Clearing and Sanitization of Media Used for Digital Storage: Towards Recommendations for Secure Deleting of Digital Files

Kruno Golubić
University Computing Centre
University of Zagreb
Josipa Marohnića 5, 10000 Zagreb, Croatia
kruno.golubic@srce.hr

Hrvoje Stančić
Faculty of Humanities and Social Sciences
University of Zagreb
Ivana Lučića 3, 10000 Zagreb, Croatia
hstancic@ffzg.hr

Abstract. *Simply deleting files with tools that are shipped with operating system isn't good option if security and privacy are primary goals. To achieve secure deletion of digital files specialized tools or software must be used. Methods that are used differ from one case to another depending on goals that need to be accomplished – whether media will be reused or disposed. At the moment there is no public recommendation in Croatia how should one treat these security challenges. Certain institutions and organizations have their own internal procedures and security policies that are available only on the "need to know" basis. Therefore, the authors provide pointers to the publicly available documents from other countries, which one could use for creation of its own polices and rules. This is an on-going process that should follow advancing trends in technology.*

Keywords. secure deletion, sanitization, clearing, recommendations

1 Introduction

Sometimes deleting files with tools that come with operating system is just not good enough option if one want's to be sure than no one can restore the deleted data. Reason for this is the fact that "files that are deleted by the user entering a delete command are not really deleted… only the references to the file are deleted from the file system administration information… the actual content of the blocks on the data medium is retained and can be reconstructed with the appropriate tools" [17, 344]. Also, there are situations when deleting files is more complex operation due to physical attributes of media, e.g. WORM media. [18] Today some data storage devices have embedded technology that makes device unusable in case of security breach [11]. Besides loss of equipment due to theft or misplacement, data can be exposed due to inadequate method of media disposal. [6]

To prevent such security incidents one should take precautionary measures in form of proper media handling and use of specialized hardware and software for deletion of digital files. If security polices exist within organization, one should follow them during the everyday work. A problem could occur if no policies are established or if users are not skilled to act according to the policies. As of the moment of writing, the authors are aware that there is no publicly available document in Croatia which could be used as a general reference in creation of security policies.

Importance of proper storage media sanitization (concept of sanitization will be explained in detail later in this paper) before decommission is stressed in article by Garfinkel and Shelat [10]. In their article they list numerous cases where confidential and private data was revealed due to lack of proper procedure before decommission of computer equipment. They have also conducted their own research in which they have bought numerous used hard drives in attempt to recover files from them, and they were successful in their attempt.

2 Relevant bodies, agencies and organizations in Croatia

The Security and Intelligence System Act of the Republic of Croatia [1] defines the Information Systems Security Bureau (ZSIS) as the central state authority responsible for the technical areas of information security of the state bodies. ZSIS is responsible for security of information systems and networks of the state bodies, for managing cryptographic materials used in the exchange of classified information between the state bodies and foreign countries and organizations, and for coordination of prevention and removal of incidents related to computer networks security of the state bodies. [26]

Within their competencies ZSIS creates recommendations that are available to public on their web site (http://www.zsis.hr). Besides public recommendations ZSIS also issues ordinances that are distributed only to interested state bodies. These ordinances are classified as “restricted” or “unclassified” in accordance with the Data Secrecy Act [5]. Article 48 of the Regulation on Information Security Measures [25] states that procedures regarding deletion, repair and destruction of medium used for data storage should be conducted in compliance with prescribed procedures.

Due to the fact that authors didn’t have access to earlier mentioned procedures, documents and ordinances they are not discussed in this paper. It is understandable why these documents are not publicly available. If they were available to the general public, such information could be exploited by malicious individuals or organizations as part of directing attack in attempt to gain unauthorized access to data.

