doi: 10.3969/j.issn.1006-1576.2011.03.015

军网安全防护问题研究

马鹏飞，常书杰
（解放军炮兵学院 5 系，合肥 230031）

摘要：随着军队信息化建设不断深入，军网规模不断扩大、作用不断深化，其安全防护问题日趋突出。分析现行军网存在的各种不安全因素，研究军网可能遭受的主要攻击手段，有针对性地提出了军网安全防护方法，总结了开展军网安全防护工作时的注意事项，对开展军网安全防护工作具有重要的应用价值。

关键词：军网；网络攻击；安全防护
中图分类号：TP393.08　　**文献标志码**：A

Research of Military Network Security Protection Problem

Ma Pengfei, Chang Shujie
(No. 5 Department, Artillery Academy of PLA, Hefei 230031, China)

Abstract: As the military information construction going deeply, military network scale enlarges and takes affect continuously, its security protection problem becomes bigger and bigger day by day. Analyzed current military network various dangerous factors, studied the possible major attack methods of military network, specially put forward military network security protection method, summarized the notices when developing military network security protection work. All of them have important application value for developing military network security protection work.

Keywords: military network; network attack; security protection

0　引言

随着计算机网络技术的快速发展，战争的形式也发生了根本性的变化，以往的火力取胜论已经被信息制胜论所取代。军队信息化建设是为作战服务的，信息战中大量的侦察信息和作战命令将会通过军网进行上传下达，一旦被敌方成功攻击将会对作战产生重大的影响。由于目前各种网络攻击用的软件越来越傻瓜化，降低了网络攻击的门槛越来越低，做好军网安全防护工作将会日趋重要，故对其进行研究。

1　军网的不安全因素

1) 接入端信息接入点的不安全

对军网来说，接入端的信息接入点大部分是在军事管理区内，非军方人员极难接触到这些信息点。但接入端也有不安全因素，主要是旅团级以下的接入点，由于其作战单位分布较散，尤其是小远散单位、侦察哨所、友邻部队临时作战单位的接入点，作战单元的信息接入点将是敌对分子可能窃入的地方。只要一个信息接入点被成功窃入，那么敌方就有可能以此为突破口对军网发动攻击。

2) 违规使用军网造成的不安全

有些同志私自将非军方下发的软件、存储介质、甚至个人 PC 连接到军网，导致病毒传播。另外，把军网内专用的存储介质在军网和 Internet 之间互用，也会造成军用信息在 Internet 上的泄露，对军网造成危害。

3) 管理上的不安全

不严格遵守管理规定，对接触军网设备（如网络设备和接入点的 PC）和使用人员没有严格检查管控，让外来人员和没有资格接触网络设备的人员接触到这些设备。

2　可能遭受的主要攻击手段及防护方法

1) 非法接入

非法接入是指不符合入网条件的人员通过各种非法手段接入网络，以获得网络服务。别有用心的人偷偷接入军用网络只是第一步，其目的是利用这个接入点展开网络攻击。有效防范非法接入，可以将最具破坏力的外来敌特分子，阻挡在门外。信息流通的信道是管理较为薄弱的环节。首先，加强线路看护是必要且有效的方法。其次是管好终端接口。网络的接口都安装在办公区，主要依靠行政管理加强办公区进出人员的管控，并辅以“MAC 地址绑定”、“固定 IP”、“身份验证”等技术手段限制。

2) 利用 IPC$空连接攻击

开启 IPC$服务的计算机允许远程建立空连接，使远程计算机可以方便地获取本地计算机的帐户列

收稿日期：2010-10-26；修回日期：2010-12-25
作者简介：马鹏飞（1979—），男，河北人，硕士，讲师，从事炮兵指挥自动化研究。

表、帐户使用情况、操作系统版本等敏感信息。当拥有帐户名和密码时，利用 IPC$服务，任何人都可以远程连接本地计算机完成各种操作。由于很多计算机用户都轻视了帐户密码的设置，使得 IPC$服务成为了黑客的常见攻击手段。假如把计算机比成一个房子，那么用户常犯的错误有以下几种：① 不锁门，即不设密码。入侵者直接远程连接计算机，获得系统管理权。② 门锁不牢，即弱口令。远程密码暴力破解软件的测试密码的速度是 300 个/s，也就是说 6 位以下的纯数字密码，可在 6 min 之内百分之百破解出来。而且该软件可以加挂黑客字典，针对生日、电话号码、姓名拼音等常见密码设置习惯进行密码猜测，大大提高密码攻破的效率。③ 忘关后门。administrator 用户是 WinXP 安装时就存在的，在登录屏看不到 administrator 用户，并不代表这个用户是未激活的，正版 WinXP 安装完成时会提示设置 administrator 帐户密码，盗版 WinXP 不会提示，采用的是一个预设的密码，甚至是空密码，为入侵者敞开了可以自由进出的后门。IPC$空连接不能算是真正的漏洞，IPC$服务是操作系统为方便管理员远程操作而设置的。对付这种 IPC$空连接，关键是计算机使用者要管理好本机上的帐户及密码。辅以“禁止远程枚举用户列表”、“关闭默认共享”、“修改 administrator 帐户名”等技术手段。保证计算机安全。

