙处于5层网络安全体系中的最底层，属于网络层安全技术范畴.作为一种隔离控制技术，它是内部网络与外部公共网络之间的第一道屏障，防火墙是最先受到人们重视的网络安全产品之一。虽然从理论上看，防火墙处于网络安全的最底层，负责网络间的安全认证与传输，但随着网络安全技术的整体发展和网络应用的不断变化，现代防火墙技术已经逐步走向网络层之外的其他安全层次，不仅要完成传统防火墙的过滤任务，同时还能为各种网络应用提供相应的安全服务。另外还有多种防火墙产品正朝着数据安全与用户认证，防止病毒与黑客侵入等方向发展。目前技术最为复杂而且安全级别最高的防火墙是隐蔽智能网关，它将网关隐藏在公共系统之后使其免遭直接攻击。隐蔽智能网关提供了对互联网服务进行几乎透明的访问，同时阻止了外部未授权访问对专用网络的非法访问。

3计算机网络攻击的常见手法及防范措施

3.1利用网络系统漏洞进行攻击

漏洞是指硬件、软件或策略上存在的安全缺陷，从而使攻击者能够在未授权的情况下访问、控制系统。许多网络系统都存在着或多或少的漏洞，这些漏洞有可能是系统本身所具有的，如windows、Linux和Solaris等都存数量不等的漏洞，也有可能是由于网管的疏忽而造成的。黑客就是利用这些漏洞来完成密码探测、系统入侵等攻击。

对于系统本身的漏洞，要及时安装软件补丁。网络管理员需要根据本单位的需求对局域网加强防护措施，。监控并及时处理流量异常现象，尽量避免因疏忽而使网络系统受到危害。

3.2通过电子邮件进行攻击

电子邮件是互联网上运用最广泛、最受欢迎的一种通讯方式。当前，电子邮件系统的发展也面临着机密泄露、信息欺骗、病毒侵扰、垃圾邮件等诸多安全问题的困扰，如黑客可以使用一些邮件炸弹软件向目标邮箱发送大量内容重复、无用的垃圾邮件。对于遭受此类攻击，可以通过邮件加密、使用垃圾邮件过滤技术来解决。

3.3解密攻击

在互联网上，使用密码是最常见的安全保护方法，用户需要输入密码进行身份校验。只要有密码，系统就会认为你是经过授权的正常用户，因此，取得密码也是黑客进行攻击的一个重要手法。

为了防止受到这种攻击的危害，可以采取以下措施：1)采用更“强壮”的加密算法。一个好的加密算法往往只能通过穷举法得到密码，所以只要密钥足够长就会很安全。2)动态会话密钥，即尽量做到每次会话的密钥都不相同。3)定期变换加密会话的密钥。

3.4后门软件攻击

后门通常是一个服务端程序，可能由黑客编写，恶意攻击者通过一定手段放在目标主机上以达到非法目的，也可能是目标主机正在运行的授权应用软件，其本身具有可被攻击者利用的特性。

为了防止后门软件的攻击，在网上下载数据时，一定要在运行之前首先进行病毒扫描.如果可能的话使用一定的反编译软件，查看源数据是否有其他可疑的应用程序.从而杜绝这类后门软件。

3.5拒绝服务攻击

拒绝服务是攻击者通过一定的方法，使目标服务器资源过载，以致没有能力向外提供服务的过程，互联网上许多大型网站都遭受过此类攻击。拒绝服务攻击的具体方法就是向目标服务器发送大量合理的服务请求。几乎占取该服务器所有的网络带宽，从而使其无法对其进行处理，而导致网站无法进入、网站响应速度大大降低或服务器瘫痪。现在常见的蠕虫病毒或与其同类的病毒都可以对服务器进行拒绝服务攻击的进攻。它们的繁殖能力极强，有些通过Microsoft的Outlook软件向众多邮箱发出带有病毒的邮件，使邮件服务器无法承担如此庞大的数据处理量而导致瘫痪。

对于个人上网用户而言，也有可能遭到大最数据包的攻击而使其无法进行正常的网络操作，所以在上网时一定要安装好防火墙软件，同时也可以安装一些可以隐藏IP地址的程序，或使用代理服务器，这样能大大降低受到此类攻击的可能性。

3.6缓冲区溢出攻击

缓冲区是一个程序的记忆区域.在此区域中存储着—些数据信息，如程序信息、中间计算结果、输入的参数等等。把数据调人缓冲区之前，程序应该验证缓冲区有足够的空间容纳这些调入的数据。否则，数据将溢出缓冲区。并覆写在邻近的数据上。当它运行时。就如同改写了程序，造成混乱。假如溢出的数据是随意的，那它就不是有效的程序代码，程序执行到此就会失败、死机。另一方面，假如数据是有效的程序代码。程序执行到此，就会产生新的功能。windows的虚拟内存技术不是很完善，还存在大量问题，于是就有专门的程序利用缓冲区溢出原理来攻击远程服务器。对于以上各种类型的网络攻击。我们可以使用网络安全技术来加以防范。以保障网络的安全。

4结束语

综上所述：为了保障网络信息的安全，我们要根据网络隐患的特征，分析信息系统的各个不安全环节，做到有针对性的防范和采取切实有效的措施，在最大限度上使安全系统能够跟上实际情况的变化发挥效用，使整个安全系统处于不断更新、不断完善、不断进步的过程中。

参考文献

【1】蔡立军计算机网络安全技术[M]北京：中国水利水电出版社2005-7

【2】肖军模.刘军.周海刚网络信息安全[M]北京：机械工业出版社2006-1

【3】张千里，陈光英网络安全新技术[M]北京：人民邮电出版社2003-1

【4】周学广等.信息安全学. 北京：机械工业出版社，2003.3

【5】 (美)Mandy Andress著.杨涛等译.计算机安全原理. 北京：机械工业出版社，2002.1

【6】曹天杰等编著.计算机系统安全.北京:高等教育出版社，2003.9

【7】刘衍衍等编著.计算机安全技术.吉林:吉林科技技术出版社.1997.8

【8】(美)Bruce Schneier 著,吴世忠等译.应用密码学-协议、算法与C语言源程序.北京：机械工业出版社，2000.1

【9】 赖溪松等著.计算机密码学及其应用.北京:国防工业出版社.2001.7

【10】 陈鲁生.现代密码学.北京：科学出版社.2002.7

【11】 王衍波等.应用密码学.北京：机械工业出版社，2003.8

【12】(加)Douglas R.Stinson著，冯登国译.密码学原理与实现.北京：电子工业出版社，2003.2

[Network security and thinking]

(HuangGang HeNanKeJiXueYuan HeNanXinXiangShi 453000)

Abstract: with the rapid development of science and technology, computer network has become a necessary condition for the knowledge economy society in the new period and social infrastructure.Based on modern network threats, inductive analysis was carried out on the network of all kinds of potential safety hazard, and put forward the corresponding precautionary measures according to various unsafe factors.

Key words: computer network;Information security;Firewall;Protective measures;

1. 黄刚，1993.10.9，男，汉，河南信阳，本科学位，听音乐 [↑](#footnote-ref-1)