Global Information Assurance Certification Paper

SANS Security Essentials

Version 1.2c

By: Kelly S. Haley

The Unintentional Disclosure of Digital Data

Unintentional Disclosure of Data

Introduction

The resurrection of data may be a welcome experience for a user whose data is lost due to an unintentional event such as accidental erasure or hard disk crash, but sometimes a user prefers the data erased stay erased forever! When data is intentionally erased or deleted, it is probably done so to avoid unintentional disclosure of the contents stored on the media. The purpose of this paper is to expose a major threat of Information Age users – the Unintentional Disclosure of Data. Unintentional disclosure of data is sometimes overlooked because of the simplicity of the methods employed by a perpetrator to obtain the data, but often overlooked because of ignorance on behalf of the owner or keeper of the data. Information covered will include a perspective of how much data is worth, an overview of how data is written to magnetic media, why data erasure (deletion) is insufficient to avoid data recovery, how the data may be resurrected, and identification of known and unknown perpetrators. In conclusion, possible solutions will be offered to protect your data based on the awareness of these potential threats.

A Perspective of Much is Data Worth?

According to Front Porch Digital, the result of one Gallup Poll conducted indicates "most businesses estimate that 100 megabytes of stored data is worth at least $1 million." New Technologies, Inc. (Forensics-intl.com) puts this amount of data into perspective, illustrating it in the following manner: 1 Megabyte of data equates to approximately 312 printed sheets of 8 ½ X 11" paper. Using this approximation to calculate the information stored on a typical current disk capacity of 10 Gigabytes roughly equals the amount of information stored on 3,120,000 pages of printed material! However massive this amount seems when used as an independent reference, individuals may find it insignificant when compared to the potential impact of information disclosed associated with National Security issues, which leave our nation susceptible to harm, and personal data including loss of identity. As illustrated by the Gallup Poll results above, data is now considered a tangible asset and the expectation by most individuals is a system administrator, the designated keeper of the data, must be infallible with regard to data security. They must be aware of the potential harm done if the information is compromised. Categories explored include company data, personal data and data pertaining to National Security issues.

The first type of data explored is company data, including trade secret and financial disclosure. Company data compromised may subject the company to severe financial setbacks and possible acquisition. Is this really an issue? According to Dorothy Denning, "companies could be losing more than $250 billion annually to information thieves, according to a 1997 American Society for Industrial Security survey of Fortune 1000 firms and the 300 fastest growing companies." Another survey cited by Denning, "found that of 12 types of computer crime and misuse, theft of proprietary information had the greatest reported financial losses for the period 1997-1999. According to the survey, more that $42 million worth of trade secrets was stolen from 64 organizations." (Denning).

A loss of personal data may prove to be an embarrassment at a minimum and stolen identity as the extreme. Exposing information stored on a personal computer may open financial records, personal letters, medical records and other personal family information. Disclosure of this data may prove to be embarrassing if exposed to the public, but emotionally you will probably recover. The threat of stolen identity is often considered the extreme personal loss of data.

Exposure of the examples of data above may have detrimental impacts on a company, individual or family unit. These may seem extreme until the threat of National Security is exploited in the same fashion. Data exploited that puts the entire country in harm's way is often considered the biggest risk. Of course all exposure is a risk, but a National Security risk has the potential to affect every person in the United States and/or the world!

A Summary of How Data is Stored on Magnetic Media

Before the risks associated with disclosure of data from magnetic media can be fully exposed, a summary of how data is stored on magnetic media must be offered. Data is stored on magnetic media by applying magnetic fields to the media and changing the "flux" or the alignment of a specified field through a process called "flux reversal". Once a magnetic force is applied to the media it is difficult, if not impossible, to return the media to its original condition or totally overwrite the data so the original data cannot be resurrected. Remnants of data remain indefinitely on the media. "Data remanence is the residual physical representation of data that has been in some way erase.". "As early as 1960 the problem caused by the retentive properties of ASI (automated information system) storage media (i.e., data remanence) was recognized." (Gallagher – cipherwar.com). Even though the problem was recognized over 40 years ago, many individuals, tasked with safeguarding sensitive data, are not aware of the issue and do not take the proper precautions when storing and disposing of magnetic media.

