计算机网络信息安全初探

熊心志
(重庆大学计算机学院基础系　重庆 400044)

摘　要　信息安全对经济发展、国家安全和社会稳定的重大影响,正日益突出地显现出来,计算机网络信息的有效性、安全性成为突出的问题。而为了保护计算机网络信息安全,除了运用法律和管理手段外,还需依靠技术的方法来实现。网络安全的基本技术目前主要有:防火墙技术、访问控制技术、网络反病毒技术、网络安全漏洞扫描技术、入侵检测技术、信息加密技术、信息确认技术等。本文通过计算机网络信息安全面临的危险及网络系统安全存在的漏洞,引出加强网络安全管理的各种技术方法,阐述了加强计算机网络信息安全的重要性。

关键词　病毒,黑客,危害,安全策略

随着 Internet 的发展,网络丰富的信息资源给用户带来了极大的方便,但同时也使得网络很容易受到攻击,计算机信息和资源也很容易受到黑客的攻击,甚至是后果十分严重的攻击,诸如数据被人窃取,服务器不能提供服务等等。因此,网络和信息安全技术也越来越受到人们的重视,由此推动了防火墙、入侵检测、虚拟专用网、访问控制、面向对象系统的安全等各种网络、信息安全技术的蓬勃发展。防火墙技术作为网络安全的重要组成部分,也格外受到关注。

1　威胁计算机网络信息安全的潜在问题

网络管理中的漏洞带来的后果令人头痛。许多企、事业单位和现有计算机网络大多数在建设之初都忽略了安全问题,未考虑安全防范措施,网络交付使用后,网络系统管理员的水平又不能及时跟上。即使考虑了安全,也只是把安全机制建立在物理安全机制上,随着网络的互联程度的扩大,这种安全机制对于网络环境来讲形同虚设。网络"入侵者"通常就利用网络管理中的漏洞,频频发起攻击,破坏网络安全。轻则网页被涂改、系统被占用,重则使重要信息被窥视或修改,甚至系统崩溃,造成重大经济损失,2000 年 YAHOO 等国际重要商业网站遭黑客袭击就是最典型的一例。

1.1　口令入侵

所谓口令入侵是指使用某些合法用户的帐号和口令登录到目的主机,然后再实施攻击活动。这种方法的前提是必须先得到该主机上的某个合法用户的帐号,然后再进行合法用户口令的破译。许多用户在设置自己的口令时,随意性很大,对密码的选择较简便,使得口令被破译的概率大大增加。目前,获取用户帐号的方法很多,如:通过网络监听非法得到用户口令、监听者往往采用中途截击的方法获取用户帐户和密码、特别是当前很多协议没有采用任何加密或身份认证技术,用户帐户和密码信息以明文格式传输过程中,更容易被截取;查看主机是否有习惯性的帐号,有经验的用户都知道,很多系统会使用一些习惯性的帐号,造成帐号的泄露;利用目标主机的 Finger 功能:当用 Finger 命令查询时,主机系统会将保存的用户资料(如用户名、登录时间等)显示在终端或计算机上;用目标主机的 X. 500 服务:有些主机没有关闭 X. 500 的目录查询服务,也给攻击者提供了获得信息的一条简易途径;从电子邮件地址中收集:有些用户电子邮件地址常会透露其在目标主机上的帐号;利用操作系统存在的许多安全漏洞、Bug 或一些其他设计缺陷进行用户帐号和密码的获取。

1.2　黑客攻击

黑客是英文"Hacker"的译音。黑客的攻击已超过计算机病毒的种类,总数成千上万,而且很多种都是致命的,从国际互联网上学习和获取黑客攻击的方式是轻而易举的。如在网上用户可以利用 IE 等浏览器进行各种各样的 Web 站点的访问,如阅读新闻组、咨询产品价格、订阅报纸、电子商务等。然而一般的用户恐怕不会想到有这些问题存在:正在访问的网页已经被黑客篡改过,网页上的信息是虚假的!例如黑客将用户要浏览的网页的 URL 改写为指向黑客自己的服务器,当用户浏览目标网页的时候,实际上是向黑客服务器发出请求,那么黑客就可以达到欺骗的目的了。利用黑客软件攻击也是互联网上比较多的一种攻击方法。BackOrifice2000、冰河等都是比较著名的特洛伊木马,它们可以非法地取得用户电脑的超级用户级权利,可以对其进行完全的控制,除了可以进行文件操作外,同时也可以进行对方桌面抓图、取得密码等操作。这些黑客软件分为服务器端和用户端,当黑客进行攻击时,会使用用户端程序登录上已安装好服务器端程序的电脑,这些服务器端程序都比较小,一般会随附带于某

