Chapter 5

EVALUATION OF REGISTRY DATA REMOVAL BY SHREDDER PROGRAMS

Harry Velupillai and Pontjho Mokhonoana

Abstract Shredder programs attempt to overcome Window's inherent inability to erase data completely. A shredder is useful when one needs to transfer ownership or dispose of a computer, but it can be exploited by a suspect for the purpose of wiping incriminating evidence. Most shredder programs claim to remove all traces of data. This paper examines these claims by conducting forensic examinations of computers on which shredder programs were used.

Keywords: Shredder tools, Windows Registry, data removal

1. Introduction

It is difficult to completely remove all traces of data from a computer system [9]. In the case of Microsoft Windows, for example, much of the "erased" data is recoverable, even when it is not visible from the Windows Explorer interface. For example, traces of a program remain after deleting it using Window's Add/Remove Programs function. Generally, the residual data takes little space and users are not concerned about this data unless it affects system performance.

The situation has changed with the release of digital forensic tools [10], which enable users to locate, recover and interpret deleted data. Initially, forensic tools were only available to law enforcement personnel; now, high performance tools are available to all at relatively low cost. The implications are obvious – data must not simply be removed, it must be removed securely. Also, data should be removed from locations that may not be quite so obvious.

Shredder programs were developed to address Window's inherent inability to erase data completely. These programs claim to wipe all traces of sensitive data, including data residing in locations that normal users

would not access (e.g., the Windows Registry). This paper examines the effectiveness of shredder programs available on the market. In particular, it evaluates their ability to completely remove Windows Registry entries. Several digital forensic tools, including a hex editor, are used to determine if deleted entries are still visible after shredder programs are executed.

2. Windows Registry

The Windows Registry is a directory that stores settings and options for all the hardware, software and users of a Windows system. Changes to control panel settings, file associations and installed software and applications are maintained in the registry. The registry files are in continuous use when the machine is running; changes to the registry are made in real time and timestamps are changed only at shutdown. Registry data is stored in multiple files whose names and locations differ according to the specific Windows edition [2, 6].

- **Windows 3.11:** The registry is stored in only one file `Reg.dat`, which is located in the directory `C:\Windows`.
- **Windows 95/98:** The registry consists of two files, `User.dat` and `System.dat`, which are stored in the directory `C:\Windows`.
- **Windows ME:** The registry consists of three files, `User.dat`, `System.dat` and `Classes.dat`, which are stored in the directory `C:\Windows`.
- **Other Windows Versions:** The registry of Windows versions released after Windows ME (excluding Vista) have six files, `Default`, `Sam`, `Security`, `Software`, `System` and `Userdiff`, which are stored in the directory `%SystemRoot%\System32\Config`. Note that these files do not have extensions. In addition, each user has two files, `Ntuser.dat` and `Usrclass.dat`, stored in the corresponding user profile directory.

The problem with registry data is that the user knows where the files are located, but he cannot wipe them because they are vital to Windows – he might as well re-install the operating system. This is why shredder programs are required.

3. Shredder Programs and Forensic Tools

This section describes the shredder programs and digital forensic tools used in our experiments.

3.1 Shredder Programs

Numerous shredder programs are available from commercial sources or are downloadable from the Internet. We selected two representative programs, CCleaner [13], which is available as freeware; and Registry Washer [14], a commercial product.

3.2 Forensic Analysis Tools

Several digital forensic tools [8] were used to evaluate the ability of the shredder programs to delete registry data.

- **Ultimate Toolkit:** This popular toolkit from Accessdata [4] consists of the FTK Imager, Registry Viewer, Password Recovery Toolkit (PRTK), Distributed Network Attack (DNA) and Forensic Toolkit (FTK). Only the FTK Imager and Registry Viewer were used in our tests.

- **FTK Imager:** FTK Imager is a forensic tool for recovering evidence from a target machine [1]. The tool can create physical and logical images of drives in a number of formats. In addition, it can extract registry files from a running machine. Because FTK Imager accesses the drive directly instead of via the operating system interface, it is able to acquire the locked system files used by the registry.

- **Registry Viewer:** The Registry Viewer is a forensic tool for viewing all Windows Registry files [3]. It provides access to user data, hardware and software information, URL/MRU lists and the Protected System Storage Provider.

- **Regedit:** This Windows Registry editor is a built-in utility for viewing and editing registry entries [12]. Regedit permits the addition, modification and deletion of registry entries.

