网络战的威胁与对策

陈　健
(海军大连舰艇学院, 大连 116018)

摘要　随着网络的发展与普及, 网络的安全和可靠性成为世界各国共同关注的焦点。分析了网络战的特点和发展现状, 并就如何应对日益严峻的网络战的挑战提出了几点攻与防的对策, 指出了要打好网络战需要坚持军民结合、全民皆兵的原则。

关键词　信息战　网络战　对策

0　引　言

随着网络时代的到来, 网络将会成为无处不有、无所不用的工具, 经济、文化、军事和社会活动将越来越依赖于网络。而 INTERNET 的无主管性、跨国界性、不设防性、缺少法律约束性的特点, 在为各国带来发展机遇的同时, 也带来了巨大的风险, 网络的安全和可靠性成为世界各国共同关注的焦点。尤其是在军事领域, 网络攻击将会成为信息战的主要作战方式, 网络战的威胁已经成为无可回避的现实。

1　网络战的特点

网络战主要有两大特点:

(1) 隐蔽性好

由于网络技术的公开化, 任何一个熟练的计算机操作人员都能够利用某些黑客软件在任何时间和地点对网络系统实施攻击, 而被攻击者却无法确定对方的攻击是个人行为还是政府行为, 无法判断其攻击性质。与传统战争的有形性相比, 网络战是隐蔽和看不见的。网络战不受时空地理气候条件限制的特点, 使得被攻击方更加难以防御。

(2) 破坏性强

信息时代的作战高度依赖于各作战单元间的信息共享, 而网络既是实现信息共享的主要媒体, 又是信息攻击的主要渠道。网络中的任一作战单元受到攻击, 都将对整个网络系统的作战效能产生不良影响, 而且网络战的重点攻击对象往往是敌方的重要节点, 如信息中心、指挥控制中心等, 一旦这些中心节点遭到破坏, 整个网络系统都将瘫痪。网络技术的飞速发展, 既加快了作战的信息化进程, 同时也提高了作战效能, 增大了战争的破坏性。同传统的战争形式相比, 网络战真的是“牵一发而动全身”。

2　网络战的主要形式

2.1　计算机病毒攻击

计算机病毒是网络战的典型武器, 1999 年 4 月 CIH 病毒在全球范围内肆虐, 使人们对计算机病毒的破坏性有了深刻认识。世界各国正利用计算机病毒的破坏性研制相应的病毒武器, 如美国国防高级研究计划局正在秘密研制一种新型计算机病毒武器 ——计算机病毒炮, 它可以从遥远的地方利用火炮投射到敌方坦克、飞机、潜艇及其他战术野战系

收稿日期: 2001-03-05

统附近,使它们的计算机在关键时刻受诱骗,导致武器系统失灵。台湾“国防部”曾表示,已经研制了上千种病毒对付中国大陆的信息基础设施。面对“台独”势力的嚣张气焰,我们必须时刻提高警惕。

2.2 网络黑客入侵

1998 年 2 月 26 日,美国国防部所在地五角大楼被黑客“光顾”,4 个海军系统和 7 个空军系统的电脑网页遭入侵。更令人吃惊的是,在美国国防部已经发现的情况下,黑客连续进行了整整 1 周的“骚扰”,而这个黑客组织的主谋竟是以色列的一位 18 岁少年。同年 4 月 22 日,1 个黑客团伙自称在“袭击”五角大楼情报网系统时已窃走控制军事卫星系统的情报,并威胁要将情报卖给恐怖组织,这一消息震惊了世界,黑客的危害之大可见一斑。有消息说,美、俄等国正在有意招募和培养计算机黑客,以期在未来的信息战中利用他们攻击敌方的重要信息系统。

