涉密计算机信息系统网络安全监控技术的运用

何美丽
（胜利油田豪威科工贸有限责任公司，山东　东营　257000）

【摘　要】随着全球信息化进程的加快，包括计算机、网络在内的现代科技已经越来越渗透到人们的日常生活中。但近几年来，由于自然灾害、黑客攻击等因素，计算机信息系统遭受了严重的威胁。涉密计算机是保障国家机密的重要手段，因此，如何提升涉密计算机的安全性，并对其进行全方位的监测，已是众多科研人员的研究热点。基于此，本文分析了涉密计算机信息系统中影响其安全性的因素，对涉密计算机信息系统网络安全监控系统功能设计进行了研究，阐述了其技术的应用。

【关键词】涉密计算机信息系统；网络安全；监控技术

引言：

目前，针对网络涉密终端信息泄露的问题，通常采取的措施是通过审计、查杀主机中的潜在病毒等。尽管上述措施可以有效地保障网络中的信息安全，但也会带来系统运行负荷的增大，以及对一些高度隐蔽性的病毒的识别不准确等问题。以涉密计算机信息系统为研究对象，分析网络安全监控方法，以突破现有安全管控手段的不足，为进一步提升我国涉密网络的安全性提供理论依据。

一、涉密计算机信息系统中影响其安全性的因素

涉密计算机主要指的是用于采集、加工、输出和存储涉及国家机密信息的计算机。近几年来，由于计算机技术的飞速发展，涉密计算机已在全球范围内大量使用。通过对涉密计算机信息系统网络安全性的研究，归纳出了影响涉密计算机信息系统网络安全性的因素 主要包括自然因素以及人为因素。

自然因素是指由于自然灾害、自然灾害或环境扰动等原因对信息系统的安全构成了威胁；而人为因素则是由人的操纵所致，可将其划分为主动与被动两类。其中，主动攻击是指通过各种方法或方法来篡改、删除或伪造信息。而非主动攻击就是在不影响系统正常运行的前提下，截取或破解系统中的有关信息。实践证明，当前对涉密计算机信息系统的安全构成了严重的威胁，其中包括计算机病毒、黑客攻击和不正当的网络信息。计算机病毒是指使用人工编写的系统病毒，将其复制到其他的程序中，从而对系统造成伤害。计算机黑客的手段就是盗取系统的密码后侵入到计算机里，进行一些违法的活动。

二、涉密计算机信息系统网络安全监控系统

涉密计算机信息系统网络安全监控系统包括三个部分，即：局域网服务端、本地机数据库以及安装在每个计算机上的客户端程序。

系统运行时，首先在局域网中选定一台计算机做主机，然后将服务器端的软件安装到主机上；局域网中的其他机器也各自安装相同的客户端软件，以确保它们之间的兼容性。另外，按照计算机网络的运作模式可以划分为域模式与工作组模式两大类。在域模式中，主机和备份控制器采用相同的存取控制策略，通过 Modem 实现拨号控制，移动存储媒体控制，网络探测等功能；在工作组模式中，由主控台对接入控制策略进行统一配置，并向其他备份控制器分配策略。

三、涉密计算机信息系统网络安全监控系统功能设计

（一）移动硬盘控制

对 U 盘、移动硬盘等介质实行“双控”：对未登记的移动媒体，不能进行身份认证且不能使用；只有在被授权的计算机上才能使用在这个系统中登记的移动媒体。

以移动式硬盘为例子，它的控制过程包括：1. 把移动式硬盘接入计算机后取得可携式磁盘的使用许可，并判定是已登记还是被禁用。不管是已登记或禁用的移动式磁盘，都必须打开检测线程。2. 判定有无添加新的设备；若发现有新的硬件存在，那么就进行对此硬件种类的判定。若获得驱动程序可删除，则表示新的硬件是可移动磁盘。3. 在对移动式硬盘中的全部档案进行扫描后，若已登记，可读出其登记代码，判定其合法性。在法律允许的情况下，执行能被正确利用的文件操作监视过程；相反，若非法，可将移动式硬盘锁住，并向计算机接口发出警报。4. 当移动硬盘被取下，或由管理员使用相应的权限进行权限解锁操作时，被锁住的可移动硬盘将会被自动解除。

（二）查看程序运行记录

这个功能可以保存计算机从开机开始到关闭期间的全部动作记录，例如网页浏览，文件浏览等。在用

户端创建一个窗口捕捉钩子，并在每一次启动后都会自动执行。每次开启一个新的视窗或使用者做其他动作，都会自动抓取作业，并且会产生标题，程序运行记录档案会储存在数据库，供使用者查阅。其具体实施过程为：1. 系统会在系统启动时将 Hook 函数的类型为 WH_SHELL。2. 判定 hook 功能的运算型参数 m。若 m<0，表示该窗口程序是无效的，必须选择其他类型的 hook 功能，然后再进行判定；若 m>0，表示该视窗程式是一个合法的视窗程式，它会读取视窗的名称及动作种类，并且会自动记录目前的视窗名称。3. 对局部使用进行确认，若有使用许可，将该软件的执行记录作为局部日志进行存储；当没有权限限制时，将钩子卸载。