4. Experimental Setup and Results

The experiments involved installing and then uninstalling eMule [7], a popular peer-to-peer program. While peer-to-peer programs can be used for illegal activities, our focus was on determining whether or not the shredder programs could remove all traces of eMule from the Windows Registry.

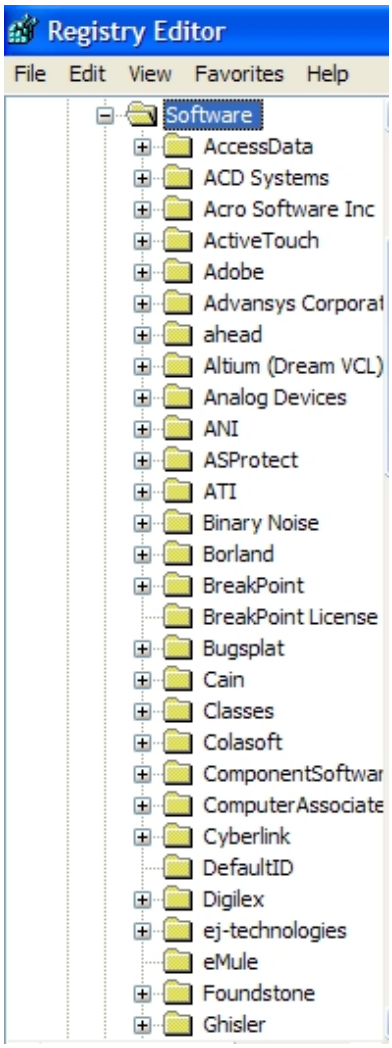

Figure 1. eMule key in the registry.

4.1 Installation

When installed, eMule creates eight entries in file `Ntuser.dat` in the Windows Registry. Note that Windows Registry folders are called "keys."

- **Entry 1 (Key):** The eMule key is located at `Software\Emule` (Figure 1). Entries 2, 3 and 4 are located inside this key.

Figure 2. Entries 2, 3 and 4 in the Registry

- **Entry 2 (String Value):** This entry is found in `Software\Emule\Install Path` (Figure 2). The first entry `Default` is ignored because it is created by the Windows Registry, not by eMule; also, it does not contain any data. Of the three entries created under the eMule key, only Entry 2 holds sensitive data.
- **Entry 3 (StringValue):** This entry is found in `Software\Emule\Installer Language`.
- **Entry 4 (Dword Value):** This entry is found in `Software\Emule\UsePublicUserDirectories`.
- **Entry 5 (Key):** This entry is at `Software\Microsoft\Windows\CurrentVersion\Explorer\MenuOrder\StartMenu\Programs\Emule`.

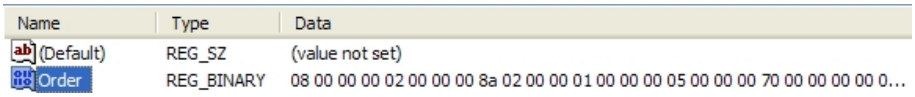

Figure 3. Entry 6 in the registry.

- **Entry 6 (Binary Value)** This entry, created under Entry 5, is at `Software\Microsoft\Windows\CurrentVersion\Explorer\MenuOrder\StartMenu\Programs\Emule\Order`. Figure 3 shows the entry; note that the default entry is ignored.
- **Entry 7 (String Value):** This entry is at `Software\Microsoft\Windows\ShellNoRoam\MuiCache\C:\Program Files\eMule\emule.exe`. This entry points to the location of the eMule executable and it is added only if eMule is executed.
- **Entry 8 (String Value):** This entry is at `Software\Microsoft\Windows\ShellNoRoam\MuiCache\O:\LocalDriveC\downloads\eMule0.48a-Installer.exe`. It points to the location of the eMule installation file.

Table 1. Comparison of shredder programs.

Entry	Windows	CCleaner	Registry Washer
1	Removed		
2	Removed		
3	Removed		
4	Removed		
5		Not Removed	Not Removed
6		Not Removed	Not Removed
7		Removed	Removed
8		Conditional Removal	Conditional Removal

4.2 Uninstallation

Several entries are removed after Windows is used to uninstall eMule. However, Entries 5,6,7 and 8 remain.

