2011 International Conference on Computer Science and Information Technology (ICCSIT 2011)
IPCSIT vol. 51 (2012) © (2012) IACSIT Press, Singapore
DOI: 10.7763/IPCSIT.2012.V51.51

SAN Data Encryption System on iSCSI

Xu Xuedong [a +], Sun Wei [a] and Li Muyuan [b]

[a] Changchun institute of Technology, Changchun 130012, China

[b] Technology Department Changchun E-sun Software Co., ltd, , Changchun 130012, China

Abstract. To protect the static data in SAN, this paper proposed and realized a SAN storage and encryption system based on iSCSI by encrypting the SAN disk static data, which realized a flexible security management strategy by multiple-key and multiple layer encryption system to project the physical resources through iSCSI protocol stack and virtualization technique. Besides, as it has optimized iSCSI's function through RC aggregation cache data pack and this system is proved to function well in simulation test. This system is as good as or better than other products in this line on the international market, by saving about 10% of the conversation expenditure.

Keywords: IP SAN, Static Data, ISCSI, Encryption

1. Introduction

As a vital capital in this information age, data's storage becomes the core of its values in the information system. According to the survey by CSI and FBI in USA, about 80% of attacks are directed at the static data[1]. Thus, the encryption disk and encryption data techniques develop quickly as more attention has been given to the techniques of encryption of static data.

With the network storage technique, here is also a problem for the data storage. Recently, information system storage devices at enterprise level have changed from DAS frame into storage area network (SAN) or network-attached storage (NAS), in which the access interface at block level has solved the problem of non-merging of NAS files interface across the networks and realized the needs of mass storage. SAN comprises FC SAN and IP SAN. As the latter employs optic fiber technique which provides better speed and flexibility but higher price and lower mutual operation. It easily becomes an isolated information island.

IP SAN, having developed from iSCSI technique, is a storage technique for data exchange through IP protocol on Ethernet. It is a step towards universalization of net storage, a direction of future development of SAN generally believed[2]. However, the storage system exposes itself to great risk of being attacked as it connects itself to Ethernet. Thus the storage encryption technique and its products for IP SAN become an urgent focus for study.

This paper, based on SecureSAN, a storage encryption system at SAN files level, proposed a protection for the disk static data in IP SAN. The system realized the data stream control at backend through virtualization of storage device and host computer. We have realized complete transparency of customers through the iSCSI protocol stack, and parsing of business data in IP data package. This system encrypts the SCSI commands and files as a whole, in which all the data in the storage are encrypted, making the data useless even the disk is stolen. With the key deleted, the data is useless minimizing the physical damage to the disk from formatting it.

2. ISCSI TECHNIQUES

[+] Corresponding author. Tel.: +86-0431-8701-4003; fax: +86-0431-8511-2886.
E-mail address: xuxuedong100@yahoo.com.cn.

2.1. The Mechanism for iSCSI

iSCSI is a SCSI protocol expanded by IMB as small computer system interface to overcome the shortcoming shorter distance transmission and fewer connection equipments. It could be realized on IP network and route selection on Ethernet. It realized a seamless connection between storage and network by combining the two protocols of SCSI and TCP/IP. iSCSI storage network will reach or surpass the band width and functions on FC network as the gigabit ethernet becomes more popular[3].

iSCSI is an end-to-end protocol, operates between the host computer (as the initiator) and storage equipment (as the target). iSCSI realizes data packaging and transmission between the two ends by starting from host computer to storage equipment. The mechanism is to package SCSI commands by TCP/IP in order to control the information, parameters and data, and forms the protocol data unit (PDU) to transmit them on the IP network[4].

2.2. iSCSI Protocol and Its Workflow

iSCSI protocol comprises iSCSI naming and addressing iSCSI, iSCSI dialogue, iSCSI fault-tolerance, and iSCSI security[5]. iSCSI equipment's name is used for ID authentication at the sending end and target end. During the logging on, iSCSI dialogue establishes a TCP connection, and ID authentication at both sending end and target end. It negotiates parameters for the dialogue and tags the TCP connections belonging to the dialogue. SCSI commands and data would be packaged into iSCSI PDU, which is sent to the target by iSCSI dialogue. iSCSI fault-tolerance detects and restores any erroneous PDU. iSCSI security mechanism comprises IPsec and ID authentication within the band.

iSCSI protocol is in fact a process of packaging data and unpackaging the data packs on the network. Data packs are packaging in three parts: IP head, iSCSI recognition packs and SCSI data. When received at the receiving end on the network, the data unpacks into the three parts in sequence. First, SCSI adapter card on the iSCSI system sends a SCSI command, packed as an information pack at the third layer. And the receiving end extracts the commands and execute them. Then the SCSI commands and data to be returned are packed into an information pack to be sent back to the sending end. Finally the system extracts data or commands and sends them to the sub-system in the SCSI[6]. All the process is transparent needs no intervention at the end customers.

