ViSolve Inc.

Open Source Solutions

Securing Data at Rest

ViSolve IT Security Team

Table of Contents

Securing Data at Rest with Encryption

ViSolve Inc

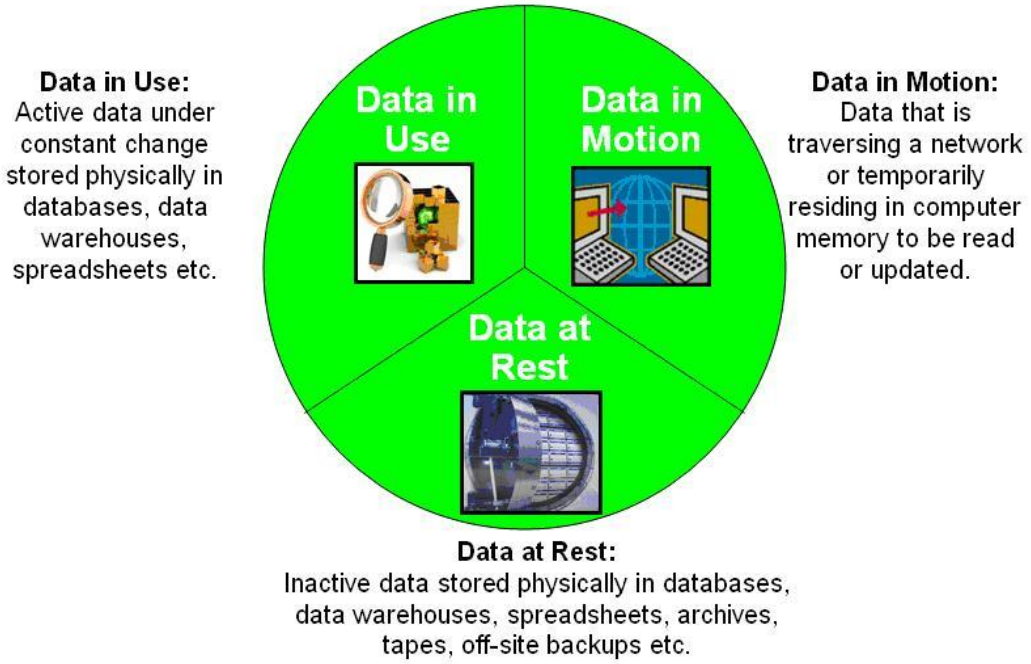
Abstract

Due to the rapid development of information technology and of the Internet, most companies keep their data stored in a digital format, in databases. Database systems have become an essential component of everyday life in the modern society, as most people perform activities that assume interaction with a database, such as: banking, reservations of any kind, searching for a book in a library or in a bookstore. This white paper describes a new approach regarding the encryption for protecting the data at rest from databases.

1 Introduction

As we mentioned in the abstract, the main target of this paper is to describe the best way of securing data at rest. There are three states of digital Data they are,

- Data in Motion
- Data in Use
- Data in Rest



2 Why Data at Rest needs to be secure?

The yardstick of measuring everything in today's business world is revenue. With large corporate relying on storage network for safekeeping their valuable data, lack of security makes the storage network environment unreliable, unstable, and unavailable which ultimately leads to the loss of revenue. Storage networks must be made reliable and stable in order to support business operations. Devices that depend on storage system elements, such as Databases, Web servers and E-Mail servers require a stable environment.

Security measures will increase the stability of an environment by ensuring that the network components that make up the storage environment are able to continue to perform in both normal and abnormal conditions. Availability is the first and foremost issue in supporting a business. Downtime can equate to loss of revenue and/or loss of production. By making the storage more secure, companies can reduce potential downtime due to unauthorized access attempts, malicious code, and other issues.

