"HENRI COANDA"
AIR FORCE ACADEMY
ROMANIA

GERMANY

"GENERAL M.R. STEFANIK"
ARMED FORCES ACADEMY
SLOVAK REPUBLIC

INTERNATIONAL CONFERENCE of SCIENTIFIC PAPER
AFASES 2011
Brasov, 26-28 May 2011

DATA ERASURE ON MAGNETIC STORAGE

Mihăiță IVAȘCU

Metra, Bucharest, Romania

Abstract: *User data is left is left on the hard drives removed from computers and storage systems, creating a data security vulnerability that many users are unaware of. This is mostly due the fact that normal "delete" or "format" commands leave data intact on a user computer. The cardinal rule of computer storage design has been to protect user data at all costs. Disk drives supply primary mass storage for computer systems designed to prevent accidental erasure of data. Techniques such as "recycle" folders and "unerase" commands are common ways that operating systems try to prevent accidental sanitization of user data. Deletion of file pointers is standard to speeds data writing, because actual overwriting of file data is far slower. These measures taken to protect and speed access to user data can make that data vulnerable to recovery by unauthorized persons.*

There is an urgent need for a capability to reliably erase data and prevent access to data from retired computer hard disk drives for security and privacy reasons. Data sanitization needs arise differently depending upon user application.

The current work presents standards for data erasure, most important methods of data sanitization of hard disk drives and presents how a customized method of data erasure can be implemented.

Keywords: *recycle, data sanitization, recovery, security vulnerability*

1. INTRODUCTION

When a computer is lost or disposed of, active and discarded data typically remains stored on its hard disk drive. Even if users "delete" all their files, they can be recovered from "recycling" folders or by special utility programs.

Data security has risen to be one of the highest concerns of computer professionals. There is a need for a capability to reliably erase data and prevent access to data from retired computer hard disk drives for security and privacy reasons. Data sanitization needs arise differently depending upon the user application.

2. COMPLETE ERASURE OF USER DATA

2.1 Known methods of "deleting" data. When you format or reformat a hard drive it doesn't erase the data on the drive – only the address tables. In a case where you have accidentally completed a format hard drive, a computer specialist may be able to recover most or all of the data that was on the drive.

Contrary to popular belief when a file is deleted from the computer or in Windows operating system when the recycle bin folder is emptied the actual data is not deleted. The default Recycle bin configuration for a Windows computer is to move the deleted files to a folder named \Recycler\%SID%\, where %SID% is the SID(security identifier) of the currently logged on user. Every user on the system will have such a directory created the first time Recycle bin is used. As well, each user will have a hidden file called INFO2 created the first time the Recycle bin is used – its purpose is to keep track of the deleted file(s) /folder(s) original location, as well as file size and deletion time. When the Recycle bin is emptied, the INFO2 file is "deleted" for the logged on user along with the file(s) / folder(s) it referenced. These "deleted" INFO2 files can be recovered by conducting a search for the INFO2 file header.

2.2 Approved methods for data sanitization. There are several approved methods for data sanitization that satisfy legal requirements or meet stringent corporate or government secrecy requirements. Many of them physically destroy disk drives to prevent any further use. Another data security measure is encryption of user data. According to newly released data sanitization document NIST 800-88 4, acceptable methods include executing the in-drive Secure Erase command, and degaussing. These data sanitization methods erase data against recovery even using exotic laboratory techniques. Such sophisticated techniques involve signal processing equipment and personnel with knowledge of specific drive engineering details, and can even involve removing the components from the hard disk drive for spin stand testing.

Secure erase is recognized by NIST 800-88 as an effective and secure way to meet legal data sanitization requirements against attacks up to laboratory level.

Four basic sanitization security levels can be defined: weak erase(deleting files), block erase(overwrite by external software), normal secure erase(current drives), and enhanced secure erase. The CMRR(Central of Magnetic Recording Research) has established test protocols for software secure erase.

Block erase is most commonly used. While is significantly better than no erase, or file deletion, or drive formatting, it is vulnerable to malware and incomplete erasure of all data blocks. Example are data blocks reassigned by drives, multiple drive partitions, host protected areas, device configuration, device configuration overlays, and drive faults.

Normal secure erase is approved by NIST 800-88 for legal sanitization of user data up to Confidential, and enhanced secure erase for higher levels. Enhanced level has only recently been implemented, initially in Seagate drives, and these drives are under evaluation by CMRR.

