A forensically tested tool for identification of notebook computers to aid recovery: LIARS phase I proof of concept

Peter Hannay, Andrew Woodward and Nic Cope
School of Computer and Information Science
Edith Cowan University
Perth, Western Australia
peter@peterhannay.com
a.woodward@ecu.edu.au
ncope@student.ecu.edu.au

Abstract

The LIARS tool was designed to enable identification, and potentially the return, to the rightful owner of stolen laptop or notebook computers. Many laptops are discovered by Police, but time constraints prevent recovered devices from being identified. This project has produced a proof of concept tool which can be used by virtually any police officer, or other investigator, which does not alter the hard drive in any fashion. The tool uses a modified version of the chntpw software, and is based on a forensically tested live Linux CD. The tool examines registry hives for known location of keys which may provide information about the owner of the laptop. This paper outlines the successful first phase of the project and looks at future directions.

Keywords

Forensic tools, software validation, linux, chntpw

INTRODUCTION

Loss of corporate data is an on-going and increasing problem. There are both reports of laptops being stolen in the media where they concern government agencies or large corporations losing important data, as well as statistical reports as to the loss of both IP and hardware.

It seems that every other week an online IT news website reports of data going missing due to the theft of a laptop or notebook computer. In July 2007, a laptop belonging to an employee of the web security firm Verisign went missing (Leyden 2007). The data was not encrypted and it contained employee records including names, addresses and social security numbers. In April of the same year two laptops containing employee data for the Chicago public school system were stolen (Cullen 2007). These are just the high profile cases where the company has made them public. It does not include those that may have been kept quiet, and the smaller cases with a lower public profile.

There are also the statistics which attest to the fact that laptop theft is an on-going problem. Costs of laptop theft have two components: the hardware and the claimed value of the data on the stolen device. The most recent Australian report on computer crime, produced by AUSCERT, the 2006 Australian computer crime and Security survey, indicated that of those organisations surveyed, 58% reported theft of a laptop (AUSCERT 2006). This was up from 53% the previous year, but the year before that was also 58% (AUSCERT 2006). They also reported that 69% of organisations suffered financial loss as a result of laptop theft. No information was provided in terms of what proportion of the loss was due to the device itself, or any information contained on it. However, a value of 2.267 million dollars was attributed to laptop theft alone (AUSCERT 2006). Considering that there were only 126 respondents, when extrapolated to the whole of the Australian financial sector, this represents a significant loss. These figures also represent just organisations: they do not take into account theft of laptops from individuals.

Whilst a number of stolen devices are found, if their legitimate owners are not able to be found, then effectively, the device at least in the eyes of insurance companies has not been recovered. This creates two issues for those who have had devices stolen. Both issues are two-fold. Firstly, if the device is not returned to the original owner then they have effectively lost all of the information on it. The other aspect to this issue is that if the original owner cannot be identified, then the hard drive will be erased, and the information contained on it is again lost. Secondly, there is the financial cost of having to replace the laptop once stolen, or in the event that it is insured, the insurance company incurs the cost of having to replace the device. In addition there is the hidden cost of increased premiums in the case of the insured.

A large number of laptops are found by police in the course of their duties, but unless the original owner can be found then the device is not considered to have been recovered. The sheer volume of devices and prevalence of more serious computer related crimes mean that the time required to properly identify the original owner of a laptop just does not exist. As a result, the official recovery rate of laptops remains low.

These facts and issues demonstrate the need for a basic tool which can be used by anyone with minimal training to allow for identification of the recovered laptops. This will allow for several important outcomes. The first, and most important for the legitimate owner, is the recovery of their laptop. Both the device itself and information contained in it will be important to them. To the police, identification of the original owners will allow for an increase in the so-called clear up rate, an aspect which is of importance to them. Thirdly, the insurance companies, who are ultimately responsible for paying for the replacement cost of the laptop, are also an interested party.

This paper outlines the tool that has been produced as a proof of concept for phase I of the LAIRS project. Namely, a tool which examines hard drives of laptop computers, which have not been formatted, and which are running Windows XP.

