Think India Journal
ISSN: 0971-1260 Vol-22, Special Issue-21
National Conference on
Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) organised by
Department of Commerce, VEL TECH Ranga Sanku Arts College,
Avadi, Chennai-62
Held on 4th January 2020

A Survey of Confidential Data Storage and Deletion Methods

Sridhar.M
Department of Computer Science,
Veltech Ranga Snaku Arts College, Avadi, ch-62
Email: sridhar482@velsrscollege.com

ABSTRACT:

As the quantity of virtual records grows, with the decrease in price of digital garage media, increasingly touchy statistics gets stored in those media. Laptop computers regularly cross missing, either because they're misplaced or due to the fact they're stolen. So does the theft of touchy information via the loss or misplacement of laptops, thumb drives, outside tough drives, and different digital garage media. Sensitive data can also be leaked by chance because of wrong disposal or resale of storage media. To defend the secrecy of the complete statistics lifetime, we should have personal ways to save and delete records.

Keywords: Data Storage, Electronic Storage Media

I. INTRODUCTION

The general concept of secure handling of data is composed of three aspects: confidentiality, integrity, and availability. Confidentiality involves ensuring that information is not read by unauthorized persons. With the decrease in cost of electronic storage media, more and more sensitive data gets stored in those media. The push toward the paperless office also drives businesses toward converting sensitive documents, once stored in locked filing cabinets, into digital forms.

A. General Security Background

The general concept of secure handling of data is composed of three aspects: Confidentiality- involves ensuring that information is not read by unauthorized persons. Confidentiality means storing data in a way that can be read only by authorized persons. No unauthorized persons should be able to read or otherwise obtain meaningful information from this data, even with physical access to the storage media.

1. Commonly Used Encryption Algorithms
2. Traditional Modes of Operation

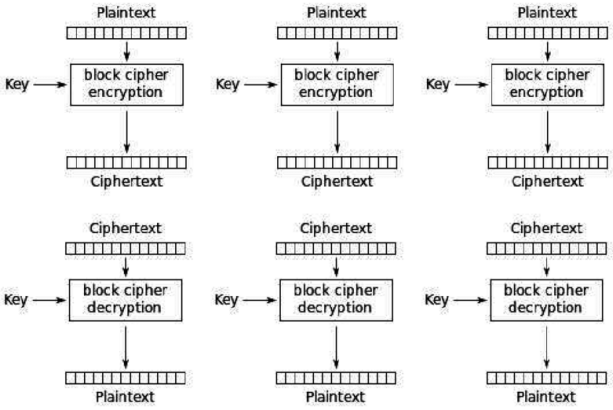
a) Commonly Used Encryption Algorithms

Think India Journal
ISSN: 0971-1260 Vol-22, Special Issue-21
National Conference on
Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) organised by
Department of Commerce, VEL TECH Ranga Sanku Arts College,
Avadi, Chennai-62
Held on 4th January 2020

Encryption -used in cryptography "to scramble information so that only someone knowing the appropriate secret can obtain the original information (through decryption)". The secret is often a key of n random bits of zeros and ones. Common symmetric key encryption algorithms : the Data Encryption Standard (DES), Triple-DES (3DES), and the Advanced Encryption Standard (AES). DES-a key size of 56 bits and a block size of 64 bits.Criticism-56-bit key length is too short. With newer CPUs, the key space of 256 can be enumerated. 3DES-built to enlarge the DES key space.
Criticism-the key space to 2168, but the strength of 3DES is only twice as strong as DES. AES-block length of 128 bits and supports key lengths of 128, 192, and 256 bits

b) Traditional Modes of Operation

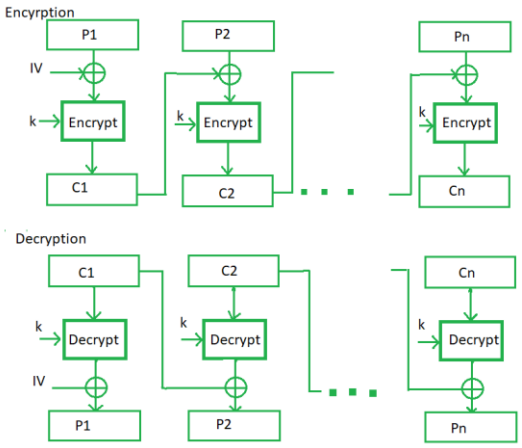
Electronic Codebook(ECB)- is the simplest mode of operation, and does not use an IV(initialization vector) .With a key, Pi as the ith block of plaintext, and Ci as the ith block of cipher text, the encryption is performed as Ci = Ekey (Pi), and decryption is performed as Pi = Dkey (Ci).



