信息化战场的新成员——网络战*

赵 黎
(武汉数字工程研究所 武汉 430074)

摘 要

自3月24日起,北约对南联盟发动军事打击,这是北约成立以来第一次大规模使用海空力量,南联盟军民奋起反抗,这是一次实力悬殊的较量。这一场战争反映了高技术局部战争的一些特点,网络战首次出现在"战场"上,北约成员国遭受来自于全球范围内的计算机黑客的攻击。虽然网络战只处于低级水平,但它是未来战争中的必争之地。本文简介了在信息化战场中,网络的安全性、网络战的技术手段、网络战的特点、网络战的一些应用实例。

关键词:网络安全 网络战 信息战 病毒 黑客
中图法分类号:TP 393.08

A New Member in the Informatization Battlefield——Network War

Zhao Li
(Wuhan Digital Engineering Institute, Wuhan, 430074)

Abstract: Since 24th, March, the NATO has launched a military attack on the Yugoslavian Federation, which is the first time that the sea and air forces have been greatly used since the foundation of the NATO. The army - civilian in the Yugoslavian Federation roused for the revolt and this is a contest where the strengths of the two parties have a big gap. Some characteristics of the high - tech local warfare have been shown and the network war has made its debut on the "battlefield". The member countries of the NATO have been under attacks of the computer hackers from all over the world. Though the network war is now in the low - level stage, it will be the place of the strategic importance in the future warfare. This paper briefly introduces the network safety, the technical methods, the characteristics and some application examples of the network war in the informatization battlefield.

Key words: network safety, network war, information warfare, virus, hacker
Class number: P 393.08

1 前言

信息时代,网络已融入社会生活的各个领域,无论是生产部门、服务部门,还是政府机构,其运作都越来越依赖于无处不在的各种结构和各种规模的电脑网络。尤其是通信、管理等系统与军事系统、国家安全有着紧密联系,对这些网络系统的攻击就是对军事系统与国家安全的攻击,所有会导致损失的病毒侵袭和黑客攻击即可视为网络战争。

1999年3月24日,北约对南联盟进行武装入侵一开始,就开启了没有边界的作战空间。来自贝尔格莱德的网络黑客对北约发言人宣布北约组织用来在网上发布科索沃战况的官方站点(http://www.nato.int)进行网上攻击。美国军方称这是全球"第一次网络战争(the first cyber war)",并称目前美国最薄弱的地方就是电子空间。

* 收到本文时间:1999年7月29日

最新的科技成果、最新的技术手段总是最先为军事所用,作为未来社会发展方向的数字化、网络化技术,其军事用途应该得到我们最密切的关注。

2 网络安全

网络最大的特点就是它的开放性,网络没有国界,网络战争实际就是网络安全的战争。其主要措施:一是对防范黑客、保护计算机系统的安全技术进行研究;二是开发网络安全技术,提高国防部门等重要机构的保护水平,制定网络入侵的警报机制;三是为企业、私人机构的计算机系统安全问题组建一个信息中心;四是提高政府电脑专家对网络系统入侵事件发生后的危机处理能力。

一般地讲,讲网络安全的问题是指发生如下一些情况:对一些机要数据的窃取:对数据的非授权增、删、改;对网络系统的蓄意破坏;计算机病毒的干扰;对网络环境的意外或突然破坏,如发生火灾。发生安全事件的途径和手段主要有:窃取口令、收买有关人员、网络和计算机系统本身的漏洞或后门、鉴定出错、协议出错、信息泄漏以及拒绝服务。因此,网络安全管理应包括物理安全、访问控制、容错手段、传输安全保密性和安全管理制度等若干方面。目前用于信息安全的技术手段包括密码技术、安全控制技术和安全防范技术。

(1)密码技术

密码技术用以解决信息的保密以及信息即使被窃取了或泄漏了也不易识别的技术。它的安全机制是伪装信息,使有关人员明白其中的含义,而无关人员却无法理解。密码技术由明文、密文、算法和密钥四要素构成。明文就是原始信息,算法是明文密文之间的变换法则,密钥是用以控制算法实现的关键信息。因此密码技术的核心是密码算法和密钥。

