

基于 LayerFileSystem 架构搭建



SEFS 透明加密平台

技术白皮书

2010 年 3 月

概述

SEFS3 是新一代的透明加密内核，基于分层文件系统(Layered FileSystem)理念, 结合独具中国特色的 防泄密、文档安全市场的需求而开发的全新透明加密平台。

简介

针对传统的透明加密驱动技术 - (依赖清楚缓存来区分不同的进程对加密文件内容的访问控制) 所带来的文件损坏、应用程序兼容性差、与杀毒软件等类似技术存在 严重冲突等问题，SEFS3 提出了独到的解决思路。真正实现了一个文件、多个缓存。不同的进程访问不再依赖于梦魇般的暴力清除文件缓存。同时 SEFS3 也 实现了一个全新的 Callback 架构的 Windows 文件系统平台，可以将应用任意的扩展到网络文件系统、远程的存储媒体如 FTP、SSH 等服务器。

原则

遵循 SEFS 一贯追求的 “**简洁 稳定 高效 兼容**” 开发原则。SEFS3 将提供您全新的文档安全、文档控制、内网防泄密、分布式存储、实时备份等应用领域的解决之道。

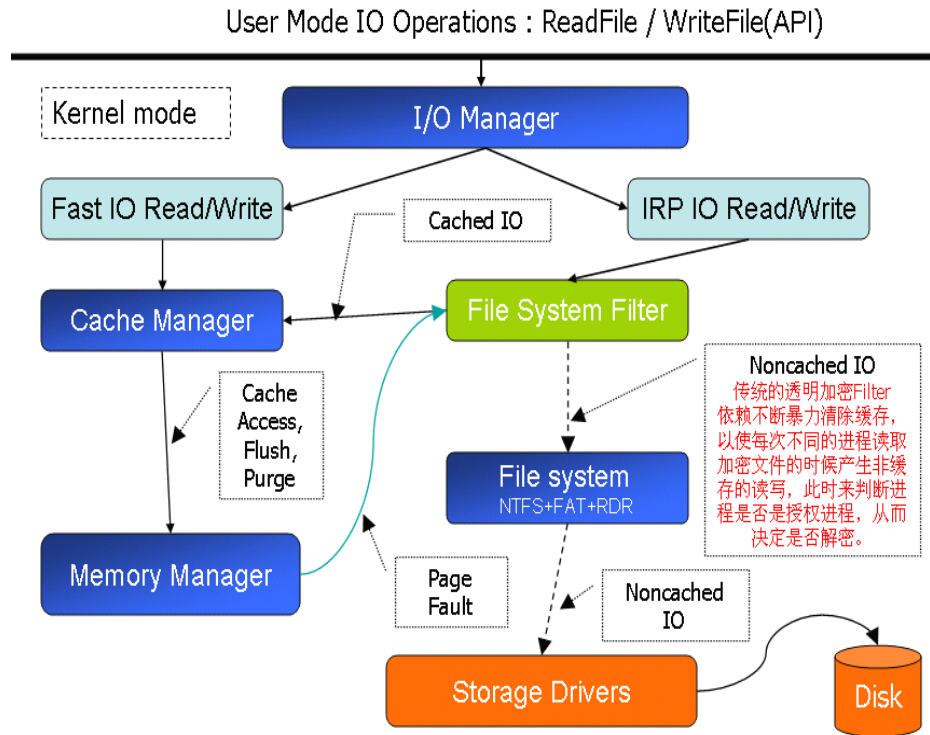
背景分析

在 Windows 操作系统中每个文件对应仅仅只有一份缓存,如果缓存脏或者是缺页将由操作系统的“虚拟内存管理器(VMM)”或者“缓存管理器(CM)” 文件系统发出非缓存(NoCache I/O)的 I/O 读写请求。系统所有的进程读写相同的文件所得到内容都是一样的。这样可以减少对磁盘的读写,从而提高系统的性能,这是 Windows 系列操作系统的设计原则。

但是随着国内对文档安全意识的逐步提高,客户和应用开发商都意识到对加密文件的读写需要区分不同的进程。也就是一个文件因为读写的当前进程不同。需要呈现出不同的内容(明文或者密文)。为了解决这一颇具中国特色的需求。国内的开发商提出了各种解决方案,应用层的加密由于性能及安全性方面的天然性欠缺,已经慢慢的淘汰出主流的市场。主流的驱动就加密技术基本都是采用实时的刷新缓存来识别进程的解密权限。

