文章编号：1000－5471(2007)04－0107－04

论磁性存储介质的数据销毁技术①

徐 菁[1]， 朱有佃[2]， 赖 凡[1]

1. 西南大学 计算机与信息科学学院，重庆 400715；2. 第二炮兵司令部，北京 100085

摘要：系统论述计算机数据销毁的方法，分析其不能彻底清除数据的原因，根据不同的保密要求提出数据销毁的相应解决措施，并就采取其措施的原理、方法、优缺点及适用范围进行详细说明，最后展望了数据销毁技术的发展趋势.

关 键 词：覆写；消磁；磁盘销毁

中图分类号：TP309 **文献标识码**：A

在计算机高度普及的今天，数据恢复技术越来越多的被研究、利用[1]，与之相对应的数据销毁技术是数据安全中不容忽视的一个重要方面，在国防军事、国家安全等重要部门有着借鉴作用，但却没有引起人们的足够重视. 所谓数据销毁是指采用各种技术手段将存储在计算机存储设备中的数据予以删除，以达到保护相应数据不泄密、不外传等目的.

本文以磁盘为论述对象(其它如磁带和各类数码设备的存储卡的工作原理与之基本相同)，论述磁性介质的数据销毁技术.

1 计算机磁盘数据销毁技术发展现状

目前，国内外数据销毁技术发展差距较大，主要体现在数据安全的观念和数据销毁设备的应用普及方面. 国外在 2000 年前后开始将数据销毁技术实用化，最早应用在军事领域. 我国从 2004 年开始进行数据销毁应用研究，进入到 2005 年下半年后，来自国家重要部门对数据销毁技术需求日益增加.

早在 1985 年，美国国防部(DOD)就发布了数据销毁标准(US. DoD. 5200. 28-STD). 在随后的 20 多年里，美国的数据销毁技术取得惊人的成就，研制了多种类型的数据销毁软件/硬件.

随着数据销毁技术的发展，为了满足野战环境的需要，美军在网系、网络安全防护建设中，提出了遥毁、自毁概念，并且已经开始在一些系统中进行研制.

2 磁盘数据销毁的原因

鉴于磁性介质的存储原理和数据读写方法，普通的数据销毁如低级格式化、数据删除等方法都无法彻底清除数据；操作系统和磁盘的隐性操作会产生残留数据. 为了避免不法分子利用数据残留恢复出原始数据信息，造成安全泄密的风险，在磁盘报废或者送修、捐献前应按不同的保密等级对磁盘数据进行销毁处理[2]. 下面先就数据销毁的主要方法及其不能彻底销毁数据的原因介绍如下：

2.1 低级格式化后的数据是可恢复的

现在流行的低级格式化，仅仅是一个简单的写标记过程，所调用的磁道、扇区是经过转换后的，并不是对物理的磁头和磁道进行操作. 经过这种低级“格式化”后，磁盘上的数据可以恢复，因此存在不安全

① 收稿日期：2007－05－31
作者简介：徐 菁(1978－)，女，山东泰安人，硕士研究生，主要从事计算机应用的研究.

因素.

2.2 高级格式化操作不能彻底删除数据

高级格式化仅仅是为操作系统创建一个全新的空文件索引,将所有的扇区标记为"未使用"状态,让操作系统认为硬盘上没有文件. 当用户对磁盘进行高级格式化操作时,先扫描磁盘的每个扇区并确保它可用,接下来,写入寻址系统,磁盘根目录,文件分配表. 格式化操作完成后,系统在磁盘上创建新的根目录,磁盘上原来保存的信息便都变的不可访问. 因此,格式化后的硬盘数据能够恢复,也就意味着数据不安全.

2.3 DELETE操作不能真正擦除磁盘信息

由于对效率等诸多方面的考虑,用户所使用的删除命令,如DEL是依靠调用WIN32函数来实现. 事实上,删除文件系统只是将文件的文件目录项的第一个字节改成一个特殊字符"E5H"(或小写的希格玛),做一个删除标记,把它们在FAT表中所占用的簇标记为空簇,在文件系统中去除目录区的文件名和数据区的文件数据之间的索引链接,仅仅破坏文件的FAT或者FDT表,数据区没任何变化. 正是操作系统在处理存储时的这种设定,可以用工具软件绕过操作系统,直接操作磁盘,恢复被删除的文件,为窃密者提供了可乘之机,因此这种清除数据的方法最不安全.

2.4 数据随意复制泄密

基于对病毒感染、数据丢失的顾虑,用户经常对重要数据进行备份. 有时这种备份操作系统自动进行. 整个复制过程很隐蔽,而且不会留下任何痕迹. 如果用户对数据进行擦除时,没有对备份数据进行相应处理,就将导致"副本"数据的残留. 这给磁盘信息的保护和保密带来很多难以解决的问题.

2.5 磁盘的内部固有机制导致部分数据无法覆盖

比如,老式磁盘的每一个磁道都有数量相同的扇区,但外圈的磁道比内圈的长,敏感数据有可能隐藏在外圈磁道扇区之间的缝隙中.