些软件上。有可能当用户下载了一个小游戏并运行时，黑客软件的服务器端就安装完成了，而且大部分黑客软件的重生能力比较强，给用户进行清除造成一定的麻烦。

1.3 病毒泛滥

计算机病毒是一个程序，一段可执行码。就像生物病毒一样，计算机病毒有独特的复制能力。计算机病毒可以很快地蔓延，又常常难以根除。它们能把自身附着在各种类型的文件上。当文件被复制或从一个用户传送到另一个用户时，它们就随同文件一起蔓延开来。除复制能力外，某些计算机病毒还有其它一些共同特性：一个被污染的程序能够传送病毒载体。当你看到病毒载体似乎仅仅表现在文字和图像上时，它们可能也已毁坏了文件、再格式化了你的硬盘驱动或引发了其它类型的灾害。若是病毒并不寄生于一个污染程序，它仍然能通过占据存贮空间给你带来麻烦，并降低你的计算机的全部性能。如瑞星全球反病毒监测网截获的恶性蠕虫病毒“硬盘杀手”，可以覆盖硬盘分区，导致硬盘被锁死，硬盘无法使用，所有数据全部被封存。“硬盘杀手”病毒的破坏力全面超越 CIH 病毒；它可以在 Windows95 以上的所有版本的操作系统中运行，将用户计算机上的所有硬盘里的所有资料瞬间清除并且无法恢复。病毒的传播途径往往通过软盘、光盘传播；通过 Ftp、电子邮件传播；通过 Web 浏览传播，主要来自恶意的 Java 控件及 Activex 控件网站等传播。

1.4 系统漏洞扫描与探测

许多系统都有这样那样的安全漏洞(Bugs)，其中一些是操作系统或应用软件本身具有的，如缓冲区溢出攻击。缓冲区溢出是指当计算机程序向缓冲区内填充的数据位数超过了缓冲区本身的容量，溢出的数据覆盖在合法数据上。缓冲区溢出是病毒编写者和特洛伊木马编写者偏爱使用的一种攻击方法。攻击者或者病毒善于在系统当中发现容易产生缓冲区溢出之处，运行特别程序，获得优先级，指示计算机破坏文件，改变数据，泄露敏感信息，产生后门访问点，感染或者攻击其他计算机。如从红色代码到 Slammer，再到日前爆发的“冲击波”，都是利用缓冲区溢出漏洞的典型。利用系统存在的漏洞进行病毒式攻击，给我们的网络安全造成了严重的威胁。因此，系统管理员应及时修补系统中存在的漏洞，将攻击扼杀在萌芽时期。

2 强化计算机网络系统信息安全的管理

计算机网络问题涉及到国家安全、社会公共安全和公民个人安全的方方面面。要使我国的信息化、现代化的发展不受影响，就必须去克服众多的计算机网络安全问题，去化解日益严峻的网络安全风险。而要把风险降到最小，则应着力抓好网络安全方案设计。

2.1 防火墙技术

防火墙技术是网络安全的重要技术手段，它是一个用以阻止网络中的黑客访问某个机构网络的屏障，也可称之为控制进出两个方向通信的门槛，其主要作用是在网络入口点检查网络通讯，根据用户设定的安全规则，在保护内部网络安全的前提下，提供内外网络通讯。它可以在被保护网络周边通过综合运用软件、硬件及管理措施，对跨越网络边界的信息提供监测、控制甚至修改的手段。利用防火墙技术，经过仔细的配置，在网络边界上通过建立起来的相应网络通信监控系统来隔离内部和外部网络，以阻挡外部网络的侵入，从而提高网络安全程度。例如网络防病毒历来是信息系统安全的主要问题之一，上下载软件和使用盗版软件是病毒的主要来源。其防病毒技术主要通过病毒防火墙，阻止病毒的传播、检查和清除病毒等。但是，防火墙通常不能提供实时的入侵检测能力，也不能隔离来自内部网络攻击的攻击，而据报道 80% 的攻击来自内部，因此仅仅使用防火墙，网络安全还远远不够。

2.2 入侵检测技术

入侵检测技术是一种新型网络安全技术，目的是提供实时的入侵检测及采取相应的防护手段，如记录证据用于跟踪和恢复、断开网络连接等。实时入侵检测能力之所以重要，首先是它能够作为防火墙技术的补充，弥补防火墙技术的不足，能对付来自内部网络的攻击，其次是它能够大大缩短“黑客”可利用的入侵时间。

2.3 安全扫描技术

安全扫描技术源于“黑客”在入侵网络系统时采用的工具，安全扫描技术与防火墙、入侵检测系统互相配合，能够有效提高网络的安全性。通过对网络的扫描，网络管理员可以了解网络的安全配置和运行的应用服务，及时发现安全漏洞，客观评估网络风险等级。网络管理员可以根据扫描的结果更正网络安全漏洞和系统中的错误配置，以提前主动地控制安全危险，在黑客攻击前进行防范。

2.4 信息加密技术

信息加密的目的是保护网内的数据、文件、口令和控制信息，保护网上传输的数据。特别是随着电子商务的迅速发展，网上传输着大量的重要信息。而开放的电子商务系统必定要建立在开放的通讯安全体系之上。基于公钥体系的认证和通讯加密系统(PKI)由于其开放性而逐渐流行，成为电子商务安全解决方案的重要基础。在公钥密码中，收信方和发信方使用的密钥互不相同，而且几乎不可能从加密密钥推导出解密密钥。比较著名的公钥密码算法有：RSA、背包密码、McEliece 密码、Diffe-Hellman、

