Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Securely Deleting Files

John Kinney

1. Introduction

Many people and companies spend thousands of dollars to secure their sensitive information and to protect it from unauthorized disclosure. They spend dollars on security isolation devices like firewalls, they install and use good authentication, and they require strong passwords to protect their computer information. Most companies practice other good security protection measures like shredding all sensitive paper and documents. Companies and individuals understand that they must protect their information.

But, when it comes time to replace their old and outdated computers with new systems, are all necessary steps taken to properly protect the information that may still reside on the old computers.

Many times the company or individuals tries to sell there old systems to unknown individuals or they simply try to do the civic minding thing and donate they're old computer to schools, and other non-profit organizations.

Companies and individuals must ensure that all information is totally destroyed and not recoverable before they lose control of their systems. If you are disposing of a computer system, you must make sure all sensitive files contained on the hard drive(s) has been completely destroyed by using a disk wiping utility or some form of secure delete program. The information on your computer and disks is a valuable asset, and we must ensure that it is protected or completely destroyed.

2. Information Storage

There are many different types of storage disks, from the simple floppy disk to the large volume IDE and SCSI hard disk drives. No matter what type of disk, they all involve turning some kind of magnetic pulses on and off as the disk moves under the magnetic read/write head(s). The various characteristics of how the information gets placed on the disk depends on the computer operating system, how much information can be put in a given space on the disk, and the precision and quality of the read/write heads.

Disks provide long-term, inexpensive method of storing information. Disks have different physical characteristics as well as different software requirements. The method of connecting the disk to the computer can also be different. But, the basic concept for all disk types is basically the same. The media stores information on the disks by writing magnetic pulses (0'and 1"s) on specific spaces (cluster or sectors) on the disk media. The number of cluster or sectors used to store files or programs can expand and contract depending on the size of the file or program. The computer operating system keeps track of where specific files and programs were placed on the disk (what cluster or sector) and

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

provides instructions on how and were to retrieve specific files and programs to access the information when needed. The operating system also keeps track of what cluster or sectors contain previously stored information that cannot be overwritten and what clusters or sectors are free for the system to use to write new information.

Deleted Files

Contrary to popular belief, deleting files and programs on disks does not erase or overwrite the information on the disk. Delete and erase commands simply removes the flags or pointers that tells the computer's operation system what specific clusters or sectors are being used to store the information. Removing the flags or pointers tells the operating system that the clusters or sectors can be reused by the computer for saving other files and programs. All of the information (0's and 1's) are still on the disk and can be easily recovered. Until those specific clusters or sectors are overwritten by new information (0' and 1's) the original information can be recovered.

Most modem operating systems have added addition features that place deleted files in a recovery folder. Files will remain protected in this folder and will not be overwritten and destroyed until they are deleted a second time. This feature allows the user to retrieve and totally recover deleted files. Once the files are deleted out of the recovery folder the spaces or cluster or sectors can be reused by operating system.

Many software manufactures (Norton Utilities UnErase, etc.) offer a wide range of programs that will search your disk and try to recover deleted files. If the clusters or sectors that originally contained the deleted file information have not been overwritten, the UnErase programs can normally completely recover deleted files.

Formatting

Most operating systems store information on your disk is two areas, the system area and data area. The system area contains bookkeeping information that tells the computer what kind of disk is being accessed, how to read the information and what specific clusters or sectors were used to store the data. The data area contains the actual data from your files. When you format a disk the operating system normally only overwrites the system information. This will erasing all information about where specific files were located on the disk, but does not overwrite the entire disk or the data area of the disk that contains the stored information. Since the information (0's and 1's) still resides on the disk it can be recovered.

Some format commands do overwrite all areas of the disk such as floppy disks and some older DOS format commands will overwrite the entire disk, however most simply overwrite the system information.

Other files

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Most operating systems like Windows creates and maintains the original files, but while processing, printing, moving or coping data files, portions of the original file may be stored in various locations on the hard drive. Swap files, .TMP files, and spool files are all files that the computer uses to temporarily store and process information. Most users believe that the information has been deleted and cannot be recovered or don't even realize that the information was temporarily stored in other locations. These type of temporary files maybe recovered using software programs on the market (such as Power Quest's Lost & Found).

Disk Editors

As described above deleted files can normally be recovered using various unerase or recovery programs. Once, the disk media has been formatted or repartitioned these unerase programs may not recover the files. Once the disk has been formatted or partitioned the disk will indicate that the disk does not contain any information or files, however until you overwrite all disk clusters or sectors information from a previously stored files can be read and recovered by a disk editor. Disk editors read data directly from the disk clusters or sectors, therefore they can read partially overwritten information or information that is not normally recoverable using other file recovery software. There are many other software programs available (Encase) that can read directly from the disk, analyze the information and recover information and files.

Destroy your Information

If and when you ever dispose computer equipment or disks that have contained sensitive information, be sure to take precautions to ensure that all information is not only deleted, but it is completely destroyed. Simply deleting a file is not sufficient to prevent a clever user from undeleting the file and recovering sensitive information

Many software programs are available such as Norton Utilities Wipeinfo, Shredder, Secure Clean and BC Wipe that addresses these problems by completely overwriting disk media and completely eliminating unwanted data. The cleaning process should securely overwrite all cluster or sectors at least three times to ensure that the information has been completely destroyed.

