

基于 AES&RSA 混合加密策略的硬盘分区加密技术

董军利, 宋福刚, 管文强, 魏广博

(解放军 72850 部队, 山东 济南 250031)

摘 要: 针对当前硬盘分区加密策略加密速度慢、安全性低, 以及只对数据加密无法实现对应用软件加密的问题, 设计了 AES(高级加密标准)和 RSA(公钥加密算法)混合加密策略, 将 AES 的安全高速与 RSA 的安全密钥分发体制相结合实现一种新的硬盘分区加密技术. 采用驱动层加密技术提升加密速度并实现操作对用户透明, 设计简易数字证书和密钥生成模块将用户与密钥一一对应, 增强系统安全性.

关键词: AES; RSA; 驱动层加密; 数字证书; USB-KEY

中图分类号: TP31

文献标识码: A

文章编号: 1000-7180(2012)01-0135-03

A Hard Disk Partition Encryption Techniques Base on AES&RSA Mixed Encryption Strategy

DONG Jun-li, SONG Fu-gang, GUAN Wen-qiang, WEI Guang-bo

(72850 Unit of PLA, Jinan 250031, China)

Abstract: The current encryption strategy of the hard disk partition, which has slow encryption speed and low security, can only encrypt data and it cannot encrypt internet applications. In order to solve this problem, we design the mixed encryption strategy that is a new encryption technique of hard disk partition combined AES and RSA. With AES, the encryption can be quicker and safer. With RSA, the key can be distributed more safely. The encryption technique, which encrypt data or internet applications in drive layer, can upgrade the speed of encryption and realize the transparence of manipulation to users. In order to enhance the system security, the encryption technique associates users with keys by designing the digital certification and the key module.

Key words: AES; RSA; drive layer encryption; digital certification; USB-KEY

1 引言

当前涉密计算机数量大、分布广、流动性强、应用环境复杂, 计算机中的数据安全受到严峻挑战. 涉密计算机一旦丢失或被非法侵入, 窃取或更改其中数据都将对信息安全带来严重后果.

2 当前分区加密现状

现有仅靠操作系统安全功能来保证硬盘数据安全性的方法过于脆弱. 当前硬盘分区加密软件在应用中存在以下不足: 通常只对数据文件进行加密, 对应用程序进行加密的相对比较少; 采用单一的对称加密算法进行加密, 加解密采用同一密钥, 存在潜在

的危险性^[1]; 加密软件采用短密码很容易被穷举法破解, 采用长密码存在记忆困难; 现有加密软件对硬盘加密速度慢、错误率高^[2].

针对以上问题, 结合对称加密算法和非对称加密算法提出了 AES&RSA 混合加密策略^[3], 并结合软件与专用 USB 分离的方法, 设计了安全系数更高的硬盘分区加密技术.

3 AES&RSA 混合加密策略

AES&RSA 混合加密策略如下: AES 对称加密算法具有加密速度快, 加密强度高的特点, 但其加解密采用同一密钥存在很大安全隐患^[4], 采用 RSA 非对称加密算法相对加密速度较慢但其安全的密钥分

发体制解决了密钥安全问题. 文中设计开发的 AES&RSA 混合加密算法将 AES (Advanced Encryption Standard, AES) 的安全高速与 RSA (Rivest-Shamir-Adleman) 的密钥安全体制结合起来^[5]. 系统框图如图 1 所示.

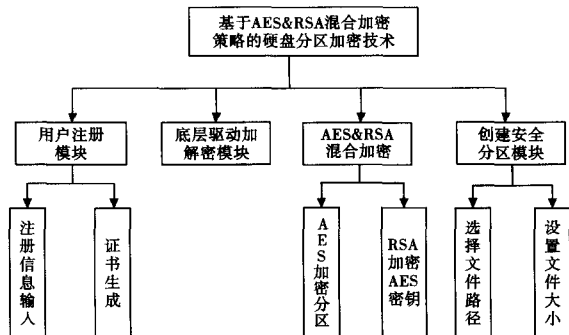


图 1 系统功能框图

首先,在驱动层实现一个系统分区,并将其与硬盘上的一个特殊格式文件建立映射关系,任何保存到这个系统分区中的数据都会被加密后写入到指定文件中,该涉密文件分区和其它磁盘分区(C 盘、D 盘等)没有任何区别,用户在该分区中的操作与真实文件系统保持高度一致,易于操作使用.