3 加强网络防御战

“积极防御”的国家战略决定了我们必须从网络环境的保护、攻击源的探测、网络系统能力的恢复以及对攻击的反应等方面下大力气加强“网络防御战”。

3.1 强化网络安全观念

网络和网络技术在现代全球军事和民用活动中的地位越来越明显,其本身注定要成为未来战争和冲突的主题。因此,加强网络系统建设的同时必须搞好网络安全工作,但现实情况是两者并不同步。网络安全建设滞后于网络的发展,这将是今后出现信息危机的重要原因。必须将网络系统的研发和安全防护作为一个大系统工程来统筹考虑,在研制的同时要考虑加密、抗干扰、防电磁辐射、防计算机病毒等技术防护措施,以提高系统在信息战条件下的对抗能力和生存能力。

3.2 自主开发军用软件

计算机网络功能都嵌于操作系统中,对网络系统的攻击实际就是对操作系统的攻击。目前,我军信息系统中的操作系统都来自国外,比如 DOS、VMS、UNIX、Windows-NT、Windows-98 等,这很可能导致我们在未来的网络战争中受制于人。当务之急是研制我军自己的操作系统来消除这一隐患,而 Linux 无疑是我们最好的选择。

Linux 强大的网络功能、对硬件支持的广泛性、更好的稳定性和对内存空间更充分的利用等特点证明它完全可以替代 UNIX 和 Windows-NT 而应用于我军的信息系统。从 Linux 出现的那天起,它的内核就是公开的,Linux 发展到今天这么成熟,也是众多 Linux 爱好者智慧的共同结晶。这种开放式研制思路有很大借鉴意义,使得开发我军自己的 Linux 系统成为可能。事实上,国内在开发 Linux 方面已经积累了一定的经验,中科院软件所、北大方正电子有限公司、康柏电脑公司共同开发的红旗 Linux 就是一个很好的例证。

3.3 力争电子装备国产化

我军信息系统中所使用的计算机元器件大都依赖进口,这是危及系统安全的一个巨大隐患。1999 年 8 月,台湾“国防部”召开了一次信息战会议,邀请了各计算机软硬件厂商、计算机专家、病毒的设计制造者(包括 CIH 病毒制造者陈英豪)。会议的中心议题就是如何利用台湾强大的计算机软硬件优势,对祖国大陆实施信息战。具体步骤包括向中国大陆出口的计算机产品注入藏有病毒的芯片,必要时通过遥控激活等。为了避免在未来可能的信息战争中受制于人,必须加大基础研究的力度,努力实现电子装备国产化。

3.4 有效利用安全工具

(1) 扫描工具

现有的 UNIX 和 Windows 等操作系统

中存在着相当多的安全隐患, 而这些隐患通常也是网上黑客入侵的方便之门。这些隐患的产生, 既有系统本身脆弱的一面, 更有系统管理员或用户在配置中的错误和疏忽的原因。利用扫描工具可以很快发现系统在配置和软件上是否存在问题, 从而降低网络遭破坏的概率。当然, 利用扫描工具也可以发现对方网络系统的安全性弱点, 为攻击寻找突破口。典型的扫描工具有 SATAN、ISS 等。

(2) 加密

虽然操作系统都提供了一些对私有信息的保护机制, 但是在网络通信方面则非常薄弱。目前, 几乎所有的网络通信都没有加密, 只要通过一些设备连接到网络上, 任何人都可以对通信进行监听。一旦用户的登录口令被监听到, 网络就无密可言。许多网络入侵者都是通过运行一个监听网络的程序, 得到了一些口令而侵入系统的。一些网络的电磁泄露也可以使信息在一定距离内被截获。加密、密钥认证和完整性保护可以使得网络和计算机系统变得更加安全, 所以必须对网络通信进行加密。

(3) 口令验证

口令验证是一个最基本的认证方式, 是系统的第 1 道防线。一个好的口令通常不少于 8 个字符, 其中包括大小写、数字和除 26 个英文字母以外的字符。如此复杂, 只是为了增加猜口令和破口令的难度。事实上, 相当多的用户由于设置了较为简单的口令而被攻击者用口令破解程序破译, 以至侵入系统, 破坏网络。口令不但要复杂, 还要经常改动, 减少被破解的几率。好的口令设置习惯可以在相当程度上提高网络安全性。