B. **Cipher-Block-Chaining (CBC)**

slightly more complicated and uses an IV, Encryption of the first block of plaintext is performed as C1 =Ekey (P1 Å IV), where C1 is the 1st block of cipher text; IV is the random, non-secret initialization vector; and P1 is the 1st block of plaintext. Subsequent blocks of plaintext are encrypted as Ci = Ekey (Pi Å Ci-1). In the same manner, the first block of cipher text is decrypted as P1 = Dkey (C1) Å IV, and the subsequent blocks of cipher text are decrypted as Pi = Dkey (Ci) Å Ci-1.

Think India Journal
ISSN: 0971-1260 Vol-22, Special Issue-21
National Conference on
Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) organised by
Department of Commerce, VEL TECH Ranga Sanku Arts College,
Avadi, Chennai-62
Held on 4th January 2020



II. CONFIDENTIAL STORAGE

Confidential storage methods are difficult to implement for reasons including complexity of method setup, difficulty of conversion of prior methods to new secure methods, training, overhead and latency in everyday tasks (e.g., reading and writing to files), key management, and password management.

III. TECHNIQUES OF CONFIDENTIAL STORAGE

There are two basic techniques of confidential storage:

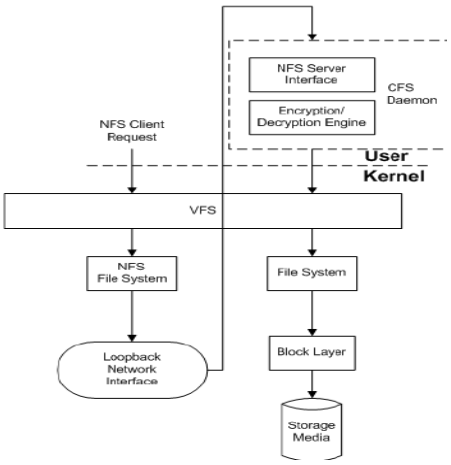
a. Software-based confidential storage

1. Encryption : Encryption is the process of transforming information (referred to¬ as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

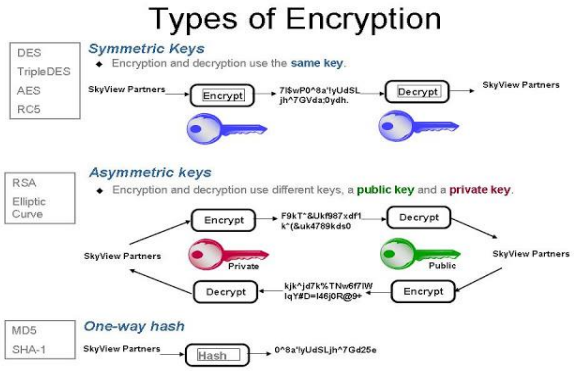
Software encryption programs come in two flavors: generalized encryption programs and built-in encryption mechanisms in applications.

Generalized encryption programs can encrypt and decrypt files using a variety of ciphers and encryption modes; several examples are mcrypt, openssl, and gpg. mcrypt [Smith2008] is a simple command-line program intended to replace the old Unix crypt pro-gram; openssl [Young and Hudson 2008] is an open-source toolkit that implementsthe Secure Socket Layer and Transport Layer Security protocols as well as a generalpurpose cryptography library. Through use of the library, we may encrypt and decrypt
files through the command line. The GNU Privacy Guard, or GnuPG [Koch 2008], implements the OpenPGP standard, which features a versatile key management systemand allows the user to encrypt and sign data and communications using public and private keys

Think India Journal
ISSN: 0971-1260 Vol-22, Special Issue-21
National Conference on
Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) organised by
Department of Commerce, VEL TECH Ranga Sanku Arts College,
Avadi, Chennai-62
Held on 4th January 2020



1. **Symmetric encryption** (secret key encryption)
2. **Asymmetric encryption** (public key encryption).



