网络存储安全分析

黄世权
(长江师范学院 网络中心,重庆 408100)

摘 要:随着存储的网络化趋势,高效安全的信息存储与传输成为网络的一个重要部分。由于系统漏洞、黑客入侵、内部人员管理不善等原因,很容易发生文件或资料丢失泄漏,由此造成的重大后果将是无法弥补的,通过网络存储安全技术的应用,能够有效地防止此类事件的发生。通过对网络存储安全的必要性以及存储安全的基本要求进行分析,利用访问控制、加密技术、入侵检测等技术,为网络存储提供了安全保证。

关键词:网络存储;安全;访问控制;加密;入侵检测
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2009)05-0170-03

Analysis of Network Storage's Safety

HUANG Shi-quan
(Network Center of Yangtze Normal University, Chongqing 408100, China)

Abstract: With the networking trend for storage, efficient and safe storage of information becomes an important part of network. As operate system's loophole, hacking, internal mismanagement and other reasons, are prone to missing documents or information leakage, the resulting consequences will be significant irreparable, through the applications of network storage security technology, can effectively prevent such incidents from occurring. Based on the need for network storage and security of the basic requirements for safe storage were analyzed, using access control, encryption technology, intrusion detection and other technologies, providing security guarantees for network storage.

Key words: network storage; security; access control; encryption; intrusion detection

0 引 言

随着人们对信息的依赖性不断增加,存储系统正逐渐成为整个信息系统的中心,数据成为最重要的资源和资产,而存储系统作为数据的储藏地,是数据保护的最后一道防线;另外随着存储系统向网络化发展,使得存储系统也容易受到攻击,成为攻击对象,从而使数据被窃取、篡改或破坏,造成不可估量的损失。

1 网络存储安全及相关概念

存储安全是指保证存储资源只被授权用户或可信网络所访问的安全措施、安全配置和安全控制,将存储与安全技术有机融合,确保数据的完整、可靠和有效调用[1]。存储安全通常包括存储设备自身的可靠性、可用性(设备安全)和保存在存储设备上数据的逻辑安全(应用安全)。

网络存储安全是指网络存储系统的硬件、软件及其系统中的数据受到保护,不因偶然的或恶意的因素而遭到更改、破坏,系统连续、可靠、正常地运行,网络存储服务不会中断。

不管是网络安全还是存储安全,其核心是保证数据信息的安全,因此保证信息安全也是存储安全的研究核心。国际存储工业协会(SNIA)对存储安全作的一个C.I.A三要素特性解释,即机密性(Confidentiality)、完整性(Integrality)和可用性(Availability)。机密性表示只有被授权者才能使用特定数据资源;完整性表示只有被授权者才能修改特定数据;可用性表示用户能及时得到服务[2]。

网络存储安全涉及网络安全和存储安全,存储安全和网络安全既有一定的关系,又有其特殊要求。存储安全既要保护不可信网络中的安全传输,又要保护存储设备上的存取过程;存储安全借鉴网络安全领域中已有技术,如身份验证、数据加密、数字签名等,对密钥管理、访问控制、数据分布、数据的访问模式等有不同的要求。

收稿日期:2008-08-20
基金项目:重庆市科学技术研究项目(KJ081310)
作者简介:黄世权(1970-),男,重庆人,副教授,研究方向为网络存储和计算机网络安全。

网络存储系统是网络资源的核心,涉及到存储技术和网络技术,其安全问题与网络安全领域的问题有很大的区别[3]。安全的存储服务是指存储系统能够根据不同用户的级别为其提供相应级别的存储资源;实用的性能保证则要解决在网络存储系统加入了安全控制机制之后,能提供可以实用的系统性能。

一个网络存储的安全系统应该包括以下几个特性:

(1)数据保密性。数据不能泄漏给非授权的用户,用户必须得到明确的授权,才能访问到数据。主要通过对数加密方式来防止黑客攻击。

(2)数据完整性。确保用户访问数据的过程中,保证所有数据的正确性。通常用 Hash 函数对数据进行完整性的检查。

(3)不可抵赖性。确保用户获得的数据确实由某个存储设备发送并且无法否认,且接收到数据的用户一定也是得到授权的用户。通常使用数字签名技术来实现。

(4)系统性能可用性。通过访问控制、数据加密保护等各种安全机制实现网络存储应用及安全系统,会增加存储系统的负载。

2　网络存储安全的目标和必要性

2.1　网络存储安全的目标

保护数据存储安全主要包括线上数据安全(存储网络安全)和磁盘数据安全(存储数据安全)。网络存储安全的目标和一般信息安全的目标是一致的,即保证数据在存储网络中传输和存储过程中的机密性、完整性和可用性[4]。计算、传输和存储是数据操作的三个主要环节,计算安全、传输安全和存储安全也是贯穿于数据安全问题的三个环节,传输安全(网络安全)位于存储系统的边界,而存储安全位于存储系统的内部[5]。

