International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 04 | Apr-2016 www.irjet.net p-ISSN: 2395-0072

Design and Implementation of Network based Key Management tool for Secure Drive Management

Vanitha M[1], Manjunath A E[2]

[1]*PG Scholar, Dept. of Computer Science Engineering, RVCE, Bangalore, India.*

[2]*Assistant Professor, Dept. of Computer Science Engineering, RVCE, Bangalore, India.*

Abstract - *Secure drive management can be the most important assets in day today world, since existing drives & data stored are more vulnerable to attacks. Few existing techniques provide security by locking and unlocking drives manually, maintain centralized key management server with or without standard protocols, where without standardized protocol would lead to incompatible services. To upgrade all existing procedures, the approach was proposed by developing self-encrypting drives along with locking and unlocking criteria using authentication keys, which were controlled at central repository using Key Management Interoperability Protocol. Since locking only can be easily hacked and encryption-only does not prevent access to data. Together by encrypting and locking, security can be enhanced. A self-encrypting drives provides hardware-based data encryption and uses Data Encryption Key for encrypting the user data on the drive, Data Encryption Key is generated by the drive and never leaves the drive. Self-encrypting drives are designed in such way that drives lock automatically on each power cycle and can be unlocked by end user using authentication key retrieved from enterprise server with respect to specific drive identifier. Temporary Locking/Unlocking of drive is in accordance with Trusted Computing Group specifications.*

Key Words: **Self-Encrypting Drives, KMIP protocol, TCG , SCSI protocol, Authentication Key.**

1. INTRODUCTION

Secure drive management is the most important assets in day today world, since existing drives & data stored are more vulnerable to attacks. A self-encrypting drive provides hardware-based data encryption, all of the data written to the storage medium is encrypted by the disk drive before being written and decrypted by the disk drive when it is read. All interface data passing between the host controller and the disk drive is in clear text and therefore, as far as read/write operations from the host controller are concerned, it's business as usual. The encryption engine is located between the drive's interface electronics and the data buffer (cache) so that all information which is temporarily at rest in the data buffer is encrypted [1].

SATA or SCSI protocols are used to communicate with the security drives.

A Self Encrypting drive can be a hard disk or a solid state drive that provides hardware-based data encryption. There is no hardware difference between a standard enterprise drive and an SED; however the SED does undergo a set of additional manufacturing procedures which configure the security features in the drive. Since all encryption is handled in hardware, there is a great performance benefit over software based encryption [2]. The Key Management Interoperability Protocol (KMIP) is a communication protocol describes message formats for the manipulation of cryptographic keys on a key management server.

Keys may be created on a server and then retrieved, possibly wrapped by other keys. Both symmetric and asymmetric keys are supported, including the ability to sign certificates. The Data Encryption Key (DEK) is used to encrypt all of the user data on the drive, generated by the drive and never leaves the drive. DEK key is stored in an encrypted format somewhere in the drive. When the DEK is changed or erased, no prior existing data in the drive can be decrypted.

2. LITERATURE SURVEY

Storage mechanisms were carried out using tape drives and standard enterprise drives, where no security configurations were applied to the data being stored and data were more vulnerable to the hackers and attackers easily. However on the process of implementing security strategies, few techniques were introduced to manually hard code the storage drives to lock & unlock [3]. Since hard coding the drives was a time and cost consuming mechanism, the centralized key management server was introduced where these drives can be locked and unlocked through the key which can be saved in a local common server and on each request can be accessed. In such scenarios of maintaining a centralized server, incompatibility occurs with systems communicating to the servers and hence service gets denied.

The key management interoperability protocol was introduced to overcome the incompatibility and provide an authenticated procedure to the central repository for

accessing the key. Key management interoperability protocol is a communication protocol that defines message formats for the manipulation of cryptographic keys on a key management server. Helps key be created on a server and then retrieved, possibly wrapped by other keys. Both symmetric and asymmetric keys are supported, including the ability to sign certificates. With this background, the approach was proposed by developing self-encrypting drives along with locking and unlocking criteria using authentication keys, which were controlled at central repository using key management interoperability protocol. Since locking only can be easily hacked and encryption-only does not prevent access to data. Together by encrypting and locking, security can be enhanced.

3. PROBLEM STATEMENT

Since existing drives & stored data is more vulnerable to attacks in the current day scenario, needs more secure way of storing and retrieving data. Standard enterprise drives can be easily stolen or hacked by hackers, which requires a more secure technology to safeguard the data being stored on the storage devices by either locking or unlocking drives with standard centralized server to manage the keys and by using a strong securitized drive like self-encrypting drives [4].

