Suspects' data hiding at remaining registry values of uninstalled programs[1]

Youngsoo Kim
ETRI
161 Gajeong-dong
Yuseong-gu, Daejeon, KOREA
+82-42-860-5856
blitzkrieg@etri.re.kr

Sangsu Lee
ETRI
161 Gajeong-dong
Yuseong-gu, Daejeon, KOREA
+82-42-860-1613
sangsu@etri.re.kr

Dowon Hong
ETRI
161 Gajeong-dong
Yuseong-gu, Daejeon, KOREA
+82-42-860-6147
dwhong@etri.re.kr

ABSTRACT
Windows registry, a central repository for configuration data, should be investigated for obtaining forensic evidences, since it contains lots of information that are of potential evidential value. Using some forensic tools, forensic examiners can investigate values of windows registry and get information can be forensic evidences. However, since windows registry contains huge amount of values and these values can be modified by users, suspect can hide his secret like password in registry values. Specially, remaining registry values not removed after uninstalling specific programs can be the best target to hide a suspect's secret without forensic examiners' notice, since generally they are not interested in registry values of removed programs, but which programs were removed. In this paper, we briefly extract some registry entries related to forensic analysis based on Windows XP and list up consideration items for hiding secrets in registry as suspect's viewpoint. And then we show that countermeasures are needed, examining remainder of registry values for specific programs uninstalled.

Categories and Subject Descriptors
K.6.5 [**Management of Computing and Information Systems**]: Security and Protection

General Terms
Security

Keywords
Digital Forensics, Windows Registry, Data hiding

1. INTRODUCTION
Windows 9x/ME, Windows CE, Windows NT/2000/XP/2003, and Windows Vista store configuration data in registry, a central repository for configuration data that is stored in a hierarchical manner. System, users, applications and hardware in Windows use the registry to store their configuration and it is constantly accessed for reference during their operation[1]. Windows registry can be an excellent source for potential evidential data, since the vast amount of information, such as user accounts, typed URLs, network shared, and Run command history, is stored in it. Using some forensic tools, forensic examiners can investigate values of windows registry and get information can be forensic evidences. However, since windows registry contains huge amount of values and these values can be modified by users, suspect can hide his secret like password in registry values. Specially, remaining registry values not removed after uninstalling specific programs can be the best target to hide a suspect's secret without forensic examiners' notice, since generally they are not interested in registry values of removed programs, but which programs were removed. In this paper, we extract to categorize some registry entries related to forensic analysis based on Windows XP and list up consideration items for hiding secrets in registry as suspect's viewpoint in chapter 3. And then we show that countermeasures are needed, examining remainder of registry values for specific programs uninstalled in chapter 4, and give some concluding remarks in chapter 5.

2. FORENSIC-RELATED REGISTRY KEYS
In this chapter, we extract some registry keys required to be investigated forensically in Windows XP and show how they can be of benefit to help describing suspect activities on the computer.

2.1 Fundamental Registry Keys
These registry keys include general system information such as who used the system, what applications and hardware are installed, and what drives were mounted[2]. Forensic examiners should look over them at the initial investigation.

Table 1. Fundamental Registry Keys

HKCR\
- provides the name of the application handler associated with a file extension
HKCU\Control Panel\
- stores all of the control panel settings under subkeys
HKCU\Software\와 HKLM\Software\
- refer to software installed on the system. Software that has been deleted or uninstalled frequently leaves registry key

[1] This work was supported by the IT R&D program of MIC/IITA. [2007-S019-01, Development of Digital Forensic System for Information Transparency].

E-FORENSICS 2008, January 21-23, Adelaide, Australia

DOI 10.4108/e-forensics.2008.33

s with user settings or machine settings after removal
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall
- represent an installed program in the computer[3]. All programs listed in Control Panel>Add/Remove Programs correspond to one of the listed subkeys
HKLM\SYSTEM\MountedDevices
- contains a list of mounted devices, with associated persistent volume name and unique internal identifier for respective devices
HKLM\SYSTEM\CurrentControlSet\Services\
- contains list of Windows services. Each subkey represents a service and contains service's information such as startup configuration and executable image path[4]

2.2 Most Recently Used Registry Keys

MRU(Most Recently Used) registry keys are main factor for investigation. Using them, examiner can determine what files, folders, or applications were most recently used. Sometimes a suspect will delete a file after viewing it. Unless explicitly cleared, the file name may still appear in these registry keys. Additionally, installed applications may have their own most recently used keys. The most likely location for these is under the HKCU\Software\%application% hierarchy.

