Encountering Encrypted Evidence (potential)

Henry B. Wolfe
University of Otago, Dunedin, New Zealand

hwolfe@commerce.otago.ac.nz

Abstract

Investigative activities involving computer related cases occasionally encounter files that have been encrypted. Encryption is a valid and legal process that enables anyone to protect the privacy of his or her data and/or communications. If the suspect is cooperative and provides not only the key but also the specific encryption software, investigation is simple. However, without that cooperation, analysis of potential evidence may not be practical or possible. This paper discusses alternatives where the suspect is not cooperative and keys are not provided. The outcome of the investigation may as well depend on what resources are available to the investigator.

Keywords: cryptography, forensics, evidence, investigation

Introduction

Forensic evidence gathering in a computing environment has become a necessary tool and technique used by law enforcement, intelligence and law practitioners alike. For most users, the information stored on their computer encompasses only what they know about. That usually consists of the software that is installed and the data files created or copied by that user. All of the ancillary, historical and supportive data written to the user's hard disk as a result of various activities is either unknown or ignored by most users. For the investigator, however, this unknown data forms one of, if not the most, lucrative sources of informational evidence to be found on any computer.

The discovery or investigative process usually entails first seizing the machine then capturing a bit-wise image of all of the storage media used by the suspect. This image forms the basis of the case and any subsequent relevant evidence discovered must be able to be demonstrably tied directly back to the original copy. Thereafter, the investigator works exclusively with exact copies of those original evidentiary copies to extract whatever information that is pertinent to the case at hand. There are many tools available for that process. Some of them are primitive and provide but a single function. Others are more comprehensive and can provide all of the analysis tools required as well as provide the functions necessary to create the actual case documents presented in a court of law.

No matter which tools are used, there comes a time for every investigator when he/she encounters encrypted information which is a part of the original image. The suspect can or will be confronted and directed to provide the key phrase that enables decryption of the data that is in encrypted form. When this occurs the investigator will face either of two situations. The first is where the suspect cooperates and provides the appropriate key phrases that enable decryption. In this situation, analysis can continue without obstruction. The second situation is

where the suspect refuses, for whatever reason, to provide the necessary key.

This paper will discuss this second situation and attempt to describe and reveal potential methods for dealing with encrypted data - potential evidence. It will also discuss specific surveillance methods that could be used in cases where the suspect is known or expected to be unhelpful with respect to encrypted data. Examples are matters of national security, suspected drug dealers, child pornographers or terrorists.

Data Encryption

For the reader that may be uncertain about data encryption it may be instructive to discuss it briefly. Cryptography describes the art/science of protecting data by transforming useful understandable data (plain text) into a form that is not understandable (cipher text) - thus making it secure from unauthorized use. And, of course, transforming back to its original form. The process of encryption creates cipher text from plain text using a procedure (algorithm) that is controlled by a key phrase. A single plain text file repeatedly encrypted with successively different keys would produce a number of different and unique cipher text files each of which would need to be solved individually (if no key were provided for the respective file). The process of solving or transforming a cipher text file without its key is referred to as cryptanalysis.

Cryptanalysis

Cryptanalysis is a very complex field based on advanced mathematics. There are a number of attack strategies developed by cryptographers (those who practice the art/science of creating and/or attacking cryptographic algorithms) over the years. Linear cryptanalysis, differential cryptanalysis, differential fault analysis, plain text attack, and brute force attack are a few. Because this is not a paper about cryptanalysis, it will be left to the reader to pursue these attack strategies further - with one exception. That is the brute force attack.

A brute force attack will cycle through the entire key space until the exact key is found. If the key space is small enough for this to be accomplished in a reasonable time using one or more computers, then the algorithm would be deemed to be weak. Part of the strength of any cryptographic algorithm is based on the size of the key space and that is represented by the number two as raised to the power of some value. For example, the *DES* [1]has a key space of $\mathbf{2^{56}}$ or seventy-two quadrillion keys. To cycle through all of these keys to find the exact key required to decrypt any given cipher text - even with the fastest computer of the day will take many hours or days. As the key length grows so too does the amount of time required to solve using the brute force technique.

