涉密内网中的移动存储介质管理问题及对策

杨力铭, 刘 炜
(兰州理工大学 计算机与通信学院, 甘肃 兰州 730000)

摘 要: 移动存储介质作为数据存储和传输的媒介被广泛使用, 在给使用者带来方便的同时, 也为企事业单位内网的信息安全带来了新的风险。移动存储介质引发的泄密问题已成为保密工作关注的重点和难点。分析了移动存储介质在涉密内网中使用存在的问题, 提出了规范和加强移动存储介质安全管理的技术保障措施。

关键词: 移动存储介质; 保密; 安全管理; 对策
中图分类号: TP309

随着计算机技术的飞速发展和计算机应用范围的不断拓展, 现在几乎所有的企事业单位都有自己的内部计算机网络, 一些涉密信息也不可避免的存储在位于内部网络的计算机当中。当前内网中的计算机的泄密途径, 主要有网络输出、移动存储介质带出、打印带出、电磁辐射泄漏、偷窥记忆带出等情况。其中, 移动存储介质以其使用方便、存储量大、隐蔽难以防范的特点, 成为内部网络泄密的主要途径。加强移动存储介质的风险分析和风险管理已成为有效保障涉密内网中信息安全的重要工作。

1 移动存储设备的安全隐患

1.1 内外网移动存储介质混用

内网移动存储介质指的是按照规定只能在企事业单位内部网当中使用的移动存储介质。内外网移动存储介质混用, 指的是通过 U盘、可移动硬盘、MP3等在内网和外网之间交替使用, 把保存有涉密信息的存储介质接入外网, 甚至接入互联网, 如此存在严重的泄密隐患。

1.2 移动存储介质公私混用

U盘等移动存储介质具有体积小、容量大、携带使用方便等优点, 因此, 常常被带到不同环境下使用, 比如: 自己的私人 U盘存放单位资料或者单位 U盘又拿来存放私人信息, U盘被借来借去使用也是很常见的情况, 这样公私混杂很容易出差错, 使得移动存储介质中的重要信息存在泄漏的风险。

1.3 移动存储介质成为病毒传播源

使用者在使用移动存储介质的时候往往忽视对移动设备的查杀毒工作。由于移动设备使用范围较广, 不可避免地会出现在外使用时感染计算机病毒的情况, 如果不能及时有效地查杀病毒, 轻易地将染毒文件在单位内网的计算机上打开, 那么就很容易将病毒带到内网使其有机会在内网中扩散。甚至有些病毒程序在插入 U盘后会立即被自动执行[1], 使得移动存储介质传播病毒的可能性大大增加。

1.4 移动存储介质感染木马成为“摆渡机”

如果病毒仅仅是破坏系统还不会造成泄密, 但一旦感染了木马, 其危害就十分严重了。其中一种被称为“摆渡机”[2]的木马, 该类木马会根据指定的关键字搜索计算机的文件夹, 并将窃取到的文件伺机通过因特网发送到指定的地址或邮箱, 使得物理隔离的内网与因特网之间有了连接的泄密渠道。

1.5 管理不善, 密级混乱

在一些企事业单位内网中, 涉密信息按照重要程度被分成不同的秘密等级, 同时对移动存储介质也划分了相应的等级, 不同密级的信息需用对应密级的移动存储介质承载。但一些工作人员常常疏忽大意或者一时图省事, 造成高密低用或者低密高用的情况。高密低用[3], 就是密级等级高的信息使用密级等级低的移动存储介质承载, 数据安全无保障。例如: 一是涉密笔记本电脑和移动存储介质接入到低密级、非涉密系统中, 会产生数据泄密隐患; 二是低密高用, 就是将密级低的移动存储介质插入到密级高的计算机当中装载高密级的信息数据, 这使得病毒传播进而感染高密级信息数据成为可能。

1.6 缺少有效的监督机制

一些单位的安全保密部门虽然制定了移动存储介质相关的规章制度, 但监管部门与使用者处于分离状态, 不能有效的行使监督和管理职能, 使用者怎么使用移动存储介质的, 什么时候做了什么, 监管部门并不清楚。即便发生泄密事件要追查责任封堵漏洞也无从下手。

