Running head: MAGNETIC DATA RECOVERY – THE HIDDEN THREAT

Magnetic Data Recovery – The Hidden Threat

Joshua J Sawyer

East Carolina University

Abstract

In presenting the dangers of magnetic data recovery, this paper gives the reader a descriptive, yet active view. The methods themselves are described, as well as possible avenues of action that can be used to prevent and mitigate this type of security breach via real-life examples from the field. The primary target of this paper is the business / corporate manager. However, the analysis given will also apply to the home user, and anyone else wanting to ensure that their sensitive data is not at risk. The concepts discussed here should be considered mandatory knowledge for those who seek to safeguard their personal information or that of their employers from unauthorized disclosure and abuse.

Magnetic Data Recovery – The Hidden Threat

The majority of today's businesses rely in some way upon computer systems to handle the tasks of everyday commerce. These businesses are increasingly using computers to work with their internal and external documents, depending more and more on digital storage every day. Most attention has been focused on well-known problems such as viruses, exploits, etc. Attacks by intruders and insiders have led to billions of dollars in lost revenue and expended effort to fix these problems (Freeman, Long, Miller & Reed, 2001, ¶1). For the most part, these attacks have been focused on software based vulnerabilities, while perhaps the most devastating vulnerabilities lie in hardware devices which exist in the majority of all computer systems in use today. In fact, physical attacks on storage hardware are common and may be the most likely and dangerous type of attack (Hasan, Lee, Myagmar & Yurcik, 2005, ¶28). Although using this new, digital alternative to paper may seem to be easier and faster, inside these seemingly harmless computers lie devices which are recording and generating audit trails of all data ever accessed on them, potentially acting as an informant to whoever possesses the devices. In fact, overlooking these devices may give an attacker a chance to steal sensitive data. Also, this could be carried out by any personnel with physical access to the machines (Goldschlag & Landwehr, 1997, ¶19).

What are these devices? Is this some sort of top-secret spy gadget? The answer, surprisingly, is no. It's the traditional, magnetic hard drive (Figure 1). Magnetic hard drives are used as the primary storage device for a wide range of applications, including desktop, mobile, and server systems (Grochowski & Halem, 2002, ¶1). All magnetic disk drives possess the capability for data retention, but for the majority of computer users, the hard disk drive possesses the highest lifespan of all magnetic media types, and therefore is most likely to have large amounts of sensitive data on it. Businesses spend large amounts of time and money on developing and implementing important and well known safeguards such as firewalls, antivirus

products, spyware scanners, and more. What is too often overlooked is perhaps the most serious threat of all: reselling or re-using used hard drives which may contain critical information on the business' customers, sensitive internal documents, the business' network layout, passwords, trade secrets, and other sensitive information. With more and more documents being converted into digital format, this is an ever-increasing threat. We will focus on the traditional magnetic hard disk, and exclude other types of magnetic media such as floppy disks, as floppies can be cost-effectively destroyed if they contain sensitive data. However, it should be noted that other forms of magnetic media can also yield a treasure trove of data to whomever has physical access to them.

In reality, magnetic media is simply any medium which uses a magnetic signal to store and retrieve information (Commonwealth of Australia, 2005, ¶1). Examples of magnetic media include: floppy disks, hard drives, reel-to-reel tapes, eight-tracks, and many others. The inherent similarity between all these forms of media is that they all use magnetic fields to store data. This process has been used for years, but now that security concerns are being brought more into focus, we are now starting to see some of the weaknesses of this technology, as well as it's well-known benefits.

One property of magnetic media is that they are very sensitive to magnetic fields, due to their use of these fields to read and store data. This has long been an issue with magnetic disks being carried in / near hospital rooms that use medical equipment which emits high magnetic fields. Signs often warn that any magnetic media could be destroyed if carried within close proximity to these strong magnetic fields. We will discuss to what degree information on magnetic media can truly be 'erased' later on. For now, we will just say that the data can be corrupted, or negatively altered, by the presence of strong magnetic fields.

