第37卷 第13期 计 算 机 工 程 2011年7月
Vol.37 No.13 Computer Engineering July 2011

·安全技术· 文章编号：1000—3428(2011)13—0101—03 文献标识码：A 中图分类号：TP309.2

加密存储算法和模式研究

梁 敏[1]，常朝稳[1]，樊雪竹[2]

(1. 解放军信息工程大学电子技术学院，郑州 450004；2. 解放军61655部队，重庆 402764)

摘 要：为提高全盘加密系统的性能，研究现有的磁盘加密算法和模式，测试不同加密算法和模式组合的性能。介绍加密存储的主要方式，对现有磁盘加密算法和模式进行分析，将不同加密算法和模式结合进行性能测试与分析，针对全盘加密系统给出相应的建议，为加密存储设计者提供参考和依据。

关键词：存储安全；加密存储；全盘加密；加密算法；加密模式

Research of Encryption Storage Algorithms and Modes

LIANG Min[1], CHANG Chao-wen[1], FAN Xue-zhu[2]

(1. School of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004, China;
2. PLA 61655 Army, Chongqing 402764, China)

【Abstract】In order to improve the performance of the full disk encryption system, this paper studies and analyzes the existing disk encryption algorithms and modes, and tests the performance of different combinations of encryption algorithms and modes. The ways of encryption storage are introduced. The existing encryption algorithms and modes are analyzed. The performances of encryption algorithms and modes are tested and analyzed. A suggestion is proposed for full disk encryption. Result provides referential basis for designers of encryption storage.

【Key words】storage security; encryption storage; full disk encryption; encryption algorithm; encryption mode

DOI: 10.3969/j.issn.1000-3428.2011.13.032

1 概述

数据的安全存储已经成为计算机安全领域中的主要问题之一。因磁盘被盗、丢失或者未授权的访问和使用而造成的信息大量泄漏已经给国家、企业和个人带来了巨大的损失。2009年，美国弗罗里达州的一家海军医院发现存有近千份军人个人信息的笔记本电脑丢失。同年，美国国民警卫队宣布存有13万个人信息的笔记本电脑被盗。全球几乎每个月都有政府、组织或者企业发生存有敏感信息的存储设备丢失或者被盗事件。最近的一个调查显示，2/3的IT行业专家工作使用的移动存储设备没有经过加密保护。另外，内部人员的非法访问或者窃取信息也时有发生。除了防止存储设备的丢失或者被盗，使用加密方法保证存储设备的安全是一种常用并且有效的方式。按实现的层次不同，现有的基于软件的加密存储方法可以分为：应用层加密，操作系统内核层加密和全磁盘加密(FDE)。在广泛部署存储加密软件之前，必须解决一些关键的问题，如选择合适的加密模式、加密算法和密钥管理方式。为解决这些问题，美国电气及电子工程师学会(IEEE)已经提出了一个新的标准P1619^{TM}/D16。

加密算法和加密模式对加密存储的安全和性能有着重要的影响。本文介绍了AES、Twofish和RC6 3种加密算法和LRW、XTS和CBC+Elephant diffuser 3种加密模式，并基于全盘加密系统对算法和模式的组合进行了性能分析。

2 加密存储

基于软件的加密存储方法大体上可以分为3类：应用层加密，操作系统内核层加密和全磁盘加密。应用层加密是一种最简单的文档加密形式，如PGP公司的邮件加密软件。由用户指定需要加密的单个文档和指定加密后的目标文件名，程序全部在应用层实现。当一个文档需要加密存放时，选择加密操作，存为密文文档。需要读取的时候，需要先解密成明文文档。这个方法的优点是实现起来比较容易，可以针对单个文档选择加密处理。缺点是需要用户干预较多，操作不便，不利于大量文件的加密处理，而且安全性较差。

为了解决应用层加密用户操作步骤繁琐、安全性差等问题，人们提出了内核层加密。所谓内核层加密，就是在操作系统内核中实现对数据的加/解密操作。根据实现方式的不同又分为：过滤驱动加密和虚拟磁盘加密。过滤驱动加密是在I/O管理器与文件系统之间插入一个文件过滤加密驱动程序，这样就可以对指定的文件或文件夹进行加密和解密，从而达到安全存储的目的。虚拟磁盘文件加密系统的基本设计思想是：在原有系统的文件系统和磁盘驱动程序之间，加入一层虚拟磁盘驱动程序，虚拟磁盘驱动程序将本地磁盘上的一块存储区映射为虚拟磁盘分区，用户需要加密存储的数据文件都通过虚拟磁盘分区进行存储，在虚拟磁盘驱动程序中动态地对存储到磁盘上的文件进行加密。操作系统内核层加密可以有效地避免用户态加密存在的各种不足，方便控制文件的操作粒度，相对提高了安全性，同时加解密操作对用户透明。但它也有一些局限性，如不能对系统文件、页文件和临时文件加密，在诸如断电或出现应用故障的情况下，这些文件可能被漏掉，导致敏感数据文件以明文形式存储在硬盘上。

