ISSN:0975-9646

Undecryptable Encryption against Network and Forensic Attack

Raana Syeda,
Dept of CSE,
G.H. Raisoni College of Eng.,
Nagpur-440016, India.

S.U. Nimbhorkar
Asst. Professor, Dept of CSE,
G.H. Raisoni College of Eng.,
Nagpur-440016, India.

Abstract:

Cryptography plays a vital role in data security. It is necessary where the integrity and confidentiality of information is needed. But use of cryptography is not sufficient for the protection of the sensitive information. There are number of cases encounter where the attacker breach the security and obtain the secret key in use or the secure information even though the strong protection against attack such as brute force, cold boot etc. has been provided. Some systems are only use for the storage purpose. Such systems are the recording devices such as CCTV, video recorders and network equipments. They just keep the information for further use in secure manner. These systems never process this stored information and even not understood it. These devices require the more protection as they either transfer the data physically or through network. Symmetric cryptography is useful when there is a huge amount of data to encrypt but provide the more access then needed. Asymmetric encryption does not provide more access but not suitable for large volume of data. So a solution is required where device is allowed to encrypt the data symmetrically, but is not able to decrypt it neither by itself nor by attacker.

Keywords: Data remanance, Image storing, Cryptography, Data Security, Computer security.

1. INTRODUCTION

Cryptography is the science of protecting the channel between two communicating parties. It becomes one of the most important contributors to privacy and data security in an increasingly interconnected world. The use of cryptography As cryptography may be used to hide data that may high light on the chain of events that constitutes an incident or crime, it also represents a challenge for digital forensics investigators.

Only protection to communication channel using cryptography is not sufficient. Endpoints of channels is now become the major security challenges. Cryptography defends against various attacks; still the endpoints have become the weakest link in the security chain. Hackers do not need decrypt data in transit, just need to implant the malicious program on machine to harvest all the secrets that it processes. Some attack make it difficult to identify the third party or remote party so it is increasingly important to secure the machine right in front of you. Information is always at risk. Attacker can follow any possible way to get the data either by using the rootkit to monitor the device or stolen physical device [1].

Various cases have occurred, where the devices contain sensitive information has stolen and disposed drive incorrectly. To defend the device from the attack, it is require that device has only useful data available to it. Information that no longer needed should be purge out properly. The data which is available in the device should be in encrypted form so that unauthenticated user will not be able to access it. Generally devices keep data available for the further processing on it. User accesses data and modify its requirement. Some devices are only used for the storage purpose. Device store data and transfer it to another device. Another device processes this data. There are a wide range of devices that would fit into this category, including sensors on scientific equipment, monitors on vehicles, and CCTV equipment. These devices do not require processing the data that it captures, but should store the data in secure manner.

Symmetric encryption is used to encrypt the bulk of a data. If the data is encrypted on a device using the symmetric encryption then it is possible to decrypt the data on the same device. It is possible that device that having the key and data can be stolen or hacked during the encryption process. As a result, attacker can compromise the device and manipulate the data. Asymmetric encryption can be used to solve this problem, but it is infeasible to encrypt large amount of data with it. Where cryptography is used to protect the content, hackers have invariably found the keys and publicly disclosed them.

The purpose of this paper is to provide a method that gives the high degree of protection to the information. It allows the device to securely encrypt the data but not allow decrypting it on the same device. It keeps the information in system which is strictly necessary. While all important information should be encrypted. Information that is no longer needed should be properly erased.

This technique is applicable where device need not to decrypt the data such as

1. Military tank where recording device is used to capture the image of battle ground and store information in hidden form. Data will open up in base camp only.
2. CCTV cameras in mails, offices etc.
3. Network equipment which are use to transmit sensitive data
4. And video recorder in Black box.

2. REVIEW OF LITERATURE AND SIMILAR WORK:

2.1 Data remanence in DRAM

Data remanence is the residual representation of data that remains even after attempts have been made to remove or erase the data.

