

基于.Net的军队计算机网络信息安全对策

赵昌伦, 武 波

(西安电子科技大学 计算机学院, 陕西 西安 710071)

摘 要:随着我军信息化建设步伐的不断加快, 计算机网络技术在部队的应用日趋广泛。但从整体情况看, 我军的网络信息安全还存在很多问题, 网络安全工作明显滞后于网络建设。针对现阶段军队网络安全存在的问题, 从 Web 服务器、数据库管理、程序源代码、网络数据传输和网络安全管理方面提出了相应的解决对策。对当前我军计算机网络安全的发展和把握未来战争形态具有十分重要的意义。

关键词: Web; 计算机网络; 安全; 对策

中图分类号: TP393.08

文献标识码: A

文章编号: 1673-629X(2009)01-0150-04

Information Security Countermeasures of Army Computer Networks Based on .Net

ZHAO Chang-lun, WU Bo

(School of Computer Science, Xidian University, Xi'an 710071, China)

Abstract: With our military's the pace of construction information accelerate, computer network technology in the military application has got increasingly widespread. However, the overall situation, the army's network information security there are still many problems, network security has lagged far behind in the network construction. At this stage the army against the network security issues, from Web servers, database management, source code, network data transmission and network security management, presented the corresponding countermeasures. On the current computer network security of our military construction and development and grasp the future form of war is of great significance.

Key words: Web; computer network; security; countermeasure

0 引 言

随着部队信息化建设的快速发展和计算机网络在部队的广泛应用, 计算机网络信息的安全问题变得日益突出和重要。就目前现状, 军队计算机网络安全主要存在信息安全技术落后、信息安全管理制度不完善、计算机网络安全防护能力较弱、兵的信息安全意识淡薄。这些安全隐患问题如果不能很好解决, 不但会引起军队大量泄密事件和网络被攻击事件的发生, 更会严重影响到作为高科技作战辅助手段的计算机网络技术在军队信息化建设中的推广和应用, 甚至会成为我军未来信息化战争中的“死穴”, 直接影响战争的结果。为此文中首先分析现阶段我军的网络安全存在的问题, 并结合作者参与的 Web 开发项目(西安移动通信

11185 呼叫业务系统, 以 .Net 为平台), 从 Web 服务器、数据库管理、程序源代码、网络数据传输和网络安全管理方面, 对基于 Web 的军队网络安全进行探讨。

1 军队计算机网络信息安全存在的问题

1.1 计算机网络安全技术问题

(1) 缺乏自主的计算机网络软、硬件核心技术。我国信息化建设缺乏自主的核心技术支撑, 计算机网络的主要软、硬件, 如 CPU 芯片、操作系统和数据库、网关软件大多依赖进口。信息设备的核心部分 CPU 由美国和我国台湾制造; 我军计算机网络中普遍使用的操作系统来自国外, 这此系统都存在大量的安全漏洞, 极易留下嵌入式病毒、隐性通道和可恢复密钥的密码等隐患; 计算机网络中所使用的网管设备和软件绝大多数是外来品, 在网络上运行时, 存在着很大的安全隐患。这使军队计算机网络的安全性能大大降低, 网络处于被窃听、干扰、监视和欺诈等多种安全威胁中, 网络安全处于极脆弱的状态。

收稿日期: 2008-05-26

基金项目: 国家部委重点基金项目(9140A24070106DZ01)

作者简介: 赵昌伦(1977-), 男, 云南文山山人, 硕士研究生, 研究方向为软件设计与理论、网络安全; 武 波, 博士, 教授, 硕士生导师, 研究方向为软件设计与理论、计算机网络技术等。

(2)长期存在被病毒感染的风险。现代病毒可以借助文件、邮件、网页等诸多方式在网络中进行传播和蔓延,它们具有自启动功能,常常潜入系统核心与内存,为所欲为。军用计算机一旦受到感染,它们就会利用被控制的计算机为平台,破坏数据信息,毁损硬件设备,阻塞整个网络的正常信息传输,甚至造成整个军队计算机网络数据传输中断和系统瘫痪。