与前2种方法相比，全磁盘加密是最安全可靠的方法，几乎对写入磁盘的所有数据都进行加密处理，包括操作系统文件和页文件，提供了最全面的加密保护措施，给攻击者设

基金项目：国家“863”计划基金资助项目(2007AA01Z479)

作者简介：梁 敏(1986－)，男，硕士研究生，主研方向：安全存储；常朝稳，教授；樊雪竹，助理工程师

收稿日期：2011-01-06 **E-mail：**lm7186345@163.com

置了无法越过的安全防护隔离墙[1]，主要的产品有 Windows Bitlocker、CheckPoint 和 PGP Whole Disk Encryption。由于操作系统在启动之前也是以密文形式存储在磁盘中，因此非法用户在没有密钥的情况下是无法启动系统的，甚至用类似 Windows PE 盘的工具都无法读取磁盘上的任何信息。有效解决了操作系统内核层加密的安全问题，保证了页文件、休眠文件和临时文件的安全性。

然而，全盘加密的安全性还依赖于加密算法和加密模式的正确选择。下面说明全盘加密在算法和模式方面的需求：

(1)明文和密文的存储空间是一样大的，不能因为加密操作而增加数据的存储空间。例如明文是 1 MB 大小，那么加密后的密文也需要是 1 MB。

(2)加密算法和模式是经过广泛验证相对安全的。

(3)密钥的管理要相对容易可行。

(4)加/解密操作的速度比较快，能够被用户所接受。

(5)加密操作的并行性可以有效提高性能，并且由于多核处理器的快速发展，硬件费用降低，故加密模式应该对并行性有较好的支持。

3 加密算法和加密模式

3.1 加密算法

本文选取了 3 种加密算法与 LRW、XTS 和 CBC+Elephant diffuser 模式进行组合。3 种加密算法都是对称密码算法，分别是：AES，Twofish 和 RC6。选择其原因是，3 种算法均为 AES 的最后 3 种候选算法，性能相对较好，适用于全盘加密，并且都支持 128 bit 分组加密，适于测试 XTS 模式。

3.1.1 AES 算法

高级加密标准 AES 由 Rijndael 提出，支持 128 bit 分组加密，密钥长度可以是 128 bit、192 bit 和 256 bit。AES 已经在 IEEE 标准 P1619 中与 XTS 模式一起使用产生了 AES-XTS[2]。AES 的安全性已经得到了广泛的验证，是相对比较安全的密码算法。

3.1.2 Twofish 算法

Twofish 是由著名密码学专家 Bruce Schneier 提出的另一个快速分组密码算法，采用 128 bit 分组加密，支持 128 bit、192 bit 和 256 bit 密钥长度。该算法是在 Blowfish 算法的基础上，采用 16 回合 Feistel network，使用了一个双射 F 函数。Twofish 使用与 DES 一样的 Feistel 结构，并吸收了 SAFER 系列密码算法的特点。在安全性方面，Twofish 没有被现在已知的密码分析方法破解，仍然保持了较强的安全级别。Twofish 是非专利密码算法，已经在许多产品中实现，并且研究表明其适用于磁盘加密。

3.1.3 RC6 算法

作为 AES 的候选算法，RC6 是在 RC5 的基础上改进的，设计十分简单，运算速度快，使用灵活，其目的是为了更好地符合 AES 的要求。该算法的简单性反映在其非常易于软硬件实现。RC6 同样是 128 bit 分组加密算法，可用采用 128 bit、192 bit 和 256 bit 密钥，通过修改参数可以支持更为广泛的分组长度和密钥长度。在 AES 的测试平台上，RC6 与其他候选算法相比是速度最快的一个。最近几年，RC6 已经变为 RSA 公司的专利算法。

3.2 加密模式

按照加密块的大小，磁盘加密模式分为窄块和宽块模式。窄块模式(narrow block mode)指分组长度小于扇区大小的分组，常用的有 ECB、CBC 和 CFB 等；宽块模式(wide block mode)指分组长度等于扇区大小的分组，常用的有 EME、XCB 和 ABL4 等[3]。本文选择 3 个著名的加密模式进行测试，分别是：LRW，XTS 和 CBC+Elephant diffuser，其中，LRW 和 XTS 属于窄块加密模式；而微软的 CBC+Elephant diffuser 是宽块加密模式。