The Croatian National CERT was established in accordance with the Information Security Act of the Republic of Croatia [15] and its main task is processing of incidents on the Internet, i.e., preservation of the information security in Croatia. According to the National CERT Operations policy, it deals with the incident only if one party of the incident is in the Croatian IP address space or in .hr Internet domain. National CERT’s power to act comes from its jurisdiction issue instructions, guidelines, recommendations, advice and opinions. [19]

On its web site (http://www.cert.hr), beside security warnings and recommendations, National CERT also has a list of tools that can be used for different security related tasks. Among those tools it is possible to find some tools that can be used for secure deletion operations. At the time of writing, category of tools for secure deletion had only two entries [20] but authors believe that the reason for this, rather low, number of tools lays in the fact that the tools can have only one category assigned at time. Simple Google search with query “site:cert.hr sigurno brisanje” (i.e. site:cert.hr secure deletion) returns a broader list of tools that have secure deletion capabilities but are classified as spyware tools, cryptography tools, etc. National CERT has also published documents on various security topics but authors didn’t find any document that would address issues of secure deletion as the main topic.

The authors have sent a survey via e-mail to the Croatian Personal Data Protection Agency (AZOP) regarding regulations or ordinances that define actual procedure how should data be properly destroyed. In their written reply they have stated that neither the Act on Personal Data Protection nor other subordinate regulations in field of personal data protection define methods for destroying personal data. They have also stated that data controllers of databases that contain personal information should form internal regulations and ordinances that would define methods and ways to delete or destroy personal information. [4] At AZOP’s web site (http://www.azop.hr) there is legal framework and additional documentation available.

Further, the survey was sent by e-mail to the Croatian State Archives. They have stated that within laws and ordinances there are neither technical details nor suggestions what methods should be used. They have stated that in the case of documents that are not stored in digital form (paper records) the problem is not the method of physical destruction of media but assurance that all copies of a document have been destroyed. [9] The authors would like to stress the fact that the same principle can also be applied to digital documents. When deleting or destroying a digital document one should be sure that there are no other copies of the same document.

3 Recommendations from other countries

There are numerous books and papers that deal with computer security and forensics. Besides those, very good sources of information on IT security are public documents published by different government bodies across the world. Some of those documents are:

- National Industrial Security Program: Operating Manual [21]
- IT Security Guidance: Clearing and Declassifying Electronic Data Storage Devices [16]
- IT-Grundschutz Manual [17]
- Australian Government Information Security Manual: Controls [2]

Based on those mentioned, and a number of adjacent documents, the authors will provide pointers and explanations of the most important terms and concepts related to the secure deletion of digital files.

IT-Grundschutz Manual stresses that “It should be borne in mind that data is not effectively removed from the hard disk either through purely logical deletion or by reformatting the disks using the relevant functions of the operating system installed. Data which has been deleted in this way can be reconstructed with certain software, often at no great effort or cost“. [17, 147]

Clearing and *sanitization* are two terms that are often mentioned in the context of data handling and deletion and data storage media. There is a difference between how certain resources define and distinguish between those two terms. We will take a closer look at two sources, National Industrial Security Program (DoD 5220.22-M) [21] and IT Security Guidance (ITSG-06) [16], for definitions of those terms.

DoD 5220.22-M defines *clearing* as “the process of eradicating the data on media before reusing the media in an environment that provides an acceptable level of protection for the data that was on the media before clearing. All internal memory, buffer, or other reusable memory shall be cleared to effectively deny access to previously stored information". *Sanitization* is defined as "the process of removing the data from media before reusing the media in an environment that does not provide an acceptable level of protection for the data that was on the media before sanitizing. Information System (IS) resources shall be sanitized before they are released from classified information controls or released for use at a lower classification level." [21, 75]