The hard drive itself is simply a metal, box – shaped device, usually made of aluminum or a

similar metal, which has two or more connectors for connection to a host system (Figure 1). In our case, the host is a computer system. Other host devices may include: ATM machines, medical devices, etc. There is typically one connector which supplies the power to the drive, and another connector which carries the actual data to / from the drive. There are various configurations, and some drives have these connections all in one connector, but the wiring will contain some variation of data and power interfaces. The inside of the hard drive consists of various parts, two of which we will be concerned with in this paper: the disc platter, and the read/write head (Figure 2). The disc platter is simply a spinning disc which is coated with material which responds to magnetic fields. The read/write head(s), there is usually one on each side of the disc, generate the magnetic field required to write data to the disc, and also pick up the field from the disc platter and convert it into an electrical signal to be processed by the host. These heads are mounted at the end of a movable arm, shown in Figure 2. This is quite an effective means of storing and retrieving data, as long as the disc platter and head are operational. What is often overlooked, however, is that the disc platter, like all magnetic media, has a tendency to 'remember' the data stored on it. This is due to the way data is written to / read from the disc platter itself.

When data is written to the disc platter, it is stored in the form of ones and zeroes. This is due to the binary nature of computers – the data in question is either on (1), or off (0). This is represented on the disk by storing either a charge (1), or no charge (0). The data is written to the actual disc platter in what are called tracks (Figure 3). These are concentric rings on the disc platter itself, which are somewhat similar to the annual rings of a tree (Kozierok, 2001, ¶1). As data is written to these rings, the head actually writes either a charge (1), or no charge (0). In reality, as this is an analog medium, the disc's charge will not be exactly at a 1 or 0 potential, but perhaps a 1.06 when a one is written on top of an existing 1, and perhaps a .96

when an existing 0 is overwritten with a 1. The main idea to grasp here is that the charge will never be exactly 1 or 0 on the disc itself. It will be different, due to the properties of the magnetic coating on the disc. In this way, data is written to the tracks of the disc. Each time data is written to the disc, it is not written to exactly the same location on the disc. Together with this, and the nature of analog signals themselves, it is possible for the original data from a hard drive to be recovered, even if it has been overwritten with other, newer data. How is this possible? The data can actually be detected by reading the charges between the tracks on the disc itself (Figure 4). Also, software can be used to calculate what an 'ideal' signal should be. Then, subtracting from this what was actually read from the disk, the software can yield the original data. Of course, no affordable digital storage medium is completely reliable over long periods of time, since the medium may degrade (Baker, Keeton & Martin, 2005, ¶14). However, most magnetic disks can hold charges and residual data for several years, if not decades. This is more than enough time for the data to potentially be viewed by an unauthorized individual, organization, or both.

Traditionally, most users simply use the 'recycle bin' or delete files from their drives when they no longer need them. In reality, all they are doing is telling the drive that from now on, this file can be considered as free space. The file is never modified at all and still remains intact on the disk drive. This is why so many undelete and recovery utilities available can so easily recover deleted files. They are all still on the disk waiting to be recovered! So what about these programs that claim to "securely erase data beyond recovery"? Using a disk wiping utility is certainly better than just deleting a file or formatting a disk, but if someone is determined enough to read the deleted data and possesses the time and money necessary, they can recover the original data, even if the drive was 'wiped'. Some common methods used to gather data from drives which might have very important information to investigations include: Magnetic Force Microscopy (MFM) and magnetic force Scanning Tunneling Microscopy (STM). Other methods

and variations exist, but are either classified by governmental intelligence agencies, or are not widely used yet. We will deal with MFM and STM. MFM is a fairly recent method for imaging magnetic patterns with high resolution and requires hardly any sample preparation. This method uses a sharp magnetic tip attached to a flexible cantilever placed close to the surface of the disc, where it picks up the stray field of the disc. An image of the field at the surface is formed by moving this tip across the surface of the disc and measuring the force (or force gradient) as a function of position. The strength of this interaction is measured by monitoring the position of the cantilever using an optical interferometer or tunneling sensor (Gutmann, 1996, ¶4). In this way, data can be extracted from a drive. Another method, magnetic force Scanning Tunneling Microscopy (STM) is a more recent method which uses a probe tip typically made by plating pure nickel onto a pre-patterned surface, peeling the resulting thin film from the substrate it was plated onto and plating it with a thin layer of gold to minimize corrosion, and then mounting it in a probe where it is placed at some small bias potential so that electrons from the surface under test can tunnel across the gap to the probe tip (or vice versa). The probe is scanned across the surface to be analyzed as a feedback system continuously adjusts the vertical position to maintain a constant current (Gutmann, 1996, ¶5). Although these methods can be quite effective, they are often reserved only for high-potential targets, which are believed to have very desirable evidence on them. The typical business or home-user's hard drive might not have any information worth going to these lengths to recover, but it is an option that can be used to retrieve information if desired. The fact that magnetic media contains residual charges from previous data even after being wiped or overwritten several times makes complete data destruction next to impossible.