(2)网络信息安全控制技术

· 数字签名

数字签名所解决的问题必须保证以下三点:(1)接收者能核实发送者对报文的签名;(2)发送者事后不能抵赖对报文的签名;(3)接收者不能伪造对报文的签名。目前实现数字签名的方法主要有三种:一是用公开密钥技术,二是利用传统密码技术,三是利用单向校验和函数进行压缩签名。

· 鉴别技术

鉴别技术用于证实交换过程的合法性、有效性和交换信息的真实性。它可以防止对信息进行有意修改的主动攻击,常用的方法主要有报文鉴别和身份鉴别。在对报文内容进行鉴别时,信息发送者在报文中加入一个鉴别码,并经加密后提供给对方检验。它利用人的身体的一个或几个独特方面来确保用户的真实性。如:指纹识别、视网膜扫描、声音验证、手型和签名识别等。

· 访问控制技术

访问控制技术是要确定合法用户对计算机系统资源所具有的权限,以防止非法用户的入侵和合法用户使用非权限内资源。它包括网络的访问控制技术、主机的访问控制技术、微型机的访问控制技术和文件的访问控制技术。访问控制可以起到如下作用:维护存储在计算机中的个人信息的保密性;保护公司重要信息的机密性;维护机器内信息的完整性;减少病毒感染机会,延缓感染的传播速度。访问控制的过程可以用审计的方法加以记载。如通过记录违反安全访问规定的时刻、日期以及用户活动,这在计算机的控制方面起着重要作用。

(3)网络信息安全保护技术

· 病毒防治技术

从技术上来讲,对计算机病毒的防治可以通过如下途径;一是在服务器上装载防病毒模块;二是软件防治,定期或不定期地用防毒软件检测计算机,三是在计算机上插防病毒卡,四是在网络接口卡上安装防病毒芯片。

· 防火墙技术

防火墙技术是一种使用很广泛的网络安全技术。顾名思义,防火墙是用来阻挡外部火情影响内部网络的屏障。

防火墙的职责就是根据本单位的安全策略,对外部网络与内部网络交流的数据进行检查,符合的予以放行,不符合的拒之门外。它的实现通常是基于"包过滤"。只有满足访问控制标准的数据包才被转发到相应的目的地出口端,其余的则被删除。防火墙只能起阻截来自外部网络的侵扰,对于内部怀有恶意的工作人员却不产生防御作用。因此,不能完全依赖防火墙来保护网络的安全,应采取包括其它技术,如加密、监控、保密手段在内的综合性安全措施。

· 信息泄漏防护技术

长期以来,计算机系统一直存在着四个脆弱性,即处理器、通讯线路、转换设备和输出设备的辐射问题。计算机在运行时,电磁辐射信号不但频谱成份丰富且携带信息,从而对信息的安全性造成威胁。美国安全局制订了有关的测试与鉴定"瞬时电磁脉冲辐射标准",它是保证信息不泄漏的标准。具体防护方式有两种:设备级防护和系统级防护,其中系统防护是对整机加以屏蔽,防止信号的各种辐射。

3 网络战争的技术手段

网络战争的技术手段主要包括黑客(远程控制/管理)、计算机病毒及软硬件后门/陷阱等。计算机网络是信息化作战的神经系统,一旦遭到破坏,整个作战体系就将全面瘫痪。

(1)黑客攻击

黑客攻击实际上是一种远程系统管理,入侵系统后的黑客像网络管理员一样具有一定的网络特权,可对系统配置、单台计算机设置进行控制、破坏或在系统中潜伏下来以窃取资料、数据。此外,黑客还可在被入侵系统中隐藏一些特定的程序,一般称为"逻辑炸弹"。作战时,将逻辑炸弹(计算机病毒软件)输入敌方网络,病毒能在预定的时间内"苏醒"过来,进行"爆炸性"的繁衍,大量的病毒开始迅速"吞噬"计算机中的各种数据和信息,使计算机网络处于一种混乱不堪的无序状态之中,整个系统将失去控制。

(2)计算机病毒攻击

计算机病毒是一种使用方便的"软杀伤"手段,计算机病毒作为一种不经授权即可执行的特殊程序具有下列特征:

传染性 计算机病毒通过各种渠道从已被感染的计算机扩散到未被感染的计算机,在某些情况下造成被感染的计算机工作失常甚至瘫痪;