Table 2. MRU Registry Keys

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\OpenSaveMRU
- maintains a list of recently opened or saved files via typical Windows Explorer-style common dialog boxes[5]
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedMRU
- correlates to the OpenSaveMRU key to provide extra information, and then, registry value is created or updated in this key whenever a new entry is added to the OpenSaveMRU key
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
- maintains list of files recently executed or opened through Windows Explorer
HKCU\Software\Microsoft\Windows\Current Version\Explorer\RunMRU
- maintains a list of entries executed using the Start\Run commands
HKCU\Software\Microsoft\Internet Explorer\Typed URLs
- contains a listing of 25 recent URLs (or file path) that is typed in the Internet Explorer (IE) or Windows Explorer address bar
HKCU\Software\Microsoft\Search Assistant\ACMru
- contains recent search terms for finding folders, filenames, and words or phrases in a file using Windows default search

2.3 Startup related Registry Keys

Registry keys related startup are also key factors for investigation, since spyware, viruses, and other malicious code will frequently continue to infect a computer after a reboot, and the code needs to be run automatically to accomplish this. Some registry keys containing numerous locations from which code can automatically be run are detailed in here.

Table 3. Startup related Registry Keys

HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- shows the items that are automatically executed on every system logon
HKCU\Software\Microsoft\Windows\CurrentVersion\RunServices HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices
- lists services set to run automatically at startup either once or every time. These keys can be used to trigger executables before a user logs on
HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
- lists programs associated with Windows Explorer that are permitted to run automatically when the users logs in
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
- has a registry value named Shell with default data Explorer.exe. Suspect could append executable file path to this registry value to run program covertly

2.4 Folder Location Registry Keys

Main folders such as My Documents folder, Startup folders, Recent folders, and Internet folders(Cache, History, Favorites and Cookies) are the most likely location for files of interest in an investigation. By altering registry settings, an individual user can change these folders, so an investigation can be directed at target locations for initial analysis by confirming the locations of these folders[6].

Table 4. Folder Location Registry Keys

HKCU\Environment
- identifies the environment variables that provide the location of the Windows temp directories
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\
- enables users to change the locations of specific folders, such as My Documents, Recent, and Startup through the various subkeys
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders\
- contains the links relevant to folders used by All Users
HKLM\System\CurrentControlSet\Control\Hivelist
- identifies the locations of registry hive files on Windows XP

3. CONSIDERATIONS FOR HIDING DATA IN REGISTRY AS SUSPECTS' VIEWPOINT

Since registry's value supports binary data type, suspect can store segments of program or the entire binary in the registry. These segments of program can be placed in several dispersed keys. Unless forensic examiner knows the relevant keywords to search in the registry, finding hiding data in tens of thousands of registry keys can be a tedious task. Suspect may consider the followings to hide all sorts of data including password, text information and binary files in registry[7].

① **Suspect may hide his information in registry values which may not affect the system itself**. Since Windows does not utilize these registry values which are nested somewhere in some registry keys, and they are merely used for storing string information, suspect can hides information such as passwords or passphrases in these values effectively.

② **Suspect may hide his information in registry values which forensic examiners don't consider as important.** Since forensic analysis should be processed quickly, the categorized items described in previous chapter are the primary target to analyze. If suspect can hide his information in routine registry values, examiner may not be able to find them easily.

③ **Suspect may hide his information in registry values related to uninstalled programs.** Even though some programs or applications are deleted from the system, registry values for them are not removed yet. It is not easy for forensic examiners to find suspect's secret, if suspect may conceal them in registry values related uninstalled program. We examine these registry values in the next chapter.

④ **Suspect may hide his information in registry keys having REG_SZ value type.** If suspect encode text-based information into binary format in hexadecimal notation and store the binary form in registry values as string using type REG_SZ, examiner may not be able to find them easily.

⑤ **Suspect may hide his information using translation gap for value types.** When an application read value's data in REG_BINARY from the registry, the application decides on how to decode the value. For example, since application can interpret REG_BINARY data as 8-bit ASCII or 16-bit Unicode, it could result in two different values. Suspect can use this technique to hide data. Some applications store REG_SZ and REG_DWORD data in REG_BINARY value, decoding and finding them can be difficult. This technique also could be used to hide data or at least confuse forensic examiner.

4. EXAMINING REMAINDER OF REGISTRY VALUES FOR UNINSTALLED PROGRAMS

In this chapter, we examine remaining registry values, when we uninstall specific programs which were installed at Windows XP based PC. These registry values can be used to hide a suspect's secret without forensic examiners' notice, since generally they are not interested in registry values of removed programs, but which programs were removed.