What Happens to the Data When a File is erased from Magnetic Media?
When data is erased from magnetic media, only the pointers to the file location on the media are deleted, but the flux reversal used still exists on the media. This is helpful to recover files that are accidentally deleted. The negative side of this process exists when data purposefully deleted, with the expectation by the user that it will never be recovered, is recovered and possibly exploited.

Data remanence is not limited only to user data files, but also to swap files which are transparent to the user. An operating system capable of using virtual memory, disk space allocated to handle the overflow of physical memory, writes data to a swap file on disk. The data stored in the swap file uses the same characteristics of all other data stored on magnetic media, magnetic flux reversal. Due to ignorance on behalf of the user, this swap file may become a target for malicious attacks by a system savvy technician.

Awareness of data remanence is a major key to securing information stored on magnetic media. Individuals who know how to view data remanence target deleted data because they know that data a user tries to delete is rarely insignificant.

Simple Daily Functions Can Put Your Data at Risk
There are several daily tasks that potentially expose data to unintentional disclosure. These include backup and restoration of data, repair of system components and providing information to Internet sites when a user is fooled into thinking the site is secure and the data provided will not be viewed by others.

A system administrator typically makes data backups weekly and daily to avoid data loss through accidental means, such as the user who unintentionally erases a file or an unforeseen need to recover from a hard disk crash. The data stored on tape is a potential threat of exposure because restoration to a different system by an unauthorized user, bypassing the original permissions, opens the access to files for invasion. This threat is sometimes unapparent to the administrator because the correct permissions are imposed on the original system. When the backup is restored to a different system, it inherits the permissions of the new file system, stripping the data of permissions imposed on the original media. To exploit this threat someone must obtain physical possession of the backup tape. Disaster Recovery Plans include storing data backup tapes in fireproof vaults typically locked with limited personnel access and offsite storage for a higher degree of disaster recovery. Disgruntled employees or simply employees with a desire to access privileged data could gain possession of these backup tapes and restore the data to a different system, bypassing the permissions assigned. Storing data offsite also has the potential to expose the data to individual without access. A tape may be copied, stolen or misplaced exposing the data to unintentional disclosure.

The following situations may also be used to exploit data. Tapes rotated out of service due to life expectancy concerns must be destroyed appropriately. When a hard disk drive upgrade is performed, the old drive must be sanitized appropriately. These tapes and hard disks cannot simply be thrown in the trash. These threats must be evaluated and appropriate action taken to destroy the contents of the media. Is erasure good enough?

Another perpetrator could be a service technician who diagnoses a magnetic media, such as a hard drive, as damaged and replaces the media with a new disk. The data on the media now in possession of the service technician may be considered unusable or unrecoverable. However, it still has the potential to be exploited due to data remanence.

User may be enticed to supply information to a Internet site with the impression the site is secure and the data will not be made available to other individuals. However, companies are selling this data to other sites and the following illustrates a major problem associated with unintentional disclosure of data. According to the Privacy Rights Clearinghouse (Givens), "the most common form of identity theft is when someone obtains the Social Security number (SSN) perhaps a few other pieces of information about an individual, and uses that information to impersonate them, and obtain credit in their name." (Givens). The same source estimates between 500,000 to 700,000 people would fall victim to the crime of identity theft during 2000. The victim of identity theft does not become aware of the problem for an average of 14 months. The average time to repair the harm to credit records was 2 years! (Givens) In addition to the potential financial harm done to an individual, an identity stolen may also become a facade for criminal. If the stolen identity is used falsely for a criminal to avoid prosecution or to assume a new, untarnished identity, the harm done to an individual may last a lifetime. This may happen through an unintentional error keying information into a criminal record or a criminal may "steal" your identity by assuming your name and social security number from discarded magnetic media. Malicious individuals, in search of a new identity may also obtain the information by accessing Internet sites where personal data is made public. Some sites offer incentives to individuals convincing them to provide personal information and then publish it without the individual's knowledge.

