ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 6, Issue 5, May 2019

Software Implementation of the System of Additional Guaranteed Deletion of Created File Objects

Sagatov Miraziz Varisovich, Kadirov Mirhusan Mirpulatovich, Karimova Dilbar, Tojikhujaeva Nodira khonZakirovna, Khamdamova Sevara Mirazizqizi

Head of Department of Information Technologies, Tashkent State Technical University, Uzbekistan
*Assistant professor, Department of Information Technologies, Tashkent State Technical University, Tashkent, Uzbekistan.
*Assistant professor, Department of Information Technologies, Tashkent State Technical University, Tashkent, Uzbekistan.
Senior Lecturer, Department of Information Technologies, Tashkent State Technical University, Tashkent, Uzbekistan.
Doctoral student, Department of Information Technologies, Tashkent State Technical University, Tashkent, Uzbekistan.

ABSTRACT: In order to protect against the theft of the processed information in practice are widely used guaranteed removal of residual information. Since the residual information does not form any object to be identified, it should be guaranteed to be deleted when deleting or modifying the file object.

The article examines ways to delete information and selects the method of guaranteed deletion of information when building access control to created files based on their automatic markup as the baseline.

KEYWORDS: information protection, computer security, automatic marking, residual information, guaranteed deletion, platform.

I. INTRODUCTION

Protection of personal data is the primary task of most organizations and individuals. It is hard to imagine what could happen if personal data (email, photos, passwords for access to banking operations, etc. important information) fall into the hands of an attacker and he will know everything that has been stored on the hard disk. And the fact that before you sell a computer or hard drive you deleted all personal information or even formatted the hard drive, it is not always an obstacle to accessing data. And after that, with a few mouse clicks, it is very easy to restore, ostensibly deleted files. Even clearing the Recycle Bin does not help: as long as there is enough free space on the disk, the operating system will not write new files instead of old ones, therefore deleted files can be restored by a specialized utility. Even when formatting storage media, such as memory cards or flash drives, only the file allocation table is cleared [1].

Not all users understand that when a file is deleted, the content of this file is not deleted from the hard disk.

Files consist of bytes, they remain on the disk, but have nothing to do with the file system. The data itself remains on the disk until the operating system uses the re-allocated disk space to write new data. Even if you format the disk, the data will usually not be deleted. Just the content will be cleared.

In order to delete files for sure, you need to record on the place where it was stored, new data. Up to this point, the file can be restored by reading it not through the operating system, but using special software, commercial data recovery software, or manually restoring it using other methods. If the record in the sectors containing files was not made, the data physically remained in their places, but information about their location was lost or distorted. Thus, it is required to determine where exactly the sectors containing the necessary information are located and to count them in the correct sequence.

There are several ways to delete a file from a hard drive for sure or to make access to it impossible. Some ways to prevent such data leakage from the hard disk include:

- disk degaussing;

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 6, Issue 5, May 2019

- rewriting data;
- encoding;
- physical destruction of the carrier.

Destroying sensitive data on a computer hard drive or other storage medium is the best way to ensure that valuable data cannot be recovered even in the best computer labs. Destruction is crucial when moving computers that store valuable information from a safe place to a less reliable one.

An even more effective approach to deleting data is degaussing the hard disk. This method disables the hard disk. But when it is used, it will no longer be possible to use the GMD for its intended purpose. (for example using a special device - Degausser).

If you want to delete data from hard drives or other media and have a guarantee that the hard drive is usable, you need to use data erasure. This is a good solution when reusing a computer in another department of the organization. For example, if a computer in your organization is transferred to a new employee, the data will be deleted, but the computer will still remain in working condition. (The most common erasing programs are: Paragon Disk Wiper, Acronis DriveCleanser, East-Tec Eraser, Secure Eraser, HDShredder, DBAN , Wise Disk Cleaner, etc.).