4.3 Evaluation of Shredder Programs

Both the shredder programs removed Entry 7. Entry 8 was removed only when the eMule installer had been deleted or moved to a different directory. However, both programs did not remove Entries 5 and 6. The results are summarized in Table 1.

Analysis of the results sheds light on how shredder programs work and why they fail to remove all traces of a program. Shredders attempt to find data that should be removed mainly by searching for broken links. This is why Entry 8 was removed only when the installation file had been deleted or moved. Entries 5 and 6 were not removed because they did not contain links to programs, just data used by programs.

4.4 Forensic Acquisition

The final step in the experiments was to use forensic tools to see if the deleted portions of the registry could be reconstructed. Our tests showed that it was not possible to recover any data deleted by the two shredders or manually using Regedit. The fact that the data deleted using Regedit was also not recoverable indicates some other mechanism is at work – perhaps the way Windows stores and changes registry files. We intend to investigate this issue in future work.

5. Advantages and Limitations

Using shredder programs has several advantages. CCleaner was very effective at wiping the detailed history maintained by Windows. Also,

CCleaner's secure deletion facility enables users to delete data as well as to overwrite the sectors that held the data to prevent any recovery [5, 9]. Moreover, it allows users to choose the number of overwrites based on the sensitivity of the data being erased [11].

Windows stores the search terms used by most applications. Therefore, when Regedit is used to delete registry entries, search data pertaining to these entries is saved – and is easily recovered. Unlike Regedit, the shredder programs do not leave any such traces.

The shredder programs examined in this work have certain limitations. The most serious limitation is the lack of user input. In particular, users cannot submit program names or terms that should be located and removed. For example, Entries 5 and 6 could easily have been deleted if the shredder programs allowed users to enter the specific entries they want erased from the registry

Regedit addresses this issue by permitting manual deletion. But this is problematic because, as described above, Windows stores the search terms used to locate the registry entries. Ironically, attempting to delete entries creates additional entries that must be deleted.

Finally, the shredder programs do not wipe all the data. As verified by our experiments, traces of eMule remained even after it was uninstalled and the shredder programs were executed.

6. Conclusions

Shredder programs are useful tools, but they are unable to erase all traces of potentially sensitive Windows Registry data. The manual deletion of data is an option, but the process of searching for the data to delete leaves traces. The burden, therefore, falls on the user to understand the nature and locations of the data that remain on a computer system. Short of wiping the entire hard drive, there is no way to remove all the sensitive data and references to its existence.

Acknowledgements

This research was supported by the Council for Scientific and Industrial Research of the Republic of South Africa.

References

[1] AccessData, FTK Imager, Lindon, Utah (www.accessdata.com).

[2] AccessData, Registry quick find chart, Lindon, Utah (www.accessdata.com).

[3] AccessData, Registry Viewer, Lindon, Utah (www.accessdata .com).

[4] AccessData, Ultimate Toolkit, Lindon, Utah (www.accessdata .com).

[5] H. Berghel, and D. Hoelzer, Digital village: Disk wiping by any other name, *Communications of the ACM*, vol. 49(8), pp. 17–21, 2006.

[6] H. Carvey, *Windows Forensics and Incident Recovery*, Addison-Wesley, Boston, Massachusetts, 2004.

[7] eMule.org, eMule (www.emule-project.net).

[8] G. Francia and K. Clinton, Computer forensics laboratory and tools, *Journal of Computing Sciences in Colleges*, vol. 20(6), pp. 143–150, 2005.

[9] S. Garfinkel and A. Shelat, Remembrance of data passed: A study of disk sanitization practices, *IEEE Security and Privacy*, vol. 1(1), pp. 17–27, 2003.

[10] W. Harrison, D. Aucsmith, G. Heuston, S. Mocas, M. Morrissey and S. Russelle, A lessons learned repository for computer forensics, *International Journal of Digital Evidence*, vol. 1(3), 2002.

[11] N. Joukov, H. Papaxenopoulos and E. Zadok, Secure deletion myths, issues and solutions, *Proceedings of the Second ACM Workshop on Storage Security and Survivability*, pp. 61–66, 2006.

[12] Microsoft Help and Support, Windows Registry information for advanced users, Microsoft Corporation, Redmond, Washington (support.microsoft.com/kb/256986).

[13] Piriform, CCleaner (www.ccleaner.com).

[14] Right Utilities, Registry Washer (www.rightutilities.com).