Lustre Security Mechanism: Models, Schemes and Research based on PKI

Liu Su-qin, Li Xing-sheng, Shuo Jun, Wang Jing, Liu Hui-hui
College of Computer and Communication Engineering
China University of Petroleum
Qingdao, China
liusq@upc.edu.cn

Abstract—**Lustre file system can improve I/O throughput in the clusters effectively, but there still be some security problems in TCP/IP network environment, such as identity theft, data interception, data modification and replay-attack. Lustre is planning to use Kerberos security mechanism which can not solve some problems in enterprise-wide, such as overhead, digital signature and password attack. To the problems, this paper presents a security model for Lustre based on PKI. The model includes a certificate management module and a client access module. Certification management mechanism based on PKI is adopted in the certificate management module. Bidirectional identity authentication and digital signature are applied in the client access module. Random number must be checked during authentication. The security model can reduce safety loopholes and enhance security in Lustre file system, such as identity theft, data interception, data modification and replay-attack.**

Keywords-Lustre; Kerberos; PKI; security; bidirectional identity authentication; digital signature

I. INTRODUCTION

In academia and industry, many research projects were developed to improve the performance of the I/O subsystems in HPCS (High Performance Computing System). Parallel filesystem is an important research topic. The global parallel file systems that are object-based offer many advantages in scalability, availability and performance. They can play an important role in the storage management system of HPCS, and Lustre file system is a typical representative of them. Lustre optimizes large files read/write. It can provide high-performance I/O throughput, global data sharing space and the independence of the data storage location. Lustre can also greatly improve the reliability, scalability and parallel access capability of cluster system. However, when Lustre transmits data through TCP/IP network, the data faces many kinds of threats from the Internet. The security problems limit the application of Lustre to some extent. So it is necessary to design an effective security mechanism according to Lustre's characteristics to improve the safety of Lustre storage system.

II. LUSTRE FILE SYSTEM AND ITS SECURITY PROBLEMS

A. Lustre Filesystem

There are three important components of Lustre: MDS (Metadata Server), OST (Lustre Object Storage Target) and Client [1-3]. The structure of Lustre is shown in Fig. 1.

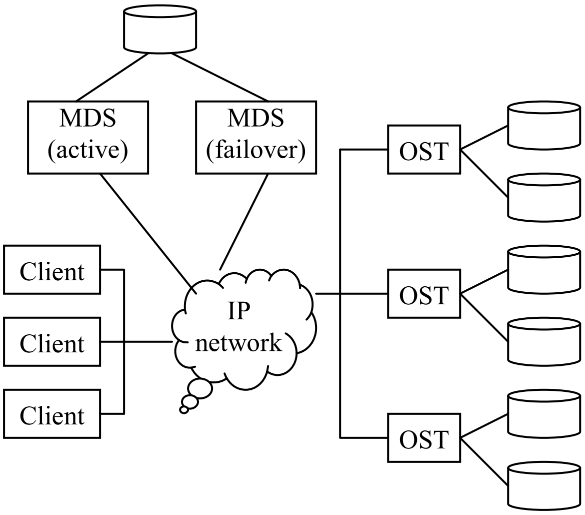

Figure 1. Compose of Lustre file system

MDS is mainly in charge of managing metadata. Metadata is "data about data". It contains the attributes of files & directories and other relevant information including files' and directories' creating time, access time, status information, the distribution and addresses of real data, the mount point information of other file systems, the information of symbolic link files, etc. Metadata is stored on a group of MDSs.

OST is mainly in charge of managing real data. The OSTs store file data as objects and directly interface with object-based disks (OBDs). The storage is physically located on underlying OBDs. The interface services that OST provides include data block allocation, lock management, parallel I/O, storage network optimization, storage policy management, etc.

978-1-4244-5874-5/10/$26.00 ©2010 IEEE

Client provides users with access to the filesystem. Users visit the whole filesystem through standard POSIX interfaces. Clients implement metadata interaction with MDSs and file data interaction with OSTs.

B. *Security Problem of Lustre*

For a data accessing, Client requests file metadata from MDS, and then Client sends the corresponding operation commands to OST directly via network. Finally data will be directly transmitted between Client and OST. In such an access process, Lustre has some security risk as below [4]:

(1) Identity theft: Attackers masquerade as Clients to obtain users' data from OST as well as masquerade as OSTs to let Clients store large-scale data in the storage location specified by the attackers.