3 Securing Data

The best way of securing the data is to restrict access to the data. This is best achieved by the process of ***authentication and authorization***. A user should be asked for authenticating information before accessing the data and should only be allowed to perform the operations for which access rights are available. If the data to be accessed is on a local machine, applying access control is easy. It is taken care of by the file-system of the local machine, but if data is accessed from a remote client using protocols like NFS, CIFS, HTTP, or FTP, user credentials and data needs to be secured on the network. It is in such cases

that security protocols like SSL (Secure Sockets Layer), TLS (Transport Layer Security), and IPSEC (Secure Internet Protocol) are used.

In the event that a malicious user somehow breaches the above security provisions and gets access to data, the solution is scrambling the data. So ***encrypting the data*** – whether it is in-motion or at-rest – is the next level of security that will make the data worthless for the hacker.

Encryption - Access control Approach

Access control is achieved by the means of Authentication and Authorization. Authentication is used to verify the identity of an entity and Authorization is used to determine which rights to grant to an authenticated entity.

Encryption - Key Based Approach

Encryption is used to scramble the data, which can only be accessed through appropriate credentials/keys. Encryption can be categorized into two types – encryption of "data-at-rest" and encryption of "data-in-motion"

3.1 Encryption - Access Control Approach

An encrypted file system solution is one of the easiest ways to protect data-at-rest through encryption. Most of these solutions, like Linux EncFS, Windows EFS and Mac OS X FileVault, are already included in an operating system's installation. Therefore, they're readily available to use.

Encrypted file system solutions typically provide transparent encryption. This means, end users can go do their normal routine of transferring files back and forth without having to perform extra steps to make sure those data-at-rest files are encrypted. If all you need is a quick and easy encryption solution for data-at-rest, then encrypted file system software is the best choice
Best tools to achieve Data at rest security (ACL):

- Truecrypt (Advanced)
- BitLocker
- EncFS

3.1.1 Limitation of Encryption - Access Control Approach

In a typical encrypted file system, the only thing that separates an unauthorized user and the data being protected is the username and password. So once those credentials are exposed, an unauthorized user can easily gain access to the contents of the encrypted folder.

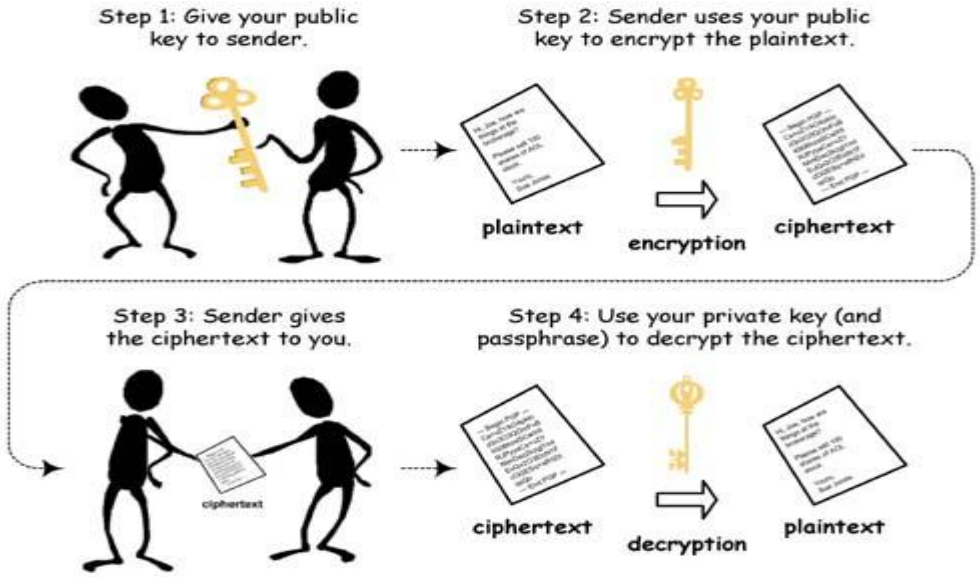
Since credentials of encrypted file systems are normally stored in the same machine as the data itself, there is still that risk of a data breach. For instance, if you manage a server that employs an encrypted file system and that server's hard disk is stolen, it would still be possible for the thief to acquire all the information available inside, once he has acquired the credentials that came with the disk.