(3)军事涉密信息在网络中传输的安全可靠性低。隐私及军事涉密信息存储在网络系统内,很容易被搜集而造成泄密。这些涉密资料在传输过程中,由于要经过许多外节点,且难以查证,在任何中介节点均可能被读取或恶意修改,包括数据修改、重发和假冒。网络中可能存在某节点在非授权和不能监测方式下的数据修改,这些修改进入网中的帧并传送修改版本,即使采用某些级别的认证机制,此种攻击也能危及可信节点间的通信。

(4)存在来自网络外部、内部攻击的潜在威胁。网络中一台无防备的电脑很容易受到局域网外部的入侵,修改硬盘数据,种下木马等。入侵者会有选择地破坏网络信息的有效性和完整性,或伪装为合法用户进入网络并占用大量资源,修改网络数据、窃取、破译机密信息、破坏软件执行,在中间站点拦截和读取绝密信息等。在网络内部,则会有些非法用户冒用合法用户的口令以合法身份登录网站后,查看机密信息,修改信息内容及破坏应用系统的运行。有些非法用户还会修改自己的IP和MAC地址,使其和合法用户IP和MAC地址一样,绕过网络管理员的安全设置。

1.2 网络安全管理问题

在军队网络建设中,高投入地进行网络基础设施建设,而相应的管理措施却没有跟上,在网络安全上的投资也是微乎其微。有些领导错误地认为,网络安全投资只有投入却不见直观效果,对军队教育训练影响不大。因此,对安全领域的投入和管理远远不能满足安全防范的要求。而且安全上出了问题,又没有行之有效的措施补救,有的甚至是采取关闭网络、禁止使用的消极手段,根本问题依然得不到实质性的解决。

国家和军队出台了系列信息网络安全保密的法规,如:《中华人民共和国计算机信息系统安全保护条例》、《计算机信息网络国际联网安全保护管理办法》、《中国人民解放军计算机信息网络国际联网管理暂行规定》等,这此法规的出台从一定程度上规范了军事信息网络安全的管理,但还不能满足军事信息网络安全管理的发展需求。网络运行管理机制存在缺陷,军队网络安全管理人才匮乏,安全措施不到位,出现安全问题后缺乏综合性的解决方案,整个信息安全系统在迅

速反应、快速行动和预防等等方面,缺少方向感、敏感度和应对能力。在整个网络运行过程中,缺乏行之有效的安全检查和应对保护制度。

网络管理和使用人员素质不高、安全意识淡薄。据调查,目前国内90%的网站存在安全问题,其主要原因是管理者缺少或没有安全意识。军事计算机网络用户飞速增长,然而大多数人员网络知识掌握很少,安全意识不强,经常是在没有任何防范措施的前提下,随便把电脑接入网络;在不知情的情况下将带有保密信息的计算机连入因特网,或使用因特网传递保密信息;对数据不能进行及时备份,经常造成数据的破坏或丢失;对系统不采取有效的防病毒、防攻击措施,杀毒软件不能及时升级。

2 军队网络安全对策

基于军队存在的网络安全问题,加强军队网络安全的总体对策是在技术层建立完整的网络安全解决方案,在管理层制定和落实严格的网络安全管理制度。

2.1 网络安全技术对策

2.1.1 Web服务器安全对策

为了让客户访问Internet,Web服务器须是Internet的任何接入点都可访问的,因此Web服务器安全保障要求很高。当今服务器安全问题主要有:a.服务器向客户提供了不应该提供的服务;b.服务器把本应私有的数据放到了可公开访问的区域;c.服务器信赖了来自不可信赖数据源的数据^[1]。

据此,提出以下解决方案:

(1)增强服务器操作系统的安全性。GB17859-1999《计算机信息系统安全保护等级划分准则》,将计算机信息系统安全保护划分为五个等级。目前使用的Windows操作系统安全等级普遍只在第一级和第二级,无法有效地防堵黑客和病毒的入侵。通过系统内核软件加固的操作系统,可使安全级别提升到国家标准GB17859的第三级,相当于解放军信息安全产品B级标准。美国国防部技术标准把操作系统安全等级分为D1, C1, C2, B1, B2, B3, A级,安全等级由低到高。目前主要的操作系统等级为C2级,在使用C2级系统时,应尽量使用C2级的安全措施及功能,及时安装系统及软件的最新补丁,建立良好的账号管理制度,使用足够安全的密码口令,并正确设置用户权限。对Web服务器进行安全配置,删除或关闭无用的或不必要的服务,只保留必要的服务,因为启用不必要的服务可能使他人获得大量的系统信息,甚至获取密码文件。对服务器进行远程管理时,使用如SSL等安全协议,避免使用Telnet、FTP等程序,因为这些程序是以明文形

式传输密码的,容易被监听;并严格控制远程 Root 身份的使用,仅在绝对需要时才允许使用具有高授权的操作。禁止或限制 CGI 程序和 ASP、PHP 脚本程序的使用。因为某些脚本程序本身存在安全漏洞,会给系统带来安全隐患。在极端重要的系统中,应采用 B 级操作系统。

(2)安装防病毒软件和防火墙。在主机上安装防病毒软件,能对病毒进行定时或实时的病毒扫描及漏洞检测,变被动清毒为主动截杀,既能查杀未知病毒,又可对文件、邮件、内存、网页进行实时监控,发现异常情况及时处理,在网关和服务器上使用多层次的防病毒系统,针对允许上传和交互信息发布的服务器,关键是防止病毒和木马程序的侵入。防火墙是硬件和软件的组合,它在内部网和外部网间建立起安全网关,过滤数据包,禁止某些地址对服务器的某些服务的访问,并在外部网络和 Web 服务器中建立双层防护,将服务器中没有必要从防火墙外面访问的服务和端口阻隔,进一步增强开放服务的安全性。它能够控制网络进出的信息流向,提供网络使用状况和流量的审计、隐藏内部 IP 地址及网络结构。它还可以帮助军队系统进行有效的网络安全隔离,通过安全过滤规则严格控制外网用户非法访问,并只打开必需的服务,防范外部来的非法服务攻击。同时,防火墙可以进行时间安全规则变化策略,控制内网用户访问外网时间,并通过设置 IP 地址与 MAC 地址绑定,防止目的 IP 地址欺骗。更重要的是,防火墙不但将大量的恶意攻击直接阻挡在外面,同时也屏蔽来自网络内部的不良行为,让其不能把某些保密的信息散播到外部的公共网络上。

(3)安装入侵检测系统和网络诱骗系统。入侵检测能力是衡量一个防御体系是否完整的重要因素。入侵检测的软件和硬件共同组成了入侵检测系统。强大的、完整的入侵检测系统可以弥补军队网络防火墙相对静态防御的不足,可以对内部攻击、外部攻击和误操作进行实时防护,当军队计算机网络和系统受到危害和恶意访问之前进行报文拦截、阻断、报警等响应,为系统及时消除威胁。网络诱骗系统是通过构建一个欺骗环境真实的网络、主机,或用软件模拟的网络和主机,诱骗入侵者对其进行攻击或在检测出对实际系统的攻击行为后,将攻击重定向到该严格控制的环境中,从而保护实际运行的系统;同时收集入侵信息,借以观察入侵者的行为,记录其活动,以便分析入侵者的水平、目的、所用工具、入侵手段等,并对入侵者的破坏行为提供证据。