(2) Data interception: Attackers could use network monitoring technology to intercept the data transferred on the transmission channel between Clients and OSTs.

(3) Replay-attack: Even if the whole storage system has a certain authentication mechanism, attackers could still defraud the data of the storage system by intercepting and resending the authentication data.

At present users and enterprises are increasingly concerned about the safety performance. If the security problems of Lustre can't be solved, it will severely affect its applications.

III. Network Security Mechanism Analysis

At present, the popular security mechanisms for distributed network are Kerberos and PKI (Public Key Infrastructure).

A. *Kerberos*

In Lustre development plan, Kerberos is chosen to enhance the level of system security. Kerberos is a service which is applied to distributed network environment. It builds on symmetric cryptosystem and provides mutual authentication -- both the user and the server verify each other's identity [5-7]. As one kind of widely used security mechanisms, Kerberos has significant advantages. Kerberos offers authentication, confidentiality and integrity to enhance security. It is relatively well standardized, supports single sign-on and provides good interoperability in the same implementation. However, Kerberos has some drawbacks, as listed below:

(1) Kerberos uses symmetric algorithm as the foundation of the protocol. This strategy brings some difficulties such as the exchanging, storage and management of keys and requires lots of management time and resources, which is often unbearable for large organizations.

(2) The digital signature policy is not applied to Kerberos, and thus it can't provide non-repudiation mechanism.

(3) Kerberos can not provide effective defense against password-guessing attacks.

(4) Kerberos uses timestamp to prevent replay attacks. The system default maximum delay time is 5 minutes, which means that the replay attacks during this time can not be found.

B. *PKI*

PKI is a universal security infrastructure which uses asymmetric algorithm principles and techniques to provide security services [8, 9].

A PKI system mainly includes EE (End Entity), CA (Certification Authority), CR (Certificate Repository), CRL (Certificate Revocation List), RA (Registration Authority) and X.509 digital certificate, which is shown in Fig. 2.

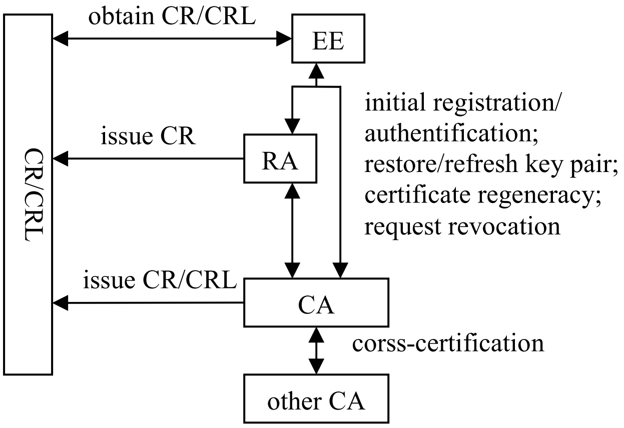

Figure 2. Compose of PKI

PKI implements secure transmission by providing authentication, security and confidentiality. PKI can also provide the function which Kerberos doesn't have, that is, non-repudiation. Compared with Kerberos, PKI has obvious advantages in the following areas:

(1) Management time and resources: Comparing with Kerberos, PKI provides more flexible management mechanisms, which could apparently lighten the management burden on system. The capability of PKI's key management is better than Kerberos and other security solutions. PKI's management functions include certificate validity and revocation, key backup and recovery, non-denial of digital signature, automatic key authentication, management of certificate and key history, time stamp, cross-certification, etc. These features make PKI perform much better than Kerberos in enterprise-wide.

(2) Certificate repository: The certificate repository based on LDAP or OCSP could effectively handle a large numbers of requests, which allows PKI to extend safely.

(3) Digital signature: PKI allows user to sign the data and messages using his private key.

(4) PKI also offers great advantages in scalability, transparency, etc.

Based on the above analysis, PKI is chosen to build the security model of Lustre in this paper.

IV. Lustre Security Model Based on PKI

A Lustre security model based on PKI is designed in this paper, which is shown in Fig. 3. This model includes two sections: the certificate management module and the user access module.

