第35卷 第20期 计 算 机 工 程 2009年10月
Vol.35 No.20 Computer Engineering October 2009
·安全技术· 文章编号：1000—3428(2009)20—0131—03 文献标识码：A 中图分类号：TP393.08

面向容灾的备份数据透明加密机制

康潇文，杨英杰，杜 鑫
(解放军信息工程大学电子技术学院，郑州 450004)

摘 要：针对备份数据的安全保护问题，设计一个基于层叠式文件系统的面向容灾的备份数据透明加密机制，采用基于虚拟磁盘的透明加密方法，在写入数据时加密，在读取数据时解密，从而在实现数据容灾的基础之上，增强对备份数据的加密保护，实现对数据的完整性、机密性的保护。

关键词：透明加密；虚拟磁盘；堆栈；容灾

Transparent Encryption Mechanism of Backup Data for Disaster Tolerance

KANG Xiao-wen, YANG Ying-jie, DU Xin
(Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004)

【Abstract】 In view of secure protection problem of backup data, this paper designs a transparent encryption mechanism of backup data for disaster tolerance based on cascading file system. In this mechanism, it uses transparent encryption function based on virtual disk. When it reads data, it encrypts. When it writes data, it decrypts. Thus, it implements data disaster tolerance, and at the same time, it enhances the encryption protection of backup data. It protects the integrity and confidentiality of data.

【Key words】 transparent encryption; virtual disk; stack; disaster tolerance

随着计算机信息技术的飞速发展，很多个人、企业将大量的重要信息集中存储在计算机上，如何保护数据的完整性和抗毁性成为人们日益关注的重要领域。尤其是很多企业由于数据丢失而导致了巨大的经济损失，这使得容灾研究在近几年来得到了高度重视，开展了大量的研究。但是在现存的容灾系统中，对敏感数据的保护还不够，更多的是采用额外的加密软件来实现对数据的机密性保护，加密软件虽然可以在一定程度上保护数据安全，但应用层的加密工具使用起来极不方便，每次加解密操作都需要用户的干预，用户的疏忽就会造成敏感信息的泄露。而将加密服务放入文件系统来实现是一种新思路，这种方式提高了安全强度和可操作性。基于这种思路，本文借鉴了层叠式文件系统开发原理，设计了一个面向容灾的备份数据透明加密机制。

1 现存容灾系统加密保护分析

数据是信息系统的核心，数据的破坏和不可恢复性将导致整个容灾的失败，数据容灾是整个容灾系统的关键所在。因而数据存储系统是搭建容灾系统的基础。随着存储技术的发展，先后出现了直连式附加存储(Direct Attached Storage, DAS)、网络附加存储(Network Attached Storage, NAS)、存储区域网(Storage Area Network, SAN)、虚拟存储等存储结构，基于不同的存储结构可以实现不同距离的容灾，但是在这些容灾系统中，较少考虑到敏感信息的存储问题，造成了一定的安全隐患。华中科技大学的外存储系统国家专业实验室提出了一种NAS环境下的安全堆栈文件系统[1]，在一定程度上保证了数据的安全，但其应用局限于NAS环境，移植性较差。Symantec公司的Backup Exec 11d软件提供了较为完备的容灾功能，并且也提供了简单的数据加密保护，但每进行一次加密操作都需要用户的手动干预，使用起来极不方便。

2 面向容灾的透明加密机制设计

根据上述分析，可以看到目前的容灾系统还存在以下问题：现存的容灾系统未能对敏感数据提供较好的安全保护，对备份数据的机密性造成了极大的威胁；通过配置额外的加密机制来保护数据，又会对系统的性能造成较大的影响。而将这些数据处理功能放入文件系统来实现既可以提高系统效率又可以增加对用户的透明度，这为开发提供了一种新的思路。

2.1 文件系统透明加密技术

根据实现方法的不同，文件系统透明加密技术可分为传输加密技术、基于NFS的磁盘加密技术和基于层叠文件系统的磁盘加密技术。

传输加密技术更注重于文件的分布式共享，它对数据保护的侧重点在于客户端到服务器的通信链路，使用的是端到端加密机制。采用该技术的典型文件系统有AFS(Andrew File System)和SFS[2](Self-certifying File System)。由于文件系统是以明文形式存储敏感数据的，只要攻击者获得服务器管理员权限，就可以随意地访问敏感数据了，并且在每次文件传输中，服务器和客户端都要对数据进行加解密操作和完整性检查，对系统的性能有较大的影响。