?1994-2015 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

1.7 体积小易丢失,重要信息也随之泄漏

移动存储介质尤其是目前被广泛使用的 U盘,体积小重量轻容量大使用方便应用广泛,却很容易丢失。装有重要信息的 U盘一旦丢失,上面的信息数据必然会随之泄漏。

2 构建移动存储介质管理系统

一直以来,国内外都非常重视涉密移动存储介质管理问题。国家保密局先后制定了《涉及国家秘密的信息系统安全审计产品技术要求》、《涉及国家秘密的信息系统终端安全与文件保护产品技术要求》和《涉及国家秘密的信息系统分级保护技术要求》等技术标准和规范。这些标准和规范都从技术和管理的双重角度对涉密信息系统中的移动存储介质的使用做出了必要的规定,目的是实现移动存储介质管理的“五不”原则[4]:进不来、出不去、拿不走、改不了、逃不掉。

随着计算机技术的不断发展,技术手段在现代化的保密工作中扮演着越来越重要的角色。针对涉密介质的使用缺乏身份认证、访问控制和审计机制等问题,根据涉密内网对涉密介质管理的要求,需构建移动存储介质安全管理系统,以提供对移动存储介质从购买、使用到销毁全过程的管理和控制。

2.1 工作原理

(1)创建标识:采用专用技术,在移动存储介质内结合用户的身份信息,创建唯一的用户标识信息,为移动存储介质的管理、用户身份认证提供鉴别基础;

(2)设备及身份认证:利用创建的唯一电子标识信息,实现计算机系统与用户设备间的身份认证,保证没有标识的设备不能在内网计算机上使用,有标识的设备不能在外网计算机上使用;

(3)数据加密:采用虚拟磁盘技术,结合专用算法完成数据包加密,采用特殊磁盘格式,并结合身份认证功能达到保护数据机密性的目的;

(4)自身防护:采用 Windows过滤驱动技术从系统底层防止客户端程序被非法删除、卸载或停用,对客户端程序进行进程、注册表和文件等级别的保护,以确保其自身安全性。

2.2 主要功能

2.2.1 移动存储介质认证

移动存储介质系统提供对移动存储介质的注册认证管理功能,没有经过管理员注册认证的移动存储介质,不能在内网计算机上使用。移动存储介质要想在网络内使用,必须经过管理员对该移动存储介质进行注册,并赋予相应的权限。管理员还可以取消对移动存储介质的注册,收回对该移动存储介质的特殊授权。

2.2.2 移动存储介质权限管理

移动存储介质管理系统对移动存储介质的权限可分为禁用、只读、安全读写和直接读写 4种方式。

禁用权限禁止移动存储介质在部署了移动存储介质管理系统的计算机上使用,禁止该移动存储介质的所有文件和数据读写操作,既不能从该移动存储介质读出文件,也不能将计算机中的文件复制到该移动存储介质中。

只读权限的移动存储介质在部署了移动存储介质管理的计算机上,只能将移动存储介质中的文件或者数据复制到计算机上,但是不能将计算机上其他存储设备的数据和文件复制或者输出到移动存储介质中。

安全读写权限的移动存储介质在指定的域内可以自由交换数据,但数据读写的时候都自动进行了格式转换,并且这些数据仅在同一个域内的计算机上能够正常使用,在非同域内的计算机上这些数据是无效的。安全读写权限实现了数据的安全共享,即数据共享的同时,有效限定了数据的使用范围,从而不会造成信息泄密。

正常读写权限的移动存储介质,在指定域内的计算机上其权限是最高的,数据使用不受任何限制,可以自由复制。该模式一般仅用作特殊权限,输出数据使用,不能作为日常的管理模式。

2.2.3 移动存储介质隔离

对于高安全级别的移动存储介质,可将其使用范围严格锁定在内部工作环境中,在外部网络计算机上无法使用注册过的内部移动存储设备。同时,未注册移动存储介质的也无法在内部网络中使用。这种内外隔离、密级隔离既避免了信息的泄密问题,也杜绝了通过移动存储介质传播病毒的问题。

2.2.4 数据透明加密保护

对于机密级别较高的移动存储介质,移动存储介质管理系统还提供数据保护功能,即所有写入移动存储介质的数据都会被自动进行格式转换;用户在读取文件时,数据能够被自动还原。这个过程应由系统自动完成,不需用户参与,与普通磁盘上操作没有任何区别。这样,即便移动存储介质丢失,上面存储的加密信息也很难被破译。

