开源加密工具 TrueCrypt

开源加密工具 TrueCrypt

本专题将介绍一款免费的、开源的、可移动的适用于笔记本电脑的加密软件 TrueCrypt。TrueCrypt 适用于个人或者小型企业和团队，可以在任何系统上运行而不需要安装。TrueCrypt 可以采用多种加密算法，有效地保护机密数据。

为什么选择 TrueCrypt

Ponemon Institute 在 2008 年六月代表戴尔进行的调查发现每周在飞机场丢失的笔记本电脑超过 12000 台，机密和/或隐私数据因此跌势。应该怎么做呢？有些公司采用商业的加密解决方案，但是这不是通用的做法。如果你想要自己做，或者可能你的业务或者团队的范围不大，就可以考虑把 TrueCrypt。TrueCrypt 是免费的、开源的、可移动的适用于笔记本电脑的加密软件。

- 为什么选择开源加密工具 TrueCrypt

TrueCrypt 的加密

虽然 TrueCrypt 还没有企业版本，但它对密码算法和加密方法的使用可以比得上相应的商业产品，而且使用更容易。TrueCrypt 的操作界面很简单而且很直接，可以允许你简单地执行你选择的加密方法。

- 开源加密工具 TrueCrypt 的工作方式
- 开源加密工具 TrueCrypt 的安装和加密原理
- 开源加密工具 TrueCrypt 的加密设置

TrueCrypt 的旅行模式

TrueCrypt 可以实现真正的可携带，而且应该选择这个选项。我们推荐最小 2GB 的存储设备。在旅行模式下，TrueCrypt 不需要安装到所运行的操作系统中。

- 开源加密工具 TrueCrypt 的旅行模式

为什么选择开源加密工具 TrueCrypt

这里有一条很重要的加密算法要记住：PD - (p0l1cy & enc) = br3ach

只是开个玩笑。被翻译后的版本可能就没这么可笑了，但是还不准确：没有清楚的策略和加密的移动设备可能会导致数据泄露。

Ponemon Institute 在 2008 年六月代表戴尔进行的调查发现每周在飞机场丢失的编辑本电脑超过 12000 台。

应该怎么做呢？有些公司采用商业的加密解决方案，但是这不是通用的做法。如果你想要自己做，或者可能你的业务或者团队的范围不大，就可以考虑把 TrueCrypt (www.truecrypt.org)。TrueCrypt 是免费的、开源的、可移动的适用于笔记本电脑的加密软件。使用 TrueCrypt，可以加密硬盘的某块空间，一部分或者整个磁盘，也可以加密移动存储设备。TrueCrypt 可以帮助减轻你对安全以及隐私的担忧，也可以指导企业执行最好的移动设备实践。

(作者：Russ McRee 译者：Tina Guo 来源：TechTarget 中国)

开源加密工具 TrueCrypt 的工作方式

TrueCrypt 目前不是和企业连接的，但是如果你比较关注敏感业务和个人数据，或者不满足于等待企业采用商业的解决方案，TrueCrypt 就是很好的选择了。

虽然 TrueCrypt 缺少中央管理、密钥管理、报告、访问控制功能以及企业商业产品的可测量性，但是它适合小型办公室和工作组的情况。多个用户可以通过在密码之外提交密钥文件就可以共享访问加密数据。你可以使用 TrueCrypt 的任意数字产生器创建任意数量的密钥文件。