2.2　网络存储安全的必要性

网络存储安全的研究之所以受到关注,是和数据价值受到重视,以及网络存储成为存储趋势分不开的。

2.2.1　数据是最宝贵的财富

数据的价值取决于信息的价值,越来越多有价值的关键信息转变为数据,数据的价值就越来越高。数据的丢失和损坏,其损失是无法估量的,甚至是毁灭性的,这就要求数据存储系统具有可靠的安全性。同时,数据总量在呈爆炸式增长,其增长速度表明企业将会更加依赖于这些关键数据,特别是对于很多大型企业,数据是最宝贵的财富,必须以尽可能可靠的措施来保证数据的安全。

2.2.2　网络存储成为存储趋势

传统直连数据存储方式成为计算机系统的 I/O 性能瓶颈,其系统结构难以满足实际需要。随着网络存储技术的成熟,网络存储成为一种迫切的技术和应用需要。

2.2.3　存储安全是薄弱环节

由于网络的开放性,决定了安全问题的重要性;同时要为用户提供 24 小时不间断信息服务,也为攻击者提供可乘之机。信息存储越来越依赖于网络,存放这些数据的存储媒介也成为恶意攻击者的主要目标。如果成功入侵一个数据存储设备,就可能能获得机密数据,甚至能阻碍合法用户的访问,造成难以估量的损失。

2.2.4　存储安全研究环节还比较薄弱

一方面,由于存储安全威胁造成的损失是巨大的;另一方面,相比于网络安全的完备研究,存储安全的研究尚处在起步阶段,成熟的网络存储安全解决方案有待进一步深入的研究。

3　网络存储安全的研究现状

按照数据信息在媒介上的存在方式,数据安全可分为传输安全和存储安全。传输安全位于存储边界之外,存储安全位于存储边界之内,保障数据的安全是两者的核心所在。对于存储安全,有物理和逻辑上两种含义,物理安全保证存储设备的安全,如防止偷窃、设备可用,逻辑安全保证存储设备的数据安全,如不被解密、不被篡改等。

从已有研究情况看,目前存储安全的研究集中于两个方面:将适用于信息安全的安全措施(如加密技术、完整性技术)移植到存储系统中;从存储系统结构出发,研究具有安全特性的存储技术,比如对象存储技术。

在学术领域,IEEE 计算机协会主办的存储安全工作组会议(Security in Storage Workshop,SISW)也将存储安全进一步关注。ACM 创办了存储安全性与可生存性工作组会议(Storage Security and Survivability,StorageSS),其研究一般围绕机密性、完整性、可用性三方面展开。全球网络存储工业协会(SNIA)成立了存储安全工业论坛(SSIF),来推动存储安全的发展。

SNIA 提出的共享存储模型是目前通用的一种数据存储体系结构模型。该数据存储模型分为三层,即块存储子系统、文件/记录子系统和应用子系统。块存储子系统负责数据的存储和传输。文件和记录子系统关注数据的组织和检索,包括数据库管理系统和文件系统。应用子系统关注数据的内容和处理。根据该体

系结构模型,可以得到不同层次的存储安全方案,比如加密应用程序、加密文件系统、SCSI 指令集层次的加密。现有研究方案基本针对上述三层的某一层次[6]。

4 网络存储安全的基本要求

要对存储数据提供可靠的安全保障,必须结合实际需求,将安全技术和存储管理技术进行有机的结合,主要应考虑以下几个方面的要求:

(1)数据备份和容灾恢复能力,是存储安全保障的重要标志,目前存储领域主要是就这些方面加强数据的安全性。

(2)抗病毒能力。确保每天在系统中存取的数据不被病毒感染也是一个重要的问题。

(3)数据加密能力。保证存储设备上的数据在丢失后不至于带来灾害性后果。要求存储系统对数据进行加密,以加强数据的安全性。通过网络传输数据时同样需要对数据进行保护,防止黑客侦听。

(4)数据恢复能力。数据存储系统正在变得越来越复杂,系统的复杂性也提高了安全问题的复杂性。做好容灾备份、异地存储、病毒入侵等防护,在事故发生后快速将丢失的数据完好地恢复[7]。

