

基于 AES 加密存储的磁盘销毁策略

于游, 付钰, 吴晓平

(海军工程大学信息安全系, 湖北 武汉 430033)

摘要: 针对在紧急时刻对磁盘内敏感数据销毁的要求, 结合 AES 加解密算法, 提出了一种基于加密存储的磁盘快速销毁的方案, 以满足在紧急时刻对数据销毁在时间和安全上的要求。详细论述了该方案的原理方法以及依据, 通过该方案可以实现快速、高效、安全地将敏感数据进行销毁。

关键词: 磁盘销毁; AES 算法; 覆写技术; 加解密技术

中图分类号: TP309.7

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2018030

Destruction strategy for disks based on AES encrypted storage

YU You, FU Yu, WU Xiaoping

Department of Information Security, Naval University of Engineering, Wuhan 430033, China

Abstract: For the requirement of destroying sensitive data in the disk in emergency, combined with the AES encryption algorithm, a strategy of fast destruction of disks based on encrypted storage was proposed. The principle, method and basis of the strategy were discussed in detail. Through this strategy, sensitive data in the disk can be destroyed quickly, efficiently and safely.

Key words: disk destruction, AES algorithm, rewrite technology, encryption and decryption technology

1 引言

随着信息技术的高速发展, 计算机应用越来越普及, 几乎所有的公司及部门都在使用计算机来存储和处理信息, 如何确保计算机中的数据的安全成为人们日益关注的问题, 敏感数据的销毁是其中的一个重要方面。敏感数据的销毁对国家安全、军事保密等存储了大量敏感数据的重要部门有重要意义, 但未引起足够的重视。如何确保这些信息的安全, 尤其是在紧急情况下确保其安全是亟待解决的问题。

当前, 市面上的存储介质中, 主要使用的是磁盘和移动存储设备, 磁盘、U 盘和光盘都是目前用来存储信息的主要载体, 本文主要以磁盘为论述对象。

数据销毁是指采用各种技术途径对存储在存储设备中的数据进行清除, 以达到保护存储介质中数据不泄露、不外传的目的。

2 现有的磁盘数据的清除和销毁方法

2.1 常规的磁盘数据清除方法

鉴于磁盘存储数据的原理以及读写方法, 一

收稿日期: 2018-03-02; 修回日期: 2018-04-01

通信作者: 于游, yy874354471.oo@qq.com

基金项目: 国家自然科学基金资助项目 (No.61100042); 湖北省自然科学基金资助项目 (No.2015CFC867); 信息保障技术国防重点实验室基金资助项目 (No.KJ-13-111)

Foundation Items: The National Natural Science Foundation of China (No.61100042), The National Natural Science Foundation of Hubei Province (No.2015CFC867), The National Laboratory of Information Security Technology (No.KJ-13-111)

般的数据销毁方法(如删除操作、格式化操作)都无法彻底将想要清除的数据销毁,会产生残留数据。利用这些残留数据,通过一定的技术手段能够恢复出原有的数据信息,存在数据泄露的风险,从而对信息的安全造成威胁。

1) 删除操作

对数据直接进行删除操作,操作简单、用时短、效率高。但使用删除命令(如 DEL)来删除磁盘中的数据,实际上是通过调用 WIN32 函数实现的。删除文件系统只是将文件的文件目录项的第一个字节改成一个特殊字符“E5H”(或 6),做一个删除标记,把它们在 FAT 表中所占用的簇标记为空簇,删除在文件系统中目录区的文件名以及数据区的文件数据之间的索引链接^[1]。这种方法仅破坏文件的 FAT 或 FDT 表,并没有真正地对数据进行删除,所以通过数据恢复等手段,仍可以读取存储在数据区的数据。

