关于防泄密系统之我所思

作者：无名氏

前言：

写此文字，不是打倒这个行业，我与这个行当没有任何冤仇，无诋毁的动机。

任何系统或者软件都不是完美的，一定存在不尽如人意的地方或者细节。

我是一个悲观的乐观者，把所有事情想到最坏，然后以乐观的心态去应对、处理这些可能发生的事情。

知己知彼方能百战不殆，如何去权衡利弊那就是您的事情了。

正文如下：

什么叫做防泄密系统？（透明加密、安全、防水墙、磁盘加密、文件保护、动态加密、文档安全管理等等），概念眼花缭乱，诱惑十足。

根本上来说就是：

1、在保存文档的时候改变了原文档的存储架构进行了改变；（或者对存储的内容进行了移位、异或、校验等等处理，当然配合一定的加密算法）。

2、在 读取的时候，做一个反向的操作。

举一个简单的事例：

Txt 文本的内容为 “协同 OA”；

我把此内容按照一定的规则、原理辨成：“ Э□ □”。□

后面的文档内容给您，您能够看懂？懂了？恭喜您到“火星球”生活了，

（“ Э□ □”这个是 “火星文”。）

当然 此类系统 实施的工作过程、提供的功能肯定比这个要复杂、完备。我只是想把这个过程简单化、具体化。这样更好理解这其中的原理性和奥秘。

如果您仅以此抨击我不懂装懂，冒充砖家，我虚心接受。

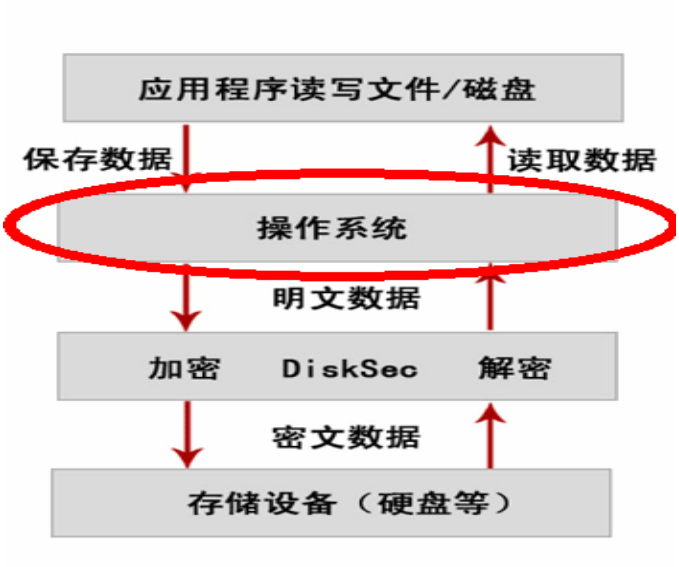
为了安全起见，我特意在百度文库里面搜索如下解释。应该算是比较客观的，即使错误了，也不是我的错，呵呵。我喜欢拉一个垫背的。

什么是加密技术 编辑本段

加密技术是最常用的安全保密手段，利用技术手段把重要的数据变为乱码（加密）传送，到达目的地后再用相同或不同的手段还原（解密）。

加密技术包括两个元素：算法和密钥。算法是将普通的信息或者可以理解的信息与一串数字（密钥）结合，产生不可理解的密文的步骤，密钥是用来对数据进行编码和解密的一种算法。在安全保密中，可通过适当的钥加密技术和管理机制来保证网络的信息通信安全。

请查看如下 2 个图片。



自动透明加解密

当系统向磁盘写入数据时，DiskSec将首先获得控制权，在数据写入之前对其进行加密；相反，在系统读取硬盘数据时，DiskSec同样能够在这之前完成对数据的解密操作，将普通明文呈现给用户。整个加解密过程都在底层自动进行，使用者完全感觉不到DiskSec的存在，数据读写操作也不会受到任何影响。

