Encryption: Protection of Sensitive Information

Fredrik Eriksson
fen05001@student.mdh.se

Johan Fogel
jfl04001@student.mdh.se

ABSTRACT

When having sensitive information on portable computers it's important to make sure that the data is secure, in case the computer is lost or stolen. An easy way to do this is to make sure that the sensitive data is encrypted. There are many tools available that can do this, and most of them are also free of charge. Encryption can be done either on just the folders and/or files that needs to be protected, or on the entire hard disk. Encryption of the entire hard disk, so called full disk encryption, can be done either in software or in hardware. Full disk encryption makes it easier for the user since he or she doesn't need to think about what files are sensitive enough to be encrypted. Although no security holes in the commonly used AES encryption standard has been found, it is still important to remember to not use common or easy to guess passwords. Our purpose with this article is to prove that using encryption is not difficult, and it is an effective way to keep sensitive data safe from prying eyes.

1. INTRODUCTION

The amount of information we keep on our computers increase every day, and with that also the amount of sensitive information for example medical records and personal data increase. This means we need to be careful about how we handle this information. There are examples of companies that have lost hard drives containing medical records of half a million people[1]. When this happens and the hard disks aren't encrypted, it would be a gigantic problem if this disc was found by the wrong person. The clothing company CAP lost a laptop containing the CV:s for 800 000 people applying for job in the company[2].

In this article we will discuss the use of different kinds of encryption for the purpose of protecting sensitive information. The paper is not meant as a tutorial of how to use the tools, and neither a technical document about how the tools work. We will only give an overview over a few of the available tools, some of their advantages and disadvantages as well as short explanations about terms that are commonly used (or that everyone should know of) when using encryption.

First we will discuss the purpose of hard disk encryption in section 2, then we will continue with some terminology in 3. After that follows the introduction of tools to encrypt files and folders in section 4, as well as tools for full hard disk encryption in software (section 5.1) and hardware (section 5.2). At the end we will discuss some of the well known attacks that exists for hard disk encryption in section 6, and at the end we have a conclusion.

2. WHY USE ENCRYPTION?

There are some laws about sensitive material. State of California claims that any company or individual that makes business in the state must notify the victims of a data theft where the data was unencrypted. In some cases the penalty of not being able to notify the victim can be as much as 10 000 $ per day[19].

Considering that there are thousands of laptops stolen every year and the enormous amount of costs and publicity that automatically comes with this. There are stories about companies that have lost laptops containing sensitive information about a million people [2]. There are enormous costs involved in this; the Croucher Brewing Company in New Zeeland offered about 300 000 SEK in reward for a laptop containing all their customer records and beer recipes [3]. How much this information is actually worth is difficult to say but the 300 000 is probably a low number. If we look at the Cap scandal [2] and the Californian law the amount of penalty that was on stake is eight billion a day for not notifying the theft. Considering the amount of technologies that can be implemented in the company to protect the information on the laptop, it's quite astonishing that the amount of companies that actually has implemented is as low as it is today. Some are even built into the operating system so why don't implement the function in the company? Some are built into the hardware, so if you buy the right hardware the problem of loosing data is almost automatically solved. The Ponemon Institute reports that only 45% of the passengers on airlines in USA used a login password to protect their computer and only 19% reported that the information on their laptops was encrypted[10]. So obviously there is a need to protect the information on business laptops.

2.1 What Happens To Stolen Information?

So why would anyone steal a computer? The computer itself is not that valuable, if the stolen computer is new and high performance, the hardware will be sold at the black market for at most a few hundred dollars. Yves Godbout has written an article in CA Magazine about what happens to stolen computers[7]. The big values is, according to Godbout, not the hardware itself, but can be found on the hard disk, and is information like

- Personal information (social security number, bank accounts, passwords)
- Information about friends (addresses, email addresses, birth dates)
- Client information (names, titles, employees)
- Classified information about the company (contracts, quotations, tax information, drawings, test documents)

This information is in many cases worth more than the hardware, the table below is an example of what information can be worth on the black market.

Information	Price
Address	$0.5
Past addresses	$9.95
Date of birth	$2.50
Unpublished telephone number	$17.50
Cellphone number	$10.00
US social security number	$8.00
Driver license info	$3.00

Figure 1: Data prices on the black market

10$ for a phone number might not sound like much, but imagine a computer with a database with about tens of thousands customers, including their addresses, phone numbers, social security numbers etc. Needless to say, an old laptop with such information is far more valuable to the thief than the hardware of any high-end laptop.