2) 格式化操作

格式化操作仅仅是在操作系统中创建一个新的空文件索引,将所有扇区的状态标记为“未使用”,从而让操作系统认为磁盘上没有文件。当用户对磁盘进行格式化操作时,先扫描磁盘的每个扇区并确保它可用,然后写入新的寻址系统、磁盘根目录和文件分配表^[2]。进行格式化操作后,磁盘上创建新的根目录,使其原有的信息都变得不可访问。因此,格式化后的磁盘数据能够恢复,这就意味着对磁盘进行格式化来销毁数据也是不安全的。

可以看出,常规的数据销毁方法并没有将数据完全从磁盘上进行清除,通过恢复软件可以将数据轻松恢复,所以常规的磁盘数据销毁方法不能确保敏感数据的安全。所以,要确保数据的安全,一般会采用直接销毁的方式。

2.2 目前的磁盘销毁方式

现阶段,针对数据销毁的方法主要分为:数据覆写、介质消磁以及磁盘销毁,其中,磁盘销毁又分为物理销毁和化学销毁。

2.2.1 数据覆写

数据覆写是数据销毁技术中最复杂也比较实用的一种方法,它是在保证介质存储读写数据等功能完好的前提下,最大限度地对数据进行清除。

针对这一技术,目前常用的有文件粉碎、Gutmann 和 US Do D 5220.22-M 等方法^[3]。其原理简单概述为:用一些无效数据来替换想要彻底删除的文件所在簇上的数据,在替换过程中向文件所在簇反复多次进行数据的写入操作,最终实现对原有数据的覆盖。即使攻击者找到已清除文件所在的簇,得到的也只是覆盖后的数据,从而保护了敏感信息的安全性。

2.2.2 介质消磁

磁盘是磁性存储介质,所以具有磁性材料的性质。将磁盘置于交流磁场中,通过施加强磁场或不断减弱的交流磁场等方法,迫使其磁性颗粒重新排列顺序,使磁性颗粒发生变化,最终导致其原有的数据信息失去意义。

2.2.3 磁盘销毁

磁盘销毁分为物理销毁和化学销毁 2 种方法。其中,物理销毁主要是指采用物理破坏的方法,通过使用工具对介质施加外力破坏,或使用砂纸等粗糙工具对磁盘表面进行破坏,还可以直接对磁盘进行焚烧等操作进行销毁。化学销毁主要是指采用化学腐蚀的方法,通过使用化学试剂来破坏磁盘表面的成分,从而达到清除数据的目的。

上述磁盘销毁方法虽然可以彻底对磁盘上的敏感数据进行消除,但所需工具复杂,销毁过程耗时,不利于在紧急时刻对敏感信息进行销毁。本文针对在紧急时刻对敏感信息进行销毁的要求,基于时效性和安全性,提出一种基于高级加密标准(AES, advanced encryption standard)加密算法的磁盘存储方法。

3 AES 加解密算法的理论基础

3.1 AES 加密算法

高级加密标准是一种分组密码算法。在 2000 年 10 月,美国国家技术协会(NIST)宣布将 Rijndael 算法作为新的 AES,用来替代原先的 DES 加密算法,现已被广泛采用。不同于 DES 算法,它使用的是代替-置换网络,而非 Feistel 架构。AES 能够实现在软件及硬件上的快速加解密,易于实作,且需要很少的存储空间。

Rijndael 算法力求满足以下 3 个标准:安全性、代价、算法和实现特性。这使 AES 算法具有

抗密码分析强度高、计算效率高、内存空间要求小、软硬件适应性好的优点。

3.2 AES 的基本结构

AES 为分组密码，将明文分成一组一组的，然后进行加密操作。需要说明的是，Rijndael 和 AES 还是有所不同的。它们唯一的差别在于各自所支持的分组长度和密钥长度的范围不同。Rijndael 是有可变分组长度和可变密钥长度的分组密码。其分组长度和密钥长度均可独立设定为 128~256 bit (32 bit 的位数)。而 AES 则将分组长度固定为 128 bit，仅支持 128 bit、192 bit、256 bit 的密钥长度。