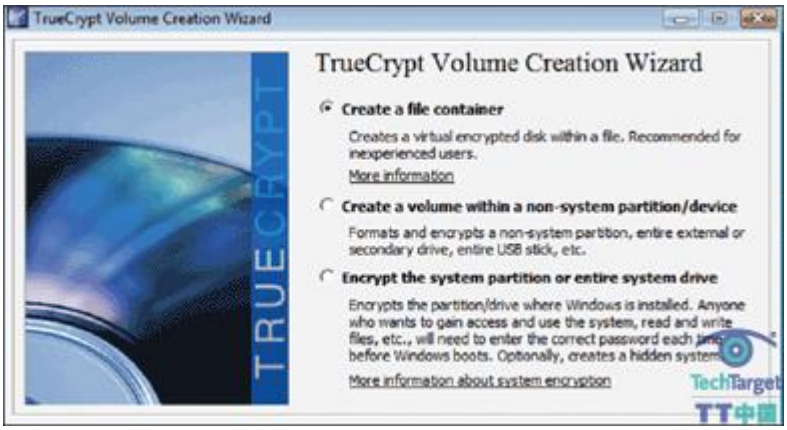
虽然 TrueCrypt 还没有企业版本，但它对密码算法和加密方法的使用可以比得上相应的商业产品，而且使用更容易。

操作 TrueCrypt 用于加密隔离区、硬盘和虚拟卷的模式是 XTS，这是 Phillip Rogaway 的 XEX 模式的一种变量。XEX 模式为两种不同的目的使用单一密钥，而 XTS 模式使用独立的密钥，尤其是自己的秘密密钥，或者独立于主要加密密钥的“调节密钥”。“调节”是指在明文文本或者密码之外可以接受的二次输入（调节）的分组加密。调节和密钥选择密码计算的排列方式。XTS 模式是 IEEE 1619 标准，它是 2007 年 12 月发布的关于密码保护基于分组的存储设备的标准。

加密算法包括 AES、Serpent 和 Twofish，而密码可以重叠，就是可以综合使用——AES-Twofish、Serpent-Twofish-AES 等。例如，一个 128-bit 的分组首先使用 Twofish (256-bit 密钥)加密，然后使用 AES（256-bit 密钥）。

哈希加密包括 RIPEMD-160、SHA-512 和 Whirlpool，而且可以在卷的创建、密码更改以及文件产生时使用。

所有的这些哈希算法都被认为是安全的，前提假设是它不能通过计算找到产生信息分类的信息。但是 SHA-512 和 Whirlpool 符合 NESSIE (New Euro-pean Schemes for Signatures, Integrity and Encryp-tion)标准，因为他们可以抵抗冲突，而 RIPEMD-160 不符合 NESSIE 标准，因为它的输出只有 160bit。



(作者：Russ McRee 译者：Tina Guo 来源：TechTarget 中国)

开源加密工具 TrueCrypt 的安装和加密原理

在 Windows 上安装 TrueCrypt 很简单，只需要下载、运行安装器、接受许可、选择安装选项钮并接受最后一步的默认选项。在 Windows Vista/XP/2000、Mac OS X 10.4 和 10.5，以及 Linux OpenSUSE 和 Ubuntu 上可以使用安装器。

此外，还可以使用操作系统选项，例如 Vista/Server 2008 的 BitLocker 或者 Mac OS X 的 FileVault，创建加密卷，部分加密或者加密磁盘，但是 TrueCrypt 提供了不可知的平台的优势——不能在任何操作系统上设置 TrueCrypt 卷。

TrueCrypt 允许创建两种容量的区：基于文件（容器）或者隔离区/基于设备。文件区是简单的正常文件，包含整个独立的虚拟磁盘设备而且可以在任何存储设备上维护。更简单的是，把它想象成存储敏感数据的硬盘或者移动存储设备上的安全区。另外，可以使用 TrueCrypt 加密整个隔离区或者整个磁盘，或者其它任何类型的存储媒介。

可以更进一步创建创建 TrueCrypt 标准区和隐藏区。标准区是常规的、可见的区，而隐藏区存在于另外一个 TrueCrypt 区中。即使你被要求（或被强制）给出密码，第三方也是看不到的。这里的技巧是 TrueCrypt 的分区在创建时，就总是充满了任意数据。隐藏区的任何一部分都和那些任意数据是不相同的。

