CBL Data Shredder Information

Introduction

The CBL Data Shredder Program is intended to eliminate the chances that information stored on your hard drive may be retrieved by anyone when it, or the computer containing it, is disposed of.
Our experience is that files thought to have been deleted years previously, containing personal details, bank account details, credit card numbers, correspondence, etc., can be recovered all too easily, and simply formatting the drive is not an effective means of rendering this data inaccessible. This situation is made worse by the availability of off-the-shelf products that will automate the recovery process in some cases.
When used in accordance with the instructions in this guide, the CBL Data Shredder Program will do what file deletion and partition formatting cannot: erase the entire contents of a treated hard drive, rendering them irretrievable to existing and future software-based recovery tools.

Erase Methods

The CBL Data Shredder Program supports a range of methods of erasing data, providing different levels of security and convenience. In general it would be true to say that each time a hard drive is overwritten, the chances of recovering any data from it become vanishingly small. (For examples of the sorts of hardware-based recovery techniques that may be attempted, please see the succeeding section).
The CBL Data Shredder Program works by overwriting the entire disk with a pattern of bits. Wiping the disk with a simple (non-random) pattern once is known as clearing or erasing. It may still be possible, with specialist hardware, to read data off the disk.
More secure methods of erasing hard drives write more complicated or random bit patterns to the drive several times to effectively frustrate hardware recovery attempts. This is known as purging or sanitising. Certain of the erase methods available in the CBL Data Shredder Program have particular characteristics that make them suitable for this task. These are explained below. It must be noted that some features of modern drives may make some areas of the disk inaccessible, even though they may have contained data in the past, and that these areas would continue to be vulnerable to hardware-based recovery. These are discussed in the following section.

Custom Method

The CBL Data Shredder Program enables you to define your own method to erase a drive. The default setting is to wipe the drive once with a bit pattern of “00”. This is the simplest and quickest way to clear a drive. You may select a different bit pattern to use, and the number of times the drive should be cleared with this bit pattern.
Increasing the number of passes the CBL Data Shredder Program should make over the drive will increase the security of the erase process. However, it is unlikely that any custom method would be regarded as sufficient to sanitize the drive. The primary purpose is to provide a simple and fast clearing solution.
For utility, options exist to write the sector number in each sector of the drive, and a custom signature at the end of each sector.

United States Department of Defence Standard 5220.22-M

The National Industrial Security Program Operating Manual, issued to the US Army, Navy, Air Force, and other US government agencies specifies standards for the clearing, and sanitising of data classified confidential, secret, and top secret.

Under this standard, data may be cleared by writing any bit pattern to the entire disk once. Disks are sanitised by writing a different bit pattern to the disk on each of three passes. This is how the CBL Data Shredder Program implements this standard.
Drives containing top secret data are not permitted to be sanitised in this manner; they must be physically destroyed, or the disks subjected to degaussing, scrambling completely the magnetic patterns used to store data on the disk, rendering the drive itself inoperable.

German BSI Verschlusssachen-IT-Richtlinien (VSITR) Standard

The German Federal Office for IT Security released the VSITR standard, which wipes the drive with seven passes. For the first 6 passes, each wipe reverses the bit pattern of previous wipe.
This method is more secure than a custom erase with 6 passes of the same bit pattern. Multiple overwrites with the same pattern would tend to reinforce each other, but advanced hardware-based recovery techniques exist that may be able to infer the data that was overwritten. Writing alternating bit patterns, as in this standard, frustrates the recovery process.
The final pass overwrites the entire disk with “01010101”.
This is widely considered to be a secure method of erasing data.

Bruce Schneier’s Algorithm

Internationally-renowned security technologist and author Bruce Schneier recommends wiping a drive seven times. The first pass overwrites the drive with the bit pattern “11”, the second with “00”, and the next five with a randomly generated bit pattern.
This has a similar effect to the VSITR standard, but the random nature of the bit patterns written in the final five passes make it very difficult for an attacker to determine how the overwriting may have affected the data previously on the disk, making it extremely difficult to recover, perhaps prohibitively so.
Although a more secure method of erasing data than VSITR, the time required to create random bit patterns makes this a significantly slower method.