Some computer users naively believe that overwriting sensitive data with new data, even numerous times, will make it impossible for the sensitive data to be recovered. In wiping, clusters (units on the disc in which data is stored that are smaller than tracks) are overwritten

several times to ensure data has been removed. Even in this extreme case, utilities exist that may recover portions of the overwritten information (Jajodia & Johnson, 1998, ¶29). Even if data is overwritten with newer data only once, it can be recovered by scanning the disk platter with a magnetic force microscope (Hughes, 2002, ¶37). Once data is placed on a drive, there is always a possibility of reading it back. Although it is not possible to completely sanitize a disk beyond recovery, it is possible to make recovery much more difficult.

What are some standards that determine how to sanitize differing levels of sensitive information? Some of the most widely known standards come from what the US government mandates for it's own data sanitization procedures. According to the DoD (Department of Defense) directive DoD 5220.22-M-Sup 1 Chapter 8, "Degaussing is more reliable than overwriting magnetic media." (DoD, 2005, pg.18). Degaussing applies a strong magnetic field to the magnetic surface of the drive, resetting any magnetic charge on the platter, effectively making the information unreadable. This directive also states that 'Non-Removable Hard Disks' can be cleared by "overwriting all locations with a character, it's complement, then with a random number." (DoD, 2005, pg.18). This is a form of disk wiping in which the entire drive is written to with a character, then with that character's complement, then again with a random number. Furthermore, the document states that these disks must remain in a secure, observed location at all times to ensure that no methods are attempted on them to recover any residual charges on the disc platters. This procedure for erasing data is recommended by the DoD for all drives, *except* those containing 'Top Secret' material. The reason why this is not enough for 'Top Secret' material is due to the possibility of recovery via magnetic remanence techniques (Valli, 2004, **¶7).** The above method is for 'clearing' the disk. The manual also states that any device that cannot be cleaned for certain, such as other types of calculators and memory devices, must be destroyed. This overwriting method is sufficient for the security levels below "Top

Secret". However, "Top Secret" disks must be degaussed / destroyed completely. This ensures that nothing can be read from the drive. So, from the DoD report, obviously the only way to be sure data cannot be retrieved from magnetic media is to degauss and destroy them. Another method is to never put the sensitive data on the media to begin with, which we will discuss in detail later on.

Are there any 'disk sanitization programs' that actually work? According to some tests run by researchers at Carnegie Mellon University, six file wiping tools were evaluated and then compared to each other based on their effectiveness, and 'All the privacy tools failed to eradicate some sensitive information' (Cranor & Geiger, 2005, pg.11). These tools were used on a standard Windows XP system, and the data recovered after the tools were run was compared to the original data on the disk. This clearly shows that, using readily available tools, data was still recoverable from the drive. However, it must be noted that these privacy tools were used to wipe only certain files on the disk, and not overwriting or wiping the entire disk. When donating a used disk drive to charity, for example, one should use a full-disk wiping utility, such as the freeware tool DBAN (Darik's Boot and Nuke), available at http://dban.sourceforge.net/. This would overwrite the entire drive's contents, making it more difficult to recover data as compared to a normal format or leaving the disk as-is. Wiping the entire disk is much more thorough than wiping individual files with the tools in the above study, as there is no chance of log files being present elsewhere on the drive. DBAN requires a user to boot from a boot disk so it has direct access to the hard drive being wiped. This ensures no part of the drive will be in use, and therefore ensures the entire disk will be overwritten.

Two gradate students at MIT purchased a total of 158 hard drives from the online auction site Ebay and other sources of used computer parts. They then scanned each hard drive with widely available recovery tools to see what data may be on the drives, if any. What they found