又如,磁盘的缺陷处理机制. 对于磁性存储器来说,通常使用映射的方法来替换受损的磁道或扇区,把坏的和磁介质不稳定的扇区记录下来,做成磁盘缺陷列表,写进磁盘的系统保留区,替换掉原来旧的磁盘缺陷列表,并且通常不再对受损的磁道或扇区进行操作. 而且,也有部分软件或病毒程序能将某些扇区故意标记为坏扇区. 如果在磁盘的记录间隙、坏的磁道、被故意标记的区域中储存着敏感信息,这些信息仍然可以通过特殊手段被读取.

再如纠错机制. 许多存储器设备支持不同的纠错方案,以便在设备受到损害时进行数据恢复. 因此即使一些数据被可靠地擦除,但通过使用存储器设备内建的纠错能力也可能恢复.

另外,支持数据缓冲或高速缓存功能的存储器,操作系统把内存数据写入硬盘前是在缓冲区中收集数据,而写入磁盘上数据的最小单位是一个扇区,因此文件的最后一部分通常不会恰好填满最后一个扇区,操作系统就会随机提取缓冲区中称为内存渣滓的数据来填充空余区域,而这些内存渣滓数据在进行删除操作时可能滞留在缓冲区中没有真正得到执行. 同样,最后一个簇中没有用到的扇区就原封不动保留原来称为磁盘渣滓的数据. 这些被称为渣滓的地方可能包含大量的敏感信息不能被彻底销毁.

2.6 剩磁效应使数据还原成为可能

所有磁介质都存在剩磁效应问题,磁介质会不同程度地永久性磁化,所以磁介质上记载的信息在一定程度上抹除不净. 同时由于每次写入数据时磁场强度并不完全一致,这种不一致性导致新旧数据之间产生"层次"差. 剩余磁化及"层次"差都可能通过高灵敏的显微镜探测方法探测到,经过分析与计算,对原始数据进行"深层信号还原"可以恢复以前的影子数据[3,4].

3 磁盘数据销毁的解决方法

根据采用的技术原理以及处理后果的不同,数据销毁技术可以划分为数据覆写、消磁、磁盘销毁三种,其中磁盘销毁又分为物理销毁和化学销毁[5].

3.1 数据覆写

数据覆写是将非保密数据写入以前存有敏感数据的存储位置的过程. 硬盘上的数据都是以二进制的

“1”和“0”形式存储的. 使用预先定义的无意义、无规律的信息覆盖硬盘上原先存储的数据，完全覆写后就无法知道原先的数据是“1”还是“0”，也就达到了清除数据的目的[6].

根据数据覆写时的具体顺序，软件覆写分为逐位覆写、跳位覆写、随机覆写等模式. 根据时间、密级的不同要求，可组合使用上述模式. 美国国防部 Network & Computer Security 的 DOD 5220.22_M 标准[7]和北约 NATO 的多次覆写标准规定了覆写数据的次数，覆写数据的形式. 美国国防部订立的磁盘清洗规范，要求数据必须对所要清除的数据区进行三次覆盖：第一次用一个 8 位的字符覆盖，第二次用该字符的补码(0 和 1 全反转的字符)覆盖，最后再用随机字符覆盖. 如先用 0011 0101 覆盖，接着用 1100 1010，然后用 1001 0111. 覆写必须完成的次数与存储介质有关，有时与其敏感性有关，有时因国防部门的需求有所不同[8]. 在不了解存储器实际编码方式的情况下，为了尽量增强数据覆写的有效性，正确确定覆写的次数与覆写数据的样式非常重要.

采用不同类型的数据，对要删除的数据的存储位置进行多次覆写的方法，是数据销毁的有效途径. 处理后的硬盘可以循环使用，适应于密级要求不是很高的场合. 特别是需要对某一具体文件进行删除而其它文件不能破坏时，这种方法更为可取. 到目前为止，数据覆写是最安全、最经济的销毁数据的方法.

覆写软件必须能确保对介质上所有的可寻址部分执行连续写入. 如果在覆写期间发生了错误或坏扇区不能被覆写；软件本身遭到非授权修改时，处理后的硬盘仍有恢复数据的可能. 因此该方法不适用于包含高度机密信息的介质.

3.2　消磁

消磁，通常被称为擦除，是磁介质被擦除的过程. 销毁前，硬盘盘面上的磁性颗粒沿磁道方向排列，不同的 N/S 极连接方向分别代表数据“0”或“1”，对存储介质施加瞬间强磁场，磁性颗粒就会改变沿场强方向顺序排列，使介质表面的磁性颗粒极性方向发生改变，失去表示数据的意义.

具体的消磁办法和技术有很多种，但实质上可分为直流消磁法和交流消磁法两种. 直流消磁法是使用直流磁头将磁盘上原先记录信息的剩余磁通，全部以一种形式的恒定值所代替. 交流消磁法是使用交流磁头将磁盘上原先所记录信息的剩余磁通变得极小. 这种方法的消磁效果比直流消磁法要好得多，消磁后磁盘上的残留信息强度可比消磁前下降 90 db，即消磁后能将测试信号减小到初始强度的十亿分之一，满足 NSA/CSS L14－4－A 规范对信号强度 90db 消减的需求.