Obviously, it would be much safer if your credentials were placed in a different location. That's one significant advantage you can have with PGP (Pretty Good Privacy).

3.2 Encryption - Key Based Approach

PGP has two important components: ***a public key and a private key***.

The public key is typically shared with the trusted members and is used for encryption, while the private key is used for decrypting any information that was encrypted using that public key.



3.2.1 Advantages of Encryption - Key Based Approach

- PGP uses private keys which you can secure in a safe location separate from the data being protected
- Can share the public key to trusted persons who can encrypt the secure data and share with owner, so that he can decrypt.
- Owner can only decrypt with his private key.
- If multiple users are employing this tech, if the private key of a particular person is stolen then ONLY his data will be vulnerable, and all others data will be safe.

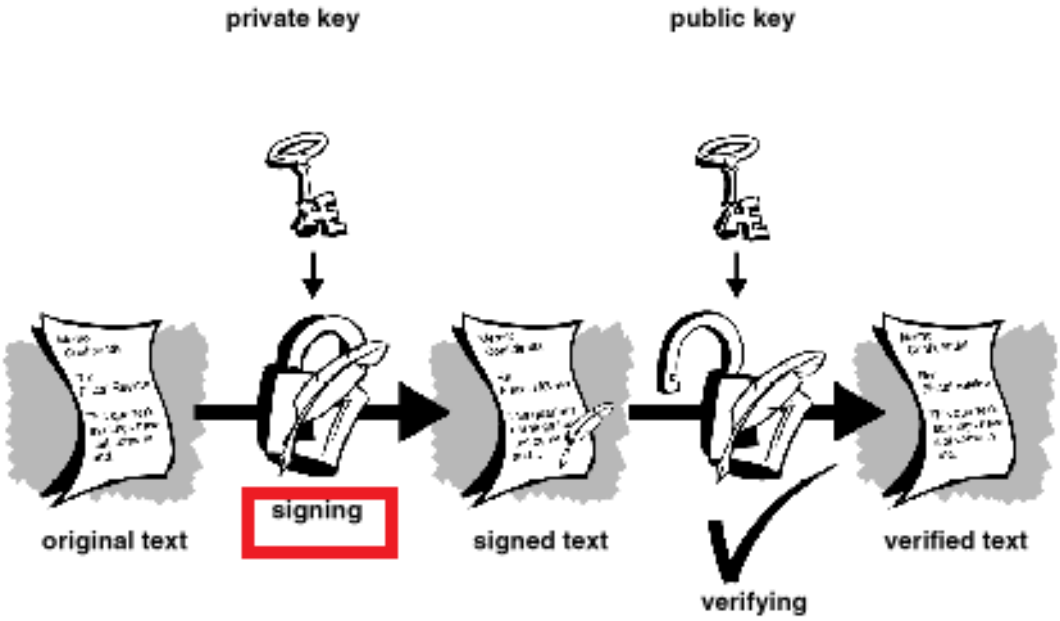
3.2.3 Added Layer of Security in Key Based Approach

Another nifty feature that comes with PGP is its ability to support digital certificates. Basically, PGP allows Administrator to affix a digital signature to a public key that certifies Administrator's ownership towards the said key. Other people can likewise affix their digital signatures on the same public key to vouch that, the key really belongs to the Administrator.

Without the above said feature, a skilled hacker can impersonate Administrator. He can employ social engineering and other nefarious techniques to deceive users into thinking, that they have

Administrator's public key. Where in turn they have is his (the Hacker's) public key. As a result, those users will encrypt data intended for Administrator but will end up sharing them with the hacker instead.

With digital signatures, it would be very difficult for hackers to fool Administrator's friends. Thus, when Administrator's friends encrypt a confidential piece of information using Administrator's digitally signed public key, they can be sure that only Administrator will be able to decrypt it.