4. MOTIVATION

Self-encrypting drives with lock and unlock mechanism would provide strong security and integrated authentication. Proposed technique enables great performance benefit and prevents negative consequences of a data breach or loses, even if the physical drive is stolen or misplaced, the data on it remains protected against intrusion. As per Storage Industry Networking Association, efficiency at enterprise level could be 40%–70% range, depending on combination of RAID levels at greater than 1-to-1 data size-to-space consumed ratio, an efficiency rises, often to over 100% for primary data, and thousands of percent for backup data [5].

5. OBJECTIVES

The goal of using self-encrypting drives along with locking and unlocking mechanism is to ensure data security and authenticated access to drive, which in turn helps to achieve secure drive management. Development of dynamic library, which provide interface between a user application and self-encrypting drives supporting command features for secure drive management [6]. A dynamic link library file contains code and data that can be used by multiple programs at the same time, hence it promotes code reuse and modularization. DLL can be used as a base interface for all the applications accessing the particular hardware for which it is been designed.

6. PROPOSED APPROACH

In a generalized way, the following steps are been performed in the proposed system.
Step 1: Discovery of self-encrypting drive.
Step 2: Check status of drive
Step 3: if (Locked)
Search and return key.
Step 4: on success, unlock drive.
Step 5: Boot operating system.
Step 6: Continue operations on drive.

SEDs with lock and unlock mechanism would provide strong security and integrated authentication. Proposed technique enables great performance benefit and prevents negative consequences of a data breach or loses, even if the physical drive is stolen or misplaced, the data on it remains protected against intrusion. Self-encrypting drives prevents back doors.

6.1 Data Flow Diagram

The level 0 DFD generally called as the context level diagram shows the flow of data at the basic level. It mainly shows the interaction between the system and outside entity such as user. The level 0 DFD for secure drive management is as shown in figure 1. In this level, there are three entities user application, secure system and Request/Response channel.

Figure 1: Level 0 DFD

Level 1 DFD divides the entire system into smaller sub modules or processes, where each module takes data from one or more sub modules, processes it and gives to next sub module for further processing. This flow together provides description of all the functionalities of the system as a whole. The level 1 DFD for secure drive management is as shown in figure 2. In this level, the “Secure System” in level 0 DFD is decomposed into two parts.

The first part is Host system with an SED and the second part is key management software. The user communicates to the drive using TCG specifications and SCSI system calls.

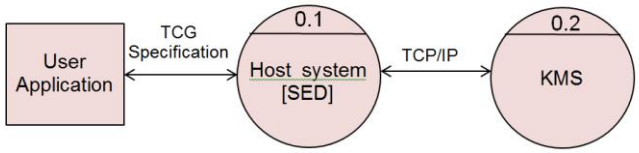

Figure 2: Level 1 DFD

Level 2 DFD divides the sub modules or process into greater detail. Level 2 DFD's are defined only when the Level 1 process is more complex and not able to bring out complete details of each complex modules which is necessary for the analysis.

The level 2 DFD of secure drive management is as shown in figure 4.3. Here both the models that are represented in Level 1 DFD are broken into smaller modules and their interaction is depicted in the Figure 3.

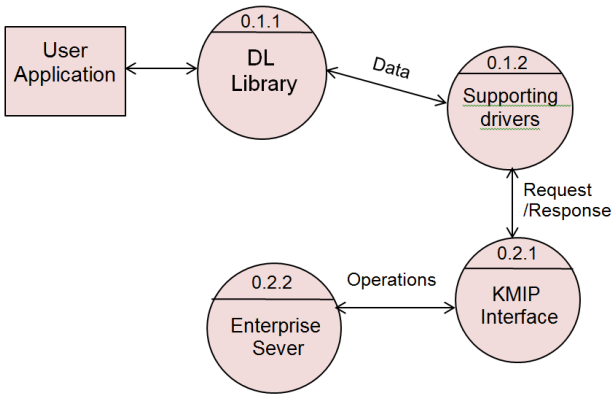

Figure 3: Level 2 DFD

The KMS is broken down into two modules namely supporting driver and library. The libraries would provide an interface for user application and disk drives. The host system with SED entity in the Level 1 DFD is broken down into two modules KMIP interface and enterprise sever entities, where interface would support the current operations like create, delete, enquire of key and enterprise server would store the key.

7. EXPERIMENTAL RESULTS

Evaluation metrics is one of promise technique to capture the size and quality of products, development process in order to assess a software development. Many software metrics based on various aspects of a product and/or a process has been proposed. There is some research which discusses the relation between software metrics and faults to use these metrics as the indicator of quality. Most of these software metrics are based on structural features of products or process information related to explicit fault.

Evaluation metrics are used to obtain objective reproducible measurements that can be useful for quality assurance, performance, debugging, management, and estimating costs.

The drives with security strategies are tested with following common criteria for all the use cases
1. Drive is tested on Ubuntu machines and windows.
2. 800GB SEDs are usually used.
3. Device/Host machine should be enabled with Internet.
4. Drive is dependent on Controller to connect to Key management server
5. Testing is done with power bricks.
6. SEDs can be individually used or in array within controller but would be preferred to use within controller or enclosure.