2.1.2 使用数据加密技术

对军事涉密信息在网络中的存储和传输可以使用

传统的数据加密技术和新兴的信息隐藏技术来提供安全保证。在传发保存军事涉密信息的过程中,不但要用加密技术隐藏信息内容,还要用信息隐藏技术来隐藏信息的发送者、接收者甚至信息本身。通过隐藏术、数字水印、数据隐藏和数据嵌入、指纹等技术手段可以将秘密资料先隐藏到一般的文件中,然后再通过网络来传递,提高信息保密的可靠性。

数据加密技术中,文中提出了以下解决方案:

(1)对数据库加密。为了保障数据的完整性、安全性、灾难可恢复性,防止非授权用户窃取、篡改数据,一般采用安全管理、存取控制、数据库备份和数据库加密等方法^[2]。在现有的复杂关系型数据库系统中,要实现数据库加密,较好的方法是对数据库内字段加密,以保护敏感数据。在多种加密算法中可根据系统所需的要求选择不同算法。例如:为了保护用户口令,防止管理员有太大的权限而危及客户的信息安全,可以使用 Hash 函数对用户口令进行散列处理,由于 Hash 函数是单向不可逆的,因此此方法对客户信息十分安全,但这种方法也有不足之处,一旦用户遗失密码,管理员无法恢复其密码。对于其他类型的敏感信息的加密,常使用非对称密钥加密法,因为信息在使用时必须还原。实现数据库加密后,各用户(或用户组)的数据由用户用自己的密钥加密,数据库管理员获得的信息则无法进行正常脱密,从而保证了用户信息的安全。

(2)对数据库连接字符串进行加密。虽然 .Net 的 Code-behind 技术在系统配置中禁止了对 .vb 之类的源代码下载,但是在服务器中的程序源代码还是可以被查看。这样代码中的一些机密信息有可能泄漏,需对源码进行一定的技术处理。最简单的方法就是用加密软件进行加密,但事实上许多代码根本没必要加密,且加密软件无法加密中文,最常见和最重要的是,对数据库连接字符串和一些机密设置进行加密。Web 程序需要一个数据库连接字符串来连接数据库,这个字符串包含要连接数据库的实例名、用户名和密码等。如该信息被攻击者取得,系统将完全掌握在攻击者手中,数据库连接字符串常以明文保存在 Web.Config 中,这样显然不安全。故采用微软的 DPAPI(Data Protection API)来对数据库连接串进行加密处理。

(3)使用 MD5 + DES 算法加密局域网内部传输数据。在局域网内部使用 MD5 + DES 的方式加密用户登录信息,登录成功后使用用户的 DES 密钥来加密进行传输数据和文件。具体算法是:在数据库中用一个字段专门存放客户的通信密钥,用于客户与服务器的通信加密。在登录时使用 MD5 算法加密用户登录口令,然后与数据库中相关字段进行比较,若相同,

则判为合法用户,读出该用户的DES对称密钥,与用户进行通信,否则导向异常处理界面^[3,4]。

(4)使用加密通信协议(SSL)保证数据在广域网中的安全传输^[5]。安全套接层协议(secure socket layer, SSL)是一种国际标准的加密及身份认证通信协议,它基于CA根证书与客户端证书的交叉验证,从而使客户机服务器应用一种不能被窃听的方式通讯。通讯双方享受了SSL服务之后两台主机之间就建立起一条安全的、可信的通讯通道。使用Windows 2K Server + IIS^[6]配置SSL服务。配置SSL之前,系统必须安装DNS、Active Directory和IIS服务。

(5)使用安全路由器和虚拟专用网技术。安全路由器采用了密码算法和加/解密专用芯片,通过在路由器主板上增加安全加密模块来实现路由器信息和IP包的加密、身份鉴别和数据完整性验证、分布式密钥管理等功能。使用安全路由器可以实现军队各单位内部网络与外部网络的互联、隔离、流量控制、网络和信息安全维护,也可以阻塞广播信息和不知名地址的传输,达到保护内部信息与网络建设安全的目的。目前我国自主独立开发的安全路由器,能为军队计算机网络提供安全可靠保障。建设军队虚拟专用网是在军队广域网中将若干个区域网络实体利用隧道技术连接成一个虚拟的独立网络,网络中的数据利用加/解密算法进行加密封装后,通过虚拟的公网隧道在各网络实体间传输,从而防止外部未授权用户窃取、篡改信息。