5 网络存储安全的基本技术

网络存储安全系统向用户提供和本地存储设备相同的访问接口,可以让用户访问存储在网络上的任何存储设备节点[8]。网络存储系统中的用户来自不同的节点,它所管理的存储资源也可能分布在不同的存储节点上,而在同一个存储节点上同时给多个用户提供服务,复杂层次造成诸多的安全隐患。以下是实现网络存储安全的基本技术方案。

5.1 访问控制

访问控制是进行安全防范和保护的核心策略,为有效控制用户访问网络存储系统,保证存储资源的安全,可授予每个存储用户不同的访问级别,并设置相应的策略保证合法用户获得资源的访问权。根据具体手段和目的的不同,访问控制策略可分别通过登录访问控制、访问权限控制、目录级安全控制、属性安全控制实现。

(1) 登录访问控制。提供了第一层访问控制。主要是控制哪些用户能够登录到网络存储系统并获取对应的存储资源。有基于用户名和口令的用户登录访问控制和基于数字证书的验证方式。

(2) 访问权限控制。对非法操作所提出的一种安全保护措施。将合法用户划分为不同的用户组,以实现对网络资源的正常访问,并且每个用户组赋予一定的权限。访问权限控制机制明确用户和用户组可以访问存储系统的目录、子目录、文件和其他资源;并且指定用户对这些文件、目录、存储设备能够执行哪些操作。

(3) 目录级安全控制。针对用户设置的访问控制,控制合法用户对目录、文件、存储设备的访问。用户在目录一级指定的权限对所有文件和子目录有效,系统还可进一步指定对目录下的子目录和文件的权限。

(4) 属性安全控制。在权限安全控制的基础上提供更进一步的安全性。当用户访问文件、目录和网络设备时,系统管理员应该给出文件、目录的访问属性,网络存储系统上的资源都应预先标出安全属性,用户对存储资源的访问权限对应一张访问控制表,以表明用户对网络存储资源的访问能力[9]。

5.2 文件系统的加密

加密文件系统目标是提供端到端的安全,在客户端执行加密操作防止数据被文件服务器和其他未授权用户窃取或篡改。系统将密码操作(加密/解密、签名/验证)嵌入文件系统中,主要是负责密钥管理,涉及密钥的粒度、存储、策略[10]。

存储系统中的数据加密技术可以通过基于主机、基于网络(数据传输)以及基于磁带机的方式实现。

5.3 基于存储的入侵检测

入侵检测的关键是保护数据不被窃取,保证数据的机密性,同时判断数据在传输过程中是否被篡改,保证数据的完整性。为防止入侵者获得数据,保证数据的机密性,常采用数据加密技术。

在存储网络中,入侵者通过被攻破的存储服务器来窃取存储设备上的数据,对于这种安全威胁可采用主动防护措施和被动防护措施来保护存储服务器。目前比较常用的主动防护技术有各种防火墙技术和容错技术,被动的防御措施有入侵检测技术。

6 结束语

随着数据价值不断提升,以及存储网络化,数据遭受的安全威胁日益增多,若无网络存储安全防范措施,一旦攻击者成功渗透到数据存储系统中,其损失将是无法估计的。要求在特定存储系统结构下,从存储系统的角度考虑存储安全,综合考虑存储机制和安全策略是网络存储安全的一个重要环节与要求。

参考文献:

[1] 王 月,贾卓生.网络存储技术的研究与应用[J].计算机

(下转第 179 页)

进行解码,将数据放入缓存供解码器解码输出,同时接收端根据 RTP 包中的信息周期性回送包含 QoS 反馈控制信息的 RTCP 包到数据发送端以检测发送端和接收端数据的一致性[9]。

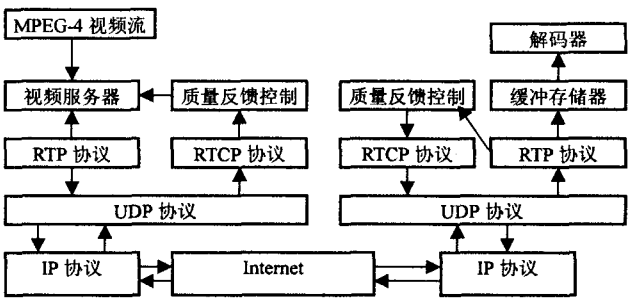

图 3　MPEG-4 数据流的 RTP 传输模型

3　结束语

基于嵌入式 Internet 的远程视频监控系统有着广阔的应用空间和美好的应用前景,能够在信息家电、电网运行监控、远程技术支持和远程故障诊断等多个领域得到应用[10]。

参考文献:

[1] Hui S C. Remote Video Monitoring Over the WWW[J]. Multimedia Tools and Applications,2003,21(2):173-195.

