https://doi.org/10.48009/2_iis_2006_48-51

SECURITY RISKS OF CARELESS COMPUTER DISPOSAL

Karen A. Forcht, Utah State University, Karen.Forcht@usu.edu
Richard Swart, Utah State University, Richard.swart@business.usu.edu
Shiloh Allen, Utah State University, shiloallen@cc.usu.edu
Daphyne S. Thomas, James Madison University, thomasds@jmu.edu

ABSTRACT

Computers are becoming a common and highly sought-after commodity. But like an automobile, it is a commodity that not everyone can afford to buy new "off the shelf." As the information age progresses, there is an almost moral obligation for individuals to get connected, but where can you get a computer if you don't have the necessary hundreds or thousands of dollars on hand to shop with? Some organizations and individuals are making a difference in the world by their efforts to meet this need.

Keywords: Computer Disposal, Data Privacy, Computer Memory Volatile Memory, Nonvolatile Memory, File Slack, Drive Slack, RAM Slack

INTRODUCTION

There is a large amount of computer equipment out there that is simply thrown away because people don't have the time to get it ready to donate or the equipment is no longer desirable to any range of consumers. With technology progressing and changing as rapidly as it has been, there is a lot of computer equipment that quickly becomes obsolete and is not fit for much else than the trash heap, in most consumers' opinions. There has arisen a logistical dilemma in finding a way to dispose of all this equipment in an efficient and environmentally friendly fashion. Some will even come pick them up from your curb like the city garbage service does.

Computers are not the only equipment that is potentially being donated, resold, or reused. Each of those computers has a memory, and if that memory hasn't been properly treated (which is highly likely), then the disposed equipment poses a security threat to the company or person who previously owned it. The purpose of this paper is to discuss the potential personal or corporate security risks posed by computer equipment that has been carelessly disposed of and to recommend a few ways to minimize those risks.

Recognizing the Risk

Information security addresses three states in which data can exist and the different security concerns relative to each of these three states: processing, transmission, and storage. The first step to managing a security risk of any kind is to recognize that a risk exists.

There is a fairly broad array of information that can pose risks to the original owner when handing down or reselling computer equipment. Almost everyone who uses a computer these days, at home or at work, uses it to access the Internet. The Internet offers all kinds of services that make life convenient, such as email, news and shopping. To identify yourself in order to use some of these services, the user must provide personal information. That information can include name, address, phone numbers, social security number, PIN numbers, credit card information, bank account information, birth date, passwords, etc. All of this information must, in one form or another, pass through the computer's memory, and sometimes it can wind up stored there.

Home and office computers are also used to do work: to write reports, store and analyze data, manage finances, create designs and images, write computer code, perform tests and simulations, etc. In this day and age, corporate information of this nature is very valuable. In many industries, keeping company information private is the main thing that allows an organization to remain profitable and competitive. Some companies maintain a vast amount of information about their individual customers, which they are legally obligated to keep private. Corporate information in the wrong hands can be risky to the company and its customers.

Now some people may say "Sure, that sounds credible in theory, but is it a real risk? Have there been any real incidents of information being salvaged from a second hand computer?" The answer is a resounding "Yes!" Two years ago, Tom Spring submitted an article entitled "Hard Drives Exposed" to PCWorld Magazine citing the experiences of scavengers who salvage discarded computer

equipment and, particularly, their experiences with the information they routinely find on hard drives [5].

According to the article, there are numerous individuals who frequent the city landfills and dumps looking for discarded computer equipment from which they can salvage and recycle computer components. There are also a number of companies, like Computer Salvage of New England and Onyx Environmental Services, who will do curb side pickups of old computer hardware. Often they find more than old parts, however. One particular individual, David Burns, remarked, "[On] almost every hard drive I pull, I'll find a tax return or a resume." That's disturbing news if you happen to be one of the people who dumped a computer in David's home town of Needham, Massachusetts [5].

The author then goes on to describe how, as an experiment, he and some colleagues purchased or salvaged ten hard drives in Boston just to see what they could find. They found data on nine of the ten. The kind of information they found ranged from medical records to bank account numbers to pornography. They then contacted the people who could be determined as previous owners of the equipment. These individuals were generally very surprised that what they considered to be private information was so easily obtained by complete strangers. Some said they were sure they had taken the necessary precautions to destroy the information before selling or junking the system [5].

