移动存储介质信息安全防范与检查技术研究

武汉第二船舶设计研究所　刘丹　陈泓青

摘 要

移动存储介质因其轻巧易用、存储稳定而在军工行业各单位广泛应用。本文结合目前移动存储介质使用的实际情况，分析了移动存储介质管理中存在的安全隐患及违规使用移动存储介质对安全保密工作的危害，从管理和技术两个层面论述了如何加强移动存储介质的信息安全防范，研究了移动存储介质安全保密检查技术手段，运用此方法不定期实施保密检查，能够及时发现违规操作，杜绝失泄密事件的发生，确保国家秘密安全。

关键词：移动存储介质　信息安全　保密检查

1　引言

随着计算机集成制造技术的快速发展，移动硬盘、U盘、SD卡等移动存储介质因其轻巧易用、便于携带、存储稳定而在军工行业各单位广泛使用。由于缺少相应的技术防范手段和有效的安全管理措施，移动存储介质的信息安全给国家秘密安全带来了极大隐患，甚至已经造成了非常严重的后果。本文从目前移动存储介质的实际使用情况出发，分析了移动存储介质管理中存在的主要问题及违规使用移动存储介质对安全保密工作的危害，从管理和技术两个层面论述了如何加强移动存储介质的信息安全防范，最后研究了移动存储介质安全保密检查技术手段。

2　安全隐患及危害

（1）易感染病毒。移动存储介质已成为病毒传播的重要途径，当移动存储介质在感染病毒及恶意代码计算机上使用时，其自身极易被病毒侵入，一旦该移动存储介质拔出后插入其他计算机后，其他计算机也会感染病毒，致使病毒广泛传播，无法控制。

（2）易丢失。移动存储介质体积小、轻便，往往被随身携带，流动范围广，致使载体失去有效的安全防护，容易丢失和被盗，其中存储的重要信息（如工作秘密、商业秘密或国家秘密）将会不受控制，给单位内部信息和国家涉密信息带来隐患，严重的会造成失泄密，危害国家安全。

（3）交叉使用。移动存储介质在非涉密计算机商使用时，有可能被植入“木马”等窃密程序。当这个移动存储介质又在涉密计算机上使用时，“木马”窃密程序会自动复制到涉密计算机中，并将涉密计算机中的涉密信息打包存储到移动存储介质。当移动存储介质再次接入互联网时，木马会自动将收集到的涉密信息发往境外情报机构指定主机，造成失泄密。近年来，在国家有关部门发现和查处的泄密案件中，有多起均为移动存储介质交叉使用，致使移动存储介质感染木马，导致涉密文件从涉密信息系统中外泄到国际互联网。

（4）信息难以清除。从逻辑结构上看，存储介质的存储部件分为两个独立区域，分别为文

刘丹　男　助理工程师　1983出生　毕业于武汉理工大学计算机应用技术专业　现从事信息安全与保密技术工作

件分配表和数据区。对文件采取的删除操作和对存储介质的格式化操作，仅仅是删除了文件分配表中的信息。数据区的信息仍然被全部保留。使用数据恢复软件，可以对数据区中的信息进行分析处理，恢复格式化前数据区中的内容。

（5）出现故障处置不当的风险。涉密移动存储介质出现故障时，如果随意选择维修、报废和销毁等方式，会造成存储介质内涉密信息的外泄。从物理结构上看，存储设备主要由控制电路和存储介质组成，如果控制电路损坏，更换电路板后就可以直接读出其中的数据。如果存储介质损坏，采取一定的数据恢复措施，也可以读出其中未损坏部分的数据。

3 信息安全防范对策

（1）加强宣传教育，增强保密意识。积极开展计算机信息安全保密宣传教育活动，定期或不定期举办安全保密、窃泄密案例教育等知识讲座，不断提高员工的安全防范能力和意识，逐步实现员工从“要我保密”、“我要保密”到“我会保密”的转变，从思想上筑起一道信息安全风险防范的“防火墙”。

