A Survey on Data Loss prevention Techniques

Surya R Raj[1], Asha Cherian[2], Abey Abraham[3]

[1,2] Rajagiri Educational Charitable Trust – Indira Gandhi National Open University,
Rajagiri School of Engineering & Technology,
Rajagiri Valley, Kochi, Kerala 682039, India
[1]*surya.rraj1@gmail.com*
[2]*ashacherian14@gmail.com*

[3]Department of Information Technology, Rajagiri School of Engineering & Technology,
Rajagiri Valley, Kochi, Kerala 682039, India
abeya@rajagiritech.ac.in

Abstract: ***This paper presents a way of encrypting data using an ephemeral cryptographic key since the importance of data loss prevention or data security is increasing nowadays. In this paper, On the fly Encryption is used for data loss prevention, by which an entire drive or a file that mounts as a virtual disk, a partition of hard disk or a device like a USB can be encrypted using an ephemeral key. The encrypted drive is made useless unless a USB drive key and a password that will be included. This paper also presents a way in which email can be downloaded and can be stored encrypted for future reference when internet connection is not available.***

Keywords: data loss prevention, ephemeral key, cryptography, encryption.

1. Introduction

The need for data loss prevention [1] is increasing for personal and organizational use. It may happen that a person can lost his data in some way. Losing the data or information is an important problem, In order to prevent data loss; one important method is to encrypt the data and storing it securely. Encrypted data loss is not a serious issue when compared to unencrypted data loss. This paper presents a way by which entire drive or even email inbox can be saved encrypted. Nowadays encryption of data for secure storage is done using Data Encryption Standard (DES), which is having limitations

On The Fly Encryption (OTFE) also called as Real Time Encryption refers to the fact that the file is stored encrypted and it can be accessed as soon as the key is provided. O-E-sis provides plausible deniability and is transparent. In O-E-sis the encryption occurs on the fly and is fastest encryption method. This method saves enough time. Data is decrypted using the ephemeral key and is stored in a temporary memory location. The user may not save the decrypted data to a file. The temporary file is deleted after it is viewed. One important feature explained in this paper is that full inbox of the email can be downloaded and can be saved in encrypted. This feature helps user to view his inbox even if there is no internet connection.

The paper presents a survey on different data loss prevention techniques used before the proposed system "On–the-fly-Encryption- Security –in –Storage"

2. Proposed System

"On–the-fly-Encryption- Security –in –Storage" (O-E-Sis) explains a way to help data loss prevention by storing data secured. Data is stored in an encrypted form. Additional password needs to be provided by user in order to encrypt the data. This password will generate a key using SHA-1 algorithm and this allows AES algorithm to provide an ephemeral key and an encrypted folder. This ephemeral key will decrypt the data automatically when the data is loading for display. The proposed system has many advantages like it provides password protection since it is stored using serialization and no database dependency. Another add on feature is mail management. The user can download the email inbox and can save the inbox encrypted, which can be used for future reference. O-E-sis works automatically and real time encryption occurs, which saves time

3. Literature Survey

3.1 Data Loss Prevention using Open DLP

Andrew Gavin developed the Open DLP [2]. It is a Data Loss Prevention suite having a centralized web frontend which will manage Windows agent file system scanners, database scanners, and Windows/UNIX file system scanners that identify sensitive data at rest. Open DLP scan the systems for sensitive data such as social security numbers or credit cards. Other text item can be searched for such as an email addresses or a person's name using regular expressions..

There are two components to Open DLP:

- A web application to manage the Windows agents and scan results
- A Windows agent used to perform the scans It is possible to use Open DLP in an agent less mode, but the agent shifts the processing to the host instead of the server.

3.2 Data Loss Prevention (DLP) using Digital Rights Management (DRM)

DRM [3] provides controls which will limit third party who are outside the firewall from accessing data. Outsiders are prevented from printing or watermarking the data.

