



DeadMan's Handle: Tips for Use

Introduction

This paper describes how to use DeadMan's Handle (DMH) effectively. It shows how you can set up your machine so that it is as secure as possible, and covers how to use DeadMan's Handle as a key component in your notebook security. This article covers Windows XP, but many of the tips are applicable to other Windows operating systems.

Notebooks and Laptops

Notebooks – or laptops – are inherently insecure devices. They are firstly eminently losable: their very portability makes this a likely event. Secondly, the Windows operating system is not very secure (although Microsoft has recently made a number of announcements stating their intention to raise the security of their systems). Thirdly, with a few rare exceptions, most notebooks have no special provision in their hardware to enhance their security.

Because of these limitations, no reasonable action can make current notebooks 100% secure. However, DMH allied with some other techniques can make it much harder for the attacker to get information off your machine.

Please note: do follow these tips with care, and if you are unsure then get the help of an IT expert. Making a mistake with some of these recommendations could severely impair your machine performance – and if you get a password wrong, you could lock yourself out of your machine!

BIOS Settings

There are some settings in your machine's system board that can greatly help your security. These are generally known as the 'BIOS settings', although they can also be referred to as the 'CMOS settings'. There will be a reference book for your machine which describes them all. In a corporate



environment, this reference documentation will usually be held by the IT department.

Many of the BIOS settings affect how the hardware works at a very low level, and should not be played with. However, there are a few which are useful for security.

To access the BIOS configuration utility, start up the machine. Pressing the correct key as soon as you start it up (typically the Delete or F2 key), or when the boot screen first appears, will enter you into the configuration utility. Usually your machine will display a message telling which key to press when you boot it up – although the display period can be very brief on modern machines.

Boot Sequence

The first BIOS setting of interest is typically called 'boot sequence', although it can have other names, such as 'boot devices'. This describes the order in which your machine will search its drives to find an operating system. Windows is (almost always) on the C: drive of your computer – the first hard disk. However, if the boot sequence is A: then C:, this means that the machine will first try the floppy drive – only if there is no disk in that drive will it then look for its operating system on the C: drive.

This allows the thief to put a floppy in your drive with a very cut-down operating system, and start ferreting about through your disk. This mechanism also allows him to change the Administrator password, which will give full access to the system.

To plug this hole, ensure that the C: drive (or the one with Windows on) is selected as the first drive in the boot sequence. The system will then always find the operating system on the hard disk, and will not look at the other boot devices. The floppy will be ignored – which is what you want.



Note that on modern machines the possible boot devices can be quite numerous; they include for example the CDROM drive and the network, where a remote machine can provide the operating system. Make sure the C: drive is the first one.

Boot Passwords

The next step to take is the use of the BIOS boot passwords. The first reason for using these is that you don't want a knowledgeable thief immediately going into the configuration utility, making the floppy A: drive the first boot device, and then rebooting the machine with his floppy in. You want to password-protect the BIOS configuration utility so that the thief cannot alter the system to his benefit.

The possible passwords that are available in the BIOS settings vary somewhat between machines, and their nomenclature is not very consistent. There are typically up to three different possible password protections that can be set:

1. Access to the BIOS configuration can be controlled so that you can read the settings – a 'read-only mode' password is used. This is often called a 'BIOS user password'.
2. Access to the BIOS configuration so that you can change the settings – a 'read/write mode'. This is often called a 'BIOS supervisor password'.
3. When the system is booted, the user can be asked to input a password. The machine will not boot without the correct password. This is often called a 'system password' or 'boot password'.

Many machines, however, do not supply three different passwords for the three capabilities. Some, for example, allow you to set the first two passwords listed above, and then you just enable the 'system password' – it uses the same password as the user password. Other systems do not separate the read-only and the read/write passwords: there is just one that gives you access to the setup utility.



The thing to do is to read the BIOS configuration utility screens carefully, to ensure that you are setting the right passwords. Note also that people often refer to the 'BIOS password' when they actually mean the third one listed above: the 'system password'.

For good security, the second of the three passwords listed above should be set: you should control access to the BIOS setup utility so that items cannot be changed without having a password. The read-only mode is much less critical, although there is no harm in setting it.

On the other hand, we do not recommend setting the third option: the system or boot password. Doing so immediately alerts the thief that the system has been secured. They may then start investigations and take steps that you would rather not encourage. In addition, the boot password can be reset by removing the small CMOS battery in the machine – which will also reset the other passwords. Ideally, you want to let the thief boot up so that they can get into real trouble with DeadMan's Handle.

One other problem with the boot password is that if it is enabled, you will typically have to enter three passwords: one at the boot, one to get into your account and one for the DMH. This will become irritating, and will lead to mistakes in password entry.

Encryption

DeadMan's Handle can work well with encryption (see Reference [1]). However, there are some comments that need to be made with regard to the Windows Encrypting File System (EFS, especially under XP). This section assumes you are using an NTFS formatted volume (you cannot encrypt under Windows using EFS otherwise).