Another method of getting rid of data is to rewrite all memory on all sections of the hard disk. One rewriting will be quite enough to make sure that the previous information can not be restored. It is important to remember that the simple deletion of the file by the operating system only results in the removal of the file path, the digital information in the simple deletion will be saved on the hard disk. Even reformatting or splitting a hard disk into sections is no guarantee that there will be no files left. And the files are saved, even if the user can not see them.

In the extreme case, if there is a need to completely delete files without being able to restore them, the physical destruction of the media is the best choice. Storage media can be destroyed in several ways, including direct damage to the surface of a magnetic disk or drum by abrasive materials. Corrosive chemicals will give the same results, provided that the recording surface is fully exposed.

II. STANDARDS FOR DATA DESTRUCTION

GOST P50739-95; The Russian algorithm GOST R 50739-95 is a recommended time-tested algorithm. The advantages of the algorithm include fast operation, and the disadvantages are that the algorithm does not provide for multiple recordings. According to GOST R 50739-95, it is determined that erasing is done by recording the masking information into it (Section 5.1.5 of GOST R 50739-95) [2], but the number of cycles and the content of the masking information are not indicated. It turns out that even after one recording of masking information on the HDD, for example, by alternating zero and unit codes (0x55, 0xAA), the residual magnetization from past data remains (the same effect of residual information) and it can be easily read using special equipment.

DoD 5220.22-M; NAVSO P-5239-26 (RLL). The standard of the Ministry of Defense of the USA which was widely adopted in the world [3]. A better standard than the Russian GOST R 50739-95, but nonetheless the US military has banned its use to remove information with a security stamp.

According to the American standard, erasing is performed in (E-edition of the algorithm) three cycles:
the first is that randomly selected characters are stored in each byte of each sector;
the second is recorded invert data (zero is replaced by a unit);
the third is a random sequence entry;

This cyclical nature provides a low degree of residual magnetization, which allows special tools to obtain a minimum set of residual information.

In another version of the algorithm (ECE), a sevenfold overwriting is used.

In addition to these algorithms, defined by state standards, there are a number of algorithms from independent experts in the field of information security.

Bruce Schneider An expert of world renown, in narrow professional circles, proposed the following algorithm of seven steps [3]:

1. Filling units over existing data
2. Filling with zeros over existing data
3. Record random data
4. Record random data
5. Record random data
6. Record random data

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 6, Issue 5, May 2019

7. Record random data

No, this is not a mistake, the expert suggests five times to fill the HDD with random data. Although, Schneider himself later stated:

"Recent studies .... using tunneling microscopes have shown that even this may not be enough."

III. Peter Gutmann ALGORITHM

Gutman proposed an algorithm with multiple cycles that are focused on the destruction of records, using equipment that supports MFM / RLL technology (magnetic force recording using coding) when a random sequence of encrypted information from 35 cycles is recorded. Although, Gutman himself in this article gives a note [4] that manufacturers of new HDDs already support this technology.

One of the standard methods for recovering data overwritten to a hard disk is to capture and process an analog signal obtained from a read/write drive, before this signal is digitized. This analog signal is close to digital, but the differences reveal important information. By calculating a digital signal, and then subtracting it from the actual analog, you can amplify the signal remaining after subtraction, and use it to determine what was previously written on the disc

For example:

Analog signal: +11.1 -8.9 +9.1 -11.1 +10.9 -9.1 Ideal Digital signal: +10.0 -10.0 +10.0 -10.0 +10.0 -10.0 Difference: +1.1 +1.1 -0.9 -1.1 +0.9 +0.9
Previous signal: +11 +11 -9 -11 +9 +9

This procedure can be repeated to see previously recorded data:

Recovered signal: +11 +11 -9 -11 +9 +9 Ideal Digital signal: +10.0 +10.0 -10.0 -10.0 +10.0 +10.0 Difference: +1 +1 +1 -1 -1 -1 Previous signal: +10 +10 -10 -10 +10 +10

Even when repeatedly rewriting a disk with random data, it is theoretically possible to restore the previous signal. The dielectric constant of the medium varies with the frequency of the magnetic field. This means that the low frequency of the field penetrates deeper into the magnetic material on the disk than the high frequency thereof. Thus, a low-frequency signal can theoretically be determined even after rewriting has been done hundreds of times at a high frequency of the signal.