The other aspect of an algorithm that defines its strength is the algorithm itself. Some of the other attack strategies make their attack on the weaknesses inherent in a poorly designed algorithm. The cryptographic community constantly analyses various algorithms for their weaknesses. Those that emerge without being found to be weak may only be attacked successfully by brute force. For example *IDEA*[2] has a key space of $\mathbf{2^{128}}$ which equates to more than all of the atoms in the entire universe. Since, after many years of assessment and testing, its process is thought to be secure, a brute force attack would be computationally im-

---

[1] *DES* - The U.S. **D**ata **E**ncryption **S**tandard. This algorithm was adopted as a federal standard on 23 November 1976 and approved for private sector use in 1981. A key space of 72,057,594,037,927,900 keys.

[2] *IDEA* - **I**nternational **D**ata **E**ncryption **A**lgorithm. This algorithm has been analyzed and attacked (unsuccessfully) since its creation by Xuejia Lai and James Massey in 1990. A key space of *340,282,366,920,938,000,000,000,000,000,000,000,000,000 keys*.

practical, Data properly encrypted using the IDEA algorithm and a properly formed key[3] would be impossible to solve in a time that would make the information of any use. For example, if we had a CPU that could test 1 billion keys per second and if we were able to create a parallel machine comprised of 1 billion of these CPU's it would take ***10,790,283,070,806*** years to cycle through the entire key space that IDEA uses[4].

The reason for this discussion is to apprise the reader of the issues surrounding encrypted data that might be found in an investigation. Once it has been determined that encryption has been used and that the suspect will not cooperate the first approach is to want to "break the code". Unfortunately, "breaking the code" does not work as seen on TV and in films. A fourteen year old computer geek is not likely to be successful (most especially when leading crypt-analysts have spent years trying to find a way and not succeeded) and certainly not in a few minutes. Therefore, this expectation of being able to "break the code" is not realistic.

Determining That Cryptography Has Been Used

This is harder than it might at first seem. There are forensic tools like *IsEncrypted*[5] and others that do just that. However, *IsEncrypted* is designed to find files that have been encrypted by specific applications software and can only identify that software that it knows about. *IsEncrypted* is a very useful forensic tool but it would not find any files that were encrypted by any other software application. Many standard applications such as Word or Excel, (and there are many others as well) make encryption with strong algorithms optionally possible. While the algorithm implemented may be computationally secure and theoretically unbreakable, the way it has been implemented within other software may be flawed and successful attack may be achieved as a result. AccessData Corporation also makes available individual modules specifically designed to resolve the password used from files encrypted by one of these designated applications. In other words, if you use the encryption option that Word offers to protect your documents, then by obtaining the Word module from AccessData and applying it to the encrypted file the password you used will be resolved and the file thereafter will be able to be decrypted by the investigator.

Another method of finding out whether encryption has been used is to look for known encryption software that is installed on the target system. Some forensic tools will do this based on a known signature pattern - a technique much like searching for a known virus. Encryption that is unknown to the methods described thus far may be more difficult to detect. Moreover, some encrypted files may be hidden within other files where steganography[6] has been used. As you can see, determining whether cryptography has been used is not a simple matter.

---

[3] *Properly formed key* - This refers to the fact that each character of the key (in the *IDEA* example 16 characters) has up to 256 possible values. If the user makes use of only a subset of those possible characters (just lower case alpha characters for example), then the strength (security) of the outcome will be reduced accordingly.

[4] *Teraflop machines* - currently there are several initiatives under way to produce a 100 terafloop (1 trillion floating point instruction per second) computer: for example the ASCI (**A**dvanced **S**uper **C**omputer **I**nitiative) project. However, the ability to array a billion of these to solve a single problem is not practical within the foreseeable future.