Definitions from ITSG-06 are similar to the earlier mentioned ones. In addition to the definition, a simple explanation is also given. Regarding EDSD (Electronic Data Storage Devices) ITSG-06 defines *clearing* as "the process of erasing an EDSD in a manner that allows it to be re-used within an equivalent or higher security environment. Clearing must be adequate to prevent data recovery using tools normally available on the Information System. Simply deleting or erasing the files or formatting a disk does not clear the media, because commands such as *undelete* or *unformat* may permit the recovery of the data. The clearing process is not expected to be proof against "hands-on" recovery methods using specialized IT utilities or laboratory techniques. For this reason, cleared media must be retained within security environments appropriate to the highest level of data the media once contained, and cannot be considered for declassification." *Sanitization* is defined as "the process of erasing or destroying an EDSD in a manner that precludes any reasonable hope[1] of recovery of the data – i.e., the risk of compromise following sanitization is low or non-existent. In addition to destroying the data, the sanitization process includes the manual removal of external indications that the device once contained sensitive data. EDSDs that have been sanitized may be declassified and disposed of as unclassified waste or as surplus equipment for sale or recycling."[16, 5]

Regardless of the fact that both sources are in their definitions oriented at classified data, those definitions can also be taken in consideration when talking about data that has no classification level associated with it. While in business environment it is not rare to find examples of data classification policies that define classification levels, it can be presumed that classification levels are not used for personal (home) use.

Australian Government Information Security Manual: Principles document [3, 33] gives only a short definition of terms regarding methods of media sanitization, destruction and disposal. More in-depth explanations are given in Australian Government Information Security Manual: Controls document [2]. This document defines *sanitization* as "the process of removing information from media. It does not automatically change the sensitivity or classification of the media, nor does it involve the destruction of media." [2, 131] Later, in the same document, it is stated that "some types of media cannot be sanitised and therefore must be destroyed. It is not possible to use these types of media while maintaining a high level of assurance that no previous data can be recovered." [2, 132]

Clearing or sanitization can be achieved with the use of special software or hardware tools. Software can be either platform dependent or independent. Hardware tools are not so much associated with clearing process as much with sanitization process. Depending on the media, proper tools should be used. DSS Clearing and Sanitization Matrix [8] gives a good review of different media types and methods that should be used for clearing or sanitization. This matrix shows that for certain data-bearing-media types, more than one action (method) should be used during cleaning or sanitization. As an addition to the matrix, summary information is provided for destruction of classified media. We will point out only to a few such methods: incineration, application of abrasive substance, degaussing or destruction, melting, disintegrating, pulverizing, destroying by the use of chemicals, etc. Some of the listed methods can be used only for one type of media while others can be used for broader spectrum of media types. It is important to mention that, although older versions of DSS Clearing and Sanitization Matrix can still be found on the Internet, current versions are now part of ISFO Process Manual [22]. This manual is not available to the general public due to the fact that "a number of documents have been removed from the ODAA portion of the Defence Security Service website. However, these documents remain available to cleared industry and are available upon request". [7]

Annex B of the IT Security Guidance [16,23] lists and explains in details the following methods for destruction of digital files or media on which they are stored: clearing, sanitizing, encryption, overwriting, degaussing, emergency destruction via physical deformation, shredding and disintegration, grinding and hammer-milling, materiel molecular separation, surface grinding for optical disks, knurling, incineration.

As it can be seen different sources recommend different methods for clearing and sanitization. If we focus on the non-destructive methods we can see that overwriting is mentioned quite often. The authors believe that this is due to the fact that this method does not require special hardware tools and it allows media to be reused (if media is such that it allows data to be physically overwritten, e.g. hard disk, magnetic tape). There is an on-going debate about the number of times that media should be overwritten to prevent possible recovery using forensic software or tools.

Schneier (1995) says that "most commercial programs that claim to implement the DoD standard

[1] Reasonable hope – if a threat agent with opportunity, motivation and capability believes the presumed value of the data is worth the time and cost of the attempt to recover it.

overwrite three times" but he recommends "overwriting a deleted file seven times: the first time with all ones, the second time with all zeros, and five times with a cryptographically secure pseudo-random sequence". [23, 229]

Gutmann (1996) says that one should use "use the sequence of 35 consecutive writes" [14]. Latter he has offered additional explanation that "for any modern PRML/EPRML drive, a few passes of random scrubbing is the best you can do… it's unlikely that anything can be recovered from any recent drive except perhaps a single level via basic error-cancelling techniques." [24] Despite this fact, there are still software tools available that offer Gutmann method as a way for file deletion or cleaning of free space. [13]