NFS以目录挂载的方式实现远程访问，客户端通过远程

基金项目：河南省自然科学基金资助项目(0611051300)
作者简介：康潇文(1983－)，女，硕士研究生，主研方向：容灾与信息安全；杨英杰，副教授、博士；杜 鑫，硕士研究生
收稿日期：2009-05-06 **E-mail：**kangxiaowen-0829@126.com

过程调用(RPC)来进行通信。基于该技术的典型代表有 CFS (Cryptographic File System)和 TCFS[3](Transparent Cryptographic File System)。在 CFS, TCFS 中，数据以密文的形式存储在磁盘上，有效提高了文件的安全性，但是 CFS 工作在用户层，频繁的上下文切换对 I/O 效率有很大的影响。而 TCFS 虽然工作在内核层，但它是基于 NFS 的工作机制，每次读写操作还会涉及到多次核心层与用户层之间的数据交换，所以 I/O 效率低下仍然难以避免。

层叠文件系统是在现有的文件系统基础上快速便捷地添加功能层。其执行流程如下：文件系统从上层文件系统接收设备对象(即数据与操作)，并执行其相关操作，然后调用下层文件系统的设备对象，因此层叠文件系统的上下层是独立的。基于层叠文件系统开发的加密文件系统运行在内核层，有效提高了 I/O 效率，基于该技术的磁盘加密文件系统的主要代表有 NCryptfs[4]。

2.2 透明加密文件系统体系结构

根据上述分析可以得出，基于层叠文件系统开发文件系统扩展功能是一种高效、便捷的方式，本文基于这种方法，设计了一个层叠虚拟文件系统来实现数据容灾和加密保护，如图 1 所示。

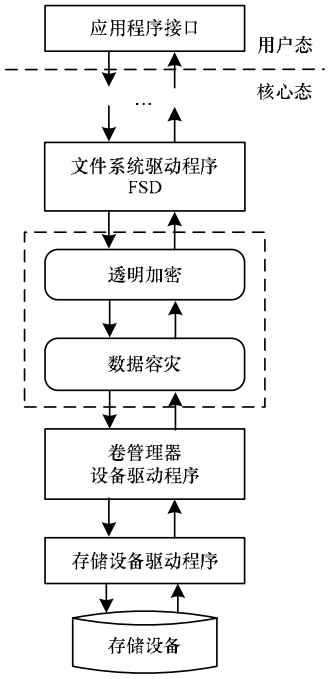

图 1 虚拟文件系统体系结构

虚拟文件系统在原有文件系统的基础上，添加透明加密层和数据容灾层，各层之间相互独立，每层只集中实现一种数据保护功能。

透明加密层：对文件系统驱动层传来的数据进行加、解密操作。在接收数据后，先根据文件的头部信息判断是否需要执行加密操作。加密标志位为 0，则跳过该层的操作；加密标志位为 1，则执行相关操作。该层以虚拟磁盘驱动程序的形式实现。虚拟磁盘驱动程序与一般物理磁盘驱动程序的功能基本一致，区别在于虚拟磁盘驱动程序不直接访问物理磁盘设备，而是以访问物理磁盘的方式来访问一个卷文件，将这个卷文件虚拟成一个磁盘。在虚拟磁盘驱动程序中实现一个加解密模块，在驱动程序处理 I/O 请求的过程中，调用这个加解密模块对虚拟磁盘的数据流进行实时的加解密处理。当虚拟磁盘驱动程序收到写数据请求的 IRP 时，就调用加密模块对 IRP 中的明文进行加密，然后将密文写到卷文件中；当虚拟磁盘驱动程序收到读数据请求的 IRP 时，先从卷文件中读出密文，然后调用解密模块进行解密，再将明文写到 IRP 的数据区中返回给应用程序。这种在操作系统内核模式下进行的加解密过程具有较高的效率和安全性，而且对上层的文件系统驱动和应用程序都没有任何影响。

数据容灾层：仅负责对透明加密层传来的数据进行相应的备份、恢复操作。同样，在执行操作前，也要根据文件头部信息进行判断。备份标志位为 0，则跳过该层的操作，备份标志位为 1，则执行相关操作。备份操作通过时间或事件触发器自动执行，无需用户的任何干预；并且根据网络空闲判断，决定备份数据是缓存在本地磁盘还是立即传输到远程磁盘，从而达到数据自动备份的目的。