3) 利用操作系统漏洞攻击

Microsoft 公司设计了代码量极其庞大的操作系统，无可避免地受到各种程序 BUG 的困扰，作为用户量最大的操作系统，全世界的顶级黑客们都在努力寻找 Windows 中可以用来入侵的 BUG，每当黑客发现并公布一个 BUG，Microsoft 公司都能及时的推出补丁修复问题，同时 Microsoft 公司自己也在不断地查找漏洞和推出补丁，帮助用户修复 BUG。但军网计算机没有这种在线升级的待遇，从安装系统以来从未打过补丁，以至于地方网已经绝迹几年的“Unicode 漏洞”、“.ida/.idq 缓冲区溢出漏洞”、“Frontpage 服务器扩展”等漏洞在军网上随处可见。为军网黑客大行方便之门。在军网上架设 Windows 补丁分发服务器，及时提供最新安全补丁，可防止军网上的“学步”黑客照搬民网的漏洞攻击案例。

4) 中间人攻击

中间人攻击指黑客通过技术手段欺骗将要通信或正在通信的 2 台计算机，将自己的计算机插入中间，充当转发站的角色，让所有传输数据都流经自己，从而监听或篡改传递的数据。这种攻击较为专业，隐蔽性强，危害非常大。首先是信息篡改。假设 A 计算机发指令给 B 计算机“3:00 部队开始总攻”，中间人将“3:00”改成“4:00”，B 计算机收到的信息变成“4:00 部队开始总攻”，从而造成非常严重的后果。其次是信息窃取。将传输的数据保存到本地，用于事后分析目标用户的网络活动，获取登录帐户、登录密码等敏感信息。中间人攻击是基于 TCP/IP 协议的弱点实施欺骗，无法杜绝。但有以下几种防范方法：① 防钓鱼网站。使用钓鱼网站是中间人欺骗的常见手段之一。中间人伪造一个目标网站，诱使他人访问，再将数据转发给真实的网站，完成欺骗。防范这种欺骗，用户要认真核对网站内容，识别网站真假。② 加密传输数据。对传输的数据进行非对称加密，为中间人分析数据制造困难。③ 加强网络监管。通过网管软件检测 IP 异常、设备异常，发现和制止中间人攻击。

5) 跨站脚本攻击

有 2 种情况：① 攻击者已经攻克网站，在网站页面里挂上木马程序，用户访问网页时，会下载安装木马程序。② 攻击者利用论坛等动态网页程序的漏洞，往网站的交互区域插入恶意 html 代码，当用户访问网页时，恶意代码被执行。根据漏洞的强度，实现偷取用户 Cookie、下载安装木马等。

防范方法：一方面要加强网站防护。配强管理员做好安全配置，防止网站被攻破；另一方面要及时更新论坛程序，堵住论坛漏洞。

6) 蠕虫病毒攻击

蠕虫病毒本身没有破坏能力，但大量的蠕虫在网络上复制，就会迅速耗尽网络资源，造成网络瘫痪，产生具大破坏力。前几年军网流行的“红色代码”、“蓝色代码”都是蠕虫病毒，因为技术手段的缺乏和低效，不得不断网杀毒，使军网中断服务将近一个月，反复大半年才得以根除，严重影响了军网的正常运行。“红色代码”、“蓝色代码”之所以产生这么大的危害，一方面它是利用操作系统的漏洞进行传播的，很多军网计算机都没有及时打补丁；另一方面，缺乏病毒监控网，不能在初期迅速发现和扼制病毒的扩散。因此，可从 2 个方面进行防范：一是在军网统一分级部署杀毒服务器，对全网进行病毒监控；二是架设补丁分发服务器，及时为存在系统漏洞的计算机提供补丁。