[5] *IsEncrypted* - An AccessData Corporation product designed to find files that have been encrypted with specific products - like Word, Excel, Pkzip, etc. - www.accessdata.com.

[6] *Steganography* - the technique of hiding data within other data. For example, using a product such as *Invisible Secrets* (NeoByte Solutions product) a user could hide an encrypted message within various graphic image files without appreciably affecting the visible quality of the image.

Social Engineering

Once the determination has been made that encryption has been used and that the suspect will not cooperate by providing their keys, there are a number of other techniques that may be used (with varying effectiveness) to obtain particular keys. The first may be referred to as social engineering. This technique makes use of whatever information is available about the suspect. Most people do not construct their keys in a way that make them difficult to guess. Their main concern is being able to remember the key themselves. Therefore, the probability is that the key will be something that they have an interest in. For example, in a particular case, the suspect was a police officer. He had a pretty good knowledge of computing and used strong encryption and it was well implemented. The chances of "breaking to code" were nil. We compiled a dossier containing personal information about this individual (his children's names, his wife and girlfriend's names, his badge number, etc.). The next step was to search the evidentiary hard drive copy for incarnations of some of these names and phrases. As it turned out, the very first search (on his badge number) turned up six candidate keys -- the third one tried was it. While this was a real life successful example the investigator could have spent many hours trying the various bits and come up with a dead end.

Physical Circumvention

There are two places where physical intervention can be used. The first is where the suspect is under investigation (such as the much publicized Nicodemo Scarfo[7] case) and is not likely to cooperate with the investigators by providing their keys. This intervention takes place **prior** to the actual seizure of hardware. The rationale is that the key may be captured in real time and always without the knowledge of the suspect.

The second place is after the seizure has occurred. An example is where a suspected child pornographer was believed to have illegal images on his computer but would not provide the key to decrypt his system. A warrant was obtained to perform the surveillance and a key logger was installed on his machine. Within three hours of returning his machine, the authorities had the needed keys and were then able to unlock the evidentiary copy of the encrypted hard disk revealing enough pornographic material to result in nineteen counts on the incitement.

The tools used to accomplish the acquisition of subject keys for both scenarios described above are varied. There are physical devices and there are software devices. Physical devices break down into a few types: the first is a radio transmitter, next is the interception of electromagnetic emanations, and finally there are devices with internal memory that record keystrokes. All three must be physically installed on the target computer.

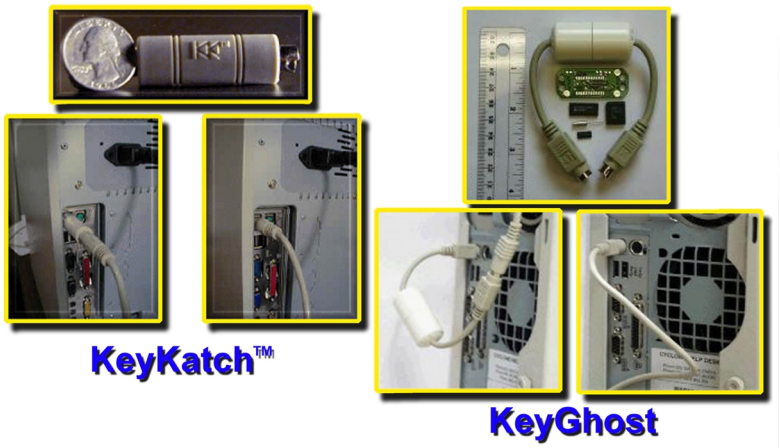
The radio transmitter would be installed somewhere between the keyboard and the CPU depending on its design. It would pick up keystrokes and transmit them over a designated radio frequency (or frequencies if spread spectrum or frequency hopping is used by the specific transmitter). These transmissions would be picked up and recorded at a surveillance receiver elsewhere. The investigator then analyses those keystrokes and finds the various keys that are being used by the suspect. These will be used for later decryption and analysis of the suspect's seized computer.