（三）无线调制解调器上网控制

为了对计算机网络进行实时动态监测，设计基于无线调制解调器的网络远程监控系统。这一功能能够定期地对用户请求接入互联网进行检查，当客户端发出接入请求时会对用户具有接入调制解调器的权限进行判定，并对其进行了无拨号连接的操作。若无授权或调制解调器有拨号上网的动作，应立即中断网络，并发出警报讯息给系统管理者。无线调制解调器接入控制的具体步骤为：1. 在开启 Modem 线程之后查看有无要求接入无线网，若无新要求，反复进行该过程，直至收到新的要求为止。2. 当侦测到有一个与无线网络相连的要求时，判定该连接特性与 Internet_Connection_Modem 相符。若满足就接受此要求，并在接入调制解调器之后顺利地接入网络；若否，此要求将被终止，并回到原来的程式，并持续侦测是否有新网络连接要求。

（四）TCP/IP 通信

用户端和服务器通过 Socket 来进行通信，并且按照 TCP/IP 通信方式进行数据交互。IP 是一种具有连通性的协议，它可以避免数据阻塞和响应时延，并且可以实现数据的非复制，从而加快通信速率。针对这一问题，针对用户端与服务端非对称分布的特点，在用户端与服务器端分别使用 SOCKET（）功能，以增强系统的协调能力。当一个连接被创建之后，用户端与服务器端可以通过 accept（）函数和 listen（）函数功能来实现对信息的传输与接收。

在客户端中，当 SOCKET 被建立之后，就建立了多路传输的特性（Sock_Stream）。调用 ACCEPT（）函数，并等候收到的数据。定期更新，直至接收到新的数据。读取数据和分析特性代码。在服务器上也会建立 COCKET，并判定连接是否顺利。在没有成功的情况下重新连接；当连接被完成时将会被传送到服务器并且等候回应指令。当出现新的回复指令时，判定是否为本系统 = 指令，若是，读取和写入数据；否则，指令将被忽视，然后再次启动等熵过程。

四、涉密计算机信息系统网络安全监控技术

计算机安全监控系统不仅具有实时性、可靠性和安全性等基本特性，而且对于其他计算机信息系统也具有一定的借鉴意义。用户登录安全增强技术、加密技术、授权和控制技术、存储介质控制技术、防火墙技术、入侵检测技术、认证技术等是当前常用的计算机网络安全监控技术，越来越多地被用于涉密计算机信息系统。

（一）用户登录安全增强技术

通过使用“USBKEY+ 动态密码”的登录方法，有效地保证了用户的安全登录，有效地防范了恶意入侵。在此基础上，利用动态密码技术对未登录的非 KEY 账号进行标识，对未登录的非 KEY 账号进行重新登录时将自动启动安全机制，对其进行拒绝，避免其在短期内进行大规模的恶意访问。而那些被标注为非 KEY 账号的账号，就算是使用系统管理员的权限也不可能将其解锁。

（二）加密技术

加密技术是当前实现大规模互联网数据传输的重要手段，也是实现数据安全监控的关键，对保障网络数据的安全性起到了非常重要的作用。在这些应用中，按照加密技术的目标可分为面向业务的加密技术和面向网络的加密技术。对于业务的加密是一种信息加密，它的核心就是对一些重要的程序或是对文件中的敏感数据进行加密，必须采用比较完备的密码算法来进行运算，还必须采用密文式的存储方法，这样可以增强整个加密的整体性能，有着更好的监控效果。但是对于网络的加密技术并没有什么苛刻的要求，网络所采用的密码也就是所谓的通信协议密码，它的核心就是对通信中所含有的数据进行加密，常用的有数位签字、侦测等，这既能防止黑客的介入又能提升网络数据的安全与可靠度。

（三）授权和控制技术

传统的计算机主机对网络的监视是根据 IP 地址进行的，因此，有些犯罪分子可以利用 IP 地址来躲避检查，给网络的安全性带来了很大的威胁。而文中提出的涉密计算机信息系统的安全监控是针对特定的网络使用者而设计的，它是针对特定的用户来实现的。在此控制方式中，不管主机 IP 地址有没有变化都不会对权限和权限有任何影响。而且，就算是多个使用者共用一台计算机，每个使用者都拥有各自的权限和控制权，彼此之间互不干扰，防止有人利用别人的账号来危害网络安全。

（四）存储介质控制技术

将移动设备与计算机连接，是导致计算机和网络中毒的一种普遍现象。然而，传统的设备扫描、杀毒等手段并不能彻底发现隐藏于其中的病毒，所以对于移动存储设备来说，依然存在着一定的安全隐患。采