[2] 王冬华,吴壮志.边海防视频监控系统的设计与实现[J].计算机技术与发展,2008,18(5):208-211.

[3] 操龙敏,蒋建国,齐美彬.RTP 协议在嵌入式网络摄像机中的设计及实现[J].计算机技术与发展,2008,18(3):214-216.

[4] 韩　云,陈祖爵,郑尚志. MPEG-4 编码技术应用及 FPGA 实现[J].计算机技术与发展,2007,17(10):219-222.

[5] 杨　晖,胡永健,林志泉.基于 Linux 和 S3C2410 嵌入式图象传输系统设计[J].微计算机信息,2007,23(8):20-21.

[6] 张　建.基于 S3C2410 和嵌入式 Internet 的家庭视频监控系统设计[D].上海:上海交通大学,2007.

[7] 吴百锋,彭澄廉,孙晓光.一种基于监测的嵌入式系统设计技术[J].计算机学报,2003,26(12):1728-1733.

[8] LIU Quan,QU Xuehong. Research on Remote Video Monitoring System Used for Numerical Control Machine Tools Based on Embedded Technology[J]. 武汉理工大学学报,2006,28(z2):617-620.

[9] Cha Kyung-ae. MPEG-4 STUDIO: An Object-Based Authoring System for MPEG-4 Contents[J]. Multimedia Tools and Applications,2005,25(1):111-131.

[10] VIAL P J. Using Embedded Internet Devices in an Internet Engineering Laboratory Set-up[J]. The International Journal of Engineering Education,2003,19(3):441-444.

(上接第 172 页)

技术与发展,2006,16(6):107-109.

[2] 黄建忠,谢长生.网络存储安全研究趋热[J].中国教育网络,2006(8):41-42.

[3] 胡天翔.网络存储技术在企业中的发展及应用[J].计算机技术与发展,2006,16(7):218-220.

[4] 李文红.网络存储安全技术研究[J].武汉理工大学学报:信息与管理工程版,2006(8):54-56.

[5] 蔡　涛,鞠时光,赵俊杰,等.存储网层次安全模型的研究[J].计算机应用,2007(6):1534-1537.

[6] 伍小龙,温雅敏.网络存储的安全问题与对策[J].江西理工大学学报,2006(3):31-33.

[7] 韩德志,傅湘林,黄建忠.基于 iSCSI 的附网存储安全系统的研究与实现[J].小型微型计算机系统,2004,25(7):1223-1227.

[8] 金　红,王　煜.网络存储技术在网络数据备份系统中的应用[J].高性能计算技术,2003(6):50-53.

[9] 赵俊杰,詹永照,蔡　涛.网络存储安全系统研究综述[J].计算机应用与软件,2008(2):271-274.

[10] 姬　耀,刘海涛.文件数据的安全存储[J].信息安全与通信保密,2008(1):68-70.

(上接第 175 页)

2003,20(11):32-36.

[2] Wiederhold G. Mediators in the architecture of future information systems[J]. IEEE Computer,1992,25(3):38-49.

[3] Papakonstantinou Y, Garcia-Molina H, Widom J. Object exchange across heterogeneous information sources[C]// ICDE Conf. Taipei, Taiwan: IEEE Computer Society, 1995:251-260.

[4] Adali S, Emery R. A uniform framework for integrating knowledge in heterogeneous knowledge systems[C]// ICDE. Taipei, Taiwan: IEEE Computer Society, 1995:513-520.

[5] Tomasic A, Raschid L, Valduriez P. Scaling heterogeneous databases and the design of disco[C]// International Conference on Distributed Computing Systems. Hong Kong: IEEE Computer Society, 1996:449-457.

[6] 李　振,曹谢东,刘世齐.基于 CORBA 的油气田异构信息系统多源集成[J].计算机技术与发展,2006,16(6):60-62.

[7] 李亚红,吴　江.基于 Web Services 实现异构数据库集成技术研究[J].计算机应用研究,2006(2):81-84.

[8] Lenzerini M. Data Integration: A Theoretical Perspective[C]// PODS. [s.l.]: ACM Press, 1997:233-246.