The table only shows what the thieves will get for the information. The amount of money that are lost for recovering the lost data is probably far more than that. The bad publicity the company get because of the incident can possible be even more costly than the loss of the data itself.

3. ENCRYPTION TERMINOLOGY

In this section we will explain some commonly used terms that you will probably encounter when looking into encryption. We will not discuss any of the terms in depth, but only give short explanations.

3.1 AES

Advanced encryption standard (AES) is a block cipher developed by two Belgian cryptographers and standardized by National Institute of Standards and Technology (NIST) in 2001. It is one of the most commonly used encryption algorithm for encryption of files and hard disks. Many people have tried to find security holes or a way to break the algorithm but as far as we know, no one has yet succeeded.

3.2 Salting

A password based encryption system has one big disadvantage: people tend to use passwords that are based on common words (“password”, “god”) or easy combinations (“qwerty”, “asdf”). Passwords are commonly stored somewhere, either in plain text, hashed or hashed with added salt. Plain text passwords are very insecure. If someone unauthorized manage to get hold of the stored password he can instantly use it to break into the system. Hashed passwords are better, however since the hashes used are commonly known (MD5, SHA1, etc.) everyone knows how to calculate the hashes. Therefore there exists utilities that can match the encrypted passwords with the hashes of common passwords. To make this more difficult one can add a “salt” to the password so that the hash doesn’t match, even if the password is the same[12]. The salt can be an extra text phrase, or a random value that is included in the calculation of the hash. This means that even if someone managed to get hold of the stored hash, the password itself is safe (as long as the thief can’t guess it).

3.3 Two-Factor Authentication

Two-factor authentication is used to add additional security by forcing the user to authenticate in more than one way[11]. There are a bunch of ways to combine this: password, smart cards, biometric methods, mobile phone, USB-memory sticks, one time password tokens, pin-codes and so on. If you want to use physical things the users laptop should be able to read the data by itself[15]. Not many users wants to carry around the laptop and a for example usb-reader for finger prints, smart cards and so on. Smart card readers are growing in popularity and at least Hewlett Packet has them as standard in many of their laptops that are targeted for the business market [9][15]. According to Ed MacBeth senior marketing vice president at ActiveIdentity says that the biggest problem has been that many companies don’t want to have one card for accessing the building and one to access the computers[15]. Since more and more companies uses smart cards to access the building this problem will disappear in the near future. Normally the smart card is combined with a pin-code. One of the negative parts of using smart cards is the amount of cost of administration and the risks of users loosing the cards.

3.4 Pre-Boot Authentication

Since BIOS by default can’t decrypt an encrypted hard disk there’s a need of a trusted layer between the encrypted partitions and the boot loader when using full disk encryption[21]. There are at least three ways to solve this. One is to have specialized BIOS that asks for the password. Another way is to have a special boot loader in the MBR-table (master boot record). Although the MBR is used by many operating systems for their own usage so tampering with the MBR might be problematic. The third and most common is that the pre-boot system is stored on a separate partition of the boot volume.

3.5 Plausible Deniable Encryption

Plausible deniable encryption is used to deny the fact that you have encrypted data.[4] Truecrypt provides a way to do this when using full disk encryption. Truecrypt does this by having two partitions on the disk with two different decryption keys. On these two partitions you have two different

installations of your operating system, where the first one is basically a decoy system. If you want to hide your encrypted data you enter the decryption key for the first partition where no sensitive data can be found. When you want to access the sensitive data, you boot the operating system on the second partition by enter the second decryption key. Inside the second partition a volume container is created that is invisible for the user unless it's known to exist. Since truecrypt fills the volume with random data it is difficult to determine if the random data is a hidden encrypted container or something entirely different[4]. However there are a few ways to figure this out anyway. One way is to scan the Windows registry files, where information about mount points are stored. This information is very limited but can reveal that the container does exist. Other features of windows that can be used to find information is .lnk files (shortcuts) or the "recent documents folder". This folder contains .lnk files to recently used documents. The .lnk files, among other things, contains filename and volume serial number. If the number is identical to the hard disk containing the operative system and the partition can't be reach this surely proves that there is a hidden volume. Another problem is the Google desktop, and similar programs, that creates an index of all the files that exist on a disk, including the files that exist on the hidden volume. This indexation is not unique for Google desktop as many more search tools uses this method to speed up searches.