The article presents its findings in support of a study that was performed by two MIT graduate students who purchased 158 hard drives on EBay and other online sources. Their findings were startling. According to the article, they found 129 of 158 that actually worked. Of those, 69 drives had information that could be readily recovered. In all they found 3,700 credit card numbers, medical records, and other personal information. Only 12 drives that they analyzed had been properly treated for disposal [5].

These real incidents demonstrate what a potentially huge problem and security risk it can be to individuals and organizations that are looking to get rid of their old computers. Most of these people thought they had safely and thoroughly removed the information by deleting their files or formatting the hard drive.

Computer Memory

Almost all computer systems utilize two types of storage, or memory, for data. These two main types of memory are classified as volatile and nonvolatile. Volatile memory is memory that only holds data as long as there is an electrical current running through it. Once the power is turned off, all the data that resided in that memory is gone. An example is the system memory or RAM. Another example would be processor cache memory [6].

Nonvolatile memory is memory that does not need an electric current to hold electronic data. There are many examples of this kind of memory, although some may not be commonly thought of as such: things like CDs, cassettes, flash drives, floppy disks, smart chips, and hard drives. Unlike RAM in a computer, the information stored on the hard drive remains, with or without an electrical current present, until it is replaced or written over. Almost all personal electronic devices these days contain a hard drive or a miniature, non-volatile memory equivalent [6].

The Hard Drive

The hard drive is a vital part of a computer. It stores all of the instructions and information that a computer needs to remember more than once. For example, every time a computer is turned on, it must go through a startup routine called the boot strap. All the information the computer needs in order to complete the boot strap is located on the hard drive. This process initializes the peripheral hardware and prepares the computer to run the software that manages the system in general. This is called the operating system. The operating system and its corresponding file system specify how the hard drive will organize and maintain all data stored on it. The operating system also serves as a platform for other software programs such as office productivity software or video games. The operating system also manages the interaction of peripheral hardware like the monitor, printer, keyboard, etc. All of the code, data, files, and other information that make up an operating system and software programs are stored on the hard drive. Files created using software programs are also stored on the hard drive [6].

The data storage on a hard drive is physically organized into cylinders, heads/tracks, and sectors. The total storage capacity of a hard drive can be determined by multiplying the number of cylinders, heads/tracks, and sectors and then dividing by the number of bytes per sector. Sometimes the physical calculation of storage space differs from what your operating system says. This is because when an operating system mounts or initializes a hard drive, it examines the entire surface of the disk for bad

sectors. These are sectors that are flawed and cannot store data. No matter how sophisticated the manufacturing process is, there is no such thing as a perfect hard drive. All hard drives have some bad sectors. Your operating system identifies these and then reports the actual storage capacity of your hard drive. Different operating systems handle bad sectors differently [6].

With all the software and files on a computer being stored in one place, the hard drive becomes a very critical part of the system. While some computer parts can fail and be replaced without affecting the software and data on a system, which is the most vital part to most people, a damaged or failed hard drive will require replacement of not only the hard drive itself, but everything that was stored on it. Many times some of those things that were stored on a hard drive are irreplaceable unless proper backups have been made. The hard drive serves a key role in the operation of the computer system, and it also serves a vital personal role for the computer user by keeping track of and storing information in which the user has a personal invested interest whether it is work, play, or hobby related.

Operating Systems and File Systems

Different operating systems use different methods to organize and store data on a hard drive called file systems. These file systems treat the hard drive, and any partitions that are created, in distinct ways, although there are some commonalities. There can be more than one partition setup on a single hard drive, and since they are logically separate from each other, each can be managed by a different file system.

DOS and older versions of Windows use FAT, which stands for File Allocation Table. The FAT system combines sectors on the hard drive into logical groups, called clusters, within the scope of the hard drive partition which it is set up on. The size of the clusters depends on the FAT version used by the operating system, and the size of the hard drive. Clusters can be as large as 32 KB. These clusters are addressed and then chained together as files are created. When a file is created, Windows and DOS reserve the minimum number of whole clusters necessary to store the file. When a file is created, the clusters it occupies are not always physically adjacent on the hard drive, so the FAT chains them together by their logical addresses. This results in file fragmentation. If a file does not occupy the entire cluster or clusters allocated to it, file slack occurs. We will talk more about fragmentation and file slack more when we discuss the way data is stored and retrieved from a hard drive [4].

File Slack

Sometimes it is not necessary to have actually saved sensitive information in a file on a computer for it to turn up on the hard drive. As mentioned above, all kinds of information about a user can be retrieved from a hard drive. Just about anything typed into your keyboard can potentially be traced. Even specific Internet activity can be derived from a close inspection of a hard drive. This is due to something known as file slack.