Most security experts assume that a computer's memory is erased almost immediately when it loses power or that whatever data remains is difficult to retrieve without specialized equipment. It is shown that these assumptions are incorrect. Ordinary DRAMs typically lose their contents gradually over a period of seconds, even at standard operating temperatures and even if the chips are removed from the motherboard, and data will persist for minutes or even hours if the chips are kept at low temperatures. Residual data can be recovered using simple, nondestructive techniques that require only momentary physical access to the machine. Previous researchers have suggested that data in DRAM might survive reboots, and that this fact might have security implications. [6]

2.2 Full Disk Encryption

To protect the data that remains in disk (such Cryptographic keys in DRAM) are need to be store in encrypted form. Now a day's device uses full disk encryption. According to the 2006 Security Breaches Matrix, a large number of the data leaks were caused due to stolen/missing laptops. Mobile devices will be stolen or lost, but one way to easily mitigate the harm is to use Full Disk Encryption (FDE) on all mobile devices. So, why don't encrypt all our HDDs? Cost and performance impact are the usual arguments. Analysis shows that the access time increases by 56%-85% after FDE. As HDDs fills up the fragmentation increases and so will the file access time. With FDE, the swap file (system's virtual memory) gets encrypted as well. This will impact the system's performance noticeably when the virtual memory is being used more often [11].

Encryption key & password management blues follow. What happens when the user forgets his/her new FDE password? How to manage the encryption key backup files? Who has possession of the backups of the encryption keys? What about when the users quit and do not hand over the password / encryption keys? Who can access the system and its encrypted files? How frequently does the password need to be changed? How to prevent the user from writing the passwords down? Using hardware token (RSA Token, smartcard etc) can alleviate many of the password management issues. But these hardware tokens are costly.

There are number of strong algorithm and techniques are available for data encryption. In most cases, a user will need to modify information continuously hence they need to have access to it on their machines. However, some devices are purely used for storage and processing done later, by a different device in a different location. The device recording the data does not need to be able to decrypt what it is storing. . There are several popular disk encryption systems, including BitLocker, TrueCrypt, and FileVault, and many similar products are also vulnerable. [5]

2.3 Attacks

Cryptographic keys held in memory can be recovered by the effect of attacks that exploit DRAM remanence. They pose a particular threat to devices such as laptop which uses disk encryption products, since an adversary who steals a laptop while an encrypted disk is mounted could employ attacks to access the contents, even though if the computer is screen-locked or suspended. While principal focus is disk encryption, any sensitive data present in memory when an attacker gains physical access to the system could be subject to attack. Many other security systems are probably vulnerable. [4]

Imaging Residual Memory

No special equipment is required by imaging residual memory contents. When the system is start booting, the memory controller begins refreshing the DRAM, reading and rewriting each bit value. At this point, the values are fixed, decay halts, and programs running on the system can read any data present using normal memory-access instructions.[3]

Memory-imaging tools:-

To boot a system and extract the contents of its memory, Memory-imaging tools use several different attack vectors. Use tiny special-purpose programs that, when booted from either a warm or cold reset state, produce accurate dumps of memory contents to some external medium. These programs use only trivial amounts of RAM, and their memory offsets used can be adjusted to some extent to ensure that data structures of interest are unaffected. [3]

USB device:-

Most PCs can boot from an external USB device such as a USB hard drive or flash device. There are numbers of plug-in that can be booted from an external USB device or a regular hard disk. It saves the contents of system RAM into a designated data partition on this device. [3]

Simple reboots:-

The simplest attack is to reboot the machine and configure the BIOS to boot the imaging tool. A warm boot, invoked with the operating system's restart procedure, will normally ensure that the memory has no chance to decay, though software will have an opportunity to wipe sensitive data prior to shutdown. [3]

Transferring DRAM modules:-

Removing the memory modules can also allow the attacker to image memory in address regions where standards BIOSes load their own code during boot. The attacker could remove the primary memory module from the target machine and place it into the secondary DIMM slot (in the same machine or another machine), effectively remapping the data to be imaged into a different part of the address space. [3]

Countermeasures

Memory imaging attacks are difficult to defend against because cryptographic keys that are in active use need to be stored somewhere. Countermeasures focus on

discarding or obscuring encryption keys before an adversary might gain physical access, preventing memory dumping software from being executed on the machine, physically protecting DRAM chips, and possibly making the contents of memory decay more readily.

- Discard encryption key.
- Key should be generated by password used for accessing the machine.
- Scrubbing memory.
- Clear memory at boot time.
- Clear during startup (before loading of OS.)
- Limiting booting from network or removable media.
- Physical protection such as locking DRAM[2]

2.4 Cold Boot Attack

In cryptography, a cold boot attack (or to a lesser extent, a platform reset attack) is a type of side channel attack in which an attacker with physical access to a computer is able to retrieve encryption keys from a running operating system after using a cold reboot to restart the machine from a completely "off" state. The attack relies on the data remanence property of DRAM and SRAM to retrieve memory contents which remain readable in the seconds to minutes after power has been removed.