3. THE DESIGN OF SECURESAN SYSTEM

The SecureSAN is defined as storage encryption system at the corporate level. Typical BBD uses backend encryption mode, and connects SecureSAN directly to IP exchange, through which it directs the data from frontend to SecureSAN. After being encrypted by SecureSAN, they are sent to the storage equipment. The system is transparent for the frontend user.

3.1. Application Model

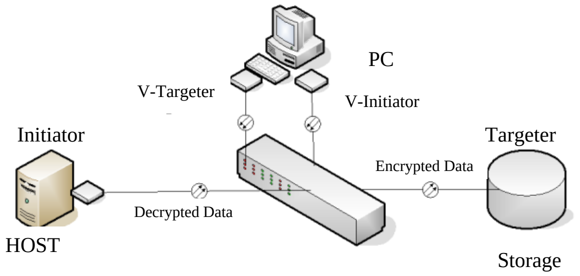

Fig. 1. SAN application model based on secureSAN.

The SAN Application Model Based on SecureSAN is shown as in Figure 1, comprising host computer and storage equipment. The SecureSAN is based on Linux system. With two network cards, one set at the V-Target mode and the other set at the V-Initiator mode. Both of the two network cards are controlled by the drivers compiled by ourselves. By data encryption and conversion, we have realized transparency at the user's backend storage equipment, and data at the backend is in plain text and data in the storage equipment is encrypted.

All the data stream passes through SecureSAN. The data at the V-Target end is in plain text and the data at the V-Initiator end is encrypted. The data is encrypted with the SM4 encryption algorithm approved by State Cryptography Administration. The key is stored in the SecureSAN, which is managed through Web management interface and command lines.

3.2. The Design of the General Frame

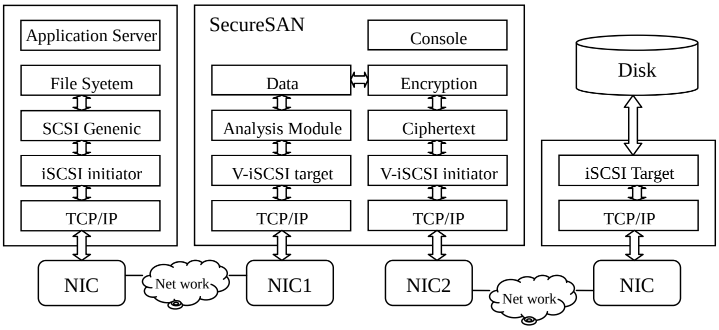

Fig. 2. The General SecureSAN Frame.

SecureSNA is realized through the software in Linux environment, as shown in Figure 2, which comprises:

- Driver in the host computer: The iSCSI Initiator driver is installed in the host computer, which, together with SCSI drivers with the system, realizes the packaging of the SCSI commands and data into PCT/IP packs, and send the requests to target equipment of the Ether network.
- SecureSAN function software: The data and encryption function software for iSCSI protocols in Linux environment is developed by ourselves, comprising V-iSCSI target at the target end, V-iSCSI initiator at the vitalizing initiator end and encryption module. The process is that V-iSCSI target monitors the data released by the iSCSI initiator. It receives data packs after establishing the dialogue. Through the parsing of iSCSI data (including the unpacking and separating of the data), it send them to the IO modules at the server kernel for encryption to be packed encrypted by V-iSCSI initiator and encryption software.
- Driver software at the storage end: The PPD iSCSI target monitors the released packs by V-iSCSI initiator and authentication, and starts dialogue on receiving the request for dialogue, processes the data packs and stores the data on the disk.
- Console software: It is used to configure SecureSAN, to form storage strategy, to supervise customers, the management of keys and other functions.
- SecureSAN restoring strategy software: It comprises the management of expiration of the key and decryption software of the data etc. It is used to restore the encrypted data to plain text when the system is crashed.