?1994-2015 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

2.2.5 文件安全删除

移动存储介质上的文件和文件夹采用常规方法删除以后,还是可以使用专门的技术和工具进行恢复的[5]。对于涉密等级较高的资料应采用更加彻底的办法加以"粉碎",确保资料在删除后不能被恢复。可采用密码置乱技术,对删除文件后的移动存储设备进行 8次随机数填充,即没有对移动存储设备进行硬件破坏又保证任何工具都不能恢复移动存储设备上的数据。

2.2.6 记录使用日志

对移动存储介质上所有的文件操作,包括文件的创建、复制、删除和重命名等操作,进行详细的监控记录,记录的要素包括时间、用户名、计算机名、文件名和其他必要的信息,以作为日后审计使用。如此一来,即便发生通过移动存储介质造成的泄密问题,也有据可查,可以为追究责任和防堵漏洞提供有力的证据保障。

2.3 三权分立的管理机制

对于某些管理要求严格的大型企事业单位的涉密内网,对移动存储介质管理除了使用技术加以管控以外,还可进一步采用三权分立的管理机制。三权指的是:管理员权限、审计员权限、操作员权限。管理员负责本级用户标识设备的创建和管理,负责下级管理员和审计员的生成和管理等;审计员负责提取所有角色的操作日志,必要时加以分析和取证。在移动存储设备的使用过程中,审计员可随时提取包括注册信息、使用人、使用计算机、使用时间、使用信息和动作等审计记录,可以对移动存储设备的整个使用过程进行监督和审计;操作员负责移动存储介质的注册、授权、注销等等具体操作。

2.4 密级对应的使用原则

信息是分密级的。在一个合格的安全体系中,不同密级的信息必须保存在不同的位置或不同的存储介质上,这样便于最大限度保障信息的安全。为此,可将可移动存储介质划分保密等级,用以存放相应密级的数据,只有具备相关权限的人员才能对涉密信息进行访问。密级对应不是说只有同等密级的计算机和移动存储介质之间才能建立互信的使用关系,按照密级对应使用移动存储介质的一般原则是:数据从低密向高密流动不受限制。如,高密级计算机能读取低密级移动存储介质上的数据,但不能对其进行写入操作[6]。按照密级对应的使用原则,即灵活又有效的构筑了一道防止涉密信息泄露的安全堤坝。

3 结束语

移动存储介质安全管理是内网信息安全管理的重要组成部分。移动存储介质的使用范围越来越广,必须因势利导,坚持预防为主的方针,通过认证和加密技术,提高了移动存储介质使用的安全性。但是,一个完整的内网安全系统应是技术手段和管理制度相结合的体系,还需要对涉密移动存储介质进行全过程监管,严把采购关、检查关、使用关、维护关及销毁关等各个环节,形成"制度保障、组织管理、技术防范"的整体合力,从而构建一个安全的可信赖的内部网络工作环境。

参考文献:

[1] 王琢,刘建华,范九伦. Autorun类病毒在移动存储中的传播方式分析[J]. 计算机安全,2008(11):108-109.
[2] 池同柱,陈平. 浅谈移动存储介质的信息安全[J]. 技术研究与应用,2008(10):62.
[3] 周俐军,王冬梅,宋皓. 政务内网中的移动存储介质管理问题及对策[J]. 电子政务,2008(10):97.
[4] 池同柱,陈平. 浅谈移动存储介质的信息安全[J]. 技术研究与应用,2008(10):63.
[5] 闫安. 论数据误删除后的恢复及数据的安全删除[J]. 网络与信息,2008(12):26-28.
[6] 张秋江,王澎. 涉密网络的一体化安全防护技术[J]. 信息安全与通信保密,2007(3):143.

(上接第 43页)

讨论的 Floyd算法基于图论的矩阵理论,是非常有特点的一个传统算法。该算法可以方便的计算每对顶点之间的最短路径和长度,如果加入车型收费标准、各路段所属业主的数学描述,便可以很方便地计算出收费费率表和拆分表。当路网结构发生变化时,只需修改模型的输入参数,即可自动计算费率,从而实现费率表和拆分表的自动维护,极大地提高工作效率,确保费率的准确性。

参考文献:

[1] 陈庆喜. 浅析高速公路路网模型的建立与清分算法的实现[J]. 筑路机械与施工机械化,2004(11):53-57.
[2] 童剑军. 高速公路联网收费路径识别技术应用问题的提出——"二义性路径"[J]. 交通信息产业,2006(3):16-17.
[3] 陈剑威,罗石贵. 路径识别技术选择的基本考虑[J]. 交通信息产业,2006(3):25-26.

?1994-2015 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net