TrueCrypt 加密模式及对应取证方法研究

彭建新　杜　威　王晓雷

（广东警官学院计算机系，广东 广州 510230）

摘　要　分析开源加密软件 TrueCrypt 的加密算法、操作模式 XTS，提出在计算机调查取证时所对应的方法。

关键词　TrueCrypt　开源加密　XTS　计算机取证

TrueCrypt 是全球著名的开源虚拟加密磁盘软件，目前支持 Windows 7/Vista/XP/2000，Mac OS X，和 Linux 等操作系统。TrueCrypt 加密之后形成的虚拟磁盘，在输入正确密码之后可以像本地其它磁盘一样正常访问，内部所有文件都会自动加密，其加解密过程均为实时进行，并且效率很高。

1　TrueCrypt 的特性

TrueCrypt 主要有如下特性：

1.1　所创建的虚拟加密的磁盘形式上为硬盘上面的一个文件，可以加载为一个方便操作的实际磁盘；

1.2　可以加密完整的磁盘分区，或者移动存取设备，如 U 盘或者移动硬盘；

1.3　可以加密一个分区或者一个安装好操作系统的完整硬盘驱动器；

1.4　加解密过程是完全自动的、实时的并且对用户透明的；

1.5　由于采用并行和流水线技术，对数据的加解密处理非常迅速，用户完全感觉不到与不作加密操作时的差别；

1.6　双重加密，即使是在胁迫的情况下也可以实现隐藏磁盘和操作系统的目的。

2　TrueCrypt 算法

2.1　TrueCrypt 采用如表 1 所示的加密算法。

表 1　加密算法

算法	密钥大小（比特）	分组大小（比特）	操作模式
AES	256	128	XTS
Serpent	256	128	XTS
Twofish	256	128	XTS
AES – Twofish	256；256	128	XTS
AES – Twofish – Serpent	256；256；256	128	XTS
Serpent – AES	256；256	128	XTS
Serpent – Twofish – AES	256；256；256	128	XTS
Twofish – Serpent	256；256	128	XTS

在 90 年代中期，美国国家标准与技术研究院（NIST）公开征集加密算法作为区块加密标准，筛选最后一轮后还剩下 Rijndael、Serpent、Twofish，这三种算法各有千秋，Serpent 被认为最安全，而 Rijndael 速度最快，Twofish 则居中。最后 NIST 选择了 Rijndael 作

为高级加密标准（AES，Advanced Encryption Standard）的算法，并在 2002 年 5 月 26 日使其成为有效的标准，至 2006 年，高级加密标准已然成为对称密钥加密中最流行的算法之一。

2.2　TrueCrypt 目前主要支持 RIPEMD－160，SHA－512 和 Whirlpool 等哈希算法，这些哈希算法被随机数生成器用来做伪随机“混淆”函数或者被头密钥衍生函数用作伪随机函数。在生成新的卷时，由随机数生成器产生主、次密钥（XTS 模式）和盐。

3　TrueCrypt 所采用操作模式 XTS

所谓模式，就是方法，就是加密的方法。TrueCrypt 所采用的 XTS 模式实际上就是 XEX 模式，XEX 模式由 Phillip Rogaway 于 2003 年所设计，XEX 模式和 XTS 模式细微的差别在于：XTS 模式使用两个独立的密钥，而 XEX 模式仅使用一个密钥。

2010 年 XTS 模式被 NIST 证明可以很好保护存储设备上面的数据机密性。而此前，已经于 2007 年被美国电气和电子工程师协会（IEEE）证明可以对面向块的存储设备上面的数据实现加密保护。

3.1　XTS 模式可以描述为：

$C_i = E_{K1}(P_i \hat{} (E_{K2}(n) \otimes a^i)) \hat{} (E_{K2}(n) \otimes a^i)$

其中各参数含义参考下表 2，数据单元的大小都是 512 字节（与扇区大小无关）。

表 2　XTS 模式参数

⊗	表示定义在模 $x^{128}+x^7+x^2+x+1$ 的二元有限域 GF（2）上面的多项式乘法运算
K1	加密密钥（对于所支持的加密算法如：AES，Serpent，和 Twofish，都采用 256－比特）
K2	次密钥（对于所支持的加密算法如：AES，Serpent，和 Twofish，都采用 256－比特）
i	数据单元里的加密块序号，如第一个加密块，i＝0
n	数据单元序号在 K1 的范围内取值，如第一个数据单元，n＝0
a	相对于多项式 x，在伽罗瓦域（2^{128}）中的本原元素，如 2