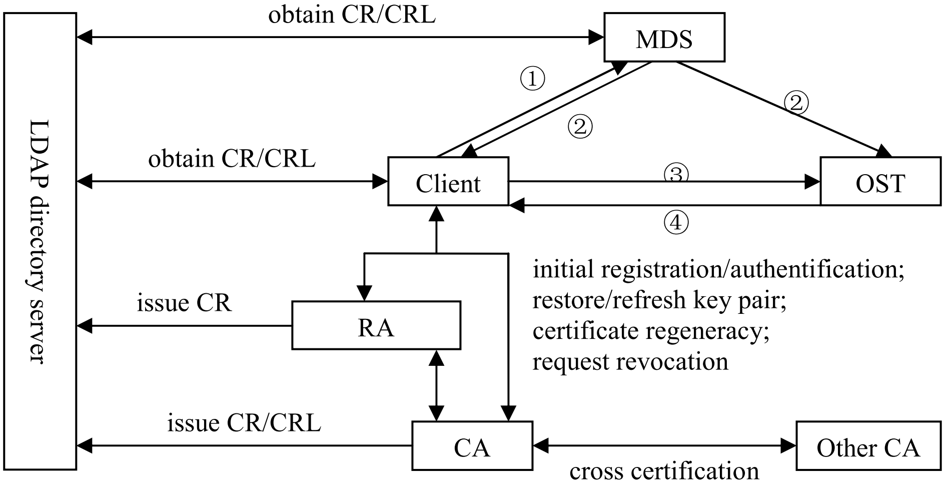

Figure 3. Security model for Lustre

A. Certificate Management

1) Certificate application

Users can't visit the Lustre file system when they have not applied for certificates, so the first step is to apply for certificates to CA. In details, the process includes four steps:

a) Step one: A user submits a certificate application request to RA and RA verifies it;

b) Step two: RA submits the certificate application that has been verified to CA;

c) Step three: CA generate a certificate for the user and registers it in CR. At the same time, CA will call the corresponding components to generate a public-private key pair for the user;

d) Step four: CA gives the certificate and the private key to the user through some kind of approach (for example, out-of-band approach).

B. User Access

It uses two-way authentication which X.509 provides when users communicate with MDS and OST. Random number testing is added to the authentication in order to prevent man-in-the-middle attack. It uses asymmetric encryption mechanism when transmitting request and authentication information. Considering the cost and speed of the algorithms, symmetric encryption mechanism is used when transmitting large amounts of data.

The model shown in Fig. 3 is based on the following assumptions: MDS and OST have already obtained certificates and recorded in CR before user access. Due to OST being managed by MDS in actual system, it is assumed that there is a pre-shared key K_{MT} between MDS and OST. The detailed descriptions of each part of user access are as follows regarding Fig. 3.

① User submits an access request to MDS

- Client generates a non-repetition random number R_C. R_C must be unique within the packet validity. MDS stores this random number until it expires and will reject all the packets which contain the same random number during the packet validity;
- Client generates m= $\{T_C, R_C, I_M, d\}$. T_C is a time stamp which includes an optional generating time and deadline, I_M is a marking that indicates the receiving end, d is the request information that notes the wanted data;
- Client carries on the signature with its own private key to m to generate $D_C\{m\}$;
- Client encrypts $\{C_C, D_C\{m\}\}$ with the public key of MDS to generate the ciphertext E_{CM} and sends it to MDS. C_C is the certificate of Client.

② MDS authenticates Client and sends the authentication information to Client and corresponding OST.

- MDS decrypts E_{CM} with its own private key to obtain $\{C_C, D_C\{m\}\}$;
- MDS authenticates C_C to get Client's public key PK_C;
- MDS verifies the signature $D_C\{m\}$ with PK_C;
- MDS checks the marking I_M in m;
- MDS checks T_C to confirm whether T_C is within the specified value;
- MDS checks R_C and compares it with the R_C in the library to confirm that it is not re-used;
- MDS generates the list L_T of target storage devices for users according to the request information, including the IP address IP_T and port number $Port_T$ of each device;
- MDS generates a random number R_M;

- MDS generates m={T_M, R_M, I_C, L_T};
- MDS carries on the signature with its own private key to m and generates D_M{m};
- MDS encrypts {C_M, D_M{m}} with PK_C to generate the ciphertext E_{MC} and sends it to Client. C_M is the certificate of MDS;
- MDS encrypts the information such as the certificate of Client and so on with K_{MT} to generate E_{MT} and sends it to the corresponding OST.