was very disturbing. Of the 158 hard drives, only 12 were properly sanitized, and more than 5,000 credit card numbers, personal, financial and medical records, email and other types of content were found (MIT News Office, 2003, ¶2). One of the drives was reportedly from an ATM, and contained over a year's worth of detailed financial records. The majority of the drives had not been properly cleaned, or not cleaned at all. This illustrates a very important fact: deleting a file does not mean it has been deleted! Formatting a disk does not ensure the disk has been sanitized. The only way to properly make a disk's contents unreadable by most attackers is to overwrite the entire drive with data, as specified by the DoD above. This does NOT guarantee the data is unreadable, as a well financed attacker can use magnetic remanence methods, similar to those previously described, to gather the original drive data. However, it is much better than simply formatting the drive or erasing files. Overwriting the entire disk drive with data as specified by the DoD above will prevent 97% or more of common recovery utilities from recovering the data. The only true threat which would still exist as a result of this method is advanced hardware electromagnetic remanence techniques. Formatting only checks each position of the drive to see if it is functional or not. The old data can still be retrieved. To make it unreadable by the average attacker, one must overwrite the entire drive as specified by the DoD above. In the special case that a drive contains particularly sensitive information that should not be recovered by anyone, the only solution is to degauss or destroy the drive; both of which will make the drive unusable. Some companies are now developing features to be built into their drives in the future which will allow for disk sanitization much more easily. The traditional file deletion utilities lack the disk-level access needed to securely wipe data. They are limited to the read / write head's position when the erase process is underway. The information between the tracks will still be accessible after using these tools. However, if one must delete sensitive files on a disk without wiping the entire drive, there is a free utility available called

'Eraser', available at http://www.heidi.ie/eraser/, which enables you to manually set overwrite settings, change other options, etc. It is one of the most respected free programs for securely wiping files without having to wipe the entire disk, and will perform wipes which comply with the DoD standard. Please note however, that this does not guarantee that the files will be unrecoverable, but it does make their recovery *much* more difficult than if it were not run. For all practical purposes, this makes software recovery virtually impossible. There have been many programs created that attempt to 'securely' wipe data once placed on a drive. There has even been some development on an addon for the Linux ext2 filesystem, in an attempt to give the user a more 'true' and transparent erase (Bauer & Priyantha, 2001, ¶24**)**.

Since there is no software solution to make private data on a magnetic disk drive absolutely unrecoverable by all methods, then what are the best options in dealing with sensitive data? First and foremost, the best solution is to prevent any sensitive data from touching the drive to begin with. This way, it is impossible for anyone to recover data from the drive using any known or unknown method. Of course, this is impossible to do with all data, as one must use the drive. An excellent solution to this is the concept of full disk encryption (Figure 5). Encryption is a procedure that transforms a plaintext piece of data (the entire drive in this case) by rearranging the letters and numbers and converting the message into an encrypted form using a mathematical algorithm and a key (Voors, 2003, **¶7).** When using this option, the user still has to set up the drive like any other disk, but at this stage the user should set it up with temporary accounts, and temporary passwords. Only installing the operating system at this stage is best. Then, once the operating system is installed, the entire disk can be encrypted with 'whole disk encryption' utilities, most of which are available on the internet. One of the most popular of these is PGP, available at http://www.pgp.com/products/wholediskencryption/. If a new drive is purchased from the factory, a temporary user account and password used to set up the operating system,

then an entire disk encryption utility used, the only trace anyone can recover from the drive is the original temporary account that was used to set up the operating system, and the rest of the activity on the drive will be encrypted. This transfers the attacker's focus from data recovery to cracking the encryption, which is a much slower process. Not all disk encryption utilities are the same, however. One must be sure to use an 'on the fly' encryption utility, as these type of programs encrypt everything before writing them to the physical drive. Even if the computer crashes with all the programs open and running, the disk is not vulnerable, as all decryption occurs in the memory of the computer – the hard disk remains encrypted at all times. A downside to using these programs is that some functions of the operating system might be disabled, such as hibernation in Windows XP, for example. Hibernation allows the computer to 'remember' where the user was the last time they told the computer to hibernate, thus writing all the currently open data directly to the hard disk. Most 'on the fly' encryption utilities will not allow this, as it would pose a security breach, and give physical attackers unencrypted data to look at on the hard disk. Overall, most users feel this is a small price to pay for the piece of mind in knowing their whole drive is encrypted. For maximum security, a good approach is to use additional encryption utilities together with the hard drive encryption utility, thus making layered walls of encryption an attacker will have to break through to reveal anything at all about the private data. Most of these 'entire disk' encryption utilities require the user to enter a passphrase or to present a token to authenticate them into the system before it will allow the operating system to boot. The token is usually a usb flash memory stick, a smart card, password, etc.