蓝屏和损坏的根源

暴力清除加密文件缓存的缓存 在文件过滤器中 截获非缓存的读取 由进程的不同 来决定是否解密从而实现不同的进程读取相同的加密文件得到截然相反的明文和密文。

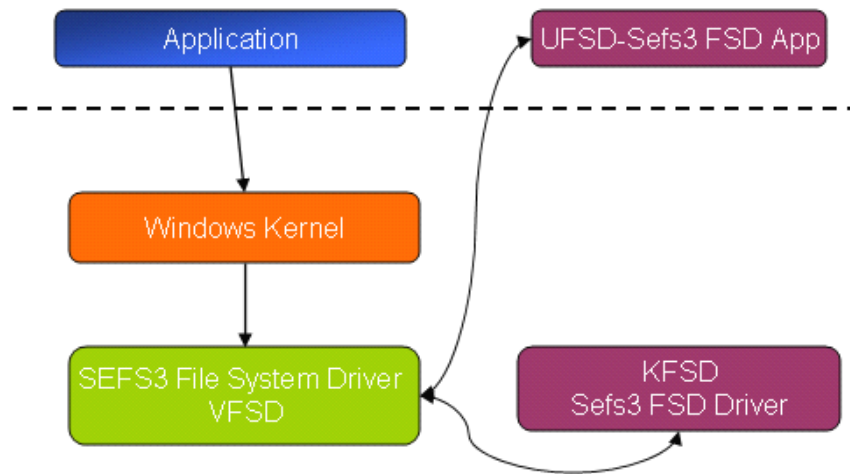


国内透明加密市场的现状

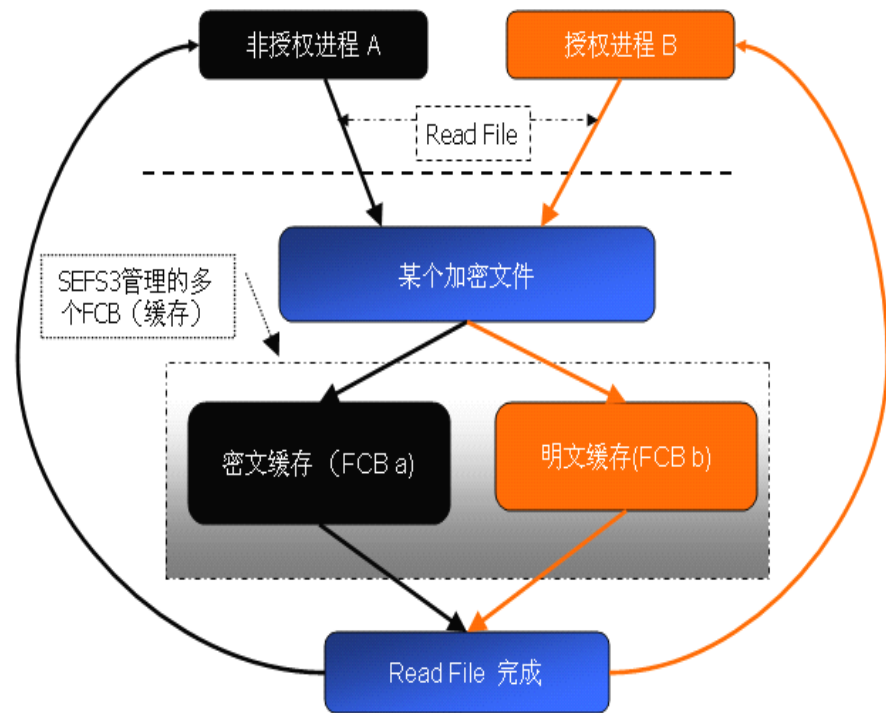
正是这样的原因，现有的驱动透明加密普遍存在损坏文件、性能降低、兼容性差等诸多问题。乃至不少的厂商在宣传中都不再强调软件的功能和特色，只要突出稳定、不破坏文件就能获得不错的市场回报。

SEFS 解决之道

SEFS3 提出了全新的解决之道。首先 SEFS3 不再是单个文件过滤器驱动。而是一个加密平台。SEFS3 架构如下图所示(点击图片可查看大图):



在 SEFS3 架构中,授权和非授权进程对加密文件的读取不同的内容不再依赖于缓存的暴力清除,而是 SEFS3 管理了多个缓存内容(多个 FCB),不同的进程的读取被指向不同的缓存块。从而安全的实现这一颇具中国特色的需求。同时也减低了同杀毒软件等基于文件过滤器技术的冲突。如下图所示(点击图片可查看大图):



技术特点

- 用户可在应用层实现自定义的文件系统,可以实现加解密文件系统、或者是压缩文件系统、又或者分布式存储
SEFS3 提供用户自定义文件的 Demo 源代码,方便您的开发
- 用户可在应用层选择 CSP 或者 PKCS11 等加密规范实现 [PKCS7 数字信封](#) 格式的文件加密封装,从容嵌入 PKI 体系,实现文件权限、身份鉴别、文件签名、文件验证等类似 [MS EFS](#) 的功能。
- 实时加解密,透明服务。SEFS3 不会有性能的瓶颈,不会改变应用程序的行为和用户使用习惯。
- 用户无选择强制加密。强制加密所有涉密进程的运行中产生的文件(包括但不限于临时文件、随机文件、导出文件等)。这样无论另存为什么样的文件名称,装换为什么样的文件格式

式（包括未知的格式），都会受到严格的加密保护。就算使用一些

文件恢复工具也无法得到某些应用程序(如 Word)的明文内容。

- 严格密文进程校验。SEFS 基于应用程序的特征值和名称同时校验。只有经过授权的进程才能完成解密从而得到明文。而非法的、
伪装的进程将不能完成解密。只有非法进程无论是通过 Email 或 FTP 等网络的传输都将是密文。
- 完善的文件缓存控制，不同进程可以同时读取加密文件，也能实现不同内容呈现

支持系统

支持 NT 架构的系列操作系统 (32/64 位)：

- Windows7.
- Windows2008.
- Vista.
- Win2003.
- WinXP.

支持软件

经过压力测试通过兼容测试的应用软件：

- 编程类：[VC6/VB/Delphi/VS2003/Vs2005](#)
- 办公类：MS Office 系列办公软件
(Word/Excel/PowerPoint)、记事本软件 NotePad
- 制图类：Photoshop 系列、CorelDraw 系列、画图
(Mspaint)。
- 二维 CAD 类:AutoCAD2004、AutoCad2006、基于 AutoCAD 二

次开发的 圆方 BtoCAD 等.

- 三位 CAD 类:Pro/E、CATIA、Protel 99E、等
- 编程开发类:VC6/VB/Delphi/VS2003/Vs2005...等

通常未列出的应用软件可以通过自定义策略来支持。

SEFS 透明加密平台技术白皮书

撰写：James Xiang

更多信息请访问：

<http://www.sefs.net>

电子邮箱：

admin@sefs.net

2010 年 3 月