Peter Gutmann’s Algorithm

Peter Gutmann, is an Honorary Researcher at the Department of Computer Science, University of Auckland, specializing in the design and analysis of cryptographic security architectures. His research into secure deletion of data from magnetic media (such as hard disk drives) is the definitive work on the subject.
The CBL Data Shredder Program implements the method he devised based on his findings, erasing data with several series of passes to minimize data remnance on drives using any current techniques of encoding data on the disk.
His algorithm makes 35 overwrite passes in total, and is considered the state-of-the-art method for data destruction.
The cost of this security, of course, is time; wiping a drive using Peter Gutmann’s algorithm will take more than 7 times longer than wiping the same drive with Bruce Schneier’s algorithm, and will likely be more than 15 times longer than suing the US Department of Defence’s standard.

Royal Canadian Mounted Police DSX Method

The Royal Canadian Mounted Police Technical Security Branch makes a tool, DSX, available to departments of the Canadian government intended to prevent information disclosure when serviceable hard disk media is removed from service.

The CBL Data Shredder Program emulates DSX's method of clearing data, writing the bit pattern "00" on the first pass, "11" on the second, and a text pattern consisting of the software version number, and the date and time the erase took place.
Wiping a drive with DSX is not a method approved by the Canadian government for sanitising classified information.

Limitations

The effectiveness of an erase operation may be affected by limitations of the computer carrying out the operation, security restrictions in place on the drive, and physical and technological characteristics of the drive. Some knowledge of these factors will help in ensuring that information stored on a drive is securely wiped.

Computer Limitations

Computers with older BIOSes may not be able to access more than 504MB or 8.4GB of a drive. The solution in this case is to remove the drive from the computer, and attach it to a computer with a BIOS with large disk support.

Drive Physical Constraints

Hard drives are manufactured to allow for a margin of error in the position of the read/write heads. This takes into account that over the life of the drive the heads will shift slightly, relative to the patter on which the data is recorded. It is possible, therefore, that data written before the heads have shifted from their original positions will be unaffected by the erase procedure.
Further, to avoid interference between the magnetic patterns between recorded tracks, a buffer space is left around the tracks. This space may become affected by the magnetisation of the surrounding bits in time.
Both these factors may be exploited by hardware-based recovery techniques, using Magnetic Force Microscopy – examining the disk platter itself using a high-resolution microscope that can read the magnetic patterns on the disk. If insufficient or predictable (non-random) wipes have been used, it may be possible to use these techniques to determine what data was on the drive before it was overwritten.
It is worth noting that the high densities of current hard drives and the complexities of encoding of the source bit pattern for storage on the drive can make this an exceedingly difficult operation, and that in any case the data will remain inaccessible to software-based attempts at recovering the data; i.e. it will not be possible for an attacker to plug a properly sanitised hard drive into a computer and examine the former contents of the drive.

Drive Technical Constraints

Various features of modern drives can impact on the effectiveness of attempts to securely erase the data they contain.
IDE / ATA drives may support the Host Protected Area feature set. This allows the computer's BIOS to limit the area of the drive the computer's operating system and any other programs may access. Subsequently, data in the protected area will not be erased. For this reason it is important that you verify that the number of sectors found by the CBL Data Shredder Program is the same as the number of sectors printed on the manufacturer's label on the drive itself.
If a drive has a protected area, it may be possible to use a utility to unprotect the area before running the CBL Data Shredder Program. If it can't be unprotected in the computer because the area has been password protected it will need to be attached to another computer instead. The BIOSes of most desktop PCs will not set a protected area, although the protected area on the drive may persist. It should be possible then to use a utility to unprotect the area.
SCSI drives may support the SET LIMITS command, which has a similar effect to the Host Protected Area on ATA drives. As long as the drive is not part of a RAID it should be possible to use a utility to unSET LIMITS. RAIDs should be broken and each drive wiped individually to ensure all areas of all drives are effectively erased.

The growing capacity of hard drives and the ever shrinking areas used to store a given number of bits place large demands on the manufacturing process to produce drives with ever greater reliability. This is difficult to achieve. To ensure that a small number of errors on the drive do not compromise the integrity of the entire drive, manufacturers employ a technique that uses spare areas on the drive to store data in place of a faulty are of the drive. If an area of the drive develops a fault while it is in operation this can be detected, and a spare area is employed, and data from the bad sectors remapped to the spare sectors.

Data contained in bad sectors that have been remapped will not be overwritten, and it may be possible to remove the platter from the drive and use specialist equipment to recover some of the data in these bad sectors.

If a drive has been password protected, it will be necessary to unlock the drive before wipe the drive. Failure to do so will result in the program reporting an error, and no overwriting will take place.