Best tools to achieve Data at rest security (Key Based):

- GPG
- Portable PGP

4 Some encryption algorithms

Some encryption algorithms are explained below.

DES

This algorithm was developed by IBM for protecting computer data against possible theft or unauthorized access. DES is now considered to be insecure for many applications; this is mainly due to the 56-bit key size being too small.

TripleDES

This algorithm is a variation of DES. It takes a 192 bit key (24 characters) as input and breaks it into three keys. First, DES is used to encrypt a file using the first key, then the file is decrypted using the second key and finally, DES is used to encrypt the file again using the third key.

Skipjack

This algorithm was developed by the U.S. National Security Agency (NSA). It uses an 80-bit key to encrypt or decrypt 64-bit data blocks and was designed for replacing DES. It has been extensively cryptanalyzed, and has no weaknesses.

Blowfish

This algorithm was designed in 1993 by Bruce Schneier. It uses a variable-length key, from 32 bits to 448 bits and a fast, free alternative to existing algorithms like DES.

Rijndael

This algorithm was designed by Joan Daemen and Vincent Rijmen and was selected for the Advanced Encryption Standard (AES). It is highly secure and has undergone extensive cryptanalysis.

Twofish

This algorithm is Counterpane System's candidate for the AES. It is a symmetric key block cipher with a block size of 128 bits and key sizes up to 256 bits. It is designed to be highly secure and highly flexible.

MARS

This algorithm was designed by IBM as a candidate for the AES. It uses a 128-bit block size and a variable key size of between 128 and 448 bits.

Serpent

This algorithm was designed by Ross Anderson, Eli Biham and Lars Knudsen and was the candidate for the AES. It supports a key size of 128, 192 or 256 bits.

RC6

This algorithm was designed by RSA Security and was the candidate for the AES. It uses a block size of 128 bits and supports key sizes of 128, 192 and 256 bits.

5 Conclusion

Understanding the need to secure your data is the first step towards securing it. In today's age every detail – personal to corporate secrets – is present in form of data. For computers and networks which store and transfer this data, it is just numbers. It is for us to realize the damage this data can do if it falls into the hands of an unscrupulous person. Whether the data is on your laptop, desktop, or on an organizations storage network, it must be secured and should not come in the hand of an unauthorized entity. Proper access control mechanism should be enforced for securing the data. While in motion, data should be well protected. It is advisable to encrypt the data before putting it on a network even if it passes through a secure channel.

Data lying on laptop, desktop, and NAS appliances can be encrypted at **file as well as block level**. However, encrypting the data at file system level provides robust security. Encryption of the file is done on per file key (or) user's unique private key. NAS appliance represents the disk space to users in terms of the file systems and can support the encryption at file system level. If encryption at file system level cannot be achieved, it is worth encrypting the data at block level before writing to disk. It is most vulnerable place for theft as data rests there for long periods of time since it is not encrypted.

Organizations having sensitive data must **encrypt** it at all levels of its lifecycle, whether it is on production server at application, file system and database layer, or at storage layer which includes primary, secondary and tertiary storage. Organizations need to carefully choose the specific place to encrypt the data on the basis of where sensitive data is managed or used.

Encryption **key based** approach (PGP) plays an important role in securing the data, since the credentials are not in the same place where the secure data remains. So if the disk is stolen or compromised, then hacker will not be able to get credentials to decrypt the data. Digital signature enables an added security level by which the end users can identify the Owner/Administrator of the data.

6 References

[1] SNIA-Encryption of Data At-rest, Step-by-step Checklist.
[2] Scott A. Banachowski, Zachary N. J. Peterson, Ethan L. Miller and Scott A. Brandt- Intra-file Security for a Distributed File System.
[3] Anthony Harrington, Christian D. Jensen- Cryptographic Access Control in a Distributed File System 2.Matt Blaze-A Cryptographic File System for Unix.
[4] Data at Rest - Wikipedia Data_at_Rest
[5] Pretty Good Privacy - Wikipedia Pretty Good Privacy
[6] Cryptography - Images