（2）健全管理制度，加大监管力度：移动存储介质的采购由指定部门进行统一配置和管理。严格准入审批管理，采取安全准入许可制度，经安全检查合格后才能使用。定期升级病毒及恶意代码库，并对计算机进行全盘查杀，确保将移动存储介质感染病毒的风险降到最低。完善操作使用和外出携带管理规定，坚持“先审批后使用，谁使用谁负责”的原则，明确责任主体，严防违规。建立移动存储介质设备台帐，逐一记录介质不同环节的变动情况，保密管理部门定期对移动存储介质的使用进行监督检查。

（3）采用技术手段，提高防范水平：使用玻璃胶物理封堵计算机USB接口，杜绝移动存储介质的接入，也可采取粘贴封条或定制保密机箱管控USB接口，履行审批手续后方可撕开封条或开启机箱。采用先进的技术手段管控移动存储介质的使用，一是使用异型口的移动存储介质，避免介质的交叉使用，二是安装安全审计软件，对介质使用的全过程进行监控审计，三是启用身份认证机制，未经授权的移动存储介质严禁在内网机上使用。

（4）严控维修销毁，防止二次泄密。报废处理的涉密信息存储介质在其他信息系统内重新使用或利用前，应进行信息清除处理，信息清除处理所采用的信息消除技术、设备和措施，应符合BMB21-2007《涉密国家秘密的载体销毁与信息清除安全保密要求》的有关规定。涉密移动存储介质不用时应及时彻底销毁淘汰，可采取物理粉碎方式将介质粉碎到一定尺寸的颗粒度，对于移动硬盘等磁记录设备可使用专用消磁仪对其进行强磁场销毁。如果需要修复涉密存储设备，则必须到国家保密工作部门指定的具有恢复资质的单位进行。

4 检查技术研究

移动存储介质成功接入计算机后，计算机操作系统会在多处留下痕迹和记录。为了更好检查出移动存储介质的使用情况，下面对检查技术进行研究。

4.1 系统日志文件检查

Windows操作系统日志文件记录了系统运行的历史信息，其中系统%SYSTEMROOT%目录下的setupapi.log和setupapi.log.x.old日志文件详细记录了移动存储介质的驱动安装过程，

利用USB移动存储设备特征关键字“USBSTOR”对日志文件进行搜索，就能得到计算机系统使用过的USB移动存储设备信息。

通过分析下面一段日志文件，我们可以获得该USB移动存储设备的厂商ID为aaaa，产品ID为0001，修正码为0100，序列号为0201014346，首次使用时间为2011/11/18 10:12。

[2011/11/18 10:12:39 1060.16 Driver Install]

#-019 正在查找硬件 ID(s): usb\vid_aaaa&pid_0001&rev_0100,usb\vid_aaaa&pid_0001

#-018 正在查找兼容 ID(s): usb\class_08&subclass_06&prot_50,usb\class_08&subclass_06,usb\class_08

#-198 处理的命令行: C:\WINDOWS\system32\services.exe

#I393 更改过的 INF 缓存 "C:\WINDOWS\Inf\INFCACHE.1"。

#I022 在 "C:\WINDOWS\Inf\usbstor.inf" 中发现了 "USB\Class_08&SubClass_06&Prot_50"；设备: "USB Mass Storage Device"；驱动程序: "USB Mass Storage Device"；提供程序: "Microsoft"；制造商: "兼容 USB 存储设备"；段: "USBSTOR_BULK"