To execute the attack, the machine is cold-booted. Cold-booted refers to when the power is cycled “off” and then “on” without letting the computer shut down cleanly, or, if available, the “reset” button on the computer is pressed. A light-weight operating system is then immediately booted (e.g. from a USB flash drive), and the contents of pre-boot memory dumped to a file. Alternatively, the memory modules are removed from the original system and quickly placed in another machine under the attacker's control, which is then booted to access the memory. Further analysis can then be performed against the information that was retrieved from memory to find the sensitive keys contained in it (automated tools are now available to perform this task).

The attack has been demonstrated to be effective against full disk encryption schemes of various vendors and operating systems, even where a Trusted Platform Module (TPM) secure cryptoprocessor is used.[2] This is because the problem is fundamentally a hardware (insecure memory) and not a software issue. While the focus of current research is on disk encryption, any sensitive data held in memory are vulnerable to the attack.

The time window for an attack can be extended to hours by cooling the memory modules. Furthermore, as the bits disappear in memory over time, they can be reconstructed, as they fade away in a predictable manner. In the case of disk encryption applications that can be configured to allow the operating system to boot without a pre-boot PIN being entered or a hardware key being present (e.g. BitLocker in a simple configuration that uses a TPM without a two-factor authentication PIN or USB key), the time frame for the attack is not limited at all.

2.5 Walsh Code

There are number of forensic identification and key extraction techniques that can recover the keys use for data hiding process. So, there is a need of method which generates a unique key which is hard to detect. Walsh code is one which can be used as key. It is difficult to detect the Walsh code as two codes are purely orthogonal.

Also known as "Walsh-Hadamard code," it is an algorithm that generates statistically unique sets of numbers for use in encryption and cellular communications.

Walsh Code Algorithm

(a’, b') = (a + b, a-b)

A new technique is proposed for optical encryption and multiplexing of binary characters and images used for personal identification information. Different binary images can first be encrypted using orthogonal code and then multiplexed together in the spatial domain. The resulting encrypted single image provides security as well as makes efficient use of storage and/or transmission capacity. The image can finally be decrypted and the individual input images can be decoded employing the same orthogonal code set. Because of the orthogonal nature of the code used, the encryption and decryption processes do not deteriorate the quality of the images employed. Also, the proposed technique involves a very simple architecture, as it does not require any mathematical transformation.

Walsh Transform

This is a special type of orthogonal transformation formed by rearranging the rows of Hadamard matrix that performs an orthogonal, symmetric, evolutional & linear operation on 2^m real numbers.

The Walsh transform Wm is a $2^m \times 2^m$ matrix, known as the *Walsh matrix*, which is a specific square matrix, the entries of which are $+1$ or -1, and the property that the dot product of any two distinct rows (or columns) is zero.

The Hadamard matrices of dimension 2^k for $k \in N$ are given by the recursive formula:

$$H_2^0 = [1] \qquad H_2^k = \begin{bmatrix} H_2^{k-1} & H_2^{k-1} \\ H_2^{k-1} & -H_2^{k-1} \end{bmatrix}$$

For example,

$$H_2^0 = [\mathbf{1}] \quad H_2^1 = \begin{bmatrix} \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{-1} \end{bmatrix}$$

Binary representation is,

$$H_2^0 = [\mathbf{1}] \quad H_2^1 = \begin{bmatrix} \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} \end{bmatrix}$$

Now, the Walsh matrix is obtained in such a way that the number of sign changes in a row is in increasing order. So,

$$H_2^0 = [\mathbf{1}] \quad W_2 = \begin{bmatrix} \mathbf{1} & \mathbf{1} \\ \mathbf{1} & \mathbf{-1} \end{bmatrix}$$

$$W_4 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{bmatrix} \quad \text{and so on.}$$

This whole matrix is used as key in case of image This whole matrix is used as key in case of image Encryption and decryption. This matrix is multiply with the image matrix to obtain the cipher image.

Another way to obtain The Walsh-Hadamard code is to generate Generator matrix G of dimension K $\times 2^n$. Where $g_i \epsilon \{0,1\}^n$ is the vector corresponding to the binary representation of *i*. In other words, g_0, g_1 … g_{2n-1} is the list of *all* vectors of $\{0, 1\}^n$ in some lexicographic order.

$$G = \begin{bmatrix} \uparrow & \uparrow & & \uparrow \\ g_0 & g_1 \ldots & & g_{2n-1} \\ \downarrow & \downarrow & & \downarrow \end{bmatrix}$$

The Generator matrix for the Walsh–Hadamard code of dimension 3 is

$$G = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

As is possible for any linear code generated by a generator matrix, we encode a message x ϵ $\{0,1\}^n$ viewed as a row vector, by computing its codeword z ϵ $\{0,1\}2^n$ using the vector-matrix product in the vector space over the finite field F_2:

$$Z = x.G$$

This code word used as key for encryption purpose.