According to a survey conducted by and posted on www.businesswire.com, 78% of users polled indicated their top concern of Internet security is having personal identities stolen using publicly available personal information. In the same survey, they asked individuals if they could be persuaded to offer information over the Internet if they were offered an incentive. Here is the breakdown of the survey results:

Information Offered	Without Incentive	With Incentive
Annual Household income	27%	47%
Credit Card Number	5%	17%
Home Phone Number	32%	43%
Home Mailing Address	38%	47%
Name	64%	67%
Social Security Number	4%	7%

This survey is a realistic representation of the data available for public view on the Internet, with or without personal knowledge or consent.

The examples of possible threats listed above can be reduced, if not totally eliminated by observing certain precautions. Before exploring the precautions that should be taken to reduce the risk, the possible exploitation will be discussed.

How to Prevent the Examples of Unintentional Data Disclosure

Data should be evaluated for sensitivity based on the worse case scenario conceivable with respect to exploitation. After this evaluation is performed, care should be taken to protect the possibility of unintentional disclosure based on the ramifications of its disclosure and possible exploitation.

One technique used to prevent the resurrection of sensitive data (not classified) on magnetic media is simply to erase it, however this offers little to no protection from the data being recovered. A better way to destroy it to overwrite the data at least once, the potential to read data is reduced with every rewrite (or overwrite) operation to the same location on the media and consideration must be taken to verify this operation has been performed properly. This is appropriate for personal data including financial records. It should be performed before the media is released for any reason including repair and physical destruction.

Some entities go to the extreme to protect the data considered by many to be the most valued of all – that which pertains to National Security. In the United Kingdom (UK), the " 'Ministry of Defense' requires the surface of all hard disk platters be ground off and the dust securely stored for twelve years. The dust is still officially classified even after this period." The rules are not as stringent in the United States. To substantiate this, the author references U.S. Navel document entitled "OPNAVINST 5239" that "classified disks can either have their surfaces sanded away or dissolved by acid!!" (Bascom). Is the U.K. too paranoid or do they have a realization of potential threats that exist in the Information Age?

Exploitation of information obtained by an Internet site is occurring at high rates. Information an individual may think is private is being sold to other companies who sell it as background information for users. This is similar to the way credit card and mail-order companies sell mailing lists. It is up to individuals to protect their privacy. This exploitation will not disappear until the Internet user community is educated on the possible issues that may arise from the exploitation of the information.

Conclusion

When data is unintentionally disclosed, the ramifications can be severe with respect to personal, company and National Security data. As technologies advance, the proper method to permanently dispose of magnetic media must be reevaluated to determine whether or not the methods are still valid. Many firms now offer services and expertise to companies on how to properly to erase, overwrite, destroy or declassify media appropriately to guarantee the data will never be recovered. A simple deletion is not ample to avoid the possible risk of someone gaining access to the information. Perpetrators may include employees of a company who want personal financial gains, an invader from the Internet who convinces an individual to divulge personal data and then sells it, a technician hired to replace a failed computer component, such as a hard drive. Educating the user community is the best approach to safeguarding data from unintentional disclosure.

WORKS CITED

Bascom, Simon Richard. "Why a normal delete is not sufficient". 26 Jan. 1997. 24 Apr. 2001. <http://www.stack.nl/~galactus/remailers/why-real-delete.html>.

Business Wire Home Page. 23 Mar. 2000 "What's Your Identity Worth?". 23 Apr. 2001. <http://www.businesswire.com/webbox/bw.32300/200831617.htm>.

Denning, PhD., Dorothy. "Who's Stealing Your Information?" Cover Story – Industrial Espionage. 17 Apr. 2001. <http://www.secure1direct.net/sys-tmpl/nss-folder/companypresentation/StealingInfo1.htm>.

Enterprise Data Media Services: Tape Assurance Services. 1998. Front Porch Digital. 20 Apr. 2001. <http://www.fpdigital.com/html/edm_tape_data_assurance.html>.

Gallagher, JR, Patrick R. et al. "A Guide to Understanding Data Remanence in Automated Information Systems". Sept. 1991. 20 Apr. 2001. <http://cipherwar.com/fight/text/books/rainbow/forest_green.htm.>

Givens, Beth. The Privacy Rights Clearinghouse. "Identity Theft: The Growing Problem of Wrongful Criminal Records". 1 Jun. 2000. 23 Apr. 2001. <http://www.privacyrights.org/AR/wcr.htm>.