3.5.1 Trusted Platform Module (TPM)

The Trusted Platform Module is an embedded security chip that is developed by the Trusted Computing Group (TCG) which was formed by some of the largest computer companies in the world. AMD, Intel, Microsoft and SUN is just a few that had contributed to TPM[15]. The TPM-chip can be used to securely store cryptographic keys and or certificates. The idea is to move some security features from the operating system to the hardware. The encryption is bound to the hardware which limits the possibilities to find the decryption key somewhere. Although there are still attacks that can extract the decryption key inside the RAM-memory (see 6.4). Since the encryption is bound to the hardware it's not possible to remove the disk from the computer nd insert it into another computer and extract the data there.

4. ENCRYPTED FILES AND FOLDERS

It is possible to encrypt just the files and folders where the sensitive data is located. Most modern operating system has a feature to do this, for example the FileVault and encrypted images in Apple Mac OS X[5], and EFS in Microsoft Windows[6]. There are also some external programs that can do this, but the main features of this kind of encryption is that it can be done "out of the box" without installing any extra software.

4.1 Benefits

The main advantage of the Apple Mac OS X encryption and Microsoft EFS is that they are not only free of charge, but they are also bundled in the operating system, which makes them automatically available and easy to setup and use[5][6][23].

4.2 Drawbacks

Since these encryption methods are commonly available and used, they are also attractive subjects for hacking. At least once a simple vulnerability has been found in the Mac OS X implementation that has made the entire system insecure [5][13]. Vulnerabilities as severe as that particular bug are not common, but the fact remains that if people know what kind of encryption you're using, and they know where the encrypted information is stored, any vulnerability found will make the system very insecure until it is fixed.

5. FULL DISK ENCRYPTION

Full disk encryption means, just like the name implies, that the whole disk is encrypted, even the operating system and the system files. Because of this, the user will have to enter a password to be able to boot the system. It is also possible to get additional security by using a decoy operating system on an unencrypted, or light encrypted part of the disk[23]. The advantages of having this decoy system is that it makes it more difficult for the thief to find the important information. This kind of encryption can be done either in software or hardware.

5.1 Software Full Disk Encryption

Full disk encryption in software is done by installing an encryption engine between the operating system and the hard disk. There are two leading developers of full disk encryption software, PGP and TrueCrypt[16][20]. Both of these systems are said by the developers to be completely automatic and transparent. The only difference the user will experience from a normal unencrypted installation, is the pre-boot authentication screen when they start their system. PGP claims that the encryption engine causes no noticeably change in the performance; however the system can be somewhat slower during the initial encryption of the hard disk. Since this is an onetime event, it shouldn't affect the user during normal usage. Unfortunately we where not able to find any benchmarks for the impact the use of these methods has on system performance.

5.1.1 Benefits

A great advantage of using full disk encryption is that it is easy to use once it is installed. Once the system is installed the user do not need to worry about where to store the data. Other benefits is that since the whole disk is encrypted you can be sure that there are no temporary files and/or swap spaces containing decrypted versions of the sensitive files.

5.1.2 Drawbacks

One drawback of this method is that there is more administrative work to set up the computer, since you have to install software for pre-boot authentication and encrypt the whole disk rather than just a part of it. Other problems is that it is more difficult to restore data in the event of a system crash as well as if the encryption key is lost. The problem with lost keys can be solved by creating rescue discs, but that requires even more administration[22].

5.2 Hardware Full Disk Encryption

In 2007 Seagate released the FDE.2 2.5inch disk specialized for companies that need to protect their laptops[17][7][14]. It offers AES encryption built into the disk. To be able

to boot the disk it uses a pre-boot authentication script. Since it uses the TPM-module the disk is bound to a specific motherboard or laptop it's impossible to remove the hard disk and insert it to another computer. There is also possible to have an external emergency password recovery file that can be stored on the headquarter servers or an USB memory.