AES 加密算法主要包括 4 部分：字节代替、行移位、列混合和轮密钥加^[4]。需要注意的是，最后一轮迭代不执行行列混合。

1) 字节代替

AES 的字节代替其实是一个简单的查表操作。AES 定义了一个 S 盒和一个逆 S 盒。在执行加密前，AES 已经将明文分为长度为 128 bit 的分组（即 16 byte），作为一个状态矩阵（4×4）。在字节代替操作中，把每个字节的高 4 bit 作为行值，低 4 bit 作为列值，映射到 S 盒（或逆 S 盒）中，取出对应元素作为输出，替换掉原有的数据。

2) 行移位

AES 的行移位是一个简单的左循环移位操作。当密钥长度为 128 bit 时，状态矩阵的第 0 行左移 0 byte，第 1 行左移 1 byte，第 2 行左移 2 byte，第 3 行左移 3 byte。

3) 列混合

AES 的列混合变换是通过矩阵相乘实现的。将经行移位后的状态矩阵与固定的矩阵相乘^[5]，得到混淆后的状态矩阵。

4) 轮密钥加

AES 的轮密钥加可以看作字逐位异或的结果。轮密钥加是将 128 bit 轮密钥同状态矩阵中的数据进行逐位异或操作，从而得到下一轮的密钥。

AES 加解密的过程如图 1 所示。其中，解密过程为加密过程的逆过程。

需要注意的是，在 AES 加密算法中，密钥长度不同，推荐加密轮数也不同，如表 1 所示。

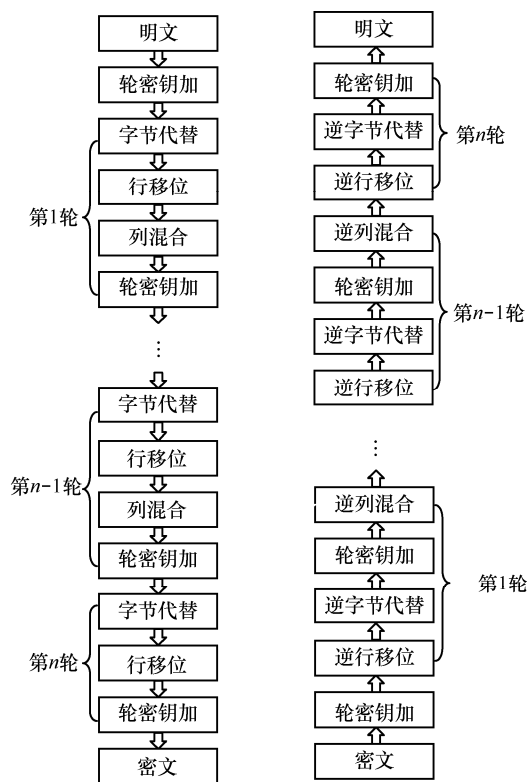


图 1 AES 加解密过程流程

表 1 AES 加密算法的几种加密参数

AES	密钥长度/bit	分组长度/bit	加密轮数
AES-128	128	128	10
AES-192	192	128	12
AES-256	256	128	14

4 基于 AES 加密算法存储的磁盘及其销毁策略

4.1 策略的实现

针对磁盘存储敏感数据，提出一种基于 AES 加密算法的磁盘存储方式，以实现在紧急情况下可以快速、高效、安全地删除并保护敏感数据不被获取。

一般情况下，系统都是直接将文件写入磁盘中，磁盘在写入文件时，按照柱面、磁头、扇区的方式进行，即最先是在第一磁道的第一磁头下的所有扇区，然后是同一柱面的下一磁头……一个柱面存储满后就推进到下一个柱面，直到把文件内容全部写入磁盘。系统也是以相同的方式读取数据。读出数据时通过告诉磁盘控制器要读出扇所在的柱面号、磁头号 and 扇区号进行^[3]。