Firstly, always encrypt folders rather than files. This ensures that temporary files also get encrypted. You should also consider encrypting your temporary folders (known to the system as the %Temp% and %Tmp% environment variables – see your local IT expert) for similar reasons.



Secondly, ensure that you take backups of your encryption certificate along with your data. This will mean that if your hard disk gets damaged, you can recover your encrypted files from backups.

Thirdly, in a corporate setting there will usually be a Data Recovery Agent (DRA): a user (often the Domain Administrator in a networked environment, but it can be the local Administrator) different from the user that encrypts the files, but who can decrypt the files should the original user be unavailable. However, this agent can be a security weakness in a poorly secured computer. This is because it can be relatively easy for the attacker to change the password of the Administrator account if they have physical access to the machine. If the Administrator is also the DRA, then the attacker can read all the encrypted files.

The reason for this is that the DRA's recovery key (known as the private key) is still on the machine. When the DRA is set up and designated, the last step should be to remove the private key: use the certificate management utility to export the file recovery certificate. In the process, ensure that strong protection is enabled and that the private key is deleted if the export is successful. This exported certificate should be saved to a location that is not on your notebook, and should be backed up. Note that any other certificates used to designate the DRA on your machine should also be removed and stored in a secure location.

This procedure means that the DRA now cannot recover and read encrypted files until the certificate is loaded, and ensures that the DRA is not a hole in your encryption system.

There is another tip that may be useful if you are using encryption. If you are confident about its quality then you can use encryption to speed up the operation of DMH. This is because you can use the minimal security setting: DMH will do a normal Windows delete, which is very fast, and the files are full of random-looking bytes anyway. The benefit is that you are using encryption and then concealing it from the attacker, and you can have very large



quantities of files as well. The one drawback is that at this setting DMH will not conceal the file names and time stamps, nor will it truncate them, so there could still be some information leakage (this is being looked at for future versions of DMH).

Clean up the Page File

DeadMan's Handle aims to keep your information out of other people's hands. However, Windows as an operating system has a number of mechanisms that allow information leakage. One example is in the spare space within files (the difference between what the operating system has allocated for your file, and what you are actually using). Typically Windows will dump chunks of memory to this spare space, which is a potential source of information exposure. This is why DMH always scrubs beyond the end of the current file (at all security settings above minimal).

One other location where information can get placed is in the Windows page file. This will tend to have items of information from files that have been recently worked on. Note that the more memory you have on your machine the less the paging, so the problem can be reduced with hardware.

However, DeadMan's Handle provides a facility to exploit a capability in the Windows NT/2000/XP/2003 operating systems: the page file can be cleared on shutdown. The option is set in the Advanced tab of the DMH configuration utility, and we strongly recommend that it is set. The clear down is not perfect, but it will remove most of the information in the page file, reducing further the chances of information leakage.

Extra Files

DMH is designed to delete everything, files and subfolders, in a nominated folder. However, it can also deal with files outside of this folder via the extra files list. We strongly recommend usage of this feature for files that are likely to contain confidential information but are difficult to move from their normal working locations.



The best examples of these are mail files (the DMH help file gives some information on where these can be located). For a number of reasons it may be preferable to leave them in their default locations: they can be nominated for deletion in the extra file list. It is highly likely that the mail file contains confidential information.

Other files that should be considered for the extra file list include:

1. Financial data files or contact lists (often these systems can place files in specific places).
2. PDA data files, especially if they also contain contact information.
3. Other communications systems data files (such as newsgroup reader files, messenger system data files and logs, and so forth).
4. Configuration files, especially those that govern access to you organization's networks.

Use the Dummy Logon Feature

DeadMan's handle provides a specific dummy logon feature under Windows XP, 2000 and 2003 Server (it is not needed under the Windows 9x and Me systems as the logon is trivial from a security point of view).

The concept is that your account will certainly have access to all your data files; it may also have super user or Administrator level privileges. However, in an ideal world we would like to trap any attacker with DMH at the earliest possible moment in the machine start up process. But we do not want to give any attacker easy access to your account.

The way around this is to create a dummy account: a user account with the most basic privileges. This account should not have access to your normal account's files. This account is made into an autologon account: when the system is started, the boot process is followed and the system automatically signs on to the low-privilege account, where the DMH challenge is promptly presented. Pass the challenge, and the system just signs off: you still have to log on to the real account. Fail the challenge, and DMH is activated. The files are deleted.



You can define what happens after the challenge has been failed on the autologon account. Using the autologoff toggle, on the Advanced tab, you can have the system either log off, and so present a logon screen to the attacker, or to stay logged in so that the attacker is left in the account. You may wish to do this if you have tracking software on the system, for example, and want to encourage the person to use the machine to connect to the Internet.