5.2.1 *Benefits*

Since the encryption engine is built into the disk it's impossible to have non-encrypted data on the disk by mistake, which is a great advantage to other solutions like FileVault or other software based systems. Another advantage is that it is easy, since you do not need any external software for the encryption. According to the manufacturer the encryption system should not limit the performance of the disk, since the encryption engine is build into a specialized ASIC chip[17].

5.2.2 *Drawbacks*

There are not that many drawbacks of using hardware based encryption solutions. One drawback is of course the limitation of using specific hardware, that probably costs more, and limits you to specific manufacturers. Another is of course, just like for the software full disk encryption, that it is much more difficult to restore data lost due to system failures.

6. ATTACKS AGAINST DISK ENCRYPTION

Although the encryption of data undoubtedly makes it safer than just to keep the data unencrypted on the hard disk, there are still some ways that the thieves can extract the data if you're not careful. Some are more easy to avoid and other, and it is up to every organisation to decide how much work should be done to prevent unauthorized access to the information.

6.1 Virus, Trojans And Worms

In most encryption systems the user will only have to sign on once, which means that when you have typed in the decryption key you have access to the whole disk without entering any more keys[8]. This makes it possible to use trojan systems that waits until the key has been entered and after that it can access the whole disk. It's also possible to use the trojan and/or keyloggers to sniff the encryption key. It's especially easy to find the key if you use pre-boot authentication since this means the first thing the user will type is the decryption key. Of course this means that it's equally important to keep the system free from malware, regardless of whether the system is encrypted or not.

6.2 Brute force

The brute force method is a quite simple but demanding operation. In general the brute force uses the simple way of testing every possible key that can have been used during the encryption. If the crypto is using a very short key this process can be quick enough, for example a key length of 8 bits is only 2^8 which is 256 different keys. The amount of 256keys can be checked by any human in a few hours, and by a computer in a matter of seconds. Although if you take a key of higher length, 128 bits is standard today, it would require 2^{128} different keys which is approximately $3.4 \cdot 10^{34}$. If you would find a device that could test a billion billion keys every second it would require approximately 10^{34} years to test all these keys. This amount of years is about the same as the age of the universe. This calculations is of course based on that is the last key that is correct and that the key can't be guessed by other methods or ways to shorten down the key.

6.3 Dictionary

The dictionary attacks use a file that contains the most common words that is being used in passwords. Usually this file contains all common English words and some extensions of common passwords like "qwerty". When doing a brute force attack most people starts with the dictionary attack since testing about 10 000 keys instead of 2^{128} takes much shorter time. This attack is although quite easy to avoid by using passwords that doesn't exist in a dictionary.

6.4 Cold-Boot Attack

The cold-boot attack uses the fact that the encryption key of the encryption is stored in the RAM-memory. This is usually not a problem since the RAM is emptied when the computer is turned off. A few scientist at Princeton University showed that the time it takes for a memory to be emptied is depending on the heat of the memory[8]. Normally the information on the chip fades away in a few seconds. The scientist cooled down the memory chip of a standard laptop down too $-50C^{\circ}$, at this temperature the memory was still almost intact after 10 minutes. This means it is possible to steal a running computer that has been locked but still be able to read the data of the disk by copying the cooled memory to an USB memory or a hard disk. There are a lot of parameters that must be in place to be able to complete this attack but it's important to know that the issue exist.

6.5 Mathematically

The best way of breaking an encryption system is to break the actual mechanism so that you find a way to reverse the encryption algorithm[18]. Many mathematics works to find a backward mechanism, not many cryptos have been destroyed this way, but if they find one it's a jackpot. AES that is the most common used crypto has not been broken in this way, at least no method has been announced to the public yet. Other things mathematicians are looking for are ways to reduce the amount of keys that are needed to be tested by dictionary and or brute force attacks. The most famous crypto that has been broken is probably the German submarine crypto machine Enigma, which was broken by a number of factors, but one of the biggest was strictly mathematic.

7. CONCLUSIONS

We have in this paper shown that there are at least three easy ways to protect sensitive data by encryption: the use of the built-in folder and file encryption, full disk encryption by software, and full disk encryption by hardware.

There are of course other things you have to think about when having sensitive information on the laptop. Aside the fact that the someone had gotten their hands on the Croucher Brewing Company's beer recipes and the personal information of their customers, it seems that they had no

backup of this information! To lose information without being able to restore it can mean death for the organisation. The point is, that just because you encrypt your information doesn't mean that you are safe from all kinds of problems a lost laptop can cause.

