文章编号:1673-5005(2009)05-0164-04

基于公开密钥基础设施的 Lustre 安全模型设计

刘素芹, 李兴盛, 硕 珺, 王 婧

(中国石油大学 计算机与通信工程学院,山东 青岛 266555)

摘要:在分析并行文件系统 Lustre 存在的安全隐患的基础上,根据其存储特点,利用公开密钥基础设施(PKI)安全机制设计相应的安全模型。该模型包括证书管理和用户访问两部分,证书管理部分采用 PKI 本身的证书管理机制,用户访问部分采用双向身份认证和数字签名方式,且在认证过程中加入对随机数的检验。在传输请求信息和认证信息时,采用非对称加密机制;在传输大量数据时,采用对称加密机制。该模型能较好地解决存储系统存在的身份冒充、数据窃取、数据篡改以及重放攻击等安全隐患,提高 Lustre 的安全性。

关键词:公开密钥基础设施; Lustre; 安全模型; 双向身份验证; 数字签名

中图分类号:TP 309 **文献标识码**:A

Security model design for Lustre based on PKI

LIU Su-qin, LI Xing-sheng, SHUO Jun, WANG Jing

(*College of Computer and Communication Engineering in China University of Petroleum, Qingdao* 266555, *China*)

Abstract: By analyzing safety loophole and storage characteristic of Lustre file system, a security model for Lustre file system was designed based on public key infrastructure(PKI) security mechanism. The model includes certificate management and client accessing. Certificate management mechanism of PKI is adopted in certificate management module. Bidirectional identity authentication and digital signature are applied in client accessing module. Random number must be checked during authentication. Dissymmetrical encryption mechanism is applied to the transmission of request information and authentication information. Symmetrical encryption mechanism is applied to the transmission of data stream. The security model can remove safety loopholes in Lustre file system, such as imitating identity, filching data, distorting data and replaying attack. It can enhance the security of Lustre file system.

Key words: PKI(public key infrastructure); Lustre; security model; bidirectional identity authentication; digital signature

为了解决高性能计算系统的 I/O 瓶颈问题,学术界和业界研究和制定了很多方案,并行文件系统是其中的一个重要方向。目前,基于对象存储的全局并行文件系统在可扩展性、可用性和性能方面有诸多优势,在高性能计算机存储管理系统中能发挥重要作用,Lustre 文件系统就是其中的典型代表。Lustre 针对大文件的读/写进行了优化,可以为集群系统提供高性能的 I/O 吞吐率、全局数据共享环境、数据存储位置独立性,大大提高了存储系统的可靠性、可扩展性和并行访问能力。但是,Lustre 通过 TCP/IP 网络传输数据时,数据面临着来自网络上的多种威胁,其安全问题在一定程度上限制了 Lustre 的应用。用户对安全性能日益关注,因此有必要根据 Lustre 系统的特点设计有效的安全机制,提高存储系统的安全性。

1 Lustre 文件系统及其安全问题

1.1 Lustre 文件系统

Lustre[1-3] 文件系统中有 3 个重要组成部分:元数据服务器(MDS, Metadata Server)、对象存储目标端(OST, Lustre Object Storage Target)和客户端,如文献[4]中图 1 所示。

MDS 主要负责元数据的管理。元数据是指文件系统中文件和目录的属性及其他相关信息,包括

收稿日期:2009-06-05

作者简介:刘素芹(1968-),女(汉族),山东东明人,副教授,博士,主要从事高性能计算和数据处理理论与技术方面的教学和研究工作。

文件和目录创建或访问时间、状态信息、真实数据的分布和地址、其他文件系统的挂接点信息、符号链接文件的信息等。Lustre 文件系统将元数据存储在一组 MDS 上，MDS 可以为单一服务器、一主一备的双机系统或多机组成的 MDS 集群。

OST 主要负责真实数据的管理，将真实数据以对象的方式存储在 OST 后端的物理存储设备上，可以是文件、跨越多个 OST 的文件条带或文件的多个扩展单元等形式。OST 提供数据块分配、加锁管理、并行 I/O、存储网络中的优化以及存储策略管理等接口服务。

客户端向用户提供对文件系统的访问。用户通过 POSIX 透明地访问整个文件系统中的数据。客户端与 OST 进行文件数据的交互，客户端与 MDS 进行元数据的交互。

1.2 Lustre 存在的安全问题

对于一次数据访问，客户端首先向元数据服务器发出请求，元数据服务器将文件所在的 OST 设备号以及文件对应的对象号和偏移地址反馈给客户端，然后客户端直接通过网络向 OST 设备发送相应的对象操作命令，在客户端和 OST 之间直接进行存储数据的传输。在这样的访问流程中，系统存在以下安全隐患[4]：