Rabin、Ong-Fiat-Shamir、零知识证明的算法、椭圆曲线、EIGamal 算法等等。最有影响的公钥密码算法是 RSA，它能抵抗到目前为止已知的所有密码攻击。

2.5 信息确认技术

安全系统的建立都依赖于系统用户之间存在的各种信任关系，目前在安全解决方案中，多采用二种确认方式。一种是第三方信任，另一种是直接信任，以防止信息被非法窃取或伪造，可靠的信息确认技术应具有：具有合法身份的用户可以校验所接收的信息是否真实可靠，并且十分清楚发送方是谁；发送信息者必须是合法身份用户，任何人不可能冒名顶替伪造信息；出现异常时，可由认证系统进行处理。目前，信息确认技术已较成熟，如信息认证，用户认证和密钥认证，数字签名等，为信息安全提供了可靠保障。设计制订一个良好的网络安全方案，并能正确客观，就能在享受网络信息化优势的同时，把风险减到最小。当然，信息系统采用先进的网络安全技术、工具、手段和产品的同时，还要有先进的系统恢复、备份技术(工具)。

3 建立、健全相应的法律、法规及管理制度

网络安全法规建设和组织建设，是网络安全的重要基础。单纯从技术角度只能被动地解决一个方面的问题，而不能长远、全面地规范、保障网络安全。因此，从根本上对网络犯罪进行防范与干预，还是要依靠法律的威严。自 1996 年以来，政府已颁布实施了一系列有关计算机及国际互联网络的法规、部门规章或条例，内容涵盖国际互联网管理、信息安全、国际信道、域名注册、密码管理等多个方面。随着网络应用向纵深发展，建设一个较为完善的网络法规，注重网络法规强制与激励并行以及网络立法规范实现的可能性，为网络法规的操作执行提供了有力的保障，有效地保护网络使用者的合法权益，增强对网络破坏者的打击处罚力度。除国家制定法律、法规外，凡使用计算机的单位都应制定相应的管理制度，避免蓄意制造、传播病毒的发生。如对接触重要计算机系统人员进行选择和审查，对系统中的工作人员和资源进行访问权限的划分，任何行动只能在保证系统安全或他人信息安全的条件下进行；要对外来人员上机或外来磁盘的使用严格限制，许多大学还规定不准随意玩游戏，或只准在网络上提供的游戏库中调用，对于联网的设备，规定下载文件要经严格检查，应规定下载文件、接收 E-mail 等需使用专用的终端和帐号，接收到的程序要严限制执行。

4 加强对计算机网络信息安全方面的宣传和教育

黑客的攻击之所以能经常得逞，其主要原因就是人们思想麻痹，没有正视黑客入侵所造成的严重后果，人们经常在有意无意之中就泄露了信息，不经意就为黑客开了方便之门。因此要大力宣传计算机病毒的危害，引起人们的重视。要宣传可行的预防病毒的措施，使大家提高警惕。要普及计算机软件的基本知识，使人们了解病毒入侵计算机的原理和感染方法，以便及早发现，及早清除。特别对未成年人，应从小培养网络用户的合法上网概念，防止有害信息的传播和渗透。另外，对工作人员应结合机房、硬件、软件、数据和网络等各方面的安全问题，进行安全教育，提高工作人员的保密观念和责任心；加强业务、技术的培训，提高操作技能；教育工作人员严格遵守操作规程和各项保密规定，防止人为事故的发生。

结论 未来的战争是信息战争，而网络战是信息战的重要组成部分，而计算机网络已日益成为工业、农业和国防等方面的重要信息交换手段，渗透到社会生活的各个领域。因此，认清网络的脆弱性和潜在威胁，采取强有力的安全策略和健全各种网络政策法规，对于保障网络的安全性将变得十分重要。

参 考 文 献

1 刘瑞挺. 网络技术[M]. 高等教育出版社，2004

2 张少俊，李建华. 网络安全综合管理系统的设计与实现[J]. 计算机工，2003，29(14)

(上接第 39 页)

以方便而经济地通过低压电力线进入国际互联网络，让全人类真正地走进数字化时代。

参 考 文 献

1 雷震洲. 初露头角的电力线通信[J]. 当代通信，2003(22)：10～15

2 刘永生、Echelon 公司的电力线载波通信技术[J]. 仪器仪表标准化与计量，2005(4)：20～23

3 刘恒，汪光森，王乘. OFDM、扩频通信技术在电力线通信中的应用分析与仿真[J]. 继电器 RELAY，2003，31(7)：41～46

4 冯秀清. 低压电力线通信及其实现[J]. 辽宁工学院学报，2001，21(6)：20～23

5 邱玉春，徐平平. 低压电力线载波信道特性分析[J]. 电力系统通信，1999(6)

6 赵洪山，刘力丰，杨奇逊. 低压电力线扩频载波通信方案[J]. 电力系统自动化，2000，24(12)

7 李志文，朱雪龙. 电力线载波通信用的数字调解器[J]. 电力系统通信，2000(4)

8 邱小宁. 浅谈电力线载波通信现状与发展趋势[J]. 广西电力技术，2001(4)：59～65