对文中用到的符号进行说明：

P：待加密明文。

C：加密后输出的密文。

X：加密过程产生的中间量。

EKey：加密密钥。

TKey：扰乱密钥。

SID：扇区编号。

GetTweak (TKey, SID)：SID 加密函数。

T：扰乱因子。

ExKey：扩展密钥。

Expand-Key (EKey)：加密密钥扩展函数。

$\oplus$：异或。

$\otimes$：定义域上的乘法。

α：伽罗瓦域运算的基本元素。

Encrypt (ExKey, P)：加密算法。

3.2.1 LRW 模式

LRW 采用可调密码模式(tweakable block cipher mode)，曾经是 IEEE P1619 窄块加密标准候选算法中最有希望的，其工作流程如下：

```
Encrypt-LRW(P, EKey, TKey, SID)
    ExKey = Expand-Key(EKey)
    T = TKey
    for i=0 to n
      T = T ⊗ SID
      P_i = P_i ⊕ T
      C_i =Encrypt(ExKey, P_i )
      C_i = C_i ⊕ T
      SID =SID+1
      end for
return C
```

由于使用非链式结构，因此它可以有效支持并行操作。LRW 的输入部分不仅有明文和密钥，还有第 3 个输入，叫做扰乱因子。其作用非常类似于 CBC 模式中的初始向量，但它具有易变性的特点。根据文献[4]中的定义，可调分组密码应该具有可改变扰乱因子的性质，这样要比更换密钥更有效率。

3.2.2 XTS 模式

XTS 是基于 XEX 的密文窃取(Ciphertext Stealing, CTS)可调加密模式，被认为是当前最适合于磁盘加密的窄块加密模式，已经被 IEEE P1619 标准所采用。XTS 加密流程如下：

```
Encrypt-XTS(P, EKey, TKey, SID)
   T=GetTweak(TKey,SID)
   ExKey=Expand-Key(EKey)
   for i=0 to n
     X=T ⊗ α^i
     P_i = P_i ⊕ X
     C_i=Encrypt(ExKey,P_i)
     C_i=C_i ⊕ X
   end for
return C
```

明文在加密前后都与扰乱因子进行了异或操作，CTS 使得输出的密文和输入的明文大小相同，这对于加密存储至关

重要。XTS 作为一种可调分组密码模式，支持的数据分组大小至少为 128 bit。密钥由数据加密密钥和扰乱因子组成。扰乱因子将数据块在磁盘中的逻辑位置与分组相结合，使得 XTS 可以有效抵抗复制粘贴攻击。在实现时，各分组之间可以并行运算，能处理任意长度的数据。

3.2.3　CBC+Elephant diffuser 模式

此种模式是由微软专门为 Windows Vista Bitlocker 而研发的磁盘加密模式，其加密流程如图 1 所示，它采用了宽块加密模式，加密粒度是一个扇区。微软已经证明了使用 diffuser 后的 CBC 模式比原来的 CBC 更难攻击，其安全性得到明显提高。加密粒度越大，攻击者需要的初始信息也就越多，因此微软希望使用宽块加密模式提高磁盘加密的安全性。微软在 CBC 模式的基础上设计了 CBC+Elephant diffuser 模式，通过 diffuser 算法来确保在明文中的很小改动也将导致整个扇区密文的变化，从而弥补窄宽加密模式在数据完整性上的不足。此外，已经有研究表明，CBC+Elephant diffuser 模式随机特性很好，甚至优于窄块加密模式[5]。

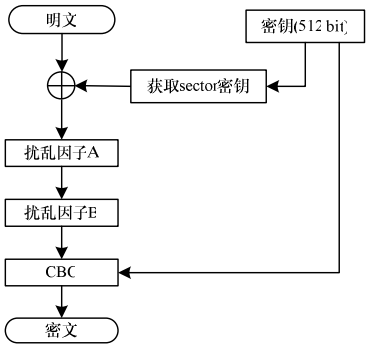

图 1　CBC+Elephant diffuser 加密流程

4　性能测试与分析

全盘加密所使用的加密算法和加密模式应该保证速度足够快，以避免在读写过程中产生速度瓶颈。全盘加密必然涉及到对操作系统文件的加密和对用户文件的加密。操作系统文件多为较小的文件，一般为几十或者几百 KB，多数不超过 1 MB，而且数量巨大，加解密操作频繁。而用户文件多数较大，使用时不会像操作系统文件那样被频繁调入调出。本文针对全盘加密系统中的这些特殊性，对加密算法和模式的组合进行测试，以选出较为适合于全盘加密的算法和模式组合。测试所用的样本数据分为 2 类：大文件组(64 MB，由大小为 8 MB 和 16 MB 的多个文件组成)和小文件组(64 MB，由 128 KB、512 KB 和 1 MB 的多个文件组成)。将每种算法和模式的组合分别对大文件组和小文件组进行加密操作，以测试其性能。