Information Security Manual states that there are differences between hard disks based on their capacity or date of manufacturing. Hard disks manufactured before 2001 or those smaller than 15GB should be sanitized by "overwriting the media at least three times in its entirety with a random pattern followed by a read back for verification". Hard disks manufactured after 2001 or larger than 15GB should be sanitized by "overwriting the media at least once in its entirety with a random pattern followed by a read back for verification". It also states that "the Advanced Technology Attachment (ATA) secure erase command was built into the firmware of post-2001 devices and is able to access sectors that have been added to the g-list". G-list contains list of bad sectors on a hard disk which cannot be accessed by software for sanitization. [2, 133]

Similarly, Guidelines for Media Sanitization state that "the advancement of technology has created a situation that has altered previously held best practices regarding magnetic disk type storage media… That is, for ATA disk drives manufactured after 2001 (over 15 GB) clearing by overwriting the media once is adequate to protect the media from both keyboard and laboratory attack". [12, 6]

4 Recommendations and conclusion

As it was shown there are state bodies and agencies in Croatia that are in charge of computer-related security and personal information issues but none of them have publicly available documents on the topic of secure deletion. Authors believe that individuals and companies should have at least some general guidelines for security-related issues such as secure deletion of digital files. Such guidelines could help companies and individuals in their effort to protect the important business and personal data. Companies, organizations and individuals should be informed how to treat media that has or had digital data stored on it. This can be especially relevant in the case of decommission – whether the media will be sold as used or it will be recycled or thrown away as trash.

As mentioned earlier, if a goal is to delete or destroy all copies of a digital file one should know whether copies do exist and where do they reside. This means that if those files were created as a part of backup procedures, in regular or irregular time intervals, all traces of those files should also be deleted from the backup. This procedure can be even more time consuming and can presume some additional hardware or software tools capable of such operations. To successfully complete deletion or destruction of such files one should have access to all backup archives. Deletion of such files can represent great challenge if a backup media is a write-once media like CD or DVD. Such situation would require duplication of existing backup archive without files that need to be destroyed. Situation can get even more complicated if incremental or differential backup methods were used, but this goes beyond scope of this article.

It is recommended to use one or more of many available software products or hardware devices that are available on market these days. Also, beside tools that are used for secure deletion, the authors would also recommend usage of forensic programs, e.g. data recovery tools, to make sure that the data is really deleted. This can be rather time consuming task but if one wants to be sure that the data is no longer available there is no other way, except for physical destruction of the data carrier..

Although physical destruction of media is a method that can offer the greatest level of security, such method is not always welcome. In situations where a single file should be deleted usage of such extreme method doesn't make sense. Physical destruction of media can be recommended when the whole media should be destroyed and no other method, such as overwriting, could provide satisfying result. DVD and CD-R are good examples of such media.

It is important to keep track of technology and its advancement. As shown, recommendations for clearing and sanitization are greatly influenced by the state of technology. It is logical to presume that advancement of technology in the field of data storage will also lead to advancement of forensic technology that can be used for data restoration. If security and data protection is one of the key demands, hardware specifications should be closely examined to see if some mode of protection is already implemented into storage device or the medium itself.

At the end, we would strongly recommend that a public recommendation at the national level is created, taking into account the advancement of technology and explained proved international best practices.

The authors will, in their further research, focus on these and similar important topics, more closely to the surveying and testing of the methods and available software solutions.

References

[1] Act on the Security Intelligence System of the Republic of Croatia. http://www.zsis.hr/Site/LinkClick.aspx?fileticket=JNkeRilvsmI%3d&tabid=69&mid=488, downloaded: March 23rd 2012.

[2] Australian Government Information Security Manual: Controls. http://www.dsd.gov.au/publications/Information_Security_Manual_2012_Controls.pdf, downloaded: March 23rd 2012.