消磁时，介质放在强磁场中，为了使消磁更为有效，一般至少要使用相当于磁性介质矫顽磁性 5 倍的磁力，确保信息真正被消磁. 如果使用手持式磁铁，除了中间隔一层防止划伤磁盘的保护片，磁铁必须几乎直接接触磁盘. 虽然消磁是净化多数磁存储介质的最佳方法，但也有风险. 例如，在消磁周期完成之前介质被拿走、消磁器出现故障或随着使用年限的增长性能降低都会影响消磁效果.

如果整个磁性介质上的数据不加选择的被全部销毁，那么消磁是一种有效的方法. 对一些曾记载过较高密级信息的磁盘，必须使用消磁技术进行处理.

消磁最突出的特点就是高效，后果是磁盘再也不能使用. 如果希望能够循环使用硬盘，就不能够采用这种方法.

3.3　磁盘销毁

对于一些经消磁后仍达不到保密要求的磁盘或已损坏需废弃的涉密磁盘，以及曾记载过绝密信息的磁盘，必须作销毁处理.

磁盘销毁通常采用物理破坏或化学腐蚀的方法把记录涉密数据的物理载体完全破坏掉，从而从根本上解决数据泄露的问题.

常见的物理破坏方法有在熔炉中焚化、熔炼；借助外力用锤子或斧头将介质粉碎；使用研磨剂(砂轮)对磁盘或磁鼓表面进行研磨等.

化学腐蚀的方法可以使用浓缩氢碘酸(浓度 55％到 58％)溶解磁盘表面的三氧化二铁微粒. 也可以使用酸活化剂 Dubais Race A (8010 181 7171)和剥离剂 Dubais Race B (8010 181 7170)处理磁鼓记录表面，然后使用工业丙酮(6810 184 4796)清除磁鼓表面的残余物.

物理破坏方法费时、费力、效果差，基本未被广泛采用. 化学腐蚀的方法只能由得到批准的专业人员

在通风良好的环境中进行.

磁盘销毁是数据销毁效果最好的方法. 它的唯一缺点就是在数据被销毁的同时，存储器也被彻底破坏，只能用于不计代价的场合.

4 展 望

随着数据销毁技术的需求越来越强烈，数据覆写和消磁技术已在相关部门应用，磁介质的化学销毁技术还需要进一步的试验研究. 数据销毁技术不能仅仅停留在目前的简单应用，它应该向着能实现与无线电、GPS定位等技术的紧密结合的方向发展，即在紧急情况下，可以应急操作、或者能通过有线/无线方式在线/遥控清除敏感数据，有时甚至是在不加电的情况下也能够销毁数据.

参考文献:

[1] 戴士剑，涂彦晖. 数据恢复技术[M]. 2版. 北京：电子工业出版社，2005.

[2] Peter F. Bennison, Philip J. Lasher. Data Security issues relating to end of life equipment[C]. IEEE International Symposium on Electronics and the environment, 2004：317－320.

[3] Magnetic-force microscopy and micromagnetic simulations on domains of structured ferromagnets. Dissertation zur Erlangung des Doktorgrades des Fachbereichs Physik der Universitat Hamburg. Vorgelegt von Miriam BarthelmeB geb. Halverscheid aus Bochum. Huberg 2003.

[4] Adarsh Sandhu, Hiroshi Masuda, Ahmet Oral, *et al*. Room temperature magnetic imaging of magnetic storage media and garnet epilayers in the presence of external magnetic fields using a sub-micron GaAs ShPM[J]. Joural of Crystal Growth, 2001：227－228.

[5] Leo Colborne, Premier, Securing Storage. Complete Data Erasure On Storage Systems[J]. Information Storage &Securtiy Journal, 2005：1－2.

[6] 王建峰. 数据销毁：数据安全领域的重要分支[J]. 计算机安全，2006(8)：53－54.

[7] A Guide To Understanding Data Remanence In Automated Information Systems[S]. Department of Defense Manual, DoD 5220. 22-M, January 1995, Version 2.

[8] Perter Gutmann. Secure Deletion Of Data from Magnetic and Solid-State Memory[C]. the Sixth USENIX Security Symposium Proceedings. San Jose, California：USENIX, 1996, 77－90.

Research of Data Destruction Based-on Magnetic Storage Media

XU Jing[1], ZHU You-dian[2], LAI Fan[1]

1. *Faculty of Computer & Information Science, Southwest University, Chongqing, 400715, China;*

2. *The Command of the Second Artillery Missile Army, Beijing, 100085, China*

Abstract: This paper disserts the methods of destroying the data from the computer systematically and analyses the reasons that the data can't be erased thoroughly. Then the paper poses the solutions of destroying the data according to the different levels of secrecy and elaborates on the theories, methods, advantage , disadvantage and applying areas. Lastly, it makes a prospect of trend of the data destruction technology.

Key words: overwriting; degauss; disk destruction

责任编辑 汤振金