(1)身份冒充。网络攻击者既可以伪装成客户端从 OST 上非法获取用户的数据，也可以伪装成 OST 使客户端将大量数据存储到攻击者指定的存储位置。

(2)窃取数据。攻击者可以利用网络监听技术，直接从客户端与 OST 的传输通道上获取数据。

(3)重放攻击。即使整个存储系统具有一定的认证机制，网络攻击者仍然可以通过截获并重新发送认证数据的方式，骗取存储系统中的数据。

在用户和企业对安全性能日益关注的今天，如果 Lustre 的安全问题不能得以解决，将势必影响它的大规模应用。

2 网络安全机制分析

目前，分布式网络安全机制主要是 Kerberos 和公开密钥基础设施(PKI)。

2.1 Kerberos

在 Lustre 的开发规划中，计划采用 Kerberos 机制来加强安全性。Kerberos[5-7]是一种应用于分布式网络环境、以对称密码体制为基础、对用户及网络连接进行认证的增强网络安全的服务。作为一种被广泛应用的安全服务机制，Kerberos 可以提供认证、机密性和完整性 3 种安全能力，标准相对完善，支持单点登录，同一 Kerberos 实现中互操作性较好等。但 Kerberos 也存在许多不足，主要体现在以下几个方面：

(1)Kerberos 使用对称算法作为协议的基础，带来了密钥交换、存储和管理的困难，需要大量的管理时间和资源，这在较大的组织中往往是难以忍受的。

(2)Kerberos 不能用来进行数字签名，因此也不能提供非否认机制。

(3)Kerberos 防止口令猜测攻击的能力较弱。

(4)Kerberos 使用时间戳来防止重放攻击，系统默认的最大延迟时间为 5 min，这意味着攻击者在这段时间的重放攻击无法被发现。

2.2 PKI

PKI(public key infrastructure)[8-10]用非对称算法原理和技术来实现并提供安全服务，是一个具有通用性的安全基础设施。遵循一定规则建立的 PKI，在提供信息安全服务时，能够提高效率、简化管理、增强可靠性，从而使真正意义上的安全性成为可能。

一个 PKI 系统主要包括终端实体、认证机构、证书库、证书撤销列表库、注册机构以及 X.509 数字证书，如图 1 所示。

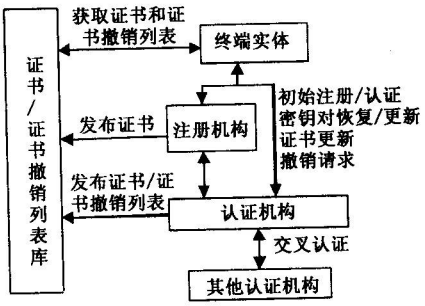

图 1 PKI 的组成

Fig. 1 Composition of PKI

PKI 通过提供认证、安全性和机密性来进行安全的传输，还能提供 Kerberos 不具备的功能，即非否认性。与 Kerberos 相比，PKI 在以下几方面具有明显的优点[11]：

(1)管理时间和资源。相对于 Kerberos，PKI 允许组织方便灵活的管理密钥，系统的管理负担要小得多。PKI 的密钥管理能力在 Kerberos 和其他密码安全解决方案之上，PKI 管理功能包括证书有效性、撤销、密钥备份和恢复、支持数字签名的非否认、自动密钥认证和证书、密钥历史的管理、时间戳和支持

交叉认证等,这使得在企业范围内 PKI 比 Kerberos 实现管理更为简单。

(2)证书资源库。通常基于 LDAP 或 OCSP 的证书资源库能够有效处理大量的请求,这允许 PKI 能够安全扩展。

(3)数字签名。PKI 允许用户使用他们的私钥对数据和消息进行数字签名。

(4)PKI 在可扩展性、透明性等方面也有很大的优势。

基于以上分析,本文中选用 PKI 机制来构建 Lustre 的安全模型。

3 基于 PKI 的 Lustre 安全模型

针对 Lustre 存在的安全隐患,结合 PKI 机制,设计了 Lustre 的安全模型,如图 2 所示。该模型主要包括证书管理和用户访问两部分。

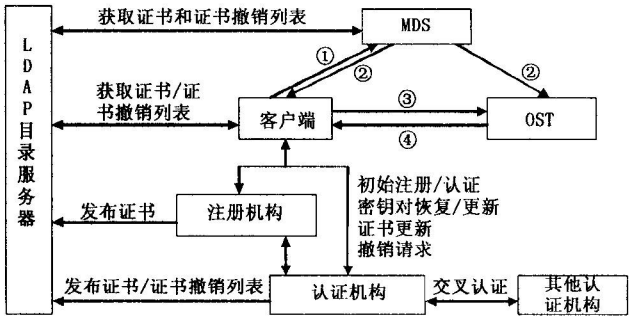

图 2 Lustre 安全模型

Fig. 2 Security model for Lustre

3.1 证书管理

3.1.1 证书申请

用户没有申请证书时,无法访问 Lustre 文件系统,所以第一步就要向认证机构申请证书。用户申请证书的过程包括 4 个步骤:

(1)用户向注册机构提交证书申请请求,由注册机构审核;

(2)注册机构将审核后的用户证书申请请求提交给认证机构;

(3)认证机构生成用户证书,并登记在证书库中,同时认证机构调用相应组件生成用户密钥对;

(4)认证机构通过某种途径(例如带外方式)向用户发放证书和私钥。

3.1.2 证书更新

在用户使用证书的过程中,PKI 自动到目录服务器中检查证书的有效期,在即将失效之前,认证机构会自动启动更新程序,生成一个新证书来代替旧证书。

3.1.3 证书撤销

在证书失效后或用户请求撤销时,撤销并废除证书。当用户身份变更、私钥泄露或用户认为不安全时,可以提交证书撤销请求。需要撤销证书时,由用户向注册机构提交证书撤销请求,注册机构将审核后的证书撤销请求提交给认证机构,认证机构发布证书撤销列表并更新证书和证书撤销列表库。

3.2 用户访问 Lustre 文件系统

用户与 MDS、OST 通信时,采用 X.509 提供的双向身份认证方式,为了防止中间人攻击,认证过程中加入了对随机数的检验。在传输请求信息、认证信息时,采用非对称加密机制;在传输大量数据时,考虑到算法的开销和速度问题,采用对称加密机制。

图 2 的模型基于以下假设:MDS 和 OST 在用户访问前已经获得证书并在证书库中有相关记录;在实际系统中,由于 OST 由 MDS 统一管理,故假设 MDS 和 OST 之间存在预共享密钥 K_{MT}。对于图 2 用户访问部分的每个步骤详细说明如下:

(1)用户向元数据服务器 MDS 提交请求。

客户端生成一个非重复的随机数 R_C,R_C 在报文的有效期内必须是唯一的,MDS 存储这个随机数直到它过期,在报文有效期内拒绝所有包含相同随机数的报文;

客户端做 $m = \{T_C, R_C, I_M, d\}$,其中 T_C 为时间戳,由一个可选的产生时间和截止时间组成,I_M 为标识,指明接收方,d 为请求信息,即想要访问的数据说明;

客户端用自己的私钥对 m 进行签名得到 $D_C\{m\}$;

客户端用 MDS 的公钥对 $\{C_C, D_C\{m\}\}$ 加密得到密文 E_{CM},将其发送给 MDS,其中 C_C 为客户端的证书。

(2)MDS 对客户端进行认证并向客户端和相应的 OST 发送认证信息。

MDS 用自己的私钥对 E_{CM} 解密得到 $\{C_C, D_C\{m\}\}$;

MDS 认证 C_C,得到客户端的公钥 PK_C;

MDS 用 PK_C 验证签名 $D_C\{m\}$;

MDS 检查 m 中的标识 I_M;

MDS 检查 T_C,确认 T_C 是否在规定值范围内;

MDS 检查 R_C,与库中的 R_C 比较,确认没有重复使用;

MDS 根据请求信息为用户生成目标存储设备的列表 L_T,其中包括每个设备的地址 IP_T 以及端口

号 $Port_T$;

MDS 生成一个随机数 R_M;

MDS 做 $m=\{T_M,R_M,I_C,L_T\}$;

MDS 用自己的私钥对 m 进行签名得到 $D_M\{m\}$;

MDS 用客户端的公钥 PK_C 对 $\{C_M,D_M\{m\}\}$ 进行加密得到密文 E_{MC},将其发送给客户端,其中 C_M 为 MDS 的证书;

MDS 将客户端的证书等信息用 MDS 与 OST 的预共享密钥 K_{MT} 加密后发送给相应的 OST。

(3)客户端向相应的 OST 发送数据访问请求。

客户端对 MDS 进行认证(方法同步骤② 中的认证部分);

客户端生成密文 E_{CT}(方法同步骤①);

客户端按照 L_T 中的 IP_T 和 $Port_T$,将密文 E_{CT} 发送到相应的 OST。

(4)OST 对客户端进行认证并发送数据。

OST 用预共享密钥 K_{MT} 对 MDS 发送给 OST 的消息进行解密得到客户端的证书等信息;

OST 对客户端进行认证(方法同步骤② 中的认证部分);

OST 生成随机对称密钥 K_{TC};

OST 用 K_{TC} 对传输数据进行加密得到密文 E_{TC};