In order to erase data using secure erase and enhanced secure erase methods NIST approved hdderase.exe, a DOS-based application developed by a team at CMRR that uses the secure erase command implemented in the firmware of ATA and SATA drives manufactured after 2001. The internal firmware secure erase command can access data that is no longer accessible through software, such as bad blocks.

2.3 Implementing a data erasure software. In order to make an application to erase data under an operating system you need to implement a block erase method. An important issue to take in account is the characteristics of the operating system the application is going to run under. The most secure operating system from this point of view are the Dos-based systems that allow the implementation of secure erase and enhanced secure erase standards. For an external software that runs under an operating systems the most obvious choices are Windows and Linux operating systems. Linux has an built-in command hdparm that reports if the hard disk has hpa and dco zones and offers the option to erase these zone on disk. Also you can erase the mbr sector using this command. Windows offers the fewest option for a secure erase of hard drive because the access to the ATA registries, which permits mbr erasure and dco and hpa removal, is restricted under Microsoft based operating systems. To compensate this problem a software written under windows can be used complementary with the DOS utility hdderase in order to first remove the hpa and dco zones before proceeding to a block erase of data under windows.

Another issue to take in account when choosing the operating system is the programming environment to work in. Linux offers gcc as a compiler and builder of a project. In Windows we can work with visual studio suite. In most of the cases sources written in one medium can be recompiled in the other medium.

After electing the programming environment, you have to decide how the application will manipulate the hard disk. One option is to erase the hard disk as one logical partition one time and another option is to allow the user the possibility to select a logical partition and erase data only on that partition.

Another issue to decide is the overwriting method to be used. The central part for this type of data erasure is the standard DoD 5220. Many commercial software packages are available using variations of DoD 5220, making as many as 35 overwrite passes. But in today's drives, multiple overwrites are no more effective than a single overwrite. Off-track overwrites could be effective in some drives, but there is no such drive external command for a software utility to use. And even three overwrites can take more than a day to erase a large capacity hard disk drive. DoD 5220 overwriting has other vulnerabilities, such as erasing only to a drive's Maximum Address which can be set lower than its native capacity; not erasing reallocated(error) blocks; or miss extra partitions.

The Gutmann method is an algorithm for securely erasing the contents of computer hard drives. It does so by writing a series of 35 patterns over the region to be erased. The selection of patterns assumes that the user doesn't know the encoding mechanism used by the drive, and so includes patterns designed specifically for three different types of drives. An overwrite session consists of a lead-in of four random write patterns, followed by specific patterns 5 to 31 executed in a random order, and a lead-out of four more random patterns. Each of the patterns 5 to 31 was designed with a specific magnetic media encoding scheme in mind, which each pattern targets.

Compared to other overwriting algorithms the Gutmann method offers the best security but is the slowest and in the light of the fact that one-pass overwriting is considered enough, it it less and less preferred. Instead programmers choose to implement a one to three pass method by overwriting the disk with random bit patterns or predefined bit patterns. It usually preferred to use a defined bit pattern as the last overwriting pattern in order to be able to verify that the overwriting rendered the expected results. The most simple bit pattern would a one-pass zeroize of the entire hard disk.

Another aspect of the security of the application is the possibility to modify to method file and the jurnal file. The method file contains all the overwriting methods that the user can choose from.
The jurnal file contains all the events that the application registered from the moment the user prompted the overwriting. It is crucial to impede an attacker to modify this files, so the best way to protect them is to encrypt the files with a password known only to the user.

Lastly, the application could permit a learning mode in which the overwriting doesn't really modify the data on the disk but merely shows the user how the sectors of the drive would actually look if the overwriting would be real.

3. CONCLUSIONS

Data sanitization of hard disk drives has become an important matter from the aspect of security and privacy of user data. Regulations and standard are in place to ensure and enforce proper erasure of data user . Secure erase and enhanced secure erase built-n commands in hard drives provide the most secure methods for data sanitization but are difficult to customize. An external application implemented to run under a chosen operating system can provide a very good level of security regarding the data erasure if used complementary with standardized tools such as hdderase.

Even though the overwriting standards targeted mainly the hard disk drives they could very well be implemented for usb mass storage drives, card memory devices and tokens.

REFERENCES

1. Hughes, Coughlin, *Tutorial on disk drive data sanitization* , UCSD CMRR.
2. Kissel, Scholl, *Guidelines for media sanitization*, NIST 800-88
3. *The Gutmann method,* www.wikipedia.org