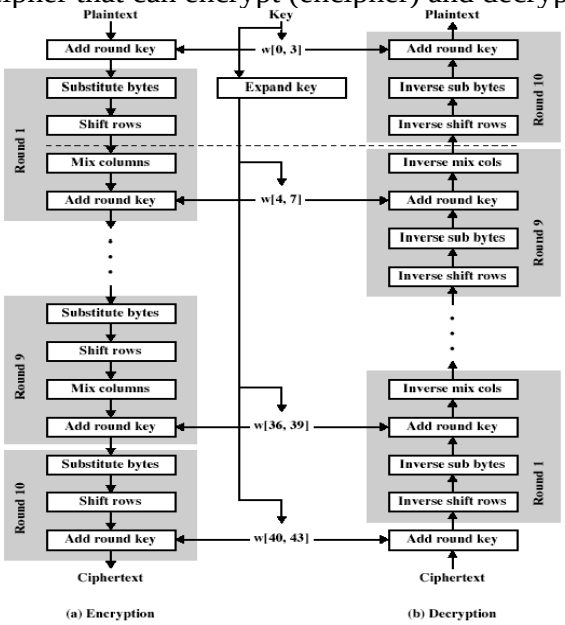
Symmetric cryptography : encrypter, and **decrypter** — need access to the same key.

1) In services that store encrypted data on behalf of a user (like cloud backup services) 2)To encrypt computer or device storage(Computer password) 3)To create a secure channel between two network endpoints, provided there's a separate scheme for securely exchanging the key
2) **Asymmetric cryptography (public key cryptography) :**public key cryptography, uses public and private keys to encrypt and decrypt data.Either of the keys can be used to encrypt a message; the opposite key from the one used to encrypt the message is used for decryption.
3) Hash : Hashing is used only to verify data the same input will always produce the same output it's impossible to reverse it back to the original data given knowledge of only the hash,

Think India Journal
ISSN: 0971-1260 Vol-22, Special Issue-21
National Conference on
Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) organised by
Department of Commerce, VEL TECH Ranga Sanku Arts College,
Avadi, Chennai-62
Held on 4th January 2020

it's infeasible to create another string of data that will create the same hash(called a "collision" in crypto parlance)

2) Advanced Encryption Standard (AES): specifies a FIPS(FederalInformation Processing Standard)-approved cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt(decipher) information.



b. Hardware based confidential storage

1.1. Secure Flash Drives : We Some secure flash drives provide only software encryption using block-based encryption methods as mentioned. Other flash drives protect data through cryptographic mechanisms provided on the flash drive itself

1.2. Enclosures and Extension Cards: Enclosures and extension cards can employ good encryption techniques and do not divulge any information about files or the structure of the file system on disk

1.3. Encrypted Hard Drives : Seagate [2006] is introducing "Drive Trust Technology" into their Momentus 5400 FDE series notebook hard drives, which implement full disk encryption. This technology is implemented in the hard drive firmware and provides encryption,decryption, hashing (for passwords), digital signature, and randomnumber generation functions.

IV. STORAGE DELETION / DATA DESTRUCTION

Think India Journal
ISSN: 0971-1260 Vol-22, Special Issue-21
National Conference on
Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) organised by
Department of Commerce, VEL TECH Ranga Sanku Arts College,
Avadi, Chennai-62
Held on 4th January 2020

When confidential data have to be removed, we must be sure that once deleted, the data can no longer be restored. A full secure data lifecycle implies that data is not only stored securely, but deleted in a secure manner. When you smash data, the goal is to make it absolutely unreadable regardless of the form of electronic media on which it become at the beginning saved. The technique of information destruction additionally includes ensuring that this facts can't be recovered and used for unauthorized purposes. Destroying data means it could not be read by way of an running gadget or application. Merely deleting a record is inadequate.

When you delete a record on an digital tool, you could not be able to see it to any extent further, but the facts continues to be saved on the device's hard force or reminiscence chip. Data destruction entails overwriting the present day facts with random information until the modern records can not be retrieved, or sincerely destroying the digital medium. Time: Is this something the enterprise regularly does or has it stockpiled antique facts garage system to do a large quantity right away? Each of the extraordinary strategies explored below operates on a distinctive timescale. Knowing how a whole lot time you want to spend on statistics destruction can affect the selection of approach.

Cost: Can your organisation manage to pay for to remove old equipment? Or is it inquisitive about reusing older electronic media for brand new purposes? Again, the solution to this question will decide the type of destruction technique you want to use.

Validation and certification: If you're destroying facts because it's a felony requirement or a regulatory trouble inside your enterprise, make sure the method you choose lets in you to show which you have met any standards or requirements for information destruction.

1. Delete/Reformat

   As we mentioned above, deleting a report from an electronic device might also put off it from a file folder but does no longer surely damage the statistics. The statistics stays at the hard power or the reminiscence chip of the device.The equal is true while you try and break records through reformatting the disc. This does not wipe the facts away both. It simply replaces the prevailing record device with a new one. It's as if you are tearing out the desk of contents from an antique cookbook while what you need to do is eliminate the cookbook itself. It could be very easy for nearly anybody to get better facts from a disk that has simplest been reformatted as many tools exist at the Internet that allow an person to do so.Using techniques of this kind is a instead lazy, unimaginative and now not very effective manner to attempt facts destruction.