（此图片都是产品厂商官方网站截图，任何篡改）

应该可以 比较清晰的说明，加密产品工作在哪一个层面。介于操作系统和磁盘存储之间的一种机制。

很多厂商都在鼓吹基于驱动层的加密、基于应用层的加密、基于磁盘的加密。其中有什么差别不？感觉在忽悠。

简单一点说是：

保存在磁盘的东西是密文，但是通过正常的操作途径看到的资料、文档是正常的。

因为中间的加密系统在操作系统与存储介质之间做了一个加、解密的动作。

问题来了。

在 操作系统和存储介质之间做了一个动作？这个动作如果不是经过操作系统授权的动作，那么就是劫持（不管厂商使用什么技术来实现）。

广义上说就是非授权操作，讲白一点就是“潜伏”在系统中的木马。

这个时候很多厂商又开始与微软攀亲了，说获得了微软的授权。

到底是不是真实的。我没有调查，不做评论，也不在我讨论范围之类。

抛出如下问题供您思考：

1、 加密系统本身的安全性如何？

如果加密服务器崩溃了怎么办？

厂家不能够恢复产品密钥？厂家能够恢复密钥？

前者的结果您死定了，数据都变成垃圾，

后者发生，您也死定了，厂家居然可以复制、恢复、拷贝，安全何在？

2、 兼容性如何？

A、说不定哪一天的杀毒软件把您的加密进程定义为病毒、木马；

（各种名目的防病毒系统也不是省油的灯。哪一天加密厂家少交了一点"保护费"，进程肯有可能进入木马序列，呵呵。后果您是知道的。）

B、客户端软件升级也要小心啦，相同的软件不同的版本对磁盘的操作是不同的。不同的软件之间有问题。

（很多厂商都会给你一个表单，让你选择或者记录需要加密的应用软件名称和版本号、甚至是文档的后缀）

3、 性能影响？

既然做了透明机密的操作，所谓透明加密，加、解密这个过程是自动的。

但是这个操作还是在后台自动的运行，一定会占用系统资源，一定会对系统有影响，说不定哪一天崩溃了。

4、 破解、系统的漏洞？

我不讨论，你懂的。网上大把方法。未做验证，不做评论。

如文件名长度溢出、伪造进程、缓存数据拷贝甚至是修改后缀名。当然没有这么简单的。

5、 操作系统、编译环境的支持？

一直以为都只支持 WINDOWS 系统，为何？（当然目前也看到对 LINUX 等系统特定版本的有限支持）

原因很简单，

A、就是 加密的动作是基于操作系统之上的进程劫持，不同的操作系统和版本都可能影响这个过程，（ 这个加、解密过程一定要稳定、可控、可逆）

B、Windows 虽然经常打补丁，但是基本的内核还是不变的，市面上主要就是 2000\XP\WIN7\2003……屈指可数。

其他操作系统呢？比如：Linux， 众多的内核版本，您可以自行搜索。

6、 全盘加密的疑虑？

全盘加密了？是否也包含了磁盘的所有文件？废话。那么系统文件是否已经加密？引导文件是否已经加密？ 如果这样 系统应该不能够启动了。

但是 神奇了， 系统的启动还是正常的。看来还是会放过区分或固定的文件的。那么加密系统是如何区分系统文件或者分区呢？

我不再深究。

喝杯茶，继续工作 ING

……

我的谬论：
无论什么软件都不是完美的，合适与否需要取舍。
每一个企业都有不一样的选择。

我的忠告：
在正式上线此类加密产品前，我请您留意一下的步骤：
一：请选择多几家产品厂商沟通、交流；（多了解）
二：请厂商介绍一下系统的工作原理；　（深入敌后）
三：请厂商介绍一下自家产品的优缺点；（黄婆卖瓜）
四：请厂商介绍一下“友商”的优缺点；（惊爆内幕）
五：加密前文件的 MD5 值，加密后 文件的 MD5 值，解密后文档的 MD5 值。

为什么这样做？从别人的眼里才可以看到缺点。
缺点看透了，您可以更从容的在利、弊之间做取舍。
取舍之后，一定会有相应的制度、对策来扬长避短。

附：

[redacted]特色：

[redacted]的透明加解密模块不同于一般市面上所见的加密技术。市场上所见的加密技术，或者是采用了个钩子（Hook）技术、或者采用
驱动技术，但这些软件或者只能达到和文件格式有关，或者实际上是硬盘加密，市场上许多硬盘如seagate硬盘已经自带硬盘加密，实际上
联网上已经有了这些加密软件的破解工具！而且和文件格式有关的软件无法适应未来的文件格式，更无法解决软件格式被加壳的情况，而
网上基本有4000余种加壳工具。[redacted]完全和文件格式无关，[redacted]的透明加解密模块处于系统内核里面，随系统启动而启动，
统关闭而关闭。可以应对未来产生的文件格式，更能应对被加壳的文件。
最大的区别是[redacted]可加密的格式和文档格式无关。管理人员可以自由定义用户（组）的加密模式或策略：全盘加密、目录加密、特
式加密、特定格式不加密、自主加密等。

主持人：那你们内部有什么监控措施没有？因为有一些情况是，比如运营商装了这个东西，那万一我的密钥丢了怎么办？这个还是需要请你们去解决的。

[redacted]：我们现在是这样，真正对数据进行管理的密钥，我们是不会去获取的，但是就数据密钥本身，我们还是会保护起来，因为我们进行产品生产的时候，每个产
序列号、管理密码这些数据还是会保护起来。那么如果用户在使用的过程中丢了数据密钥，我们可以帮助进行初始化，但是还需要再配个密钥，如果用户原来的数据真的
全部没有了，但是这种情况一般不会发生，因为用户会进行备份，但真的是没有备份，数据全部丢失的话，我们也是没有办法的，因为我们也不能够把用户的数据全部搜
来，我们只能管理跟产品相关的密码。

主持人：运营商在采用明朝万达或者其他安全厂商的一些软件系统时，企业怎样能够取得运营商的信赖呢？合作伙伴之间的互信关系怎么去建立起来？用户会不会担买了一把锁之后，我这里有一把钥匙人家那也有一把钥匙？

[redacted]：这个不会，因为最终加密其实还是一个密钥管理的问题，加密都涉及到密钥，比如运营商在买我们的产品的时候，以每个服务器来说，它的密钥都是每个产现场安装的时候随即产生的，这也确保了每两个产品和服务器之间它的密钥都是不一样的，密钥不一样的话，相互之间的数据是没有办法互通的，除非说经过特别的授权门双方都同意这样的授权才能够互通，这个是没有问题的，从形式上面可以实现这种设计。