隐蔽性 病毒一般是具有很高编程技巧、短小精悍的程序,通常附在正常程序中或磁盘较隐蔽的地方,也有个别的以隐含文件形式出现,如果不经过代码分析,病毒程序与正常程序不容易区别开来;

潜伏性 大部分病毒感染系统之后一般不会马上发作,它可长期隐藏在系统中,只有在满足其特定条件时才启动其表现(破坏)模块,并进行广泛传播;

破坏性 任何病毒只要侵入系统,都会对系统及应用程序产生程度不同的影响,轻者会降低计算机工作效率,占用系统资源,重者可导致系统崩溃;

软硬件后门/缺陷(Trap door/Chipping)是指计算机产品在设计开始时有针对性和无针对性设置的安全缺陷,在系统入侵时被利用。

目前,计算机病毒已多达 7000 余种,按性质可分为六种类型:

(1)"定时炸弹"型。这种病毒进入敌方计算机系统内,并不影响敌方计算机系统的正常工作,待到预定时间或特定事件发生时,便突然起破坏作用,毁坏其内存的作战数据或破坏系统正常运行。

(2)暗杀型。它是专门用来销毁敌方特定的一份文件或一组文件,并且不留任何痕迹。

(3)强制隔离型。这种病毒能自动关机,中断计算机工作,迫使敌方计算机系统陷入瘫痪,无法发挥整体效能。

(4)超载型或复制型。这种病毒进入敌方电子计算机系统后,便可大量复制、加长,覆盖其作战数据和文件,大量占据计算机系统内存,使其超载而不能工作。

(5)间谍型。这种病毒能按命令寻找指定的作战数据、信息和文件,并将它们转发到指定地点,从而窃取敌方有用信息。

(6)矫令型。这种病毒可有意错报敌方下达的命令,扰乱敌方的行动使敌军不战自乱,甚至可使敌方某些智能武器反戈一击。

4　网络战争的特点

随着计算机网络技术的迅速发展及在军事上的应用,未来战场将是一个由众多计算机通过有线或无线等方式,把陆、海、空、天、电等诸领域的基本作战单元连接在一起而形成的网络世界。敌对双方在网络上的斗争将构成战争的主要内容。它们主要有以下一些特点:

首先网络在军事上的地位和作用日益加强,从 C^3I 到 C^4ISR 的每个环节无不与计算机、计算机网络有着密不可分的联系。其次,网络战争易攻难守,网络是一个庞杂的系统工程,系统本身存在许多缺陷和弱点;网络又是一个整体,一点受损可致使整个网络受到不同程度的影响。系统的庞大和技术的复杂使网络的安全性不易得到保证。另一方面,网络协议、网络技术和计算机软硬件技术的通用性、公开性又使网络缺陷更进一步暴露在入侵者面前。因为隐蔽性正是黑客攻击的核心原则。第三,对社会经济影响巨大。知识经济将主导 21 世纪,技术的可靠性将直接影响社会经济的正常运作。第四,网络是一种新的媒体,网络安全事件对国家、社会的影响力日渐增强。第五,网络战争是一个持久战。大量的黑客组织、电脑狂人的积极活动无时无刻不对网络安全构成真实的威胁。第六,网络战争是一种资源消耗战。无论多么强大的网络服务器、网络组织,它们的负载总是有限的。第七,整体技术上的优劣并不能完全决定网络战争的胜负。第八,新技术的不断发展使网络攻击手段日新月异,危害程度不断深化。

今天,网络更多地被认为是一种通信工具,但随着网络安全攻守形势的进一步演化,网络本身将既是一个新战场又是一个新武器,既是一种进攻武器又是一种防御武器。我们应该将网络作为一个武器系统而积极开展相关的情报研究,同时进一步探讨网络安全保障的问题。

5　网络战争的发展态势

21 世纪的战争是不分疆界的立体信息战,信息化的战场就是打"网络",谁控制了"网络",谁就拥有战场的主动权。网络战将改变今后战争的形式。将是一场看不见流血,听不见撕杀的较量。网络战今后的发展更具有:

(1)战略威慑

运用网络战的目标不仅限于攻击敌方的军用计算机网络,破坏和控制敌方军事指挥和控制系统,同时亦可以攻击敌方国家的经济、民用计算机网络,破坏和控制整个社会的信息系统,直接威胁一个国家、一个民族乃至全社会的生存与发展。而网络入侵行动不再是指传统意义上的"越境行动",网络战将成为今后另一种新的战略威慑手段。