③ Client sends data access request to the corresponding OST.

- Client authenticates MDS (the method approaches to the authentication part of step ②);
- Client generates the ciphertext E_{CT} (the method approaches to step ①);
- Client sends E_{CT} to the corresponding OST according to IP_T and $Port_T$ of L_T.

④ OST authenticates Client and transmits data to it.

- OST decrypts E_{MT} with K_{MT} to obtain the certificate of Client;
- OST authenticates Client (the method approaches to the authentication part of step ②);
- OST generates random symmetric key K_{TC};
- OST encrypts the transmitted data with K_{TC} and generates the ciphertext E_{TC};
- OST encrypts {C_T, D_T{T_T, R_T, I_C, K_{TC}}} with Client's public key and generates K(K_{TC}), C_T is the certificate of Client;
- OST carries on the signature with its own private key to the transmitted data and generates E_T;
- OST puts E_{TC}, K(K_{TC}) and ET into a digital envelope and sends it to Client.

V. CONCLUSION

Lustre file system could eliminate the I/O bottleneck problem in high performance computing, while there are certain security risks. In this paper, a security model is designed with PKI according to Lustre's characteristics. The model has the following security features:

(1) Preventing identity theft: All users must apply for certificates before they visit Lustre. MDS and Client, OST and Client must undergo a two-way authentication to ensure the legitimacy of the identity.

(2) Preventing data interception: Real data is encrypted with a random symmetric key and then encrypted with the recipient's public key before being transmitted to ensure data security. Because the stealer doesn't have the recipient's private key, even if the data is stolen during transmitting, attacker can't get the random symmetric key which making it impossible to steal data.

(3) Preventing data modification: Digital signature technology is used in data transmitting which could effectively prevent distorting data.

(4) Preventing replay attacks: The random numbers are disposable and can effectively prevent replay attacks.

REFERENCES

[1] Yang Xin and Shen Wen-hai, "The Evolution of Lustre File System and the Perspective of Application to the Meteorology Filed," Journal of Applied Meteorological Science, vol 19, pp. 243-249, Apr. 2008(in Chinese).

[2] Dong Yong, Zhou En-qiang and Chen Juan, "Infiniband-based High-Performance Distributed File System-Lustre," Computer Engineering and Applications, vol 41, pp. 103-107,228, Aug. 2005(in Chinese)

[3] Jeremy Logan and Phillip Dickens, "Towards an Understanding of the Performance of MPI-IO in Lustre File Systems," Proceedings of the 2008 IEEE International Conference on Cluster Computing, IEEE Press, pp. 330-335, Oct. 2008.

[4] Chang Xing-hua, "Security Model Design for Lustre Storage System," Information Security and Communications Privacy, pp. 80-82, Apr. 2008(in Chinese).

[5] Huang Jian-hua and He Xi, "Improvemnet of Kerberos Agreement Based on Dynamic Password System", Computer Security, pp. 66-69, Feb. 2009(in Chinese).

[6] Frederick Butler, Iliano Cervesato, Aaron D. Jaggard, et al, "Formal Analysis Kerberos 5," Theoretical Computer Science, vol 367, pp. 57-87, Nov. 2006.

[7] Fan Hong-sheng, Ye Zhen and Hou Bao-hua, "Improvement of Kerberos Protocol Based on Public Key Cryptosystem," Computer Technology and Development, vol 16, pp. 224-227, Apr. 2006(in Chinese).

[8] He Yun-ting and Zhang Zong-fu, "Reserch on Confident File Transfer Based on PKI," Computer Knowledge and Technology, vol 3, pp.885-887, Aug. 2008(in Chinese)

[9] Ali Nasrat Haidar and Ali E. Abdallah, "Formal modelling of PKI Based Authentication", Electronic Notes in Theoretical Computer Science, vol 235, pp. 55-70, Apr. 2009.