With the current trends in malware, a coming threat is attackers injecting malware into the actual BIOS program that runs on the motherboard. As most 'full disk' encryption utilities ask for a password / token at the BIOS level, an attacker could potentially grab the password as

the user enters it. This type of BIOS attack has not been used widely as of yet, but security professionals are warning about it. Overall however, entire disk encryption is currently the safest method in protecting data if one plans on using a new hard drive anytime soon. It can also be used on an older hard drive, but remember, any data ever written to the drive in the past has a chance of being recovered. For the majority of attackers, this is beyond their grasp, but for a determined attacker with tools, resources, and time at their disposal, the old data can be recovered. Therefore, the best way to use 'entire disk encryption' is to use it on a new disk drive. That way, the only data present will be the encrypted data. If more companies would encrypt their entire drives, there would be a lot less stolen information such as social security numbers, credit card numbers, passwords, etc, as the information would be useless to the attacker. With the increasing number of entire disk encryption utilities available today, there's really no excuse why businesses which store personal data, especially customer data, shouldn't use encryption utilities. In my opinion, anything less is asking for the information to be abused. Without encryption, any information on the drive or that has been on the drive at any time is potentially under the control of whoever has physical access to the disk, whether this be a criminal, a rival company, another country, or the government. The company should care enough about the data to secure it properly. Home users can do the same for any data they deem sensitive enough that it should not be made public knowledge.

Encryption is not currently legal in all countries, and one must be careful in knowing what regulations exist before employing encryption. However, most utilities now offer ways of giving the user 'plausible deniability', a concept which allows the user to hand over one set of encryption keys to parties requesting access (i.e., a government), while keeping another set for their true data. This is another feature which may be needed in some cases.

There are many good encryption programs available. There's no excuse as to why data can't

be securely stored beyond reach of attackers. Even if a home / business user cannot afford to purchase one of the above mentioned utilities, there are plenty of open source programs that secure files as well. One of the best is Truecrypt, available at http://www.truecrypt.org/. This free utility can create encrypted volumes within a disk drive, or encrypt an entire partition. It uses strong algorithms such as AES to encrypt data, so it is excellent for the home / business user. If an 'on the fly' full disk encryption utility is beyond one's budget, then this is the next best thing. This tool also runs with Windows XP, Linux, and other operating systems. It is also freeware, which means one can review the source code to verify for themselves that there is no 'backdoor' or alternate method to gain access without entering the password. This makes it more reliable than a program which one can't verify as to what backdoors may be present. This is not the only tool however, there are plenty of other excellent open source utilities now available. A comparison of the discussed sanitization methods and solutions shows the advantages and disadvantages of each approach (Figure 6).

Magnetic media are not the only forms of data storage that possess the ability to hold data for future retrieval. Computer memory also poses a threat. Data can be retrieved from these semiconductors, especially if the same data has been written to the memory for an extended period of time. The current type of computer memory holds data for a shorter period of time than older types, but can still keep traces of data. To minimize the risk of data retention, one should keep the memory at elevated temperatures such as at room temperature. Lower temperatures will cause the memory to retain data more easily (Gutmann, 2001). The more frequently one keeps different types of data going through the memory, the less the chances are of the memory remembering the data. For most users, this will not be enough of a threat to worry about. However, semiconductors can also act like data reservoirs, even if for a very short period of time. This will soon become a more researched issue, with the rise of flash drives replacing the

traditional magnetic drives. Once the capacity of flash memory increases and the price decreases, the traditional magnetic disk drive will eventually become obsolete. This will introduce a whole new side to the hidden threat of data retention.

In conclusion, the security of sensitive information when discarding obsolete computer equipment and media is extremely important (Mattord & Whitman, 2004, ¶14). It can mean the difference between sending a drive out into the public arena with sanitized data on it, being unrecoverable by most individuals, or filled with sensitive data, just waiting to be recovered with common recovery software. There are several avenues by which a business / home user can mitigate the risk of yielding personal information to the recipients of their used magnetic media. First and foremost, if possible and legal in one's area, full disk encryption should be used *before* writing any sensitive data to the magnetic media. This will deprive attackers of easy data recovery, and in most cases, make recovery impossible. Second, if sensitive data is already present on a drive and must be erased quickly, then a file wiping utility such as 'eraser' mentioned earlier, should be used to overwrite the sensitive data multiple times, and thwart most software recovery techniques. When donating or re-using any drive which had potentially sensitive information on it at any time, a disk wiping utility, such as DBAN, discussed earlier, should be run first, which will overwrite the entire disk, making sure sensitive data cannot be recovered by software recovery techniques. Formatting or deleting files should not be considered a method of sanitizing magnetic media. In most cases, this only makes recovery easier. It is always best to start out right. If possible, installing entire disk encryption utilities before placing any sensitive data on the drive will provide the best protection for unauthorized data disclosure and recovery to date, short of degaussing or physically destroying the drive itself. Perhaps the main reason for the ease of sensitive data being recovered from second hand hard drives is due to the average computer user's lack of awareness of the problem, or more importantly, not knowing

how to fix the problem. Users should realize that unless magnetic media is properly sanitized, all data on it is easily recoverable, mostly within minutes of running widely-available recovery software.