THE PROOF OF CONCEPT – LAIRS PHASE I

There are three main components to the LIARS system: the underlying Live CD, the tool itself, and testing. All three are equally as important, but the Live CD needs to be established firstly, as the tool requires it to run. Testing will be very important, because although the information may not be used in a legal proceeding, there is the chance that it will, and therefore it needs to meet established forensic standards.

Assumptions

There is one main assumption or decision that has been made for this project and it relates to the operating system. This project will work from the assumption that the majority of laptops are running Windows XP as their primary operating system. This is a reasonably safe assumption, as Windows XP was released in 2001, and although Windows Vista is due for release shortly, it is not yet available other than in beta form. This assumption will cause some issues later on, particularly with Windows Vista being made available shortly. However, as with Windows XP, it is likely that it will be some time before Windows Vista achieves widespread adoption. It is estimate by the Western Australian police force that it took windows XP approximately 2 years to achieve majority use (D. Taylor, personal communication 18th June 2007).

The Application - chntpw

The application to be developed for use will need to be able to extract information from the Windows registry, as user and owner data for Windows XP systems is stored in the registry hives.

One of the advantages of using a linux distribution is that it is covered by the GPL, meaning that source code of all components is available. It also means that the software is available without any financial commitment. Although there are programs such as Registry Viewer available, this is proprietary software, which requires both licensing fees and the use of a dongle for its operation (AccessData 2006). Also, it will only run in a Windows environment, making it unsuitable for this project.

This project will use the chntpw utility, a program designed to change administrator passwords on Windows computers (Hagen 2004). Although designed for locating passwords in the SAM (security account manager) registry hive and resetting them, this program also has registry viewing and editing functionality. It is this aspect of the chntpw utility which is desirable, as much information relating to legitimate owner and any organisational registration information can be found in the registry. This software is also open source under the GPL and LGPL licenses, which provides several advantages. The first advantage is that the code can be examined to make sure that there are no unexpected features or pieces of code which may affect the host system in an unwanted manner. The second is that as we have the source code, it can be altered or changed to suit our purposes, saving a lot of development time. The third is that in this case there is no financial cost, as long as the original author is acknowledged.

Location of Information on the hard drive / Hives examined

The LIARS tool interrogates the following registry hives:

- SAM (HKEY_LOCAL_MACHINE\SAM)
- Security (HKEY_LOCAL_MACHINE\Security)
- Software (HKEY_LOCAL_MACHINE\Software)

- System (HKEY_LOCAL_MACHINE\System)
- NTUSER.dat (HKEY_USERS\DEFAULT)

It should be noted that the tool is capable of interrogating other registry hives if required. The currently used hives are simply a matter of configuration.

When a Windows XP operating system is installed, the user is prompted to enter both their name, and that of the company, if applicable. This may or may not happen where the laptop is bought from a local supplier, but it is highly likely that this will be done where a corporate or standard operating environment (SOE) image is used. A search of an ECU laptop with an SOE image reveals many registry keys where the word "ECU" is found. In addition, there are numerous other applications which also store user information in the registry hives. Information is also stored about other applications, such as messenger clients and email programs (AccessData 2005). Table 1 contains a list of common user information and its location in the registry. Some of this information is stored in the NTUSER.DAT file. In addition to the information contained in the table, there are other locations and applications which store information about the user or registered organisation / owner of the laptop.

There are registry keys created by Office 2003, Office XP, Office 2000, Outlook Express and Outlook. In addition, virtually any software package that installs itself correctly will also create registry information which will contain the user's details. For example, the Adobe family of products contains this information. This is very useful, as virtually every computer has a copy of the freely available Adobe Reader in order to read PDF files (Adobe 2007).

Table 1: Information about the registered user, company, and other software variables and their respective location in the registry hive.

Identifier	Key	Value
Office XP Company name	HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\< GUID>	RegCompany
Windows XP User name	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	RegisteredOwner
Windows XP Company name	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion	RegisteredOrganization
Windows XP User name	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\<GUID>\Products\<ID>\InstallProperties	RegOwner
Windows XP Company name	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\<GUID>\Products\<ID>\InstallProperties	RegCompany

Technical Implementation

A number of components are utilised as part of the LIARS project, the first of these is the underlying Linux operating system that forms the base of the live environment, from which LIARS runs (Figure 1). This live environment has been provided by the Simple Image Preview Live Environment (SImPLE) project. This environment ensures that all data is accessed in manner in which the forensic integrity of the host system is not compromised. The LIARS tool itself exists on top of this live environment.