2.2 网络安全管理对策

(1)强化思想教育、加强制度落实是网络安全管理工作的基础。搞好军队网络安全管理工作,首要的是做好人的工作。军官、兵要认真学习军委、总部先后下发的有关法规文件和安全教材,更新军事通信安全保密观念,增强网络安全保密意识,增长网络安全保密知识,提高网络保密素质,改善网络安全保密环境。还可以通过举办信息安全技术培训、组织专家到基层部队宣讲网络信息安全保密知识、举办网上信息战知识竞赛等系列活动,使广大官兵牢固树立信息安全领域没有“和平期”的观念,在每个人的大脑中筑起军队网络信息安全的“防火墙”。

(2)制定严格的信息安全管理制度。设立专门的信息安全管理机构,人员应包括领导和专业人员。按照不同任务进行分工以确立各自的职责。哪类人员负责确定安全措施,包括方针、政策、策略的制定,并协调、监督、检查安全措施的实施;另类人员负责分工具体管理系统的安全工作,包括信息安全管理、信息保密员和系统管理员等。在分工的基础上,应有具体的负责人负责整个网络系统的安全。确立安全管理的原则:

一是多人负责原则,即在从事某项安全相关的活动时,必须有两人以上在场;二是任期有限原则,即任何人不得长期担任与安全相关的职务,应不定期地循环任职;三是职责分离原则,如计算机的编程与操作、机密资料的传送和接收、操作与存储介质保密、系统管理与安全管理等工作职责应当由不同人员负责。另外,各单位还可以根据自身的特点制定系列的规章制度。如要求用户必须定期升级杀毒软件,定期备份重要资料,规定军用计算机不得随意安装来路不明的软件,不得打开陌生邮件,对违反规定的进行处理等等。

(3)重视网络信息安全人才的培养。加强计算机网络指挥人员的培训,使网络指挥人员熟练通过计算机网络实施正确的指挥和对信息进行有效的安全管理,保证部队的网络信息安全。加强操作人员和管理人员的安全培训,主要是在平时训练过程中提高能力,通过不间断的培训,提高保密观念和责任心,加强业务、技术的培训,提高操作技能;对内部涉密人员更要加强人事管理,定期组织思想教育和安全业务培训,不断提高人员的思想素质、技术素质和职业道德。积极鼓励广大官兵研究军队计算机网络攻防战的特点规律,寻找进入和破坏敌方网络系统的方法,探索竭力阻止敌方网络入侵,保护己方网络系统安全的手段。只有拥有一支训练有素、善于信息安全管理队伍,才能保证军队在未来的信息化战争中占据主动权。

3 结束语

随着网络应用的不断深化,技术手段的日趋成熟,基础平台的持续开放,要适应越来越严格规范的信息安全需求,必须有更新的安全策略来确保网络信息的安全。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,对于保障军队网络信息的安全性将变得十分重要。

参考文献:

- [1] 朱铁锋,徐永晋.如何构造安全可靠的Web数据库应用系统[J].微计算机信息,2000(12):13-15.
- [2] 朱鲁华,陈荣良.数据库加密系统的设计与实现[J].计算机工程,2002,28(8):61-63.
- [3] 段刚.加密与解密[M].北京:电子工业出版社,2003:45-47.
- [4] 卢开澄.计算机密码学[M].北京:清华大学出版社,1998:130-136.
- [5] 孔静萍.Internet的安全通信协议SSL与SET的剖析和比较[J].现代计算机,2000,89(4):40-42.
- [6] Tulloch M. IIS6 管理指南[M].北京:清华大学出版社,2004:278-285.