现将系统要写入磁盘的文件先经过 AES 加密之后, 再将解密密钥及已加密的文件一同写入磁盘。在读取文件时, 先根据密钥的物理地址将文件对应的解密密钥提取出来, 然后根据文件的物理地址将所需文件提取出来, 经解密操作后得到所需内容的文件。

经过 AES 加密存储的文件, 在没有读取权限(未获得密钥)的情况下, 是无法对文件的内容进行正常读取的, 保护了文件内数据的安全。

在紧急情况下, 如敏感数据面临被窃取、抢夺的威胁, 需要在短时间内, 立刻对敏感数据进行销毁, 防止攻击者得到内容, 以确保数据的安全。这时可以采取直接对存储在磁盘中的 AES 密钥进行销毁的方法, 使攻击者无法得到解密密钥, 即使得到磁盘中的内容, 也无法进行解密, 从而无法获得真实的内容, 保护了敏感数据的安全。

在对磁盘中 AES 密钥进行销毁时, 采取覆写的方式。利用这种方式, 时间短、代价小, 操作简单。数据覆写是将非保密数据写入以前存有敏感数据的存储位置的过程。硬盘上的数据都是以二进制的“1”和“0”形式存储的。使用预先定义的无意义、无规律的信息覆盖硬盘上原先存储的数据, 完全覆写后就无法知道原先的数据是“1”还是“0”, 也就达到了清除数据的目的^[4]。具体的覆写在上文中已经说明, 这里不再赘述。根据数据覆写时的具体顺序, 软件覆写分为逐位覆写、跳位覆写、随机覆写等模式。根据时间、密级的不同要求, 可组合使用上述模式。美国国防部 Network & Computer Security 的 DoD 5220.22-M 标准^[5]和北约 NATO 的多次覆写标准规定了覆写数据的次数以及覆写数据的形式。对所需覆写的数据进行覆写的次数越多越安全。

4.2 策略可靠性论述

随着密码技术的不断发展, 越来越多的加密手段被提出。这些密码加密方法各有其特点, 适用环境也有所不同, 下面就为何使用 AES 加密算法作为磁盘保护算法进行详述。

根据密钥类型不同将现代密码技术分为两类: 对称加密算法和非对称加密算法。其中, 对称加密算法主要有 DES (data encryption standard)、3DES (triple DES)、AES (advanced encryption standard), 非对称加密算法主要有 RSA、DSA (digital signature algorithm)、ECC (elliptic curves cryptography)。由于不同加密方法的加密过程不同, 所以它们在性能和安全上也存在差距, 具体如表 2 所示。

由表 2 中数据可以看出: AES 加密算法在加解密速度、资源消耗及安全性上都具有优越性。尤其在加解密速度上, AES 的运算速度是公钥算法的 100~1 000 倍, 可以满足磁盘在数据读取时对时间的要求, 几乎完成了隐形的加解密操作; 且对仅在系统内部使用的密码算法而言, 对称密码算法在速度和资源消耗上优于非对称加密算法。

磁盘在读写数据时的传输速率约为 100 MB/s, 假设一个 500 GB 的磁盘(柱面数 1 024、扇区数 64, 每个扇区 4 kB), 若要在紧急情况下采用覆写的方式将磁盘中的数据进行清除, 若在写入数据的时候没有对数据进行加密直接写入, 则需要将整个盘进行覆写, 覆写一次的时间约为 1.5 h; 若是先将数据进行加密再写入, 密钥所占的存储空间不到磁盘总存储空间的千分之一, 所以若只对密钥部分进行覆写, 覆写一次的时间不超过 1 min, 根据美国的 US DoD 5220.22-M 覆写标准, 是对需要消除的数据进行 3 次覆写, 第 1 次使用一个

表 2 几种加密算法的性能对比

算法名称	密钥长度/bit	算法速度	资源消耗	破解时间	安全性
DES	56	较快	中	1 天	低
3DES	112/168	慢	高	46 亿年	中
AES	128/196/256	快	低	1 490 000 亿年	高
RSA	1 024/2 048	慢	高	2 年/80 年	高
DSA	1 024/2 048	慢	只适用于数字签名	2 年/80 年	高
ECC	160	快	低	2 年	高