The passages used are designed to apply an alternating magnetic field of various frequencies and different phases on the surface of the disk, thereby approximating the demagnetization of the material under the surface of the disk.

The composition of the rewritable session is as follows: randomly selected characters are written to each byte of each sector in the first 4 passes, a specific sequence of characters is recorded from 5 to 31 passes (see lines from the table below), randomly selected characters are again recorded in the last 4 passes.

Each pass from 5 to 31 was designed with a specific magnetic encoding scheme, that is, as a target pass. All tracks are recorded on the disc, although the table shows only bit passes for tracks that are specifically oriented on each coding scheme. The end result should hide any data on the disk, so that only the most advanced physical scanning technology (for example, using a magnetic power microscope) drive is likely to be able to recover any data.

The algorithm of this method is as follows (table 1.1).

Table 1.1. Algorithm Method Gutmann

ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 6, Issue 5, May 2019

Pass	Record		Template		
	In the 2nd form	In the 16th form	(1,7) RLL	(2,7) RLL	MFM
1	(By chance)	(By chance)			
2	(By chance)	(By chance)			
3	(By chance)	(By chance)			
4	(By chance)	(By chance)			
5	01010101 01010101 01010101	55 55 55	100…		000 1000…
6	10101010 10101010 10101010	AA AAAA	00 100…		0 1000…
7	10010010 01001001 00100100	92 49 24		00 100000…	0 100…
8	01001001 00100100 10010010	49 24 92		0**0**00 100000…	**1**00 100…
9	00100100 10010010 01001001	24 92 49		100000…	00 100…
10	00000000 00000000 00000000	00 00 00	101000…	1000…	
11	00010001 00010001 00010001	11 11 11	0 100000…		
12	00100010 00100010 00100010	22 22 22	**0**0**0**00 100000…		
13	00110011 00110011 00110011	33 33 33	10…	1000000…	
14	01000100 01000100 01000100	44 44 44	**0**00 100000…		
15	01010101 01010101 01010101	55 55 55	100…		000 1000…
16	01100110 01100110 01100110	66 66 66	**0**000 100000…	0**0**0000 10000000…	
17	01110111 01110111 01110111	77 77 77	100010…		
18	10001000 10001000 10001000	88 88 88	00 100000…		
19	10011001 10011001 10011001	99 99 99	0 100000…	00 10000000…	
20	10101010 10101010 10101010	AA AAAA	00 100…		0 1000…
21	10111011 10111011 10111011	BB BBBB	00 101000…		
22	11001100 11001100 11001100	CC CCCC	0 10…	0000 10000000…	
23	11011101 11011101 11011101	DD DDDD	0 101000…		
24	11101110 11101110 11101110	EE EEEE	0 100010…		
25	11111111 11111111 11111111	FF FFFF	0 100…	000 100000…	
26	10010010 01001001 00100100	92 49 24		00 100000…	0 100…
27	01001001 00100100 10010010	49 24 92		0**0**00 100000…	**1**00 100…
28	00100100 10010010 01001001	24 92 49		100000…	00 100…
29	01101101 10110110 11011011	6D B6 DB		0 100…	
30	10110110 11011011 01101101	B6 DB 6D		100…	
31	11011011 01101101 10110110	DB 6D B6		00 100…	
32	(By chance)	(By chance)			
33	(By chance)	(By chance)			
34	(By chance)	(By chance)			

ISSN: 2350-0328
International Journal of AdvancedResearch in Science, Engineering and Technology
Vol. 6, Issue 5, May 2019

35	(By chance)	(By chance)			

In bold, the coded bits are highlighted, which should be represented in the ideal model, but due to the coding of the extra bits, they are actually at the beginning.

IV. RESULT

This program module of additional guaranteed deletion of file objects created on the basis of their automatic markup is designed to clean the computer from various debris and speed up the operating system. It has a user-friendly interface.