仿真实验在 Windows XP 操作系统下进行，使用开源免费的 FreeOTFE 作为全盘加密测试软件，加密数据分组为 128 bit 大小，密钥长度为 256 bit。为了更好地评估性能，发挥各种模式的并行执行优势，以提高加密操作的效率，选用多核处理器成为必须。实验使用的硬件平台是联想启天 M7000(CPU：Intel Core2 Quad Q9400 2.66 GHz，内存 2 GB，硬盘 320 GB)。为了保证测试的准确性，实验将会重复进行 10 次，求出平均值，测试结果精确到毫秒。为了便于记录数据，将 CBC＋Elephant diffuser 模式简记为 CED。

从实验结果，即图 2 可以看出，窄块加密模式 LRW 和 XTS 对小文件组加密的性能明显优于对大文件组加密的性能，分别高出 8%~11%和 13%~16%(与采用的加密算法有关)。宽块加密模式 CBC＋Elephant diffuser 则更适于加密大文件，性能比窄块模式高出 8%~13%。RC6 是 3 种算法中加密性能最好的。由此得出对于全盘加密系统，RC6-XTS-CBC+Elephant diffuser 方式加密性能最好，即采用 RC6-XTS 对操作系统进行加密，而采用 RC6-CBC+Elephant diffuser 对数据块较大的用户文件进行加密。针对全盘加密的这种混合方式的加密速度比单一的 RC6-XTS 方式快 7%。

宽块加密模式以扇区整体作为输入，对于大文件组而言，数据划分后的分组数较窄块加密模式少许多，在进行加密运算之前所产生的相应开销(如扇区密钥、初始向量的产生)也较少，因此宽块加密模式下的性能较好。对于小文件组，由于数据本身比较小，宽块加密模式下的分组数并没有比窄块模式下的分组数量减少很多，因此性能开销降低有限，同时，窄块加密模式对单个分组的加密处理速度较快，对于小文件组的加密性能有显著优势。从图 2 中可以看出，加密模式是产生不同数据块加密性能差别的原因，加密算法只是影响着性能差别的程度。

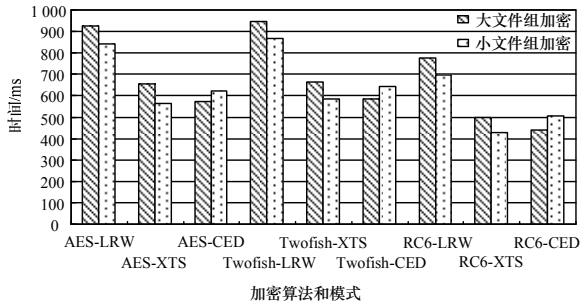

图 2　大、小文件组加密性能比较

5　结束语

本文对磁盘加密的算法和模式进行了性能上的评估，实验结果说明，RC6 是进行测试的 3 种算法中最快的，窄块加密模式(LRW 和 XTS)更适用于加密数据块较小的文件，而宽块加密模式(CBC+Elephant diffuser)适用于对大文件进行加密处理。在全盘加密系统中，性能最优的结合方式是操作系统文件加密使用 RC6-XTS，用户文件加密使用 RC6-CBC+Elephant diffuser，即 RC6-XTS-CBC+Elephant diffuser 方式。

参考文献

[1] Casey E, Stellatos G. The Impact of Full Disk Encryption on Digital Forensics[J]. ACM SIGOPS Operating Systems Review, 2008, 42(3): 93-98.

[2] IEEE. IEEE Standard for Cryptographic Protection of Data on Block-oriented Storage Devices[EB/OL]. (2008-09-09). http://grouper.ieee.org/groups/1619/email/pdf00086.pdf.

[3] 张　慧, 郭翠芳, 牛夏牧, 等. 磁盘加密模式分析[J]. 计算机工程, 2010, 36(5): 134-136.

[4] Liskov M, Rivest R, Wagner D. Tweakable Block Ciphers[C]//Proc. of CRYPTO'02. London, UK: Springer-Verlag, 2002: 31-46.

[5] El-Fotouh M A, Diepold K. Statistical Testing for Disk Encryption Modes of Operations[EB/OL]. (2007-12-14). http://eprint.iacr.org/2007/362.

编辑　任吉慧