---

[7] *Nicodemo Scarfo* - Under investigation by the FBI for several months prior to being indited in December 2000. Scarfo used strong encryption to hide his alleged illegal activities. The FBI assumed that he would not cooperate and installed a key logger on his computer that captured his keys and made them available at their (the FBI's) discretion.

All electronic devices radiate electromagnetic emanations. These signals can be received with the appropriate equipment at a distance and translated back into their original form. Keystroke and the image on the screen can both be recreated and recorded in real time. In the case of keystrokes, these are recorded and analyzed as above for later use.

The third type of device is a small plug like device that is inserted between the keyboard and the CPU. Two examples of this type of device are KeyKatch[8] and KeyGhost[9] as pictured. These devices essentially work the same way. You simply install them and retrieve them after the surveillance is completed or periodically as required. They are then installed on a forensic computer, given a password and the contents of the device's memory are then downloaded to a text file for later processing. These have a distinct advantage over software key loggers in some circumstances. These devices will record ALL keystrokes on a given machine. Software key loggers can only begin recording AFTER the logging software becomes operational. In the event that the target machine uses CMOS based encryption, the keys are not available to such software until after the entire boot-up process is completed and therefore after the keys have actually been entered.



These are a sample of the kinds of hardware approaches that might be taken in an investigation. In the past they have provided good results and if used with the appropriate authorities (warrants) evidence gathered in this way can make or break a case.

Software Circumvention

There are a number of software surveillance tools available that can capture keystroke data albeit with the proviso stated above and are used to capture and record useful evidence before seizure is effected. These are stealth[10] type applications designed to operate without the user's knowledge. Some of them have the capability to report over the back channel of the user's Internet connection. Most of these tools have the capability of recording many things including keystrokes. Normally, the recorded data is encrypted and compressed before being stored so that it will not be recognizable to the user should it be seen accidentally.

Some examples are STARR[11], D.I.R.T[12], ABCKeylogger, Ghost Keylogger and the FBI's recently announced Magic Lantern. All of them must be installed on the target machine, however, that installation is

---

[8] *KeyKatch* - This device is produced by Codex Data Systems and further information may be obtained directly from the vender at: www.codexdatasystems.com/keykatch.html.

[9] *KeyGhost* - This device is produced by KeyGhost Ltd. and further information may be obtained directly from the vender at: www.keyghost.com.

[10] *Stealth* - In this context software applications installed on an operational computer that without special knowledge or other tools whose presence will not be apparent to the user.

[11] *STARR* - This is a PC & Internet Monitor produced by Iopus Software and further information may be obtained directly from the vender at: www.iopus.com.starr.htm.

accomplished in a number of different ways. Some are installed through a Trojan, others are installed by having physical access to the target machine, and still others are installed through the computer virus vector (as admitted in the Magic Lantern's description by the FBI). No matter what the vector, this class of surveillance tool has produced good results.

Conclusions

Encountering encrypted files can be dealt with in many instances, however, the notion that "breaking the code" is the way to solve the problem may not be the answer that produces results. This paper has attempted to introduce the reader to the potential methods that can be used to circumvent encryption and to pave the way to producing good evidence from what might have previously been considered too hard.

One last comment: on encountering data that is encrypted, it might be natural to assume that the suspect is guilty merely because he/she has chosen to use this powerful privacy tool. That would be a wrong assumption. In 1948 more than 100 nations adopted the Universal Declaration of Human Rights[13] which enshrines in Article 12 the most basic of human rights - the right to privacy. Everyone, good and bad, has the right to opt to maintain their privacy and should, in no way be penalized for choosing to exert that right.

References

Anderson, Douglas T, Tribble, Mike, *The Hard Disk Technical Guide*, Eleventh Edition, Boulder, Colorado, Micro House, 1995, **ISBN: 1-880252-28-7**.

Bodo, Marlin, *Hard Drive Bible*, Eighth Edition, Sunnyvale, California, Corporate Systems Center, 1996, **ISBN: 0-9641503-1-X**.