妄想吗？可能吧，但是考虑这样一种情况，你到国外了，而你的笔记本被鉴别为“值得关注”并被没收检查。做为一个有合作精神的人，你会给出 TrueCrypt 第一个分区的密码。找到一些无害的数据后，检查的人就会满意了。但是他们不知道的是，已经用不同的密码使用了隐藏区选项，而这个区仍然是安全地隐藏着的。

（作者：Russ McRee 译者：Tina Guo 来源：TechTarget 中国）

开源加密工具 TrueCrypt 的加密设置

TrueCrypt 的操作界面很简单而且很直接，可以允许你简单地执行你选择的加密方法。

在开始之前，在你的文件系统中选择一个位置，在这里你可以存储 TrueCrypt 区，并创建新的空文件。

创建文件区，只需要点击 “创建区”按钮，登录到独立窗口中的区向导，选择创建文件容器选项按钮，然后决定选择标准区还是隐藏区。

下一步，选择你创建的一个空文件，并在被询问到你是否想要用新的 TrueCrypt 区替换的时候选择“是”。然后就是加密选项。默认的加密方法是 AES，而哈希加密的默认选项是 RIPEMD-160。因为我们想到的很多，我们选择三种方法的叠加，但是性能也会随复杂度的增加而受到影响。使用 TrueCrypt 基准功能，你可以在加密和性能之间选择合适的尺度。例如测试系统上的性能指示器显示的 AES 加密/解密性能是 64.7 MB/s，而 AES-Twofish-Serpent 是 14.5 MB/s，所以 AES-Twofish 的平衡比较合理。

然后你可以选择哈希加密算法，我们喜欢 SHA-512，它比 Whirlpool 快一些，而比 RIPEMD-160 更安全。

下一步是容量。在你想到需要的空间之外，需要考虑可携带性。例如，你可以在 2GB 的硬盘中选择 1800MB。

现在，选择一个强大的设置。TrueCrypt 可以给你的密码评定强度，所以可以增强（考虑密码短语）。如果你选择少于 20 个字符的密码，你可以因此受责备，并被提醒密码可以被轻易破解。

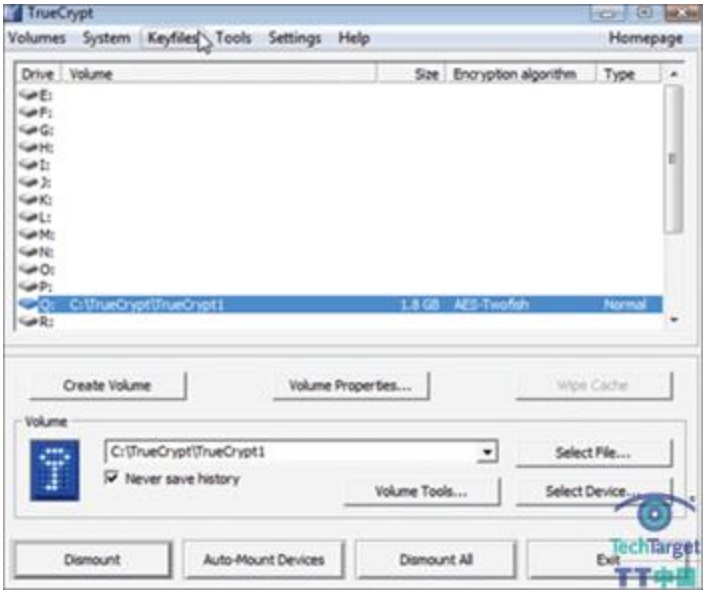
我们还推荐使用密钥文件。就像在前面提到的，在允许共享访问之外，密钥文件可以防御对密钥破解登录者和可能破解你的密码强力攻击。

（注意：如果你丢失了密码或者密码文件，还有密码恢复机制或者设备。）

最后选择格式（FAT、NTFS 或者不选）和束大小（最大 64KB）。你可以在这个窗口中看到 Random Pool，代表用于产生群加密密钥的任意数据产生器（RNG）；注意在系统静止和快速移动鼠标的时候的平均信息量的差异。鼠标移动越多，RNG 创建的任意数据（平均信息量）越多，密钥就越强大。选择格式是最后一步。