#I023 实际安装部分: [USBSTOR_BULK.NT]。等级: 0x00002000。驱动程序有效日期: 07/01/2001。

#-166 设备安装函数: DIF_SELECTBESTCOMPATDRV。

#I063 从 [USBSTOR_BULK] 中的 "c:\windows\inf\usbstor.inf" 选择驱动器安装服务。

#I320 设备的类别 GUID 依旧为: {36FC9E60-C465-11CF-8056-444553540000}。

#I060 设置所选的驱动器。

#I058 选择最兼容的驱动器。

#-166 设备安装函数: DIF_INSTALLDEVICEFILES。

#I124 正在做“仅复制”安装 "USB\VID_AAAA&PID_0001\0201014346"。

#-166 设备安装函数: DIF_REGISTER_COINSTALLERS。

#I056 注册了共同安装程序。

#-166 设备安装函数: DIF_INSTALLINTERFACES。

#-011 正在从 "c:\windows\inf\usbstor.inf" 安装段 [USBSTOR_BULK.NT.Interfaces]。

#I054 安装接口。

#-166 设备安装函数: DIF_INSTALLDEVICE。

#I123 进行 "USB\VID_AAAA&PID_0001\0201014346" 的完整安装。

#I121 "USB\VID_AAAA&PID_0001\0201014346" 的设备安装成功完成。

4.2 注册表相关信息检查

Windows注册表（Registry）是一个庞大的数据库，存储着计算机系统的大量设置和使用信息，设备、服务的安装和启动都会在注册表中留下痕迹，它为我们提供了一个注册表编辑器（Regedit.exe）工具用来查看和维护注册表。

USB移动存储设备成功连接计算机后，操作系统会在注册表HKEY_LOCAL_MACHINE\SYSTEM\Current ControlSet\Enum\USB下创建一个子键，形如Vid_1043&Pid_8012，第一个四位数是USB协会分配给销售商的厂商代码，第二个四位数是由销售商分配其产品的

代码。该键的子键记录了设备序列号，查看序列号子键下ClassGUID（USB移动设备在操作系统中的全局唯一标识符）和Service，如果键值分别“36FC9E60-C465-11CF-8056-444553540000”、“USBSTOR”，则表示为USB移动存储设备。

查看HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR键值下的内容，可得到每一个正在连接和曾经连接过的USB移动存储介质信息。展开USBSTOR键，形如Disk&Ven_SMZY&Prod_UDisk &Rev_0.00 的字符串代表了USB移动存储设备的厂商（SMZY）、型号（UDisk）和修正码（0.00），其子键为USB移动存储设备的序列号。选择某一序列号，查看窗口右侧，它记录了一些描述USB移动存储设备信息，其中DeviceDesc表示对USB移动存储设备的描述，FriendlyName表示设备的显示名称，HardwareID表示设备ID。

如果计算机接入USB存储设备，还会在HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\DeviceClasses\下留有痕迹。打开｛53f56307-b6bf-11d0-94f2-00a0c91efb8b｝，形如##?#USBSTOR#Disk&Ven_SMZY&Prod_UDisk&Rev_0.00#0201014346#{53f56307-b6bf-11d0-94f2-00a0c91efb8b}子键，代表了计算机接过SMZY厂商的序列号为0201014346 的USB移动存储设备。{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}子键下形如##?#STORAGE#RemovableMedia#8&15cbbf47&0&RM#{53f5630d-b6bf-11d0-94f2-00a0c91efb8b}的字符串，其中“STORAGE#RemovableMedia”表明这是一个可移动存储设备。{a5dcbf10-6530-11d2-901f-00c04fb951ed}子键下也保存了计算机曾经和正在接入USB设备的Vid和Pid。

为了获取USB移动存储设备的最近使用时间，我们可以展开HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR键值，用鼠标选择子键（USB移动存储设备序列号），打开注册表编辑器的文件菜单，导出成txt文件，文件前置处的最近写入时间为该USB移动设备最近使用时间。

5 结束语

移动存储介质因可重复多次擦写、轻便而广泛使用，军工行业各单位不可避免使用移动存储介质存储涉密信息，因此，移动存储介质信息安全是确保国家秘密安全的重要举措。但目前USB移动存储介质管理中存在很大安全隐患，如何进行信息安全防范，及时有效发现违规操作，堵塞漏洞，消除隐患，本文提出了多种防范对策，探讨了如何加强移动存储介质的信息安全防范，研究了移动存储介质安全保密检查技术手段。由于本文只论述了移动存储介质使用痕迹的手动常规检查方法，对于痕迹恢复的深度检查，还需要进一步研究。