Walsh function generation using basis vectors

The Walsh sequences of order N form a K-dimensional vector space over GF (2), i.e., all the N- tuple Walsh sequences can be spanned by a set of linearly independent basis vectors. There exists a K× N generation matrix G such that $W_j = X_j G$, j = 0, 1… $2^K = N$.

W=XG,

G is K×N generation matrix

$N=2^K$

$X=(x_1, x2 \ldots x_k)$

For Example

N=8 K=3

G= 01100110 X_5 = (101)

00111100

00001111

W_5 = (01101001)

The Walsh codes now have variable lengths that range from 4 to a total of 256.The one effect with utilizing variable length Walsh codes is that if a shorter Walsh code is being used, then it precludes the use of the longer Walsh codes that are derived from it. For instance, if Walsh code 2 is used, then it precludes the use of all the Walsh codes in the code tree that were derived from it.

3. PROPOSED WORK

To solve the stated problem, assuming two separated device. One for recording purpose called Recording device and another for processing called Master device. Recording and Master Device will perform some initial communication. Recording device perform some initial operation in secure area. In this initial operation Recording device divide the memory into blocks and generate the secret key and the initialization vector. Store the secrete key and initialization vector in encrypted form in one of the block. This encryption will do with the help of another key either sends by Master device or generated by itself. To fill the remaining blocks, XOR operation on initialization vector will carry out called Mask and store into a block .This operation will repeat for each block. Recording device will generate another secrete key to encrypt the data. Second secrete key will also store in one of the block in encrypted form. Encrypted data will then XOR with the mask and store back to the same block of used Mask. After completing this initial operation all the key have been cleared from the system. Even the attacker get all the key material during encryption, is able to obtain the current block only. Without the keys form initial pass, they cannot decrypt anything.

Recording device send this encrypted information to Master Device where decryption will carry out. During decryption Master device will decrypt the blocks that contain the keys and initialization vector. Next step will to remove the mask. To remove the mask, encrypt the Initialization vector using the obtained secrete key and XOR with the content of the block which gives the cipher text. This cipher text is the decrypted using the second secret key which was used during the encryption process, will gives the original data.

4. CONCLUSION

If the devices use the full disk encryption still there is threat to the confidential information. With full disk encryption, it is required that attacker will not be able to obtain the data remain in disk. Even if attacker compromises the device at the time of encryption, information remains secure.

5. REFERENCES

1. Thomas Martin 2011,"UNDECRYPTABLE SYMMETRIC ENCRYPTION" IEEE GCC Conference and Exhibition (GCC),, Dubai, United Arab Emirates February 19-22, 2011
2. A. Jones, G. Dardick, G. Davies, I. Sutherland, C. Valli, "The 2009 Analysis of Information Remaining on Disks Offered for Sale on the Second Hand market" Journal of International Commercial Law and Technology, North America, Jul. 2009.
3. C. Maartmann-Moe, S. E. Thorkildsen, and A. Arnes, "The persistence of memory: Forensic identification and extraction of cryptographic keys" Digital Investigation, 6(1):S132–S140, 2009.
4. 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. 17th USENIX Security Symposium (Sec '08), San Jose, CA, July 2008
5. FERGUSON, N. AES-CBC + Elephant diffuser: A disk encryption algorithm for Windows Vista. Aug. 2006.
6. SKOROBOGATOV, S. Low-temperature data remanence in static RAM. University of Cambridge Computer Laboratory Technical Report No. 536, June 2002.
7. GUTMANN, P. Data remanence in semiconductor devices. In Proc. 10th USENIX Security Symposium (Aug. 2001)
8. R. Cramer, V. Shoup, "Design and Analysis of Practical Public-Key Encryption Schemes Secure against Adaptive Chosen Cipher text Attack" SIAM Journal on Computing Vol 33 2001.
9. Yuen, C. 1972. Remarks on the Ordering of Walsh Functions. IEEE Transactions on Computers. C-21: 1452.
10. "Image Encryption & Authentication using Orthogonal Transformation on Residual Number System".
11. http://slashdot.org/story/06/10/20/2250246/Why-Not-Use-Full-Disk-Encryption-on-Laptops