4. Core Technique in the System

4.1. The Encryption and Decryption System in SecureSAN

To lower the risk of misconduct and leakout by insiders, SecureSAN adapts a management strategy of “Power Sharing”. We have designed a multi-level encryption system with keys in many categories for data encryption at customer’s end through SM4 encryption card. The keys comprises start key, management key, restoring key, local key and base key (as shown in Table I).

Table 1. System key categories

Categories	Type	Uses
Start key	Asymmetrical	System starts key, protecting management key at two levels.
Management key	Asymmetrical	System management key, restoring and decrypting keys.
Restoring key	Symmetrical	Encryption key for local key, protected by key encryption.
Local key	Symmetrical	Encryption key for base key, protected by restoring key.
Base key	Symmetrical	Data encryption key, protected by local key

Encryption Processing Flowchart is shown in Figure 3.In the encryption and decryption system, data is encrypted in the storage processors and sent to the storage equipment. The base key generates a K1 through encryption by local key, which generates K2 through decryption restoring local key, which generates K3 through decryption by restoring key, which generates T through primary start key. Secondary start key encrypts T into TT. The K1, K2, K3, T and TT together are stored in the parameters databank of SecureSAN.

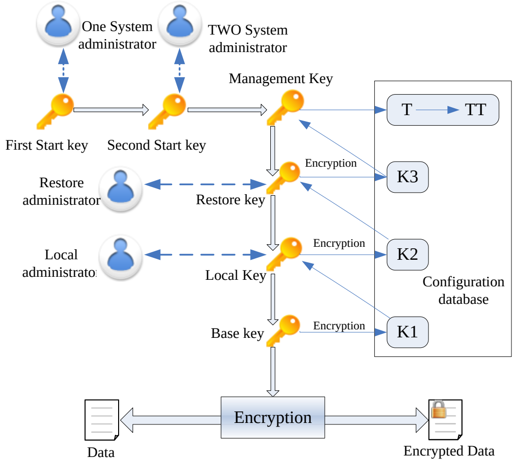

Fig. 3.Encryption Grade System in SecureSAN.

In this encryption system, the emphasis of protection is that the password stored in the key rather than in the data, in the base key is encrypted at multiple layers. This disperses the management power and lowers the risk of leakout and simple the steps of data encryption but with better functions.

4.2. Virtualization Management in SecureSAN

To filter by-pass data in the SecureSAN, a management of the virtualization of host computer and storage equipment in SAN is necessary. First, a V-storage is virtualized in Secure SAN with a virtual IP address, which is bound with the host-side NIC at the customer’s end port. It monitors and receives the packs from the host computer iSCSI initiator. After it parses and encrypts the iSCSI data packs, it establishes a client virtual host in SecureSAN with virtual IP address, which is bound with storage-side-NIC at the storage end for packaging and releasing of the encrypted data on these mapping relations between the virtual host IP and host IP.

A user-level library and two loadable Linux kernel modules were developed to realize the above process. Through the address mapping table, the virtual address is translated into the physical address recognizable by net card for the sequential process of data packs.

4.3. The Optimization of Cache on RAM

We found that the size of data in iSCSI influences the transmission and small size of data lowers width performance of the network[7]. A better performance of iSCSI is realized with a plan of aggregation data packs by cache technique.

A space is opened up in the system non-paged pool, and two-layer structured RC cache is created though a log disk Small data packs are collected in the pool thus created and the data is written in the log disk with the advantage of fast reading and writing of log files system. Thus large log files are formed and sent to the storage system at the far end. This plan is proved to have increased transmission efficiency by 20%.

5. Evaluation of SecureSAN's Functions and Performances

Typical SAN storage encryption products on the market are those by DataFort in three series (E, FC and S), supporting IP network, optical channels and SICI bus respectively. Its technique is a commercial secrete and expensive. In comparison, DataFort is similar in function, but cheaper and flexible in safety strategy.

To evaluate its performance, we have set up the simulation test on following configuration: the SecureSAN is deployed on a PC server (with CUP of Intel Xeon Processor X3430 4 Core, RAM of 2GB, data ports of two 1000Mbps Ethernet NIC, a management ports of a 10/100Mbps Ethernet NIC) on the system of RedHat8.0 with Apache, SCSI card of double-channel Adaptec AIC-7889 Ultra160, disk-array of 4-digit SCSI disks (Seagate ST336607LC, 36.2GB) of total volume of 4*36.2GB.