The LIARS tool is currently comprised of a database, a file system analysis script and a modified version of the chntpw utility. The database stores information relating to the registry hives of interest and the registry keys to be examined, this database is utilised by the file system analysis script and the modified chntpw utility.

The file system analysis script retrieves information relating to the registry hives, primarily expected file names and mime types. This information is then used to locate registry hives of interest; the location and hive types of the located hives are then stored in the database for later use.

The database is then read by the modified chntpw utility which cross-references the previously stored hive locations with a list of registry keys of interest. The modified chntpw utility then reads the value of each of these keys from the applicable registry hives and displays them to the user (Figure 2). At this stage the operation of the LIARS tool has completed and the system can be powered off at the user's discretion.

Preliminary investigation into LIARS vs Vista

The LIARS proof of concept tool has been tested on a Vista machine, and while it ran without problem, it did not return any registry values. This is likely due to the values currently being used by LIARS being specific to Windows XP. These values are likely to be differently named which would mean that they are not present at all on a Windows Vista PC. Available technical data on the Windows Vista registry indicates that the registry structure and location is the same for that of Windows XP (Microsoft 2007). Investigation of the Windows Vista registry for keys relating to the location of registered owner and registered company returned several values (Table1). This makes it likely that the LAIRS tool can easily be reconfigured to work on Windows Vista as well as Windows XP.

Table 2: Registry keys found in the Windows Vista registry relating to registered company and owner

Identifier	Key	Value
Windows Vista	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\5820D59FFDE05A2418084F7929EC5388\InstallProperties	RegCompany RegOwner
Windows Vista	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\7B6E62F3B230B4042903A325C7F63EB6\InstallProperties	RegCompany RegOwner
Windows Vista	HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\B1F8F46A682D28A4689BE77F64CCD443\InstallProperties	RegCompany RegOwner

LIMITATIONS

There are a number of limitations that effect the current implementation of the LIARS project, it should be noted that the majority of these will be addressed as part of the future development of the project. In its current state the LIARS software is unable to extract data from hard disks that have been formatted or where the contained data is otherwise deleted. As a current limitation of the libraries used by LIARS it is not yet possible to recover information from systems that are running and operating system other than Microsoft Windows XP. Finally there have been instances in which the underlying Linux live environment provided by the SImPLE project has failed to operate on some hardware.

FUTURE WORK

Whilst development of this proof of concept tool has been successful, there is still more work to be done. This includes, dealing with formatted hard drives, other operating systems (Windows Vista) and the inclusion of more registry keys. Lastly, and most importantly, is to recode the tool so as to not use any of the chntpw source code.

Examining formatted drives

The second phase will be to expand upon the basic module, and look at deleted data. In the event that a laptop has been formatted, no data will be available to an investigator at a topical level. At this point, it will be necessary to examine the drive using a forensic analysis tool in order to attempt to recover information. This functionality will be added to the basic application, but user intervention, and thus training, will be kept to a minimum. As with Phase I, this phase will also be built upon the forensically validated Live CD, with the application also undergoing thorough testing.

Windows Vista

At the time of writing, numerous organisations have published statistics as to the low rate of uptake of Microsoft's latest desktop operating system, Windows Vista (Whipp 2007; Larsen 2007; Orion 2007). Whilst there may be doubts as to the accuracy of these surveys, they all indicate a low rate of usage, meaning that the majority of laptops are likely to be running Windows XP. A report on a survey conducted by the Sunbelt company reported that for all users, Windows XP accounted for approximately 83% of operating systems present, with Vista accounting for only 9.3% for home users and a very low 0.03% in business machines (Orion 2007). However low the uptake of Vista may be, at some point it will become an issue if the LIARS tool is not able to extract data from its registry. As part of ongoing development the project will be expanded to include support for Windows Vista and other operating systems as is deemed appropriate by the developers. This will allow for LIARS to remain useful as adoption of this new operating system increases.