OST 用客户端的公钥对 $\{C_T,D_T\{T_T,R_T,I_C,K_{TC}\}\}$ 进行加密得到 $K(K_{TC})$,其中 C_T 为 OST 的证书;

OST 对数据进行签名并用其私钥加密得到 E_T;

OST 将 E_{TC},$K(K_{TC})$ 和 E_T 放入一个数字信封中发送给客户端。

当客户端接收到 OST 发送来的数据后,首先用自己的私钥对 $K(K_{TC})$ 解密得到 $\{C_T,D_T\{T_T,R_T,I_C,K_{TC}\}\}$;然后客户端对 OST 进行认证并得到随机对称密钥 K_{TC},利用 K_{TC} 对 E_{TC} 解密得到相应的数据;最后用 OST 的公钥解密 E_T 并对 OST 的签名进行验证,确保数据的真实性和完整性。

4 结束语

利用 PKI 机制设计的安全模型具有以下安全功能:

(1)防身份冒充。所有用户在访问 Lustre 系统之前都必须先申请证书,元数据服务器与用户、目标存储设备与用户之间都要进行双向的身份认证,确保身份的合法性。

(2)防数据窃取。真实数据传输前都经过随机对称密钥加密,然后使用接收者的公钥对随机对称密钥进行加密,确保了数据的安全性,由于窃取者没有接收者的私钥,即使数据在传输途中被窃取,攻击者也无法得到随机对称密钥,从而无法窃取数据。

(3)防数据篡改。数据传输过程中采用了数字签名技术,通过验证签名可以有效防止数据篡改。

(4)防重放攻击。用户与元数据服务器、用户与对象存储设备之间认证而产生的随机数都是一次性的,可以有效抵抗重放攻击。

参考文献:

[1] 杨昕,沈文海. Lustre 并行文件系统的发展及在气象领域的应用前景[J]. 应用气象学报,2008,19(2):243-249.
YANG Xin, SHEN Wen-hai. The evolution of lustre file system and the perspective of application to the meteorology filed[J]. Journal of Applied Meteorological Science, 2008,19(2):243-249.

[2] 董勇,周恩强,陈娟. 基于 Infiniband 技术构建高性能分布式文件系统——Lustre[J]. 计算机工程与应用,2005(22):103-107,228.
DONG Yong, ZHOU En-qiang, CHEN Juan. Inifniban-based high-performance distributed file system-lustre[J]. Computer Engineering and Applications,2005(22):103-107,228.

[3] DICKENS Phillip, LOGAN Jeremy. Towards an understanding of the performance of MPI-IO in Lustre file systems[J]. 2008 IEEE International Conferenc E,2008:330-335.

[4] 常兴华. Lustre 存储系统安全模型设计[J]. 信息安全与通信保密,2008(4):80-82.
CHANG Xing-hua. Security model design for Lustre storage system[J]. Information and Communication Security, 2008(4):80-82.

[5] 黄建华,何希. 基于动态口令体制的 Kerberos 协议改进[J]. 计算机安全,2009(2):66-69.
HUANG Jian-hua, HE Xi. Improvement of Kerberos agreement based on dynamic password system[J]. Computer Security,2009(2):66-69.

[6] BUTLER Frederick, CERVESATO Iliano, JAGGARD Aaron D, et al. Formal analysis of Kerberos 5[J]. Theoretical Computer Science, 2006,367(1/2):57-87.

(下转第172页)

(上接第 167 页)

[7] 范洪生,叶震,侯保花. 基于公钥密码体制的 Kerberos 协议的改进[J]. 计算机技术与发展,2006,14(4):224-227.
FAN Hong-sheng, YE Zhen, HOU Bao-hua. Improvement of kerberos protocol based on public key cryptosystem[J]. Computer Technology and Development, 2006, 14(4):224-227.

[8] 何蕴婷,张宗福. 基于 PKI 的文件安全传输方案研究[J]. 电脑知识与技术,2008,3(5):885-887.
HE Yun-ting, ZHANG Zong-fu. Research on confident file transfer based on PKI[J]. Computer Knowledge and Technology,2008,3(5):885-887.

[9] HAIDAR Ali Nasrat, ABDALLAH Ali E. Formal modelling of PKI based authentication[J]. Electronic Notes in Theoretical Computer Science, 2009,235:55-70.

[10] [美]NASH Andrew, DUANE William, JOSEPH Celia, et al. PKI:实现和管理电子安全[M]. 张玉涛,陈建奇,杨波,等,译. 北京:清华大学出版社,2002.

[11] 刘上栋,杨林,王建新. 分布式网络安全服务 Kerberos 和 PKI 比较分析[C]//信息产业部. 全国第八届通信保密与信息安全现状研讨会论文集. 成都:中国电子科技集团公司第三十研究所,2002:106-113.

(编辑 修荣荣)