Although, short of degaussing or physical destruction, we cannot securely clean magnetic drives of all sensitive data beyond reach of all known recovery techniques, we can make that recovery much more difficult, and defeat the most commonly used attacks. This discussion should motivate one to think twice the next time they donate or reuse a disk drive. Wiping drives before they are donated or re-used will play an important part in stopping this hidden threat.

References

Baker, Mary, Keeton, Kimberly, Martin, Sean (2005). *Why Traditional Storage Systems Don't Help Us Save Stuff Forever;* in Proceedings of the 1st IEEE Workshop on Hot Topics in System Dependability, Yokohama, Japan, June 30 2005

Bauer, Steven, & Priyantha, Nissanka B. (2001). *Secure Data Deletion for Linux File Systems;* in the Tenth USENIX Security Symposium Proceedings, August 13-17, 2001, Washington, D.C., USA

Bennison, Peter F., & Lasher, Philip J. (2004). *Data security issues relating to end of life equipment;* in Electronics and the Environment Conference Record. 2004 IEEE International Symposium on May 10-13, 2004, pages 317-320

Charles M. Kozierok (2001). *Hard Disk Tracks, Cylinders and Sectors.* Retrieved January 31, 2006 from http://www.pcguide.com/ref/hdd/geom/tracks-c.html

Commonwealth of Australia (2005). *Protecting and handling magnetic media.* Retrieved January 31, 2006 from http://www.naa.gov.au/recordkeeping/rkpubs/advices/advice5.html

Cranor, Lorrie Faith, & Geiger, Matthew (2005). *Counter-Forensic Privacy Tools: A Forensic Evaluation.* Retrieved February 1, 2006 from http://reports-archive.adm.cs.cmu.edu/anon/usr/ftp/home/anon/usr0/ftp/isri2005/CMU-ISRI-05-119.pdf

Department of Defense (1995). *DoD 5220.22-M-Sup 1: National Industrial Security Program; Operating Manual Supplement (Chapter 8)*. Retrieved February 1, 2006 from http://www.dtic.mil/whs/directives/corres/pdf/522022msup1_0295/cp8.pdf

Freeman, William, Long, Darrell, Miller, Ethan, Reed, Benjamin (2001). *Strong Security for Distributed File Systems;* in Proceedings of the 20th IEEE International Performance, Computing, and Communications Conference (IPCCC 2001), Phoenix, AZ, April 2001, pages 34-40

Goldschlag, David M., Landwehr, Carl E. (1997). *Security Issues in Networks with Internet Access*; in Proceedings of the IEEE, Vol. 85, No. 12 (December 1997)

Grochowski, E. & Halem, R.D. (2002). *Technological impact of hard disk drives on storage Systems*; in the IBM Systems Journal, Vol. 42, No. 2, 2003

Gutmann, Peter (1996). *Secure Deletion of Data from Magnetic and Solid-State Memory*; in the Sixth USENIX Security Symposium Proceedings, July 22-25, 1996, San Jose, California, USA

Gutmann, Peter (2001). *Data Remanence in Semiconductor Devices*; in the Tenth USENIX Security Symposium Proceedings, August 13–17, 2001, Washington, D.C., USA

Hasan, Ragib, Lee, Adam J., Myagmar, Suvda, Yurcik, William (2005). *Toward a Threat Model for Storage Systems;* in Proceedings of the 2005 ACM workshop on Storage security and

survivability, Fairfax, VA, USA, 2005, pages 94-102

Hughes, Gordon F. (2002). *Wise Drives*; IEEE Spectrum, August, 2002, pp. 37-41. Retrieved February 1, 2006 from http://www.simson.net/ref/2002/WiseDrives.pdf