4.1 Investigating Targets and Methods

We selected 7 programs as targets for investigating registry remainder. Winamp and GOM Player are freeware and the others are commercial tools. Since freewares usually have a menu for uninstalling, we use it for deleting them. On the other hand, some commercial tools do not have uninstalling menus, so we used Add/Remove programs of start→setting→control panel.

Table 5. Selected Target Programs

Program Name	Freeware/ Commercial	Using uninstalling menus	Using Add/Remove programs
Hangul2005	Commercial	-	O
ACDSee 6.0	"	-	O
Adobe Acrobat 5.0	"	-	O
MS office Professional Edition 2003	"	-	O
Source Insight 3.5	"	-	O
Winamp	Freeware	O	-
GOM Player	"	O	-

4.2 Results

Remaining registry keys after uninstalling a specific program are examined twice, before and after rebooting, but the result is the same. Registry remainders for each target programs are as follows.

- When Winamp is uninstalled, registry keys of HKCU\Software\Winamp are removed, but there are some remainders at HKLM\SOFTWARE\Nullsoft\Winamp. "Command" subkey value of HKLM\SOFTWARE\Microsoft\Shared Tools\MSConfig\startupreg\WinampAgent is still set to "C:\Program Files\Winamp\winapma.exe". Additionally, there are even 19 winamp-related registry values under HKCU\Software\Netscape\Netscape Navigator\viewers.
- If GOM Player, a playing tool for moving pictures, is uninstalled, almost keys of HKLM\SOFTWARE\GRETECH and HKCU\Software\GRETECH are deleted. However, some basic values of them still exist and one of the subkeys of HKCU\Software\nProtect\Process is still set to "C:\PROGRA~1\GRETECH\GOMPLA~1\GOM.exe"
- When the Korean word-processor hangul is uninstalled, a number of registry values are not deleted at Hwp, HwpCtrl, HwpUserAction, and Shared registry keys under HKCU\Software\HNC and some keys under HKLM\SOFTWARE\HNC\Shared\HncUpdate.
- There exist some registry key values at Device Detector and PlugIns under HKCU\Software\ACD Systems, even though ACD See is uninstalled. Additionally, more 100 registry values relating to ACD See are still left at InfoCache and V2 under HKLM\SOFTWARE\ACD Systems\PlugIns.
- If Adobe Acrobat is uninstalled, there exist some registry key values relating Adobe Acrobat at HKCU\Software\Adobe\Adobe Acrobat and HKCM \SOFTWARE\Adobe\CommonFiles.
- When Microsoft Office is deleted, there exist a number of keys at HKCU\Software\Microsoft\Office and HKLM\SOFTWARE\Microsoft\Office. Additionally, in case of Outlook Express, many key values are maintained under HKCU\Software\Microsoft\Outlook Express\5.0 and HKLM

\SOFTWARE\Microsoft\Outlook Express.

- When Source Insight, an analyzing tool for programming codes, is removed, many registry key values of HKCU \Software\Source Dynamics\Source Insight\3.0 and HKLM \SOFTWARE\Source Dynamics\Source Insight\3.0 are remained.

5. CONCLUDING REMARKS

We have extracted some registry entries related to forensic analysis and have listed up consideration items for hiding secrets in registry as suspect's viewpoint. And then we looked over remainder of registry values, primary target for hiding a suspect's secret, for uninstalled programs. This paper talks that the remaining registry values from uninstalled programs should be investigated by examiner. However, it is not easy for forensic examiners to check out a number of remaining registry values manually, so we are considering some ways to find these remainder values automatically.

6. REFERENCES

[1] J. Honeycutt, "Microsoft Windows XP Registry Guide," Microsoft Press, 2003.

[2] M. Russinovich, "Inside the Registry," Windows NT Magazine, 1997.

[3] K.J .Jones, R. Bejtlich, and C.W. Rose, "Real Digital Forensics," Addison-Wesley, 2006.

[4] H. Carvey, "Windows Forensics and Incident Recovery," Addison-Wesley, 2004.

[5] C.Steel, "Windows Forensics," Wiley Publising, Inc., 2006.

[6] L.W. Wong, "Forensic Analysis of the Windows Registry," Forensic Focus, 2006.

[7] Y.S.Kim, S.S.Lee, and D.W.Hong, "Windows Registry and Hiding Suspects' Data in Registry," the First Workshop for Anti-Forensics and Countermeasures, 2007.