7) DOS 和 DDOS 攻击

DOS 攻击，即拒绝服务攻击。通过向服务器发送超负荷的服务请求，耗尽服务器系统资源，使其失去响应正常服务请求的能力。随着硬件技术的发展，服务器的运算能力越来越强，单靠一台或几台计算机 DOS 攻击已经不能拖垮服务器，已经很少使用。因此，出现了 DDOS 攻击，即分布式拒绝服务攻击。攻击者远程遥控成千上万的计算机向目标服务器发起 DOS 攻击。攻击者先要以入侵并植 DDOS 控制软件的方式，控制大量的计算机，在需要攻击时，再通过控制台发送控制指令遥控受控计算机攻击目标。这种攻击的难点是：如何入侵大量计算机？如何管理这些计算机？一般情况下，攻击者为了快速控制大量计算机，使用网络病毒携带 DDOS 控制软件在网上传播，或者使用批量漏洞扫描软件，进行批量入侵。再设置一台 DDOS 服务器管理所有“受控计算机”。因此，防范这种攻击的方式是通过网管监控网络流量异常，发现和制止批量入侵，阻止更多的计算机被控制，并同步检测出 DDOS 服务器的 IP 地址和位置，对该服务器进行安全处理。

3 军网安全防护工作的注意事项

1) 防火墙并非万能

病毒防火墙。不能过于迷信杀毒软件。网络上是先有病毒，而且这个病毒足够“嚣张”以致被杀毒软件的病毒监测网络捕获到样本，然后工程师们从样本中提取“特征码”并导入病毒库，杀毒软件才能查杀。所以病毒总是先于杀毒软件一周或更长时间流行。一些特制的流行不广的病毒很可能逃脱监控，在杀毒软件的眼皮底下搞破坏。网络防火墙。没有攻不破的防火墙，计算机上安装的防火墙都是简单的基于 IP 规则检测的软件防火墙，阻止来自外部的非授权连接，并检测本地监听端口，判断是否存在木马程序，对计算机起到一定的保护作用，但这种保护非常有限。“端口反弹”技术可以轻松破除这种防火墙，木马程序通过“进程注入”加载到 IE 进程空间中，打着 IE 的伪装，从防火墙内部向外连接，从而顺利突破防火墙。

2) 网络安全人人有责

网络安全并不完全是管理员的事，每个人都要管好自己的计算机，不要让自己的计算机沦为攻击者的帮凶。目前网络上被成功入侵的计算机，90% 以上是用户缺乏安全意识，没有设密码、打补丁的习惯。批量扫描软件上只要设置一下要扫描的网段，不到几分钟，就能检测到大量存在问题的计算机。这些不是单靠管理员能解决的，设密码、打补丁不是很能难的技术问题，关键是用户自己要提高安全防护的意识。

3) 用好 Windows

近年来，Windows 的安全性一直被诟病，可是事实上 Windows 是一个优秀的操作系统，安全性并不差，只是没有用好它，多数人根本不知道如何进行 Windows 安全设置，对 Windows 的一些高级设置更是所知甚少。要真正用好 Windows 必须要深入掌握控制面板、组策略管理、CMD 命令行等。

4 结束语

研究表明，分析军网自身存在的安全漏洞，掌握敌方网络攻击手段，有针对性地采用军网安全防护措施，能有效阻止网络攻击，对做好军网安全防护工作意义重大。

参考文献：

[1] 连一峰, 王航. 网络攻击原理与技术[M]. 北京: 科学出版社, 2004.
[2] 沈伟锋. 面向攻击的网络漏洞扫描[D]. 西安: 西北工业大学硕士学位论文, 2004.
[3] 马闯. 军网安全漏洞检测系统的研究与实现[D]. 吉林: 吉林大学硕士学位论文, 2008.
[4] 王晓飞. 基于入侵检测技术的军网安全模型分析[D]. 哈尔滨: 哈尔滨工业大学硕士学位论文, 2008.

****

（上接第 47 页）

参考文献：

[1] 赵耿, 郑德玲, 方锦清. 混沌保密通信的最新进展[J]. 自然杂志, 2001, 23(2): 97-106.
[2] L. M. Pecora, T. L. Carroll. The Synchronization in Chaotic Systems[J]. Physical Review Letters, 1990, 64(4): 821-830.
[3] H. Nijmeijer, M. Ymareels. An observer looks at synchronization[C]. IEEE Trans on Circuits Syst I, 1997, 44(10): 882-890.
[4] 方锦清. 驾驭混沌与发展高新技术[M]. 北京: 原子能出版社, 2002: 231-239.
[5] 李华青, 罗小华, 代祥光. 一个超混沌系统及其投影同步[C]. 电子学报, 2007, 37(3): 654-657.
[6] 申敏, 刘娟. Rossler 超混沌系统的同步及其在保密通信中的应用[J]. 重庆邮电大学学报, 2009, 21(3): 372-375.
[7] 王晓燕, 瞿少成, 等. 异结构混沌系统同步及其在保密通信中的应用[J]. 计算机应用研究, 2009, 26(5): 1874-1876.
[8] 张静, 等. MATLAB 在控制系统中的应用[M]. 北京: 电子工业出版社, 2007: 137-140.
[9] 求是科技. MATLAB 7.0 从入门到精通[M]. 北京: 人民邮电出版社, 2006.