It may be seen that these features, when allied with the others, makes your notebook a highly protected machine: a trap for the unwary. At the background level, encryption is protecting your files, and clearing the page file is reducing leakage. If you lose the machine, the thief is caught the moment the notebook is turned on. Floppies or CD-ROMS will be ignored, and at the end of the boot the attacker is presented with the challenge. One wrong step – and pressing Cancel is the most likely one – and DMH is activated (assuming you allow only one try). Your information is safe.

Turn it Off

If you do not need the security of DMH – you will be in a secure area for a while – then do not forget that you can disable DMH. It is perfectly valid to do so, as long as you remember to turn it on again when you leave the safe harbour. Note that the challenge and the panic button can be disabled independently.

Attempts and Prompts

You can define the number of tries that the challenge will allow before going into deletion mode. We recommend the minimum: one, for maximum security. However, this can act as a 'hair trigger', with any mistake leading to deletion. You can allow yourself up to nine tries, or allow an unlimited number (we strongly do not recommend the last option). Keep the number of allowed tries to the minimum you can live with.



One other feature you can set up is the prompting. DMH can prompt you if you are passing or failing the challenge, and you can define these prompts. You can use these to help entrap the unwary; you can also use the prompts to give you subtle cues as to what your password or key code is.

Things to Watch Out For

DMH has a number of features. One of these is its self-protection capability. During the challenge and deletion phases it will try to lock out all special keyboard combinations (such as Ctrl-Alt-Del) and will also try to disable Explorer windows (and the Task Manager under Windows 2000, XP and 2003 Server). It will also attempt to lock out the desktop and the task bar.

However, certain actions can undermine all this. For example, putting programs in the Startup folder can cause problems. If the program is opened up fully on the desktop and gives you access to an Explorer-like interface then DMH will not be able to lock it out. This gives a potential attacker an opportunity to try to interfere with the challenge or deletion process. On the other hand, if the program is immediately put into the system tray then it will be locked out and no problem will arise.

Extra toolbars like the Office toolbar can represent a security weakness. These can often give access to windows that DMH cannot lock out and give attackers other ways to interfere with the DMH system. Try to activate such toolbars after the challenge has been dealt with.

DMH tries to delete itself, so that there is no evidence that it was ever on the machine if it is activated. However, the system restore feature under Windows XP can undermine this. You may wish to consider disabling the monitoring of the DMH folder and creating new restore points to try to remove information about the existence of DMH.

Do not select the entire system drive as the target secure folder. You can select other drives and DMH will delete their contents as expected. The problem with nominating the system drive is that DMH will start deleting it, and it will get to the system folders at some point. It is impossible to predict at



what stage this will happen in the process, as it will be dependent on the folder structure of the drive. What will happen is that a large number of system files will get deleted, and then the whole system will fail.

It then may well not reboot. However, the risk is that the confidential information may still be on the machine. If the attacker can repair the drive they may be able to access the secure folder. To avoid this, select a specific folder as the secure folder.

Other Tips

There are some other actions you can take which will generally help DMH in protecting your system:

1. Keep the number of confidential files as low as possible on your machine. This will allow DMH to work more quickly through them if it is activated.
2. Try to reduce the number of programs and services that automatically start when you boot up and sign on. The more programs that are run, the slower the boot and the longer it takes for DMH to activate.
3. Keep the number of icons on your desktop to a minimum. This reduces information leakage (the icons are visible), and again contributes to speeding up the boot process.
4. Ensure you understand the deletion process: see Reference [2] for details on this.

Safe Boot Mode

One way a thief may try to circumvent security is by booting the machine into Safe mode. DMH detects this, and regards a safe boot as an attack: it will immediately go into delete mode (on 2000/XP/2003 systems only). This behaviour can be disabled by use of the 'Safe Delete?' option on the Advanced tab. If this is set to 'No' then the automatic delete will not take place (but you may still be presented with the challenge, depending on the operating system).

Conclusions and Synopsis



This paper has attempted to give tips and procedures to ensure the maximum protection for your notebook. The key lies in the combination of security measures: they interlock to provide a coherent defence for your system. The best way to end this document is to simply list the important recommendations as bullet points, so they act as a checklist.

1. Make sure the hard (C:) drive is the first boot device.
2. Protect access to the BIOS configuration utility with a password.
3. Use encryption (carefully) on your machine.
4. Ensure the page file is cleared down.
5. Use the extra file list in DMH.
6. Apply the dummy logon feature to present the challenge automatically.
7. Keep the number of allowed challenge attempts to a minimum.
8. Check your Startup folder and the use of special toolbars.
9. Reduce the number of confidential files on your machine.



References

- [1] *DeadMan's Handle and Cryptography*. DeadMan's Handle Ltd, <http://www.deadmanshandle.com>.
- [2] *The Operation of DeadMan's Handle: Installation and Deletion*. DeadMan's Handle Ltd, <http://www.deadmanshandle.com>.