祺安系统使用痕迹分析及擦除工具

产品介绍

北京弘信安科技有限公司

2010 年 2 月

1．背景介绍

在政府机关、涉密企事业单位,尤其是安全保密部门的计算机中存储的重要、敏感、甚至是涉及国家秘密的数据，因此在挪用、弃置、转售或捐赠前必须将其所有数据彻底删除，否则会造成信息泄露。

在使用了 Windows 本身提供的删除工具，通常认为清空回收站之后，被删除的文件已经彻底消除了。不过事实并非如此，只要有专用的硬件和软件， 即使数据已经被覆盖、驱动器已经重新格式化、引导扇区彻底损坏，或者磁盘驱动器不再运转，还是可以恢复几乎所有的文件。通常情况下往往由于数据意外丢失会寻求恢复帮助，但是此技术同样也会被不法分子所利用，因此必须使用专门的工具对剩余信息进行彻底删除！

在国家政策方面有涉及国家秘密的载体的相关规定，《中共中央保密委员会办公室、国家保密局关于国家秘密载体保密管理的规定》第九条：制作秘密载体过程中形成的不需归档的材料，应当及时销毁。第三十四条：销毁秘密载体，应当确保秘密信息无法还原。国内的相关法规 BMB21-2007《涉及国家秘密的载体销毁与信息消除安全保密要求》该标准规定了涉密载体销毁和信息消除的等级、实施方法、技术指标以及相应的安全保密管理要求，适用于涉密单位、保密工作部门授权的涉密载体销毁机构对涉密载体销毁和信息消除，以及涉密载体销毁设备和信息消除产品的研制、生产和检测。

2．系统功能及特点

“系统使用痕迹分析及擦除工具”是依据国家相关保密政策、标准研制开发，应用完美的数据消除算法实现对磁盘的数据彻底销毁。主要功能包括：对文件、目录、剩余磁盘空间、分区、整个磁盘进行数据销毁消除，对操作系统和应用程序的使用痕迹及垃圾敏感数据进行清洁消除。产品操作简单快捷，可定制消除时间任务及灵活选择多种不同级别的消除算法，完全消除磁盘中的残余信息，确保数据不被恶意恢复而造成信息泄露。

2．1 主要功能

核心功能列表：

功能编号	功能	功能点
1	文件目录消除	单个或多个文件销毁消除。消除文件的相关信息，包括（文件内容、簇剩余区、文件名）。
2		单个或多个目录销毁消除
3	磁盘剩余空间数据消除	单个或多个磁盘剩余空间对残留数据销毁消除。消除磁盘剩余空间的相关信息，包括（剩余空间内容、簇剩余区（现有文件）、目录入口（已删除的）。
4	分区数据消除	单个或多个分区信息销毁消除
5	磁盘数据消除	单个或多个磁盘进行整盘信息销毁消除
6	系统清洁	分析系统的选择项目的清理后可能释放的磁盘空间或使用痕迹。 清理系统的选择项目永久删除项目包括的垃圾文件及使用痕迹。
7	应用程序清洁	分析应用程序的选择项目的清理后可能释放的磁盘空间或使用痕迹。 清理应用程序的选择项目永久删除项目包括的垃圾文件及使用痕迹。
8	系统登陆控制	系统管理员必须进行密码登录验证通过后才能使用本系统。

		帐户登录超过无效阈值控制。
9	消除审计	记录程序的启动、操作、错误记录日志，并能查看。
10	计划任务	系统能执行计划任务的文件、目录、未用磁盘空间的信息消除工作，并能正确显示任务消除状态及进度，能停止消除任务； 系统能修改已添加的计划任务的任务执行时间及消除算法。
11	选项设置	系统能正确设置常规选项中的启动、SHELL扩展、托盘参数、帐户安全选项及高级选项中的日志、报告参数。
12		能维护系统管理员登录密码，对系统管理员密码进行位数及强度校验。
13		系统能设置信息消除任务的默认擦除算法。
14	语言切换	系统界面能选择用中、英文语言展示。
15	资源管理器扩展支持	支持资源管理器的扩展操作，包括“擦除文件”、“擦除未用空间”、“消除回收站”菜单。
16	自动运行	工具随系统启动后自动运行。
17	系统分析及清理结果导出	系统清理分析、消除结果导出。