The power consumption has become an important design parameter for battery operated, portable and embedded systems. Since the amount of power available to these systems is limited, it is desirable to have the power consumption as low as possible. This provides the performance scores of secure drive management with frequency threshold and without frequency threshold.

8. CONCLUSIONS AND FUTURE WORK

The approach of developing self-encrypting drives (SED) along with locking and unlocking criteria using authentication keys, which were controlled at central repository using Key Management Interoperability Protocol, enhanced the level of security with encryption and locking criteria. Since locking only can be easily hacked and encryption-only does not prevent access to data.

SEDs are designed in such way that drives lock automatically on each power cycle and can be unlocked by end user using authentication key retrieved from enterprise server with respect to specific drive identifier. Temporary Locking/Unlocking of drive is in accordance with Trusted Computing Group specifications.

Dynamic link library has to be built to provide an interface between a user application and SEDs with supporting operations like Discover Drive, Drive Locking and unlocking…Etc. SATA or SCSI protocols are used to communicate with drives.

SEDs with lock and unlock mechanism would provide strong security and integrated authentication. Proposed technique enables great performance benefit and prevents negative consequences of a data breach or loses, even if the physical drive is stolen or misplaced, the data on it remains protected against intrusion.

REFERENCES

[1] Nobayashi, Daiki, "Development of single sign-on system with hardware token and key management server", IEICE TRANSACTIONS on Information and Systems 92.5, Vol.E92-D No.5, 2009, pp.826-835.

[2] Muller, Tilo, and Felix C. Freiling, "A Systematic Assessment of the Security of Full Disk Encryption", IEEE Transactions on 12.5, Erlangen-Nuremberg, Germany, 2015, pp. 491-503.

[3] Joyashree, and Subir Kumar Sarkar, "Implementation of a Key Distribution Server Based Data Security Scheme for RFID System", Advanced Computing & Communication Technologies (ACCT), Fifth International Conference on. IEEE, Haryana, India, 2015, pp. 581-585.

[4] Santa, Jose, et al, "A framework for supporting network continuity in vehicular ipv6 communications", Intelligent Transportation Systems Magazine, IEEE 6.1, Murcia, Spain, 2014, pp.17-34.

[5] Lei, Sun, Dai Zishan, and Guo Jindi, "Research on key management infrastructure in cloud computing environment", Grid and Cooperative Computing (GCC), 9th International Conference on. IEEE, Chicago, 2010, pp. 404-407.

[6] Murali, Krishnamurthy, "Secure communication using a chaos based signal encryption scheme", Consumer Electronics, IEEE Transactions on 47.4 , Calgary Univ., Alta., Canada, 2001, pp. 709-714.

[7] Abd El-Aziz, and Ajaykumar Kannan, "JSON encryption", Computer Communication and Informatics (ICCCI), 2014 International Conference on IEEE, Coimbatore, 2014, pp.1-6.

[8] Sanyal S, " SPIKE: A novel session key management protocol with time-varying secure cluster formation in wireless sensor networks", In Privacy, Security and Trust (PST), Eleventh Annual International Conference, Tarragona, IEEE publication, July 2013, pp. 151-160.

[9] Chung, H. H., Wang, P. S., Ho, T. W., Hsiao, H. C., & Lai "A secure authorization system in PHR based on CP-ABE", in E-Health and Bioengineering Conference (EHB), Iasi, IEEE publication, 2015, pp. 1-4.

[10] Wei-min, L., Run-Sheng, W., & Jian-qiu, "A simple key management scheme based on WiMAX", in Computer Science and Computational Technology, ISCSCT'08, International Symposium in Shanghai, IEEE publication, Vol. 1, 2008, pp. 3-6.

[11] Nobayashi, D., Nakamura, Y., Ikenaga, T. and Yoshiaki, H.O.R.I., "Development of single sign-on system with hardware token and key management server", IEICE TRANSACTIONS on Information and Systems, 92(5), in Cap Esterel, 2009, pp.826-835.

[12] Shantharajah, S. P., Duraiswamy, K., & Kadhar Nawaz, G. M, "Key management and distribution for authenticating group communication", in Industrial and Information Systems, First International Conference in Peradeniya , IEEE publication, 2011, pp. 133-137.

[13] Chou, K. Y., Chen, Y. R., & Tzeng, W. G, "An efficient and secure group key management scheme supporting frequent key updates on pay-tv systems", in Network Operations and Management Symposium (APNOMS), IEEE, 2011,13th Asia-Pacific, pp. 1-8.

[14] Labiod, H., & Duffau, R. "KMS: a key management system for multi-provider interconnected Wi-Fi WLANs", in Global Telecommunications Conference, GLOBECOM'04, IEEE, 2004, Vol. 4, pp. 2061-2066.