PostMark was used to evaluate the capacity of the system, and Iometer developed by INTEL was used to evaluate the response time and conversation expenditure. Here we regarded the conversation success rate as the units of conversation expenditure, which reflected the utilization rate of cache and the potentials of the system.

Table 2. SecureSAN performance test

I/O Mode	Data Block Size	Concurrent Process	Data Transmission rate	Average Response time	conversation expenditure
Sync	8KB	16	64MB/S	5.6ms	90%
Sync	16KB	16	60MB/S	8.9ms	86%
Sync	32KB	32	54 MB/S	16.9ms	88%
Sync	64KB	32	50 MB/S	35.2ms	84%

As shown in Table Ⅱ.It is proved the in the test that the capacity of SecureSAN and transmission efficiency and average response time of the data functioned well. conversation expenditure more than 84%, by saving about 10% of the conversation expenditure.

It is found from the technical documentaries that Datafort is gateway-product based on software and with better functions. DataFort optimized specifically the hardware in the aspects of cache, parallel processing numbers with data transferring rate at 200MB/S and average response time at less than 2 ms. It is estimated from our experience that the optimized hardware could have its performance increased by 1-2 times. Considering the conversation expenditure of SecureSAN, it is reasonable to believe that SecureSAN is expected to be as good as or better than DataFort Products.

6. Conclusion

This paper has analyzed the iSCSI protocol and technique and proposed a new storage encryption system of SecureSAN on iSCSI. The design realized an iSCSI protocol stack and the encryption of SAN static data on SM4encryption card. It differs itself from the common encryption disk or encryptor in its adaptability of SAN secure storage, the end-to-end security between host computer and storage equipment, transparent connection with the network, and maximum protection of the customer's investment. In the future, we shall optimize this software system realized in Linux system and its related hardware, and develop special SAN encryption equipment for the market, which is at present dominated by the techniques and prices of foreign corporations.

7. Acknowledgements

The authors would like to thank Professor Yao Nianmin From Harbin Engineering University for kindly sharing his dataset with us.The work was supported by "Fund for Electronic Information Industry Development (No. IIMF [2009]453)";"Jilin Science and Technology Support Plan (No. 20090312)"; "Changchun Science and Technology Plan (No. 09KT21)";"The 12th Five Year Planning by Jilin Education Bureau(No. 2001[238])".

8. References

[1] ROGERW Future hard disk drive systems[J] Journal ofMagnetism andMagneticMaterials, 2009, 321(6): 555–561

[2] David Lie, John Mitchell, Chandramohan A. Thekkath, Mark Horowitz. Specifying and Verifying Hardware for Tamper-Resistant Software. Symposium on Security and Privacy, 2003, pp.166-177.

[3] Suh, D. Clarke, B. Gassend, M. van Dijk, and S. Devadas. Efficient memory integrity verification and encryption for secure processors. The 36th International Symposium on Microarchitecture, pp. 339-350, 2003.

[4] Gregory R. Ganger, Pradeep K. Khosla, Mehmet Bakkaloglu, et al. Survivable Storage Systems. DARPA Information Survivability Conference and Exposition, Anaheim, CA, IEEE, Vol.2, June 2001,pp.l 84-195.

[5] M. Blaze. A cryptographic file system for unix. In 1st ACM Conference on Communications and Computing Security, 1993, pp.9-16.

[6] Ethan L. Miller, Darrell D. E. Long, William E. Freeman, and Benjamin C. Reed. Strong security for network-attached storage. In Proceedings of the 2002 Conference on File and Storage Technologies (FAST), Monterey, CA, January 2002, pp. l 一 13.

[7] Jonathan Corbet,Alessandro Rubini,Greg Kroah-hartman. Linux Drivers.3rd edition[M]. American:O’Reilly,2005.pp:458-482

[8] WANG Jun, YAO Xiao-yu, CHRISTOPHERM, et al A NewHierarchicalData Cache Architecture for iSCSI Storage Server[J] IEEE Transactions on Computers, 2009, 58(4), 433-447

[9] ROBERT L,GU Yun-hong,MICHAEL S, et al Computer and storage clouds using wide area high performance networks[J]. Future Generagtion ComputerSystems, 2009, 25(2): 179-183