综上所述，该虚拟文件系统具有以下优点：

(1)各层之间相互独立，可实现较为完善的安全功能，层间没有相互制约。

(2)透明加密层和数据容灾层起到了中间人的角色，它可以为操作系统提供安全和透明的数据存储保护服务。

(3)透明加密层和数据容灾层采用了简单的头文件标识判断，可以灵活地控制对数据的加密和备份操作的选择。

3 文件系统中的加密实现

3.1 加密子层内部结构

为了适应多密级保护需求，同时保证文件系统运行效率，根据用户对加密强度的要求，选用不同的加密算法，以达到加密强度与运行效率之间的平衡。

透明加密子层内部结构如图 2 所示，由 3 个模块组成，即信息获取模块、算法选择模块和执行模块。

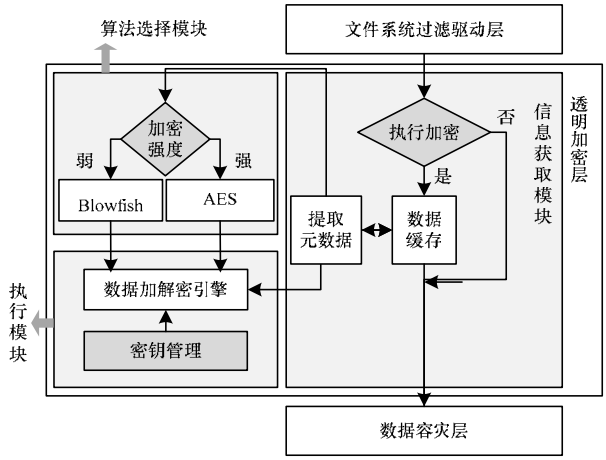

图 2 加密子层体系结构

信息获取模块的主要功能是进行加密判断、缓存加密数据以及从元数据中提取加密强度标识信息，为算法选择模块提供判断依据，并在算法选择模块完成选择后将缓存的数据送往加密执行模块。

算法选择模块的主要功能是执行加密强度判断，并将选择的加密算法标识发往加密执行模块，以满足用户的不同需求。

执行模块是整个加密子层的核心部分，它根据信息获取模块和算法选择模块传来的信息，执行加解密操作，执行完毕后，将数据送回信息获取模块，最后由信息获取模块将数据送往下一层。

3.2 内核数据加密

对于数据加密，仍然选择适于大量数据加密的分组加密算法，为了便于理解加密子层的体系结构，只描述了 2 个最具特点的算法：Blowfish 和 AES。Blowfish 算法是中等安全加密等级、运算量较小的一种加密算法，其算法结构简单，易于实现，执行效率很高。密钥长度可以达到 448 位，因而完全不必担心受到穷举攻击。AES 算法的加密解密相似但不对称，有较好的数学理论作为基础，该算法支持长度为 128 位、192 位和 256 位的密钥。在安全性方面还没有发现弱密钥或补密钥，能有效抵抗目前已知的攻击算法。相比于 Blowfish，AES 可以提供更强的加密保护，但其执行效率低于 Blowfish。加密模式选择 CBC 模式，但仅在数据块内使用，这样系统便可以独立解密每个块，也可以减少数据的丢失，如果一个字节损坏了，最多影响一个数据块的数据。

接下来将加密算法应用到读写 vnode 操作中。执行加密的块大小是 8 192 Byte。当请求读一个字节域，计算出到下一块边界的扩展字节域，使用扩展域将操作应用到下层文件系统。操作成功后，请求的精确数返回给 vnode 操作的调用者。写一个字节域比读要复杂得多，如图 3 所示。一个字节依赖于前一个字节，必须读取和加密块的一部分，然后再写入块的另一部分。