Casey, Eoghen, *Digital Evidence and Computer Crime*, Academic Press, London, 2000, **ISBN: 0-12-162885-X**.

Guidance Software, Inc., *EnCase Legal Journal*, Second Edition, South Pasadena, California, October 2001.

Mandia, Kevin, Prosise, Chris, *Incident Response: Investigating Computer Crime*, New York, 2001, **ISBN: 0-07-213182-9**.

Rosenblatt, Kenneth S., *High-Technology Crime Investigating Cases Involving Computers*, San Jose, KSK Publications, 1995, **ISBN: 0-9648171-0-1**.

Schneier, Bruce, *Applied Cryptography*; 2nd Edition, New York, John Wiley & Sons, Inc., 1996, **ISBN: 0-471-12845-7**.

Stephenson, Peter, *Investigating Computer-Related Crime*, Boca Raton, Florida, CRC Press, 1999, **ISBN: 0-8493-2218-9**.

US Department of Justice, *Electronic Crime Scene Investigation: A Guide for First Responders*, Washington D.C., July 2001, **NCJ-187736**.

Zaenglein, Norbert, *Disk Detective*, Paladin Press, Boulder , Coloradso, 1998, **ISBN: 0-87364-992-3**.

---

[12] *D.I.R.T.* - This is a Law enforcement only product produced by Codex Data Systems and further information may be obtained directly from the vender at: www.codexdatasystems.com/menu.html.

[13] Universal Declaration of Human Rights - Article 12 - No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks. - Adopted and proclaimed by General Assembly Resolution 217 A (III) of 10 December 1948.

Additional Sources of Useful Information:

Periodicals

Computers & Security, Oxford, England, Elsevier Advanced Technology, 8 issues per year, **ISSN: 0167-4048**.

EnCase Legal Journal, South Pasadena, California, Guidance Software, Inc., monthly.

Information Systems Auditor, International Newsleters, United Kingdom, monthly, **ISSN: 1466-4569**.

International Journal of Forensic Computing, West Sussex, United Kingdom, monthly, **ISSN: 1363-6650**.

Vogon Electronic Bulletin, Oxfordshire, United Kingdon, monthly, **www.vogon-international.com**.

Internet Sites of Interest

http://www.ojp.usdoj.gov/nij/pubs-sum/187736.htm
Electronic Crime Scene Investigation: A Guide for First Responders and other related reports.

http://www.encase.com/html/cf_resources.htm
Guidance Software, Inc. - forensic firm ---- Producers of *EnCase* -- *forensic software*

http://www.vogon-international.com/index.htm
Vogon International Limited - forensic firm

http://www.computer-forensics.com/
Computer Forensics UK Ltd - forensic firm

http://www.forensics-intl.com/
New Technologies Armor, Inc. - forensic firm

http://www.neobytesolutions.com/invsecr/
NeoByte Solutions - producers of *Invisible Secrets 3* - a steganography product

http://members.tripod.com/steganography/stego/software.html
General source of steganography software

http://www.elcomsoft.com/prs.html
ElcomSoft Co.Ltd - producers of password crackers

http://www.accessdata.com/
AccessData Corp. - producers of password crackers

http://www.lostpassword.com/
Passware, Inc. - producers of password crackers

http://www.iopus.com/starr.htm
iOpus Software Gmbh - producers of *STARR* --- *surveillance software*

http://www.codexdatasystems.com/menu.html
CodexDataSystems, Inc - producers of *D.I.R.T.* --- *surveillance software*

NOTE: The Internet is a fluid living thing. What is valid today may not be valid tomorrow. One or more of these addresses may no longer be active but give them a try.

Biography

Henry B. Wolfe is a faculty member of the University of Otago's School of Business, where he teaches computer security and networking courses. Dr. Wolfe has been a computer professional for more than forty years and has authored numerous papers on the subjects surrounding computer security (forensics, cryptography, viruses, E-Commerce, surveillance etc.).