用储存媒体管理方法将一般的储存媒体登记为涉密化媒体，以保证系统内只有授权的使用者或机构可以读取。其具体实施方式为：通过对可移动存储装置中的磁盘进行读取，并依据磁盘上的符号来决定其唯一的特性，并将此特性值授予使用者或机构。将便携式存储装置接入计算机主机后，必须对其进行特征值的校验。而其他未经授权的用户和机构，由于不知道这些特征值就不能通过验证，此时，具有潜在危险的移动存储装置就不能与计算机主机相连，这样就能保证计算机信息系统的安全。

（五）防火墙技术

防火墙技术是一种对计算机系统安全保护所采取的一种保护手段，它是一种将两个不同信任水平的网络连接在一起的一种软硬件结合的方式，它能够对网络间的信息交流、访问行为进行监控和全面的检测，从而更好地保护网络的安全，防止非法获取信息资源等，并能有效地保护系统的安全。通过对防火墙技术的分析，认为它既是一个分裂器、限制器，又是一个分析器，可以监测内外网的行为，防止不安全的协议或业务的产生。从物理上讲，防火墙可以分为路由器、主机和其他可以进行自定义的插件，而通常的防御方法有过滤类型、代理服务器类型和状态侦测类型。但是，防火墙在实际应用中也有一些限制，比如不能有效地防止病毒等威胁，所以必须与其他监测手段结合起来才能取得良好的监测效果。

（六）入侵检测技术

入侵检测技术就是一种通过对入侵的行为进行实时监测来预防的一种报告系统，它由传感器、分析器和管理器等组成，能够通过各种系统或者网络收集信息资源，并根据自身的攻击规律来分析这些信息，从而判定有没有入侵。在实际应用中，入侵检测技术能够动态追踪用户行为，发现违规行为，并为其提供专业的解决方案，从而实现对整个网络环境的全方位监测与诊断。按照入侵检测的方法，可以将其划分为以网络为基础和以主机为基础的两类。前者是指使用感应器在互联网上收集有关的信息，然后对这些信息进行监控和分析，查看有没有什么可疑的行为。后者监控某一特定系统中的行为，并从主机那里获取与之有关的信息。将入侵检测与防火墙有机地结合起来，能够更好地实现对网络安全的保护，但是，它不能解决网络协议上的不足，不能有效地处理垃圾数据。

（七）认证技术

认证是一种对已有授权的使用者进行身份验证的方法。当前，常用的认证内容有身份编号、智能卡和人体生理信息等，而认证技术主要有一次密码、时间密码、单站式签到等。一次密码技术主要用于两种情况，一种是将用户密码存储在客户端和中央服务器的系统中，另一种是将用户密码存储在中央服务器系统中，每一条密码只能被用一次，所以都是纯文本传输的。时间密码技术是一种从时间的观点，使用时间和外界的一种安全设备，它又叫安全令牌，当使用者登录的时候，首先要输入自己的 ID 号，然后在安全令牌上键入一次出现的密码，从而完成认证。一站式签到是指只需要一次认证就可以在任何时候使用各种不同的系统及软件。

（八）防病毒技术

防病毒技术是信息网络的重要组成部分，也是涉密计算机抵御病毒的重要手段。当前，常用的防病毒技术有三种：病毒预防技术、病毒检测技术和病毒清除技术，病毒预防技术是指通过使用系统的控制对整个系统进行监控，判定有没有病毒，从而防止病毒入侵。病毒检测技术是通过对网络中的病毒特征的分析来有计划地监控涉密计算机中有没有病毒，从而建立起一个多层的防护体系，从而提升涉密计算机的防病毒性能。病毒清除是指对已入侵到病毒中的机载计算机进行攻击，利用杀毒等方法将其删除，从而将其污染的范围缩小到最小。

五、结束语

伴随着互联网技术的持续发展和运用，它逐步渗透到社会的方方面面，对行业的发展起到了巨大的促进作用，但同时也给企业造成了巨大的经济损失，也给我国的保密工作造成了很大的风险。涉密计算机是涉及国家机密的重要装置，其信息系统的安全性直接关系到一个国家的发展。所以，应该与正在发展中的现代网络安全监控技术相联系，在涉密的计算机信息系统中引入多种技术，从而提升我国目前的网络安全性。

参考文献：

[1] 饶瑶 . 谈计算机信息系统维护与网络安全漏洞的处理方法 [J]. 中国科技期刊数据库　工业 A,2022(3):0273-0276.

[2] 邱璐 . 区块链技术在网络安全中的应用研究 [J]. 计算机应用文摘，2023，39（9）：58-60.

[3] 左晓峰 . 论如何加强道路养护工程施工中的安全管理 [J]. 中文科技期刊数据库（引文版）工程技术，2021（12）：0369-0371.

[4] 高倩文 . 浅谈网络技术在消防防火工作中的应用 [J]. 中文科技期刊数据库（全文版）工程技术，2021（9）：0156-0156.

[5] 杨绚，张立生，王铸 . 基于机器学习算法的县域台风灾害经济损失风险评估 [J]. 热带气象学报，2022，38（5）：651-661.

[6] 王华伟 . 破坏计算机信息系统罪的教义学反思与重构 [J]. 复印报刊资料（刑事法学），2022（5）：61-73.