系统基于 PKI 非对称密钥体制和传统的对称密钥体制相结合^[6],从根本上防止对称密钥体系的密钥分发弱点并通过非对称密钥体制增强安全性. 系统采用 AES 对称密钥对文件进行加密^[7], RSA 非对称密钥的公钥对对称密钥进行加密,系统加密策略如图 2 所示.

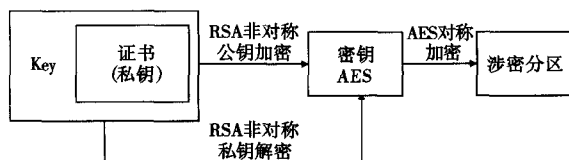


图 2 AES&RSA 混合加密策略

系统在驱动层设置 AES&RSA 混合加密策略的数据加解密模块,其完全接管操作系统及应用软件对该分区的读写请求,写入磁盘数据时,该模块首先取得控制权,USB KEY 中私钥对 AES 对称密钥进行解密,AES 取得密钥后对写入分区数据进行加密取得密钥进行加密操作,然后将加密过的数据写入磁盘指定位置^[8];读取磁盘数据时,该模块同样首先取得控制权,到磁盘指定位置读取数据并根据从 USB KEY 中取得的密钥进行解密操作,然后将解密后的数据提交给相应程序. 系统将特殊格文件进

行隐藏并卸载分区实现数据的二层安全防护,只有将 USB KEY 插入时,通过口令才能够使加密分区显示出来. 即便是硬盘被拆卸到另外的计算机上,如果没有相应的 USB KEY 也无法读出硬盘涉密分区中的内容.

系统主要通过以下几种方法实现硬盘分区加密的安全与高速:

(1) 应用驱动级加解密技术,工作在受系统保护的内核层,运行速度更快,加解密操作更稳定.

(2) 采取 U-Key+口令的双因子保护模式,增强了应用数据的安全性.

(3) 安装于加密分区中的涉密软件也是通过加密存储的,保证程序能够得到安全保护,未经授权程序无法正常运行.

(4) 对称算法 AES 与非对称算法 RSA 两种加密模式相结合,在保障加密速度的基础上也满足系统的高安全性要求.

4 关键技术及创新应用

(1) 采用驱动层加解密技术提升加密速度并实现应用程序加密

系统通过底层驱动实现一个加密文件分区,并将该分区映射到硬盘上的一个特定格式的文件,任何保存到这个加密分区上的数据都会被写入到该文件中. 通过系统对该分区的操作都先经过驱动层的加解密处理,保证应用数据的安全. 驱动层加密技术是基于 Windows 的文件系统(过滤)驱动技术,系统开发采用 Microsoft DDK 7 驱动开发软件,首先创建直接读写的系统 IO 设备,然后再捕获 windows 系统 IOCTL_FILE_DISK_OPEN_FILE、IOCTL_FILE_DISK_CLOSE_FILE、IOCTL_FILE_DISK_QUERY_FILE 等系统 IRP 请求,将读写请求序列化,放入队列中. 为每个设备对象生成一个系统线程,来依次处理这些请求,在访问数据前先访问加密模块进行加解密. 对请求进行处理,其中最主要的处理在系统的读写处理上,如果系统触发写 IRP 请求,则执行加密操作,如果系统触发读 IRP 请求,则执行解密操作. AES 对称密钥加密保存在加密分区中,驱动层对文件的加解密在驱动层实现,与应用程序无关,相对于应用层加密技术其运行速度更快,加解密操作更稳定.

首先建立特殊格式的文件,通过底层驱动创建加密分区,将特殊文件和加密分区挂接在一起,完成加密分区的创建,操作系统对加密分区的操作,最终

都转化为对读写文件的操作. 本系统驱动在 Windows 操作系统中属于用户态驱动,在物理设备驱动和中间层驱动之上,直接向应用程序提供服务,它用来扩展底层驱动的功能,实现特定的文件系统,为用户提供在特定存储介质上存储信息以及从这些存储介质中取回信息的方法.