(2)以"劣"胜优

在未来的网络战中,并非总是大国、强国占上风,发达国家的风险会更大。其原因有两方面:其一,由于在发达国家中信息化程度高,网络的应用已经极其广泛,这使得发达国

家遭受网络战攻击的可能性更大,其二,由于研究网络攻击的手段和方法只需很少的人力和物力,而研究防范的手段和措施则要困难得多,这种易攻难防的特点,使得任何国家在未来战争中都将难以避免网络战的攻击。从一定意义上讲,这也为以"劣"胜"优"创造了新的条件。

(3)全民皆"兵"

网络战使未来战争的社会性更加突出。任何一个熟悉计算机及网络知识的公民都有可能参与并发挥无法估量的作用。近年来活跃于西方计算机网络数以万计的"电脑黑客"中,真正的军事人员和间谍微乎其微,不难想象,一旦进入战争状态将会有更多的人参加进来,直接为军方服务。未来网络战将有可能成为全民皆"兵"的战场。

在科索沃战争中,美国和北约超过上千个网站被黑。攻击中亲南黑客使用了一些很先进的黑客软件工具。这种软件可以让电脑自动扫描一些特定的网络区域,自动找出一些网站的后门,然后从不同路径潜入,"大闹天宫"。导致北约服务器(http://www.nato.org)过载,一度瘫痪。4月4日,计算机病毒使北约的通信系统一度陷入瘫痪,美海军陆战队所有作战单元的电子邮件服务器均被阻塞。尽管攻击手段比较原始,也使北约遭受了巨大损失。[因特网1999年6月19日]报道,位于美国圣迭哥市的"太空及海上系统战中心"网络受到俄罗斯黑客的攻击,他们突破网络防线之后,侵入网络打印机,修改了路由表,把打印文件送往俄罗斯的服务器。黑客攻击的手段归纳起来主要有:通过"PING"命令,向北约计算机网络发送成千上万空数据包和电子邮件(称为"PING炸弹"),使服务器阻塞;用"梅利莎"、"爸爸"病毒和"宏"病毒等,影响计算机正常操作,甚至使用户的机密文件外泄;绕开网络安全保护系统,针对系统缺陷进行攻击。

我们可以想象,如果敌方以网络战作为一种极其有效的"软"攻击武器,使用了真正凶险的手段,其后果如何呢?

6 结束语

信息网络是战场信息化的基础,离开了它,信息化战场就是无源之水,无本之木。在科索沃战争中互联网络突破了传统意义上的信道,成为作战能量迸发出强大"催化剂"。人们发现目前还没有任何国家或组织能够达到美国常规武器所具有的优势。而信息入侵活动比传统的武装攻击形式更具有吸引力。网上入侵活动可使国内外黑客的破坏活动得逞,他们自己却不会受到任何伤害,而且很难被抓住。他们可以是分散的,也可以是有组织的利用互联网络采取协同行动,同时对力量强大的敌人在实施某项行动的关键时刻进行攻击,扰乱其计划。因此,计算机网络攻击与防御手段将引起各国的高度重视。

未来战争中计算机病毒、网络"蠕虫"、"特洛伊木马"程序、逻辑炸弹、计算机陷阱等软杀伤手段对网络系统、计算机软件和硬件设备的破坏将令人防不胜防。威胁预警、多层防御、安全防火墙等技术及对付"黑客"入侵都将是我们今后研究的重要内容。今后信息化战场上的网络之争势必对战争的胜负产生巨大的影响。

参考文献

[1]齐振恒,科索沃危机中的计算机战,现代军事,1999.6

[2]张书杰、苏剑飞,信息化战场矛盾面面观,现代军事,1999.4

[3]邹泉,网络战争初现端倪,舰船技术经济简报,1999.10

[4]刘炳华,网络信息系统的技术攻击及其安全对策,中国国防科技信息部,1997.3

[5]顾伟德,试论战争活动中的信息对抗,中国国防科技信息,1998.6

[6]池建文、邹泉,北约入侵南联盟战事剖析,现代军事,1999.6