8 bit 字符覆盖, 第2次使用它的补码覆盖, 第3次使用随机字符覆盖^[8]。US DoD 5220.22-M 覆写标准的安全性是经过论证的^[9], 其安全性较高, 可以满足敏感数据消除的要求, 所以采用 US DoD 5220.22-M 标准对磁盘中密钥进行覆写, 总时长不超过 5 min, 满足在紧急情况下对销毁快速性的要求。

相比传统的数据清理和销毁方法, 这种基于 AES 加密的磁盘存储方式可以较好地满足在紧急情况下的敏感数据销毁问题, 在销毁时间和销毁程度上均得到了保证。

5 结束语

随着数据销毁技术的需求越来越强烈, 它应该以安全为前提, 向着更加快速、高效、无痕的方向发展, 下一步考虑对加解密密钥进行保护存储, 使用更加复杂高效的密码机制对数据进行保护。

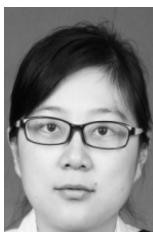
参考文献:

- [1] 林向辉. 一种数据库容灾技术的设计与实现[D]. 成都: 电子科技大学, 2011.
LIN X H. Design and implementation of a database disaster recovery technology[D]. Chengdu: University of Electronic Science and Technology of China, 2011.
- [2] 徐菁, 朱有佃, 赖凡. 论磁介质的数据销毁技术[J]. 西南师范大学学报(自然科学版), 2007, 32(4): 107-110.
XU Q, ZHU Y D, LAI F. Discussion on data destruction technology of magnetic media[J]. Journal of Southwest China Normal University(Natural Science), 2007, 32(4), 107-110.
- [3] 刘铭, 孙宝辉. 浅谈计算机存储介质的数据销毁技术[J]. 电子技术与软件工程, 2013(16): 207.
LIU M, SUN B H. The data destruction technology of computer storage media[J]. Electronic Technology & Software Engineering, 2013(16): 207.
- [4] NIELS F. BRUCE S, TADAYOSHI K, 著. 密码工程——原理与应用[M]. 北京: 机械工业出版社, 2017: 32-33.
NIELS F. BRUCE S, TADAYOSHI K. Password engineering——principle and application[M]. China Machine Press, 2017: 32-33.
- [5] KATZ J, LINDEL Y. 现代密码学——原理与协议[M]. 北京: 国防工业出版社, 2012.
KATZ J, LINDEL Y. Modern cryptography——principle and protocols[M]. Beijing: National Defense Industry Press, 2012.
- [6] 袁胜昔, 盛双艳, 相利辉, 等. 磁盘结构与原理[M]. 北京: 清华大学出版社, 2015.
YUAN S X, SHENG S Y, XIANG L H, et al. The structure and principle of disk——principles and protocols[M]. Beijing: Tsinghua University Press, 2015.
- [7] 王建峰. 数据销毁: 数据安全领域的重要分支[J]. 计算机安全, 2006(8): 53-54.
WANG J F. Data destruction: an important branch of data security[J]. Computer Security, 2006(8): 53-54.
- [8] A guide to understanding data remanence in automated information systems[S]. Department of Defense Manual, DoD 5220.22-M, 1995.
- [9] DoD national industrial security program operating manual (NISPOM)[P]. 1995.

[作者简介]



于游(1995-), 女, 山东威海人, 海军工程大学硕士生, 主要研究方向为信息安全。



付钰(1982-), 女, 湖北武汉人, 博士, 海军工程大学副教授, 主要研究方向为信息安全风险评估。



吴晓平(1961-), 男, 山西新绛人, 博士, 海军工程大学教授、博士生导师, 主要研究方向为系统分析与决策。