(2) 利用 AES 对称加密和 RSA 非对称加密算法互补实现加密安全、高速

系统在驱动层采用 AES 对称加密算法对读写文件进行块加密,用 RSA 非对称算法的公钥对 AES 的密钥进行加密^[9],用私钥对其解密. RSA 非对称密钥算法是基于素数分解难题的公钥体系密码算法,目前 1024 比特被认为是既安全又高效的公钥算法之一,用 1024 位高强度密钥满足了系统的安全性,其缺点是相对对称加密速度较慢. AES 高级加密标准,是世界绝大多数国家采用的的标准对称加密算法,其特点是加密安全性高、速度快,但缺点是对称密钥体系的密钥安全性低. 本系统使用 AES 对称算法进行加密,从而克服加密速度慢的问题;涉密硬盘分区加密系统利用公钥体制为基础,保护 AES 对称密钥,把 RSA 公钥体系的安全性和 AES 对称加密体系的高速度结合,保证数据存储的安全快速. 同时私钥及证书存放于专用的 USB KEY 中,未经授权不能使用,进一步保证密钥安全,从根本上保证了应用数据的安全.

(3) 采用数字证书技术解决身份认证和 AES 密钥安全问题

为保证系统文件存取速度,系统采用 AES 对称加密算法,为保证对称密钥的安全性,文中采用 RSA 非对称密钥加密算法,使用公钥对密钥进行加密,并将其私钥存放于 KEY 中,在此设计了密钥生成和数字证书模块. 数字证书基于 PKI/CA 体系,是当前网上电子商务/政务中进行身份确认、数据完整性最安全的方法之一. 本系统通过数字证书实现用户实际身份和密钥对的统一,密钥写入 KEY 中,无法导出,保证密钥安全性. 系统采用非对称加密技术,通过 RSA 算法,采用 1024 位高强度密钥,对对称密钥进行私钥加密. 系统内嵌简易数字证书和密钥生成模块,在用户注册时自动生成用户证书和非

对称密钥对,保证数据的完整性和安全性,密钥模块能够生成 RSA 1024 比特密钥,按照 X. 509 标准生成证书,满足了系统需求.

5 结束语

该策略基于底层驱动加解密技术,以“软件+硬件”相融合的方式,综合运用 AES 对称密钥加密算法及 RSA 非对称密钥加密算法,在驱动层对数据进行加密,RSA 私钥存放于 USB-KEY 中,与系统物理隔离,保证了数据安全,具有很强的实用价值.

参考文献:

- [1] 龙冬阳,王常吉,吴丹. 应用编码与计算机密码学[M]. 北京:清华大学出版社,2005.
- [2] 冯登国. 密码学分析. [M]. 北京:清华大学出版社,2005.
- [3] 单玉峰,潘孟贤. 一种新的加密标准 AES [J]. 信息技术,2002(11):32-33.
- [4] 21 世纪美国高级加密标准推荐算法 Rijndael 文集 [R]. 总参谋部第五十一研究所,2000.
- [5] 杨德山,陆魁军. 一种改进的 RSA 加密算法设计与实现[J]. 计算机应用与软件,2007(10):189-191.
- [6] 关振胜. 公钥基础设施 PKI 及应用[M]. 北京:电子工业出版社,2009.
- [7] 钱松,周钦,俞军. AES 算法的一种高效 FPGA 实现方法[J]. 微电子学与计算机,2005,22(7):89-91.
- [8] 景为平,徐晨,陈海进. AES 密码算法的结构优化与实现 [J]. 微电子学与计算机,2007(2):36-38.
- [9] 范黎恒,陈开颜,张鹏. 抵御简单功耗分析的 RSA 模幂算法实现 [J]. 微电子学与计算机,2009(26):227-229.

作者简介:

董军利 男,(1961—),硕士,高级工程师. 研究方向为密码学.

宋福刚 男,(1971—),本科,工程师. 研究方向为计算机应用.

管文强 男,(1974—),硕士,工程师. 研究方向为计算机应用.

魏广博 男,(1977—),硕士,工程师. 研究方向为计算机应用.