Some highly sophisticated techniques are available that may be able to recover information from a disk even after it has been overwritten. If your information is highly sensitive you may need to take additional steps such as physically destroying the disk or degaussing the drives.

Conclusion

Disks provide long-term storage of information and will retain the information until it has been overwritten by new information. Simply deleting files only removes markers used by the operating to prevent the files from being inadvertently overwritten by new data. It

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

is vital that computer resources released out of our control be completely overwritten to protect sensitive information that may be retained on the disk media. If the information is highly sensitive them additional measures such as physical destruction of the disks may be required.

Jim Aspinwall and Mike Todd. "Trouble Shooting Your PC", MIS:Press p. 390

"Secure File Wiping", Tao Security
http://security.tao.ca/why-real-delete.shtml

Gutmann, Peter. "Secure Deletion of Data from Magnetic and Solid-State Memory", Aug 31 2000
http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html
http://security.tao.ca/secure_del.shtml

Holley, James "Computer Forensics", SC Info Security Magazine, Sep 2000, p56

"Format" September 1 1996
http://webopedia.internet.com/TERM/f/format.html

http://security.tao.ca/secure_del.shtml

© SANS Institute 2000 - 2002, Author retains full rights.

Last Updated: April 18th, 2014

Upcoming Training

Click Here to {Get CERTIFIED!}

SANS Austin 2014	Austin, TX	Apr 28, 2014 - May 03, 2014	Live Event
Community SANS Albuquerque	Albuquerque, NM	Apr 28, 2014 - May 03, 2014	Community SANS
Community SANS Toronto	Toronto, ON	Apr 28, 2014 - May 03, 2014	Community SANS
Security Leadership Summit	Boston, MA	Apr 29, 2014 - May 07, 2014	Live Event
Community SANS Atlanta	Atlanta, GA	May 05, 2014 - May 10, 2014	Community SANS
Mentor Session - SEC401	Jackson, MS	May 07, 2014 - Jul 09, 2014	Mentor
SANS Security West 2014	San Diego, CA	May 08, 2014 - May 17, 2014	Live Event
SANS Secure Europe 2014	Amsterdam, Netherlands	May 10, 2014 - May 24, 2014	Live Event
SANS Security West 2014 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	May 10, 2014 - May 15, 2014	vLive
Community SANS Madison	Madison, WI	May 12, 2014 - May 17, 2014	Community SANS
Mentor Session - SEC 401	Williamsburg, VA	May 14, 2014 - Jul 16, 2014	Mentor
Mentor Session - SEC 401	Champaign, IL	May 15, 2014 - Jul 17, 2014	Mentor
SANS Bahrain May 2014	Manama, Bahrain	May 17, 2014 - May 22, 2014	Live Event
Mentor Session - SEC 401	Ft Lauderdale, FL	May 22, 2014 - Jul 24, 2014	Mentor
Mentor Session - SEC 401	Tulsa, OK	May 27, 2014 - Jul 29, 2014	Mentor
Community SANS Naperville	Naperville, IL	Jun 02, 2014 - Jun 07, 2014	Community SANS
SANS Rocky Mountain 2014	Denver, CO	Jun 09, 2014 - Jun 14, 2014	Live Event
Mentor Session - SEC 401	Seattle, WA	Jun 09, 2014 - Aug 11, 2014	Mentor
Mentor Session - SEC 401	Indianapolis, IN	Jun 10, 2014 - Aug 12, 2014	Mentor
Community SANS Pittsburgh	Pittsburgh, PA	Jun 16, 2014 - Jun 21, 2014	Community SANS
State of South Carolina - SEC401: Security Essentials Bootcamp Style	Columbia, SC	Jun 16, 2014 - Jun 21, 2014	vLive
Community SANS Madrid SEC401 (in Spanish)	Madrid, Spain	Jun 16, 2014 - Jun 21, 2014	Community SANS
Mentor Session - SEC 401	Toronto, ON	Jun 19, 2014 - Aug 21, 2014	Mentor
SANSFIRE 2014	Baltimore, MD	Jun 21, 2014 - Jun 30, 2014	Live Event
SANSFIRE 2014 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Jun 23, 2014 - Jun 28, 2014	vLive
SANS Canberra 2014	Canberra, Australia	Jun 30, 2014 - Jul 12, 2014	Live Event
Community SANS Orange County	Orange County, CA	Jul 07, 2014 - Jul 12, 2014	Community SANS
SANS Capital City 2014	Washington, DC	Jul 07, 2014 - Jul 12, 2014	Live Event
Community SANS Newark	Harrison, NJ	Jul 14, 2014 - Jul 19, 2014	Community SANS
SANS San Francisco 2014	San Francisco, CA	Jul 14, 2014 - Jul 19, 2014	Live Event
Federal Bureau of Investigation (FBI)	Houston, TX	Jul 21, 2014 - Jul 26, 2014	