This report is only an overview over different methods of encryption, but there are a few things that can be interesting to look further into when it comes to encryption. We have three ideas about what could be worth looking into in the subject:

- What do you need to think about when taking backups of encrypted information?
- What impact does full disk encryption have on system performance?
- Comparison of different encryption systems from an end user's point of view (usability).

Of course there is another important thing for most organisations that want to apply a encryption system: cost. While there exist free alternatives, the commercial alternatives might be more attractive for some reason. For example it might include some backup solution or some other service that the organisation needs. Then we get to the question about cost efficiency. While this is an important question for many organisations, it is probably something the organisation itself will have to look into, since every organisation have different priorities and conditions.

8. REFERENCES

[1] P. Backlund. Borttappad hårddisk innehöll en halv miljon personuppgifter. *IDG.se: http://nok.idg.se/2.1046/1.96667 (2008-10-06)*, February 2007.

[2] C. Berg. 10 värsta förlusterna av laptops. *Dataföreningen: http://www.d4d.se/node/2243 (2008-10-06)*, June 2008.

[3] C. B. CO. Reward offered. *http://www.croucherbrewing.co.nz/news%20archive%202007.html (2008-10-08)*, 2008.

[4] A. Czeskis, D. J. S. Hilaire, K. Koscher, B. Schneier†, S. D. Gribble, and T. Kohno. Defeating encrypted and deniable file systems: Truecrypt v5.1a and the case of the tattling os and applications. 2008.

[5] S. de Vries. *A Corsaire White Paper: Securing Mac OS X*. Corsaire, 2005.

[6] J. Gebusia. *Data Encryption on File Servers*. December 2007.

[7] Y. Godbout. What have you got to lose? *CAmagazine*, August 2007.

[8] J. A. Halderman, S. D. Schoen, N. Heninger, W. Clarkson, W. Paul, J. A. Calandrino, A. J. Feldman, J. Appelbaum, and E. W. Felten. Lest we remember: Cold boot attacks on encryption keys. *Proc. 2008 USENIX Security Symposium*, February 2008.

[9] Hewlet-Packard. Protecttools smart card security manager. *http://www.hp.com/sbso/security/protect-tools-for-smart-cards.pdf (2008-10-07)*, 2008.

[10] P. Institue. Airport insecurity: The case of missing & lost laptops. *http://www.dell.com/downloads/global/services/dell_lost_laptop_study.pdf (2008-10-09)*, June 2008.

[11] M. John. Security tool still strong. *eWeek*, November 2005.

[12] R. Laboratories. Pkcs #5 v2.0: Password-based cryptography standard. Mars 1999.

[13] A. Laub. Practical mac os x insecurity. December 2004.

[14] V. Loh. A laptop circle of trust. *eWeek*, 24(11):29–31, march 2007.

[15] E. Malykhina, L. Greenemeier, K. J. Higgins, and S. Gaudin. Laptop lockdown. *Information Week*, April 2007.

[16] PGP Corporation. Pgp whole disk encryption proactively secure confidential data on disks and removable media. *http://www.pgp.com/products/wholediskencryption/ (2008-10-08)*, 2008.

[17] Seagate Technology. Product overview: Momentus 5400 fde.2 best-in-class security for data at rest. *http://www.seagate.com/docs/pdf/marketing/po_momentus_5400_fde.pdf (2008-10-06)*, 2008.

[18] S. Singh. *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. Anchor, 2000.

[19] W. Smith. Encrypt your warriors' laptop. *Computer & Information Security*, February 2007.

[20] TrueCrypt. Introduction. *http://www.truecrypt.org/docs/intro.php (2008-10-08)*, 2008.

[21] TrueCrypt. System encryption. *http://www.truecrypt.org/docs/?s=system-encryption (2008-10-08)*, 2008.

[22] TrueCrypt. Truecrypt rescue disk. *http://www.truecrypt.org/docs/?s=rescue-disk (2008-10-08)*, 2008.

[23] TrueCrypt Foundation. Hidden operating system. *http://www.truecrypt.org/docs/?s=hidden-operating-system (2008-10-06)*, 2008.