如果创建了区，就回到初始界面，操作新创建的区并进行设置。你会受到用户密码提示，而且也可以选择更高级的设置选项，包括把新建区设置为可移动媒体。这个选择在希望防御 Windows 自动在创建回收站和/或系统去信息文件夹（这些文件夹是回收站和系统还原设备使用的）的时候非常重要。

使用基准功能选择加密，维持安全和性能的平衡



设置高级选项，包括设置为可移动媒

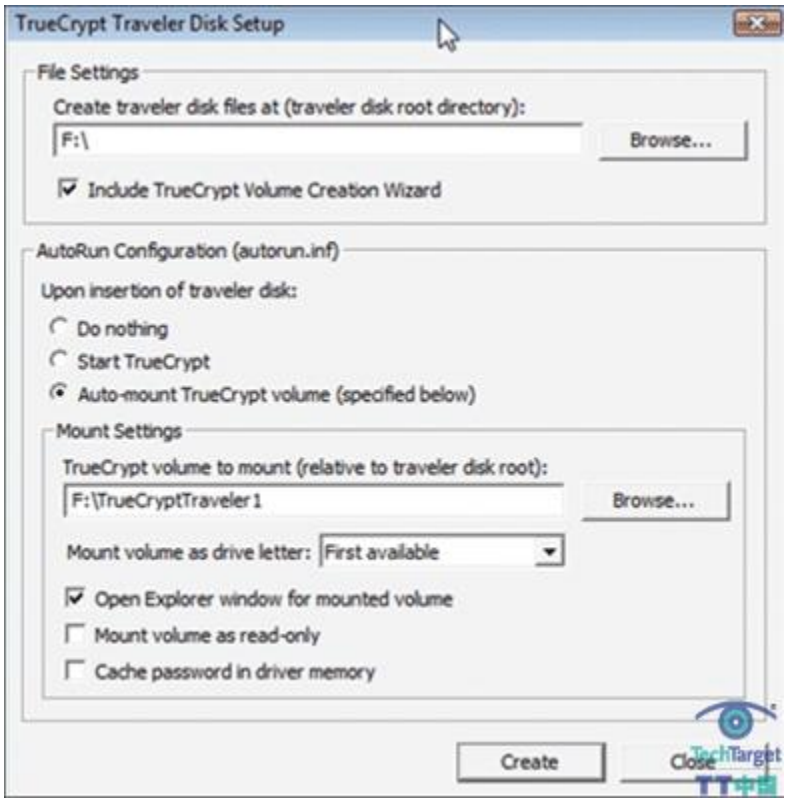
(作者：Russ McRee 译者：Tina Guo 来源：TechTarget 中国)

开源加密工具 TrueCrypt 的旅行模式

TrueCrypt 可以实现真正的可携带，而且应该选择这个选项。我们推荐最小 2GB 的存储设备。在旅行模式下，TrueCrypt 不需要安装到所运行的操作系统中。

如果，但愿不会如此，你选择了使用外部的计算机，就会证明它很有用。假设你需要带着数据到国外出差，但是不携带电脑。旅行模式可以让你在目标计算机上插入 USB 设备，并直接从 USB 设备上运行 TrueCrypt。TrueCrypt 不需要安装到目标计算机中。旅行模式创建过程也有驱动向导，而且应用简单。

不管你时候选择加密整个磁盘、磁盘的一部分或者一个文件贮存器，使用 TrueCrypt 都很好。如果你携带了私人数据或者公司的机密数据，和/或个人认证信息，TrueCrypt 强大俄加密方法都可以提供保护。



在旅行模式中，你可以在 USB 设备上安装 TrueCrypt，并在任何系统中运行。

（作者：Russ McRee 译者：Tina Guo 来源：TechTarget 中国）