系统清理项包括：Internet Explorer 浏览器的临时文件、Cookies、历史、最近输入的网址链接、最近的下载位置、自动完成表单历史，Windows 资源管理器的最近打开的文档、开始菜单中运行的历史记录、搜索助手自动完成、资源管理器的其他搜索历史项、缩略图缓存，系统的临时文件、剪贴板、内存转储文件、CHKDSK 文件碎片、Windows 日志文件、Windows 错误报告、开始菜单快捷方式、桌面快捷方式、高级中的未用的预读数据、菜单次序缓存、托盘通知缓存、窗口大小/位置缓存、用户援助历史、IIS 日志文件、Hotfix 卸载程序、USB 设备接入信息、打印机的缓存文件、拨号连接。

应用程序的痕迹分析支持：OFFICE 系列、Adobe Acrobat Reader、 Adobe Photoshop、Windows Media Player、Real Player、XML Spy 系列、Installshield Developer、Macromedia Flash、MS Management Console、MS Wordpad、MS Paint、Nero Burning ROM、eMule、WinISO、Windows Live Messenger、WinZip、WinRAR、RegEdit、Microsoft AntiSpyware、OpenOffice、MS Office Picture Manager、ImgBurn、QQ、TM、KMPlayer、暴风影音应用程序清理。

2．2 主要技术参数

1.支持所有常见的磁盘类型和分区格式。支持 FAT16、FAT32、NTFS 4.0、NTFS 5.0 等常见分区格式，可以对各种硬盘、软盘、移动硬盘、U 盘、存储卡进行数据销毁。

2.完善的数据消除算法，确保磁介质数据信息彻底消除。根据不同的分区格式采用不同的数据消除算法，对文件、目录在磁盘上所有存放位置进行一一消除，并且能够有效的消除文件簇剩余区、文件名、磁盘渣滓、内存渣滓、及图片缩略图，对磁盘物理扇区擦写多次，确保被消除后的涉密数据无法通过技术手段恢复。

3．强大的系统及应用程序的使用痕迹及垃圾清理功能。可清理 25 种以上 Windows 系统、50 种以上应用程序的使用痕迹及垃圾。

2．3 擦除算法

1、BMB21-2007《涉及国家秘密的载体销毁与信息消除安全保密要求》

本标准规定了涉密载体销毁和信息消除的等级、实施方法、技术指标以及相应的安全保密管理要求，适用于涉密单位、保密工作部门授权的涉密载体销毁机构对涉密载体销毁和信息消除，以及涉密载体销毁设备和信息消除产品的研制、生产和检测。

2、Gutmann method

依据 1996 年奥克兰大学计算机科学学院皮特.古特曼教授在第六届 USENIX 安全会议上所作的论文-《安全删除磁固存储器上的数据》形成的信息消除技术，是至今为止最安全的数据删除方法，覆盖数据 35 次，采用此方法消除信息数据后，不论是采用软、硬件的恢

复方式均无法将所消除的数据复原，但是这种方法会耗费相当长的时间。

3、美国国防部 5220.22-M 标准

美国国防部于 1995 年提出的安全建议中所发展出来的方法。它所执行的速度比 Gutmann 快一些，不过安全性略差，可用硬件的方式让数据信息复原。只是这种方法通常很昂贵。

4、伪随机数 Pseudorandom Data

直接以伪随机数来填写磁盘上的所消除的数据信息占用空间，可定制次数。如果次数少则消除速度快。本方法可防止一般常用数据恢复软件对所消除的数据信息进行恢复。

2．4 特点

可选择使用多种级别完美高效的数据擦除方法、擦除数据不可恢复；

操作简便，易用。支持中文简体、英文语言；

提供U盘版擦除伴侣，通过U盘内预置的擦除程序进行信息消除工作；

附加强大的系统及应用程序的使用痕迹及垃圾清理功能。

3．相关规范及约定

根据 BMB21-2007《涉及国家秘密的载体销毁与信息消除安全保密要求》标准要求进行数据消除。

工具运行平台：Windows2000/XP/2003/2008/VISTA/WIN7。并能运行于以上操作系统的 32 及 64 位软硬件平台。

适应的客户群：个人用户、政府、企事业及军工单位。