Jajodia, Sushil, & Johnson, Neil F. (1998). *Steganalysis: The Investigation of Hidden Information;* in Proceedings of the IEEE Information Technology Conference, Syracuse, New York, USA, September 1-3, 1998

MIT News Office (2003). *Grad students uncover mountains of private data on discarded hard drives.* Retrieved February 1, 2006 from http://web.mit.edu/newsoffice/2003/diskdrives-0129.html

Valli, Dr. Craig (2004). *Throwing out the Enterprise with the Hard Disk*. Retrieved February 1, 2006 from http://scissec.scis.ecu.edu.au/publications/forensics04/Valli-2.pdf

Voors, Matthew Parker (2003). *Encryption Regulation in the wake of September 11, 2001: Must We Protect National Security at the Expense of the Economy?;* in Federal Communications Law Journal, 2003. Retrieved from http://www.law.indiana.edu/fclj/pubs/v55/no2/voors.pdf

Figure Captions

Figure 1. JPEG image of a typical hard drive's exterior.

Figure 2. JPEG image of a typical hard drive's interior.

Figure 3. JPEG image of tracks on a hard drive disk platter.

Figure 4. JPEG image of area between tracks on a platter.

Figure 5. JPEG image of platter containing encrypted data.

Figure 6. JPEG image of comparison between disk sanitization methods and solutions.