4　TrueCrypt 加密之后的取证方法

TrueCrypt 加密之后的文件，目前没有好的办法破解，因此在调查取证的时候，可以考虑以下方法：

4.1　分析和检查是否有 TrueCrypt 加密之后的文件存在。

（a）TrueCrypt 加密之后的文件没有固定的特征，如果加密者把这样的文件保存为常见格式的文件时，利用 Encase、Winhex、取证大师等软件分析文件特征，对于不匹配的文件重点分析，进行排查是否为加密文件；

（b）搜索系统所安装软件，包括历史安装记录，检查是否有安装 TrueCrypt 软件的痕迹；

（c）搜索大文件，作为加密容器，一般都存放着多个文件，因此，较大的文件可能性会比较大，不过也不排除特别重要的文件单独加密的可能。

4.2　TrueCrypt 能设置双层加密，即在一个加密卷中再隐藏另一个加密卷，隐藏卷形象的来说就是“嵌套”在普通加密卷里边的。当用户被胁迫解密加密卷时，用户可以把隐藏加密卷的“外套”普通加密卷解密，透露一些无关紧要的信息，而真正的受保护的信息则隐藏在隐藏卷中，数据得以保护。加密卷的加载流程如下图所示：

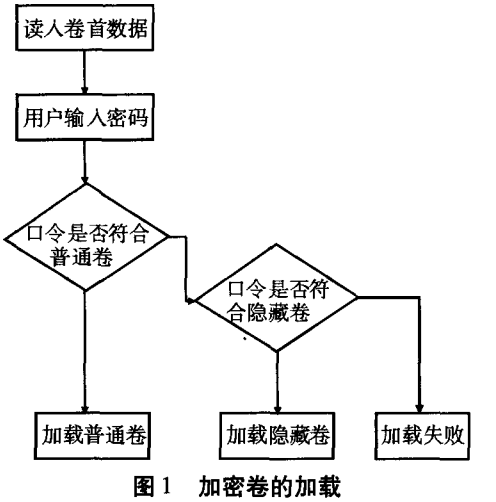

图 1　加密卷的加载

对于此类情况，首先要考虑是否能得到隐藏卷的密码，如果不能，应该把数据备份

之后，用无用数据填充的方式覆盖普通卷空余的空间，可以把伪装在普通卷里面的数据破坏，让加密者自己也无法再恢复这些隐藏的数据。

4.3　TrueCrypt 对数据的操作都是在内存（RAM）中进行，因此软件不确定是否在计算机的内存中保存有密码、主密钥和一些未加密的数据。而最新的研究成果显示，即使计算机关机后，内存保存的资料，包括加密程序的安全锁和口令仍未消失，最长可能达数分钟之久，透过冷冻计算机记忆芯片，还可延长内存暂存资料的时间，普林斯顿大学一班计算机保安专家组成的研究小组组长——计算机科学家费尔滕解释：只要以液态氮（摄氏－196 度）冷冻计算机芯片，即使电源已中断，内存仍可保持状态至少数小时。然后将芯片安装回计算机，就可读取里面的资料。

4.4　在使用者机器上安装使用间谍或者监控程序，开机自动运行，利用键盘记录钩子记录 TrueCrypt 加载卷的密码。此外，还可以利用政策，社会工程学方法（如通过其他途径获得其他帐号密码或者其他方面的信息来分析加密文件的密码）等方式来获取密码，并注意是否可以获取隐藏卷的密码。

5　总结

TrueCrypt 是全球著名的开源加密软件，有着安全、易用、功能强大等优点，也适用于可移动存储设备的加密。随着在国内应用的推广，对使用该软件加密之后的计算机数据的取证也变得越来越困难，因此有必要对这方面加强研究，总结规律，以提高取证的效率。

参考文献：

[1] 王超峰，姜梅，宋嘎子．开源加密软件 TrueCrypt 研究．微计算机信息．2010 年第 26 卷第 2－3 期．

[2] 宣龙，朱兴星，侯方勇．T rueCrypt 软件保护机密文档的研究和应用．科技信息（学术版）．2008 年第 3 期．

[3] TrueCrypt 软件用户指南．

[4] http://www.cnr.cn/nx/shtc/it/200802/t20080229_504719237.html.