



DeadMan's Handle: Benefits and Features

Introduction

DeadMan's Handle refers to an old train device: the dead man's handle. It was typically some form of switch that the driver would keep closed. Should he suffer a calamity - such as a heart attack - his hand would loosen and the switch would open, stopping the train automatically. The aim of the dead man's handle was to protect the passengers, even in the worst possible case.

This paper describes the benefits and features of DeadMan's Handle (DMH): a new software security solution for notebook and laptop computers.

Description

DeadMan's Handle is a software product that tries to protect your laptop. Should the worst happen and your machine be lost or stolen, DeadMan's Handle will try to ensure that your confidential information does not fall into inquisitive hands. Once you have set it up, each time you - or the thief - boots up there will be an innocuous-looking challenge. Fail the challenge and the system will quietly delete the files you have told it to and then delete itself, removing any audit trail. Whoever has your machine probably will never know the information was on it and that you took steps to protect it.

Benefits

DeadMan's Handle protects your information even if you have lost control of your notebook. This provides a number of benefits, which we describe here.

1. DeadMan's Handle can stop information exposure. This can directly save you loss of business due to the leakage of information: imagine the consequences of your marketing plans ending up in competitors' hands.
2. It can prevent the loss of information relating to clients, suppliers and contacts. Such a loss could lead to legal liabilities, which DMH will help you avoid.



3. Quite often, the loss of information event needs to be communicated to external bodies. In California, for example, Senate Bill 1386 requires any organization with a computerized database of personal information to alert customers if their information security has been compromised. It is expected that this legislation will spread to other states. Such announcements can obviously lead to embarrassment or loss of professional credibility: the use of DeadMan's Handle can help support the business image of a responsible company.
4. Businesses will usually have information protection strategies in place, including the use of encryption. DeadMan's Handle has the benefit of integrating with current strategies without requiring any major changes to the current installations, reducing cost and increasing ease of implementation.
5. Because of the different approach DMH takes, it helps provide security in depth for a business: a powerful concept in the security field. If, for example, notebooks already utilize encryption then DMH can complement this approach and so reduce the likelihood of information loss.
6. More and more governmental agencies have requirements that businesses are well-managed. Using DeadMan's Handle carries the benefit that it is direct evidence of corporate good governance: it reinforces the professional reputation of the business with authorities.
7. Aside from the general reputation of the business, DeadMan's Handle directly helps an organization meet certain specific legal obligations: the Data Protection Act in the UK is an example, along with Sarbanes-Oxley in the USA. DeadMan's Handle protects the information and by its existence is evidence for that protection.

The strength of DMH lies in the way it acts in concert with your other security procedures. It limits the opportunities for an attacker as any slip or error will lead to the deletion being activated: this is even more likely when the attacker is under time pressure. When there is an integrated set of security measures for your notebooks and laptops then it becomes very difficult to get at the information.



Features

DeadMan's Handle comes with a large number of features, to make it an effective security solution for the business. These are now briefly explained.

1. The system is highly customizable: many of the parameters can be modified, and access to these parameters can be controlled.
2. The system is also policy-driven: this can be extremely useful in a corporate environment where consistency may be essential.
3. DMH is designed to turn your notebook or laptop into a trap for unwary attackers.
4. You can select your own challenge screens (including both text and graphics challenges) and create your own screens if you wish. Full details are provided on how to produce your own screens.
5. The challenge can appear automatically on boot up, or after log on.
6. The challenge system allows user-definable prompts and number of attempts.
7. File deletion can be set to any of five different security standards, one of them military and one to the most exacting file deletion specification yet given.
8. Deleted files will have their names altered, their date stamps randomized, the file contents and slack space overwritten and files will be truncated to 0 bytes: all these steps make recovery and audit extremely difficult.
9. DeadMan's Handle is extremely easy and quick to install and set up.
10. A panic button capability is provided. The system can be manually activated from the system tray in an emergency.
11. The system provides a facility to clean up the swap file on NT4, 2000, XP and 2003 systems whenever the system is shut down, to reduce information leakage.
12. When activated, the system will delete all the nominated information and then delete itself. This removes all trace of its existence: any attacker will not know there was anything of interest on the machine.
13. When it is active, DeadMan's Handle protects itself from interruption. It locks out all the special key combinations (such as Ctrl-Alt-Del), the desktop and the task bar. Under some operating systems it also disables open Explorer windows and the task manager.



14. First-rate context-sensitive help is provided with the system. In addition, support papers are provided to help customers get the best from the product.
15. The product is fully supported. Web site and eMail support is free. Corporate customers may also take out optional phone support contracts.
16. DeadMan's Handle incorporates advanced encryption and random number generation technology.
17. The system operates with and is completely compatible with encryption utilities and systems.
18. The system has been developed to Governmental quality standards and is fully documented. DeadMan's Handle has been subjected to a rigorous and documented QA process throughout its development.
19. DeadMan's Handle works on Windows 95, 98, Me, NT, 2000, XP and 2003 Server (some capabilities vary depending on the operating system).
20. Special tools and documents are available for registered customers, to help manage large scale distribution across systems and other tasks.

It may be seen that DeadMan's Handle provides a large number of features, to make it an effective tool for all users.