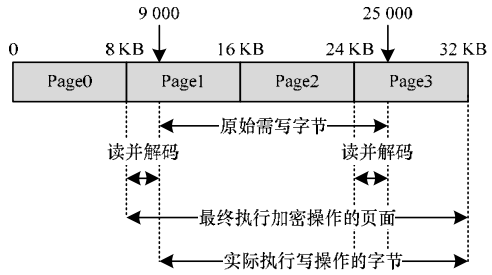

图 3　写操作

从 9 000 Byte~25 000 Byte 写入文件的工作流程：

假设 *V* 表示虚拟节点层的字节流，*V'*表示透明加密层的字节流：

(1)在 *V* 上的 9 000~25 000 域调用写操作。

(2)计算这个区域的扩展页边界，即 8 192~32 767(共 3 页)。

(3)根据 *V* 定位 *V'*。

(4)分配 3 个空页。

(5)从 *V'*读取字节 8 192~8 999(页 1)，解密他们，将他们放在第一个分配的页中。不需要读或解密页 1 中 9 000~16 383 的字节，因为他们将被复写。

(6)跳过写操作将要复写的中间页。在这种情况下，不打开文件的页 2(也是写请求的第 2 页)。

(7)从 *V'*读取字节 24 576~32 767(24 KB~32 KB)(文件的第 3 页)，解密他们，将其放在第 3 个分配的页中。因为 24 576~25 000 部分的数据发生了变化，会对页 3 中 25 000 以后的数据有影响，这次需要读取和加密整个页。

(8)将发送的字节复制到分配的 3 页中 9 000 Byte~25 000 Byte 域里。

(9)有 3 个包含未加密数据的有效数据页，执行加密操作，这样整个写操作就完成了。

3.3 密钥管理方案

加密数据的安全性依赖于保护密钥使用的策略强健度。其中密钥撤销更新机制对加密系统的性能会产生较大的影响，特别是对于磁盘加密文件系统，每进行一次密钥撤销更新操作，就需要对受影响的文件块重新执行加密操作以及计算文件块的哈希值，同时文件的拥有者需要对相关用户重新分发密钥。为了减少系统开销，文献[5]提出了一种懒惰撤销密钥更新机制，该机制有效缓解了密钥管理效率低下的问题。

在本文的虚拟文件系统中，就采用了该更新机制，密钥更新后，对文件的重新加密将推迟到下一次对该文件执行写操作的时候。在本文设计的虚拟文件系统中，将文件按照访问权限分组，在同一组的文件都具有相同的访问权限。初始时刻，同一组的所有文件使用同一个密钥进行加密，假设由文件的拥有者负责向已认证用户生成和分发密钥，因此，在本文的密钥更新模型中，用户的拥有者是一个可信实体，它管理一个文件组的密钥和对文件组具有访问权限的用户。

当一个用户从一组文件的访问域中撤销后，文件的拥有者运行更新算法，以生成新的状态和时间戳，然后文件拥有者将用户密钥分发给现在有权访问该文件的所有用户。当一个用户要对该文件执行写操作时，就使用最近的时间间隔产生的密钥。而解密文件时，用户需要知道加密该文件时使用的密钥版本。然后从用户密钥中提取出适当的加密密钥。

4　结束语

本文在分析了透明加密技术的基础上，设计了一个面向容灾的备份数据透明加密机制，并对加密子层进行了详细的阐述。该系统主要具有以下特点：该系统基于层叠文件系统，使得文件系统功能模块化，简化了实现过程；在文件系统中同时实现了数据容灾和文件加密，强化了对敏感数据的保护；可以根据用户的需求进行加密算法选择。

参考文献

[1] 谢长生, 黄建忠, 刘朝斌. 堆叠式文件系统的研究及其在 NAS 整合中的实现[J]. 小型微型计算机系统, 2005, 26(3): 515-518.

[2] Mazieres D, Kaminsky M, Kaashoek M F, et al. Separating Key Management from File System Security[C]//Proc. of the 17th ACM Symposium on Operating Systems Principles. Kiawah Island Resort, SC, USA: [s. n.], 1999.

[3] Cattaneo G, Catuogno L, Sorbo A D, et al. The Design and Implementation of a Transparent Cryptographic Filesystem for UNIX[C]//Proc. of the Annual USENIX Technical Conference. Boston, Massachusetts, USA: [s. n.], 2001.

[4] Wright C P, Martino M C, Zadok E. NCryptfs: A Secure and Convenient Cryptographic File System[C]//Proc. of General Track of the USENIX 2003 Annual Technical Conference. San Antonio, Texas, USA: [s. n.], 2003.

[5] Backes M, Cachin C, Oprea A. Lazy Revocation in Cryptographic File Systems[C]//Proc. of SISW'05. San Francisco, USA: [s. n.], 2005.

编辑　任吉慧