3.3 Cisco Security Agent's new Data Loss Prevention (DLP) feature

Cisco developed a method to provide security to Data in the network. Cisco Security Agent's new Data Loss Prevention (DLP) [4] feature is having many capabilities. It can classify

and tag the file based on the result of a content scan or its location on the host system, based on which applications attempt to read or write it. User is notified when he is working with content that is sensitive. The awareness of the presence of sensitive data will prevent accidental data loss.

The DLP feature allows CSA to tag files based on the types of file content, including specific characters or phrases. CSA also allows optimized pattern matching for credit card numbers and Social Security numbers which are subject to government regulatory control.

3.4 R-Crypto Data Security for windows

R-Crypto [5] is disk encryption software that protects the confidential information and personal data on a desktop, notebook, or a removable data storage device from unauthorized access. R-crypto creates a virtual disk that is encrypted. These disks provide encryption and decryption of data which is a real time process. This process will be fully transparent to user. The software uses the DES algorithm for encryption and decryption of data. The software has got limitations since DES algorithm can use only a predefined set of keys for encryption.

3.5 True Crypt Software

True Crypt Software [6] was released in 2009. This software was developed to encrypt the data using AES Algorithm. Entire hard drive or a storage device like USB can be encrypted and saved. On the fly encryption was used and data is encrypted just before it is encrypted and decrypted just after the data is loaded. This software rectifies the limitations of using DES Algorithm. This software uses an additional key file, without which the data cannot be decrypted.

3.6 Data Loss Prevention Using Ephemeral Key

Data Loss prevention using ephemeral key [7] was presented by William J. Blanke in 2011. This paper explains the way in which a data can be encrypted and can be transferred to a remote device. In this concept data is secured using an ephemeral key. When the data is transferred to another device, encryption occurs in the background. Using additional password entered by the authorised user, he can view the decrypted data. The ephemeral key that is randomly generated from the password provided will decrypt the data

4. Conclusion

Data Security can be provided by saving the data encrypted using On the Fly Encryption Using ephemeral Key. The data is stored secure by encrypting it using AES Algorithm. When the authorized user login he can view the decrypted data. The data is decrypted on the fly using the Ephemeral key generated along with the password entered by user when he logins. This paper presents a way of On the Fly encryption of Drives, storage devices and even downloaded email inbox.

5. Future Scope

In O-E-sis it is planning to provide full support for Windows 8 Operating System .In feature the ability to encrypt Windows system drives or partitions on the Unified Extensible Firmware Interface (UEFI) based computers (GPT) will be developed .Command line options for volume creation which already implemented in Linux and Mac OS X versions will be implemented in Windows Operating systems.

References

[1] S. Liu and R. Kuhn, “Data loss prevention”, IT Professional. Vol. 12, No. 2, pp. 10–13, 2010
[2] Data Loss prevention Using Open DLP by Andrew Gavin in available at http://www.maine.edu/pdf/DataLoss Prevention using Open DLP.pdf
[3] Data Security using Digital Rights management available http://www.locklizard.com
[4] Using Management Center for Cisco Security Agents 6.0 Volume 16,pp 1-25,2010
[5] R-Crypt Software available on the link :http://www.r-tt.com/data_security_software/
[6] TrueCrypt Software available on the link http://www.truecrypt.org/docs
[7] “Data Loss prevention Using Ephemeral Key” By William J. Blanke, Symantec Corporation, 2011.

Author Profile

Surya R Raj received the B. Tech Degree in information Technology from Kerala University, Trivandrum in 2010 and currently doing M. Tech. Degree in Information System Security.

Asha Cherian received the B. Tech degree in Computer Science Engineering from Mahatma Gandhi University, Kottayam, India and currently pursuing M. Tech Degree in Information System Security.

Abey Abraham got her M. Tech degree in Network and Intern from Karunya University, Coimbatore, India and is presently working as Assistant Professor at Rajagiri School of Engineering & Technology, Kochi, India.