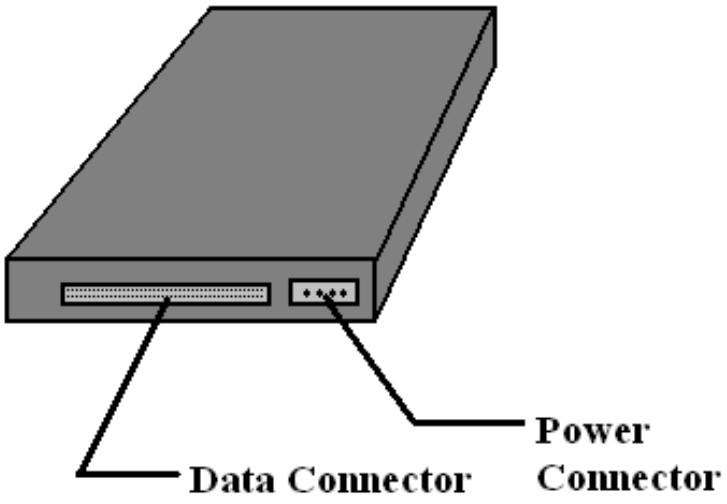

Figure 1. JPEG image of a typical hard drive's exterior

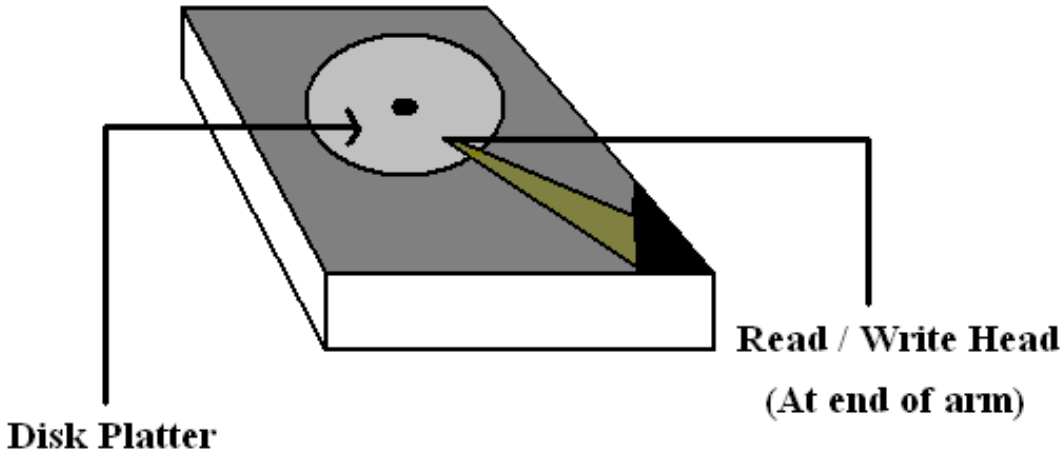

Figure 2. JPEG image of a typical hard drive's interior

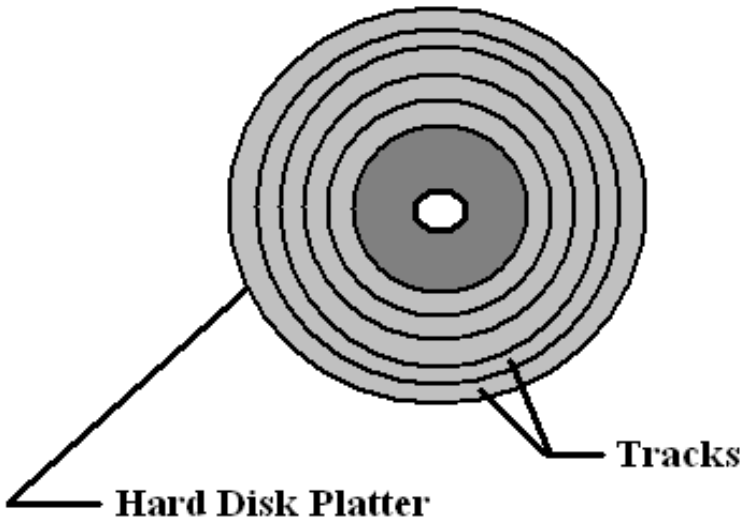

Figure 3. JPEG image of tracks on a hard drive disk platter

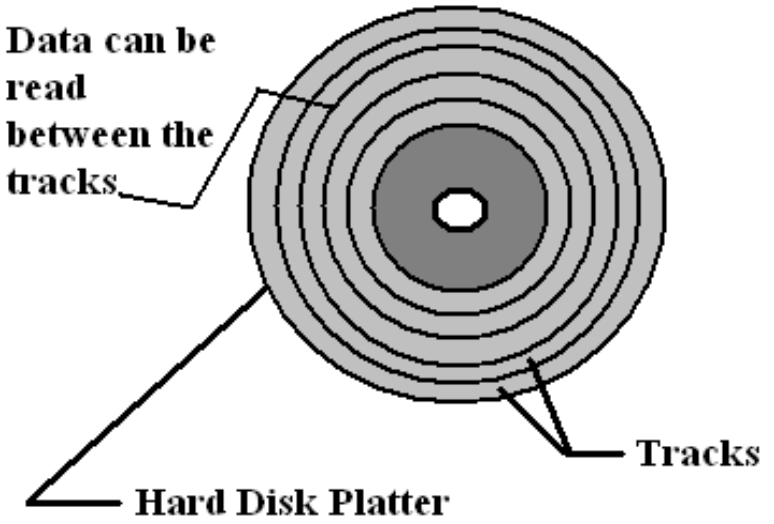

Figure 4. JPEG image of area between tracks on a platter

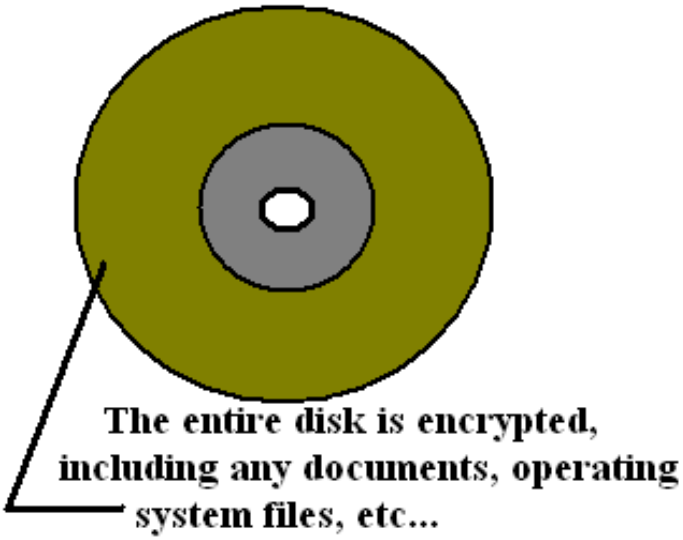

Figure 5. JPEG image of platter containing encrypted data

Method	Recovery Techniques Defeated	Best Used For	Disadvantages
File overwrite using tools like 'Eraser'	Some software techniques	Wiping files only - not entire disks	Temp files can remain on disk
Drive overwriting using tools like DBAN	Most software techniques	Wiping entire disks before reuse, donating, etc.	Hardware recovery can be used
Degaussing, Drive Destruction	If done properly, all	Top Secret data	Can be expensive
Full Disk Encryption	All - must be cracked	Data that should not be recovered	May be illegal

Figure 6. JPEG image of comparison between disk sanitization methods and solutions