



The Operation of DeadMan's Handle: Installation and Deletion

Introduction

This paper gives some background details on what DeadMan's handle does when it is activated, and how it takes steps to protect your information. It will be updated on a regular basis, but please note that your version of DeadMan's Handle may differ slightly from this description. This is because the product is under constant development.

This paper also gives tips and advice on how to use DeadMan's Handle. It assumes familiarity with usage of the system.

Installation

DeadMan's Handle installs in the usual way, although it does not use the new Microsoft Windows Installer service. This is because we wanted a consistent and simple installation across all platforms: older operating systems would have to carry out an extra download from Microsoft to get the installation service. In addition, our own installer allows rapid deinstallation.

During installation, DeadMan's Handle offers rather cryptic folder names for the installation and protected (secure) folders. This is because when activated it will delete and rename these folders. However, should there be a problem (such as a folder being locked when the panic button is used, as files are being edited), then the obscure names still make identification and analysis of the folders more difficult — especially as all unlocked files will have been deleted.

At the end of installation, you are placed straight into the configuration utility. This is because configuration is extremely quick and simple, so it is worthwhile getting it done straight away.



Deletion Activation

There are two ways to activate the deletion: either when the machine is booted up at the first signon (the “challenge system”), or during normal use (the “panic button”). DeadMan’s Handle’s core functionality revolves around the challenge system. The panic button is an extra feature that extends its capabilities.

The challenge system operates by presenting an innocent-looking screen, which has on it a key code or password requester (even though it may not be especially highlighted). You are presented with this when you fire up and start up the machine – and so is the thief.

Tip: don’t make your password or key code too complex. This is not a situation where the thief will have many opportunities to break your password – the moment he/she gets it wrong the deletion process will be activated.

Once the challenge has been failed, the system starts the deletion process. Under the challenge conditions (at log on) this means that no work is being done on the machine so all the secured files should not be locked. It also means that the deletion process will be maximally successful.

The panic button, on the other hand, activates the deletion process interactively. This may be when you are in the middle of working with files. Thus some of your target files may be locked as they are being edited. In this case although DeadMan’s Handle will try to delete the files, it cannot guarantee to do so — it does depend on the software that is being used to edit the files. So deletion via the panic button may not be quite as successful as deletion via the challenge system.

The Deletion Process

DeadMan’s Handle tries to completely wipe each file that is to be deleted. These are all the files in the secured folder (and subfolders), plus any files that were added via the Extra Files list. Unless you have chosen the minimal



security level, DeadMan's Handle takes considerable pains to wipe the file as much as possible.

The system does the following to each file:

1. It overwrites it, according to the security level that you have selected. Medium is one overwrite with random numbers, ranging through to Martian, which involves some 35 writes, eight of which are random numbers.
2. In the overwrite process, all the unused space in the file also gets overwritten. This is because this space often has data from the computer's memory dumped to it.
3. The timestamps are randomized.
4. It is renamed with a random sequence of letters.
5. It is truncated to 0 length. This makes it impossible for file recovery utilities to rebuild the file.
6. It is then actually deleted.

In addition, as subfolders within the secure folder are deleted, they go through a similar procedure as above, being renamed and having their time stamps altered. Throughout this process, DeadMan's Handle tries to ensure that it is not interfered with by locking out the special keyboard combinations, the desktop, the Start button and open windows such as the Explorer and the Task Manager (where applicable).

There are some limitations to all this, depending on the operating system. For example, the Windows 95/98/Me series will not allow the folders to have their time stamps altered. However, in general DeadMan's Handle will try to obscure as much information about the files as possible.

After the information files have been deleted DeadMan's Handle then removes itself from the system. It generally deletes itself to the same level as the information files (so it gets deleted at a military level if that was the security level). This is not possible for every file, but DeadMan's Handle does mangle its own system as much as possible. It also removes its installation folder.



This deletion process is followed for both the challenge system and the panic button.

Comments and Tips on Deletion

DeadMan's Handle does all it can to remove all traces of your confidential information. It tries to leave your system functional, but with nothing of interest on it.

DeadMan's Handle is a useful security tool even if you are already using encryption on your notebook. This is because the very existence of encrypted files is likely to pique the interest of someone who is nosing around your stolen machine. In addition, encryption itself may fail for a number of reasons [see reference 1 for a good general discussion on security], so DeadMan's Handle acts as an extra level of security for your notebook.

If you do use disk-based encryption or compression, then the usage of the Martian level encryption is completely pointless. This is because the Martian level uses bit patterns optimised to efficiently wipe as many different types of hard drive as possible. These patterns are subverted by encryption or compression. We would advise use of the Medium security setting in such cases. Please also see [2] for some further discussion on using DeadMan's Handle with encryption.

In general, you should be using either the Medium or one of the Military level settings for most purposes. Whilst there are many theoretical methods of recovering data from disks that have been overwritten one or more times, in practice there do not seem to be many instances where this has happened. For example: go to a disk recovery service and ask them to recover a file you have purposefully overwritten. You will find few takers. If you are dealing with an organization that can recover your information from overwritten disks, then they have probably already suborned your staff.



Minimal security is just a straight deletion, using the Windows file delete. This means that the files are still on your disk, and any file recovery tool will allow the thief to bring them back. Minimal delete just protects the files from a very cursory examination: it's only benefit is that it is very fast.

It is worthwhile noting that if files are locked, the DeadMan's Handle will try to delete them. If it cannot, then it will still try to rename them, and will also try to rename and delete the parent folder. In these cases, what happens is operating system-dependent. For example, The Windows 9x series allows the folders to be renamed, so even if the files are not deleted they are hidden as much as possible. In general, DeadMan's Handle will try to do as much as possible to hide the files if they are not destroyed.

Try to keep the amount of confidential information on your notebook to a minimum. This is a straightforward good security policy. In addition, whilst DeadMan's Handle is fast, the less it has to do the quicker it will complete, making it less likely anyone will notice something going on.

Backup your information! DeadMan's Handle will delete it if activated! Make sure that you have backups and do not keep them with your notebook.

File Sizes

DMH cannot handle file sizes greater than 4GB minus two bytes. However, you should not be even thinking of trying to protect files of any such size – the deletion process will be very slow (unless you select minimal security).

Under NTFS (typically Windows 2000, XP and 2003 Server) there is a special issue with regard to small files. When they are less than about 800 bytes in size their data can end up in the disk transaction log. DMH could flood this log file to clear it, but it would take a long time. Thus this feature is not currently implemented.

As a rule of thumb, make sure that no file is less than 1 KB in size. This is most unlikely with modern application software, where even empty files are larger than 1KB.



Safe Mode Boot

DeadMan's Handle will automatically regard a safe boot as an attempt to circumvent the protection system. On logon, it will immediately go into delete mode (2000/XP/2003 only). However, this capability can be toggled via the 'Safe Delete?' option on the Advanced tab. Setting this to 'No' will disable this feature.

Conclusion

This paper has tried to expand on the DeadMan's Handle deletion processes. In general, DeadMan's Handle should be viewed as part of an integrated security policy for your organisation: an extra backstop for when the worst happens.

References

- [1] *Security Engineering*, Ross Anderson, John Wiley & Sons Inc, ISBN 0-471-38922-6. See also <http://www.cl.cam.ac.uk/~rja14/>.
- [2] *DeadMan's Handle: Tips for Use*, DeadMan's Handle Ltd, <http://www.deadmanshandle.com>.