Increase the number of registry keys examined

In addition to the other changes listed, the database of included registry entries will be enhanced to include information that is made available by selected third party applications. In particular those programs that are used by almost everyone would be likely candidates. For example, there would not be many users that do not have Adobe Acrobat Reader installed on their computers. The portable document format (PDF) is in widespread use, and Acrobat Reader is an essential utility if you wish to view these files. A preliminary examination by the authors has found that this product has several registry entries which would be of use to the project. Others may include third party web browsers, such as Mozillas Firefox (Mozilla 2007).

Re-write the code

In the event that the tool is to gain a commercial profile, it is important that there be no intellectual property or other licensing issues in relation to the use of the chntpw code. Whilst this is an open source tool, it would still be preferable that there be no issues of ownership. This will entail some additional work, but the authors now have a greater understanding of how the registry is structured, and how to extract information from it.

CONCLUSION

The first phase of LIARS is now complete, with a proof of concept tool able to interrogate the registry hives of aim of the LIARS project is to develop a tool that can be used by a police officer, or other investigator, with little knowledge of computers. The tool will be produced and subsequently tested to determine its forensic validity with an appropriate framework. The Live CD which will be used as the base for the examination tool is currently undergoing testing. It is hoped that when the application has been successfully developed, that it will be used by the WA Police force in the field, and that its use will result in a significant increase in return of laptops to the official owners.

Future phases will add additional functionality to the LIARS system, with the ultimate aim to the ability to examine deleted sectors of the hard drive. Future research will look at examining Windows installations for other sources of identifying information, in addition to those being used now. Searching of email for user details is a potential avenue which will be explored. With the slow, but increasing, uptake of Windows Vista, it will also be necessary to examine the tools functionality in relation to its ability to locate the same information.

REFERENCES

AccessData (2005). Registry quick find chart, URL http://www.accessdata.com/media/en_us/print/papers/wp.Registry_Quick_Find_Chart.en_us.pdf accessed 18 September 2007

AccessData (2006). AccessData Registry Viewer, URL http://www.accessdata.com/products/rv/ accessed 18 September 2007

Adobe (2007). Adobe Reader, URL http://www.adobe.com/products/acrobat/readermain.html accessed 19 October 2007

AUSCERT (2006). 2006 Australian computer crime and Security survey, URL http://www.auscert.org.au/images/ACCSS2006.pdf accessed 10 October 2007

Cullen, D. (2007). Laptop thefts expose 40,000 Chicago teachers, URL http://www.theregister.co.uk/2007/04/09/chicago-teachers_security_breach/ accessed 16th October 2007

Hagen, P.N. (2004) The Offline NT Password & Registry Editor, URL http://home.eunet.no/pnordahl/ntpasswd/ accessed 19 October 2007

Helix (2006). The Helix Live CD page, URL http://www.e-fense.com/helix/ accessed 20 October 2007

Knoppix (2006). Knoppix, URL http://www.knoppix.org/ accessed 15 October 2007

Larsen, E. (2007). Vista uptake slow as companies shy away, URL http://www.itweek.co.uk/personal-computer-world/news/2185624/vista-uptake-slow-research accessed 20th October 2007

Leyden, J. (2007). VeriSign worker exits after laptop security breach, URL http://www.theregister.co.uk/2007/08/06/verisign_laptop_theft/ accessed 16th October 2007

Microsoft (2007). Windows registry information for advanced users, URL http://support.microsoft.com/kb/256986/ accessed 20th October 2007

Mozilla (2007). Firefox web browser, URL http://en.www.mozilla.com/en/firefox/ accessed 22nd October 2007

Orion, E. (2007). Vista uptake is barely more than Windows 98 share: Less than 1 per cent in businesses, URL http://www.theinquirer.net/gb/inquirer/news/2007/10/08/vista-uptake-barely-windows accessed October 20th 2007

Whipp, M. (2007). Vista uptake is slow - Net Applications, URL http://www.pcpro.co.uk/news/103914/vista-uptake-is-slow-net-applications.html accessed 20th October 2007

COPYRIGHT

Peter Hannay, Andrew Woodward and Nic Cope ©2007. The author/s assign SCISSEC & Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to SCISSEC & ECU to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.