Over time, a lot of information accumulates on the hard disk of a computer. These are temporary and not used files for a long time, their duplicates, not completely deleted programs, various logs and system data, registry errors, missing entries and much more. All this is not enough that takes up too much space, it also reduces the performance of the computer, it also increases the possibility of breaching information security. To clean the operating system from all of this, a software module of an additional guaranteed removal was created, designed to find and remove (fix) all unnecessary, without disturbing the stability of work.

First you need to install it on a computer that has a standard process (Figure 1.).

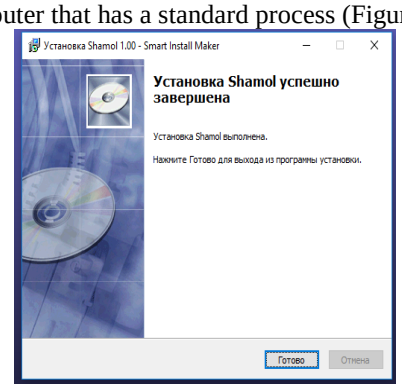

Figure 1. Successful completion of the installation

After installing and running the software module for the additional guaranteed removal, you can see the “Shamol” item in the context menu of the operating system (Figure 2). This item in the context menu performs the function of guaranteed deletion of information based on the algorithm given in section 3.

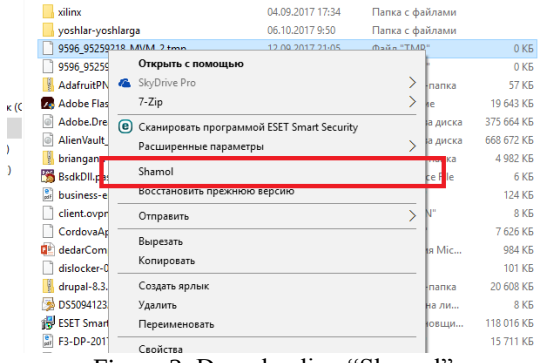

Figure 2. Downloading “Shamol”

V. CONCLUSION AND FUTURE WORK

Ways of deleting information are examined and the method of guaranteed deletion of information is chosen as the base when building access control to the created files based on their automatic markup.

An algorithm for the sequence of guaranteed deletion has been developed and software methods for deleting information have been considered.

ISSN: 2350-0328

International Journal of AdvancedResearch in Science, Engineering and Technology

Vol. 6, Issue 5, May 2019

REFERENCES

[1] Tashkov P A. Vosstanovleniyedannых na 100 % (+CD). Piter 2008. p.208.

[2] GOST R 50739-95 “Computing facilities. Protection against unauthorized access to information. General technical requirements. Resolution of the State Standard of Russia of February 9, 1995 No. 49

[3] American national standard DoD 5220.22-M. 1995.

[4] D.Rugar, H.Mamin, P.Guenther, S.Lambert, J.Stern, I.McFadyen, and T.Yogi. "Magnetic force microscopy: General principles and application to longitudinal recording media", Journal of Applied Physics, Vol.68, No.3 (August 1990), p.1169.

AUTHOR’S BIOGRAPHY

SagatovMirazizVarisovich-Doctor of technical sciences. Professor in department of “Information technologies” Tashkent State Technical University named after Islam Karimov. Author of 2 monographs, 4 textbooks, 4 patents and 200 scientific articles.

KadirovMirhusanMirpulatovich. Assistant professor.

.

Has more than 90 published scientific works in the form of articles, journals, theses and tutorials. Currently works at the department of “Information technologies” in Tashkent State Technical University.

Karimova Dilbar.Assistant professor.

Has more than 20 published scientific works in the form of articles, journals, theses and tutorials. Currently works at the department of “Information technologies” in Tashkent State Technical University.

TojikhujaevaNodirakhonZakirovna.Senior Lecturer.

Has more than 18 published scientific works in the form of articles, journals, theses and tutorials. Currently works at the department of “Information technologies” in Tashkent State Technical University.

KhamdamovaSevaraMirazizqizi.Doctoral student.

Has more than 8 published scientific works in the form of articles, journals, theses and tutorials.