

Forced encryption solutions

H. B. Wolfe

University of Otago, P.O. Box 56, Dunedin, New Zealand

Abstract

This paper is intended to introduce the reader to various techniques and tools that can be used to force a solution of encrypted data without the use of cryptanalysis. The relevance of these techniques becomes apparent when attempting to view potential evidence files that have been encrypted and the suspect refuses to cooperate by providing their keys.

Keywords: electronic evidence, surveillance, forensics, chain of evidence, evidentiary copy, evidence acquisition, encryption.

1 Introduction

Investigation and capture of electronic evidence inevitably includes encrypted data. In the first instance, the Court can and usually will direct the accused to provide their keys. If this directive is successful then no further action is necessary and the techniques outlined in this paper will not come into play. However, when keys are not forthcoming the investigator is faced with the difficult problem of trying to find them. The first thought after watching some teenager on TV break encryption codes in a few minutes at his PC is to break the code. TV and movies are fictional and the common portrayal of such activity is also a fiction. If strong encryption is used, breaking it is not an option. The investigator is left with a few options, however, and they will be outlined in this paper.

2 Data encryption

Encryption is the art/science of codes and ciphers. Its main usage is to protect data in transit and at rest. Data in transit refers to communications and data at rest refers to data being stored. In today's world it is an advanced branch of mathematics. People spend their whole life on the pursuit of this complex topic.



Information is protected 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 files). The process of solving or transforming a cipher text file without its key is referred to as cryptanalysis.

3 Cryptanalysis

Cryptanalysis is a very complex field based on the advanced mathematics mentioned above. 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 256 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 2128 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 impractical. 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 Detecting cryptographic use

This is harder than it might at first seem. There are forensic tools like IsEncrypted [4] and others that do just that. However, IsEncrypted is designed, as a companion utility to the Password Recovery ToolKit (PRTK), 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 software applications that it was not designed to detect. 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's Password Recovery ToolKit is specifically designed to resolve the password used from files encrypted by one of fifty or so designated applications. In other words, if your suspect uses the encryption option that Word offers to protect his documents, then the PRTK will be able to derive the keys for all documents protected in that way – even if the suspect refuses to provide their keys.

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 [5] has been used. As you can see, determining whether cryptography has been used is not a simple matter.

5 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.

6 Physical techniques

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 [6] 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. A video camera and transmitter might be used to record the keystrokes. While not actually being connected to the computer, it would still have to be placed where it could record such activity – not a particularly easy task.

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. Keystrokes 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 or soldered inside the target's keyboard (this takes about 15 minutes). Two examples of this type of device are KeyGhost and KeyKatch. KeyGhost has both external and internal models. 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 WordPad 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.

7 Software techniques

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 affected. These are stealth 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*, *D.I.R.T.*, *ABCKeyplogger*, *Ghost Keylogger* and the FBI's recently announced *Magic Lantern*. All of them must be installed on the target machine, however, that installation is 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.

AccessData's *Forensic ToolKit* has an interesting capability. One option is to create a target profile of the suspect and then use it to perform a dictionary search. As mentioned earlier, knowing the background of your suspect can be fruitful when attempting to gain access to encrypted data. Additionally, this tool has a wide range of other dictionaries that can also be used to attempt to find keys of an uncooperative suspect.

8 Reverse engineering techniques

Reverse engineering also holds some potential. While there may be laws in some jurisdictions that make this avenue illegal, it can produce results if you're not in one of them or if you can get the target encryption software reverse engineered in a jurisdiction where it is not illegal. If an encryption application can be broken,



then files that have been encrypted using it may no longer be secure. This is different than “cracking” the encryption code. This technique takes the software apart to see how it works. There are lots of software producers out there but there are not a lot of cryptanalysts out there. For practical purposes, many encryption product creators are not cryptographers and are making use of public or licensed algorithms by incorporating the cryptographic code within their product. Occasionally, this is done in a way that weakens the potential security that might have otherwise been provided. Within law enforcement circles, this information is circulated and used where appropriate.

Some manufacturers of cryptographic applications also build into their products back-door access in case a client has a problem using the vendor’s product. These vendors have been helpful when asked by the appropriately identified parties and may also be a source of a solution to a cryptographic problem.

9 Conclusions

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* [7] 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

- [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 keys.
- [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] *IsEncrypted* - An AccessData Corporation product designed to find files that have been encrypted with specific products - like Word, Excel, Pkzip, etc. - www.accessdata.com.
- [5] *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.
- [6] *Nicodemo Scarfo* - Under investigation by the FBI for several months prior to being indicted 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.
- [7] *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.
- [8] Casey, Eoghen, *Digital Evidence and Computer Crime*, Academic Press, London, 2000, ISBN: 0-12-162885-X.
- [9] Guidance Software, Inc., *EnCase Legal Journal*, Second Edition, South Pasadena, California, October 2001.
- [10] Mandia, Kevin, Proise, Chris, *Incident Response: Investigating Computer Crime*, New York, 2001, ISBN: 0-07-213182-9.
- [11] Schneier, Bruce, *Applied Cryptography*; 2nd Edition, New York, John Wiley & Sons, Inc., 1996, ISBN: 0-471-12845-7.
- [12] Stephenson, Peter, *Investigating Computer-Related Crime*, Boca Raton, Florida, CRC Press, 1999, ISBN: 0-8493-2218-9.
- [13] US Department of Justice, *Electronic Crime Scene Investigation: A Guide for First Responders*, Washington D.C., July 2001, NCJ-187736.