[3] Australian Government Information Security Manual: Principles. http://www.dsd.gov.au/publications/Information_Security_Manual_2012_Principles.pdf, downloaded: March 23rd 2012.

[4] Correspondence between Kruno Golubić and Croatian Personal Data Protection Agency, 17 March 2011, 29 March 2012

[5] Data Secrecy Act. http://www.zsis.hr/Site/LinkClick.aspx?fileticket=ORnfuvKK%2bFk%3d&tabid=136&mid=488, downloaded: March 23rd 2012.

[6] Diesburg, S, Wang, A. A Survey of Confidential Data Storage and Deletion Methods. ACM Computing Surveys (CSUR), 43 (1), 2010.

[7] Document Request. http://www.dss.mil/isp/odaa/request.html, downloaded: March 23rd 2012.

[8] DSS Clearing and Sanitization Matrix. http://www.oregon.gov/DAS/OP/docs/policy/state/107-009-005_Exhibit_B.pdf?ga=t, downloaded: March 23rd 2012.

[9] E-mail correspondence between Kruno Golubić and Croatian State Archives, 2 March 2011, 29 March 2012

[10] Garfinkel, S, and Shelat, A. “Remembrance of Data Passed: A Study of Disk Sanitization Practices”. IEEE Security and Privacy, (1)1: 17 - 27, 2003.

[11] Garfinkel, S. Complete Delete vs. Time Machine Computing. ACM SIGOPS Operating Systems Review, 41 (1): 42 - 44, 2007.

[12] Guidelines for Media Sanitization. http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf, downloaded: March 23rd 2012.

[13] Gutmann method. http://en.wikipedia.org/wiki/Gutmann_method#Software_implementations, downloaded: March 23rd 2012.

[14] Gutmann, P. Secure deletion of data from magnetic and solid-state memory. SSYM'96 Proceedings of the 6th conference on USENIX Security Symposium, pages 77–90, San Jose, USA, 1996.

[15] Information Security Act. http://www.zsis.hr/Site/LinkClick.aspx?fileticket=evhpScf1ReY%3d&tabid=69&mid=488, downloaded: March 23rd 2012.

[16] IT Security Guidance: Clearing and Declassifying Electronic Data Storage Devices. http://www.cse-cst.gc.ca/documents/publications/itsg-csti/itsg06-eng.pdf, downloaded: March 23rd 2012.

[17] IT-Grundschutz Manual. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/download/it-grundschutz-kataloge_2005_pdf_en_zip.zip?__blob=publicationFile, downloaded: March 23rd 2012.

[18] Mitra, S, Winslett, M. Secure deletion from inverted indexes on compliance storage. StorageSS '06 Proceedings of the second ACM workshop on Storage security and survivability, pages 67-72, Alexandria, USA, 2006.

[19] Nacionalni CERT, About us. http://www.cert.hr/en/start, downloaded: March 23rd 2012.

[20] Nacionalni CERT, Alati. http://www.cert.hr/alati?field_tool_cat_value=SFD&field_os_value=All&body=, downloaded: March 23rd 2012.

[21] National Industrial Security Program: Operating Manual. http://www.dss.mil/documents/odaa/nispom2006-5220.pdf, downloaded: March 23rd 2012.

[22] ODAA Links. http://www.dss.mil/isp/odaa/odaa_links.html, downloaded: March 23rd 2012.

[23] Schneier, B. Applied Cryptography: Protocols, Algorithms and Source Code in C. John Wiley & Sons; New York, USA, 1996.

[24] Secure Deletion of Data from Magnetic and Solid-State Memory. http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html, downloaded: March 23rd 2012

[25] Uredba o mjerama informacijske sigurnosti. http://narodne-novine.nn.hr/clanci/sluzbeni/339036.html, downloaded: March 23rd 2012.

[26] ZSIS, About us. http://www.zsis.hr/Site/Default.aspx?alias=www.zsis.hr/site/eng, downloaded: March 23rd 2012.