File slack occurs when any file is created either by the user or by the operating system and consists of two major components; drive slack and RAM slack. As I have explained above, when a file is created, a certain amount of drive space is allocated to accommodate that file. This space nearly always exceeds the actual size of the file being saved. The amount of excess depends on the file system [4].

RAM slack, as a component of file slack, only pertains to the last logical sector of space allocated by the operating system. It is called RAM slack because the data contained in it is pulled at random from whatever is residing in system memory, or RAM, at the moment the file is created. Sometimes the result is random and meaningless data, but often it can result in the unintentional storage of more important information. RAM slack has been known to contain things like credit card numbers, passwords, and other sensitive information [1].

Drive slack makes up the other component of file slack and is so named because it is made up of whatever data was already residing in the sectors it occupies. Drive slack often contains fragments of old files that had previously been deleted or lost. The data contained in file slack is not recognized as legitimate or interpretable information by the application which created the file and is, therefore, not included in the main data body of the file [4].

Deleted vs. Overwritten

When a file is deleted, nothing in the actual file data is erased, so for purposes of permanently removing all traces of a file from a system, deletion falls short. The system merely marks the cluster chain as being available space. This means that it can be written over and the operating system will make no effort to conserve the data that formerly occupied those clusters [1].

Anything that has not been overwritten on a hard drive is potentially fair game for anyone who happens to acquire that hard drive second hand. We have already demonstrated how a hard drive can contain information the user didn't even know it was recording. I have mentioned that there are tools and utilities available for that can retrieve this data without the intervention or help of an operating system. Most of these software programs merely record every bit of data on the hard drive and then leave it up to the person using it to sift through the data and try to make sense of it. There are other tools that look for things like file markers that identify the type of file the data used to belong to, or they look for pointer or inode values to determine where a file started and ended and what type of cluster chain it used and made available for new data. Essentially any bit of data lingering on the hard drive is retrievable with one of these methods and can be viewed by anyone who knows how to use them, unless that data has been over written.

Precautionary Measures

Deleting files that are no longer needed, but that contain information someone would rather not have public, should be done sooner than later. Operating systems are constantly writing new files and modifying old ones through activities as common as the booting up. Defragmenting the hard drive is an operation that should be performed at different intervals, depending on your operating system and file system. For example, a computer using the FAT32 file system needs to be defragmented more often that one using the NTFS file system. The specifics and recommendations for each can be found either in the operating system user's manual, website, or by contacting an authorized support center. Defragmenting the hard drive improves the performance of your computer by placing file segments in adjacent clusters, so the hard drive doesn't have to seek as many locations to retrieve files [2, 3].

Finally, there are a couple of things computer owners should know about before going ahead and disposing of or re-selling a computer. Many people consider formatting (also known as initializing on some systems) to be a fail-safe method of erasing all traces of data, effectively destroying all information *about* the data, so the operating system no longer knows that it exists [4, 5].

SUMMARY

Being aware of and identifying a risk is the first step in managing and minimizing it. As computer equipment becomes more and more integrated with business operations, as well as with individuals' personal lives, more and more personal and sensitive information is being shared with stored in those computers. Understanding how computers handle and store that information will empower businesses and individuals to more effectively regulate the kind of information that resides in their computer's memory and, subsequently, control what kind of information is potentially made available to any future owner or user.

REFERENCES

1. File Slack Defined. *New Technologies Armor, Inc*. January 6, 2004. http://www.forensics-intl.com/def6.html.
2. Kozierok, C.M. (2001). High Level Formatting. April 17, 2001. http://www.pcguide.com/ref/hdd/geom/formatHigh-c.html.
3. Kozierok, C.M. (2001). Low-level Format, Zero-Fill and Diagnostic Utilities. April 17, 2001. http://www.pcguide.com/ref/hdd/geom/formatUtilities-c.html.
4. Nelson, B., Phillips, A. Enfinger, F. & Steuart, C. (2004).. *Guide to Computer Forensics and Investigation*. Boston, Massachusetts: Course Technology.
5. Spring, T. (2003). Hard Drives Exposed. *PC World Magazine*. May, 2003. http://www.pcworld.com/news/article.
6. Whitman, M. E. & Mattord, H. J. (2003). *Principals of Information Security*. Boston, Massachusetts: Course Technology.