2. Wipe

   Data wiping entails overwriting records from an electronic medium so that this records can not be examine. Data wiping is commonly achieved through physically connecting any media to a bulk wiping tool. It also can be finished internally by using beginning a PC from a network or CD. As a method, it lets in you to reuse any media wiped in this way without losing storage ability

Think India Journal
ISSN: 0971-1260 Vol-22, Special Issue-21
National Conference on
Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) organised by
Department of Commerce, VEL TECH Ranga Sanku Arts College,
Avadi, Chennai-62
Held on 4th January 2020

3. Overwriting data

In a sense, overwriting facts can be a form of facts wiping. As soon as statistics on associate degree tool is overwritten, a sample of ones and zeros is written over the prevailing information. The pattern doesn't need to be random — set patterns may be used. In most cases overwriting as currently as can accomplish the challenge. However if the medium will be a high-protection one, it will want a couple of passes. This guarantees that all expertise is completely destroyed and no bit shadows can also be detected.

A bit shadow can be a remnant of facts that has been overwritten however will in spite of this be detected mistreatment accomplice diploma microscope. It's like whereas any person writes a look at on a pad. They will put off the very best sheet of paper, but companion diploma have an impact on of what they wrote might also moreover notwithstanding be visible on the sheet without delay underneath. Bit shadowing remains a mission for excessive-security operations, but low-hazard corporations possibly don't need to trouble themselves accomplice degree immoderate quantity of. Ill facts the use of companion diploma microscope takes quite a number some time and prices sort of coins.

Overwriting is probably the utmost common way to wreck statistics. However, it is able to take a range of a while and best works as soon as the medium being overwritten has now not been damaged and might however have records written to that. It similarly will not offer any protection protection at a few degree within the overwriting technique. Overwriting doesn't paintings on any effective drive that contains superior garage management components. If you are overwriting a tool resulting from prison necessities, you will need a license for each piece of media this can be being overwritten. It is now not foolproof.

4. Erasure: Erasure need to be complete and smash all facts saved on a difficult drive, and supply a certificate of destruction showing that the statistics on an digital device has been successfully erased

5. Degaussing destroys pc information the use of a high-powered magnet which disrupts the magnetic area of an electronic medium. The disruption of the magnetic area destroys the records. Degaussing can effectively and quickly ruin the statistics in a tool storing a huge quantity of data.

Think India Journal
ISSN: 0971-1260 Vol-22, Special Issue-21
National Conference on
Recent Advances in Commerce, Management and Computer Science (NRCACMC-2020) organised by
Department of Commerce, VEL TECH Ranga Sanku Arts College,
Avadi, Chennai-62
Held on 4th January 2020

6. Physical destruction (drill/band/crush/hammer)Physical destruction techniques offer tremendous confidentiality. We cannot securely delete handiest one record using those techniques. Therefore, this approach does not guide flexible safety guidelines

7. Electronic shredding
   Shredding is a first-rate manner to run in information when you have a massive information organisation center or a big stockpile of vintage difficult drives and media that you want to damage. It's very at ease, rapid and green. Shredding reduces digital devices to pieces no larger than 2 millimeters. If you work in a high-safety environment with high-protection facts, shredding need to be your primary choice because it guarantees that every one statistics is obliterated
8. Solid state shredding: There are two issues with Solid-state drives. First, it's terribly troublesome to erase something extremely secure. Second, it's terribly troublesome to recover info in spite of that approach it's been erased. Pretty much everything aforesaid higher than solely applies to traditional magnetic exhausting drives, USB flash drives and older SSD drives with no TRIM support.

9. Encryption with Key is the third way to securely delete data is to encrypt the data and then delete the key securely. Using overwriting methods, the encryption key is often safely deleted. That combination allows for a much quicker, safer deletion by overwriting only a small key instead of the whole file (which could be very large).

CONCLUSION

By ordering encounters and limitations of different classified stockpiling and erasure strategies, we trust that information from examine zones that have been advancing autonomously can cross spread, to shape arrangements that are tolerant to a more extensive scope of constraints. The heading of the Acknowledgment segment and the References area must not be numbered.

REFERENCES

[1] https://www.researchgate.net/publication/220566117_A_Survey_of_Confidential_Data_Storage_and_Deletion_Methods
[2] http://computer-trickster.blogspot.tw/2015/11/encryption.html
[3] https://www.dataspan.com/blog/what-are-the-different-types-of-data-destruction-and-which-one-should-you-use/