4　发展网络攻击技术

进攻是最有效的防御。在搞好网络防御的同时, 还要大力发展网络攻击技术, 以其人之道还治其人之身。

4.1　计算机病毒攻击

从病毒防御的角度出发, 首先要严格管理, 如使用公用软件和共享软件应十分谨慎; 新入网的计算机系统应仔细检查; 限制计算机网络中可执行代码的交换; 所有系统留用文件进行写保护; 绝不执行来历不明程序和网络公共板上的程序; 对系统中的主要数据、文件定期进行拷贝并对网络中的通信线路这一薄弱环节加强防护力度等。其次, 从软、硬件技术方面加强计算机病毒的预防, 改变网络数据共享结构, 运用以毒防毒的方法编制特定的计算机病毒, 本身对网络系统某些薄弱环节进行保护等。在搞好防御的基础上, 还要以攻为守, 发展我军的计算机病毒武器和病毒攻击战术。尽管我军计算机对抗技术起步较晚, 但我国有很好的计算机软件人才储备, 只要发挥我们的聪明才智, 是能够在未来的信息作战中有所作为的。

4.2　成立网络战特种部队

1998 年春, 美国国防部探测到大量的计算机非法入侵事件, 于是成立了计算机网络防御联合特遣部队。该部队的使命是: 当国防信息系统遭受攻击时, 迅速地探测和识别, 并采取有效的反制措施。另据报道, 美国国防大学已组建了“第 1 代计算机网络勇士班”, 运用鼠标、键盘, 通过信息高速公路漫游互联网络, 寻找潜在的敌人。

为保障我军信息系统的安全, 也应当成立 1 支由网络专家和精通网络战的军人组成的网络防御特种部队, 其使命是在信息空间与看不见的对手进行信息对抗, 防御敌人的网络入侵, 确保系统安全。同时, 还应成立 1 支网络攻击特种部队, 以未来信息战为背景, 模拟敌人可能采用的各种网络攻击方法和我军应当采取的对策, 并让 2 支部队进入攻防对抗演练。通过这种近实战的对抗可以找到系统的缺陷及改进方法, 提高系统防御能力;

(下转第 34 页)

常工作。

在一般开关电源中, 功率开关管及整流器件在开闭翻转过程中, 微秒量级上升下降时间内的大电流变化所产生的射频能量已成为纹波的主要来源。而这一点在谐振式电源中得到很大的改善。由于其零电流开关的技术, 使得在功率开关器件及输出整流器件上, 开闭翻转过程中无大电流变化, 所以产生的射频能量也就非常小, 纹波远小于一般开关电源。

3 结束语

谐振式电源的诸多优点, 使它将成为取代传统开关电源的一种主要电源模式。在我们的产品中, 尤其在发射机中采用此电源, 不仅提高了电源的效率, 减小了体积, 同时由于电源纹波的减小, 直接降低了发射机的相位噪声, 使其多项指标得到很大的改善。

参考文献

1 叶慧贞, 杨兴洲. 开关稳压电源. 北京: 国防工业出版社, 1990
2 王英剑. 新型开关电源实用技术. 北京: 电子工业出版社, 1999

(上接第 31 页)

同时积累对敌信息系统攻击的方法、手段和经验, 为取得未来信息战争的胜利打下可靠基础。

5 结束语

并非拥有先进的网络战设备和网络战技术就一定是战争的胜利者, 因为越是网络战技术先进的国家, 其对网络的依赖性越强, 因而受攻击后的损失会更大。网络战的参与者可能是军人, 也可能是平民, 只要具备了相应的计算机和网络知识就可以成为一名“战士”。因此, 无论网络战技术先进或落后的国家, 其“网络防御”都是困难的。网络攻击不但针对军事目标, 重要的民用目标如金融系统、信息中心等也是攻击对象, 而且很多为未来攻击而准备的“信息炸弹”正是平时通过民用网络系统而潜入军事系统的。可以说, 网络战已经模糊了平时和战时的界限。因此, 我们要坚持军民结合、全民皆兵的原则来建设网络系统, 军民共筑“网上长城”, 打一场网络时代的人民战争。