

使用外壳加密方式
保护软件防盗版解决方案
(ET99)

北京坚石诚信科技股份有限公司

2008-10-14

外壳加密是软件加密的一种方式，它不同于传统的嵌入源代码的加密方式，但是通过加壳同样可以有效的防止自己的软件轻易地被他人“借鉴”。外壳加密不需要任何的开发经验，更不需要您是编程高手，您需要就是坚石公司为您量身打造的外壳加密程序和 5 分钟的时间，即可完成软件的加密，加密其实就是这么简单。

所谓“外壳”就是给可执行的文件加上一个外壳，这个外壳与动物的外壳有着异曲同工之处。外壳就是为了保护程序不被其他人随意的窃取或改动而制作的加密程序，运行加壳程序时，用户执行的实际上是这个外壳的程序，而这个外壳程序负责把用户原来的程序在内存中解压缩，并把控制权交还给解开后的真正的程序，由于一切工作都是在内存中运行，用户根本不知道也不需要知道其运行过程，并且对执行速度没有什么影响。

加密程序在插有加密锁的情况下正常运行，外壳程序完全透明；在没有插加密锁的情况下会弹出找不到加密锁的提示。说明：外壳加密的对象主要是 EXE、DLL、ARX 等 Win32PE 格式的文件，并不能对 DOC 等数据文件加密。

下面介绍如何使用 ET99 实现外壳加密：

需要使用 Et99Setting.exe 对 ET99 进行初始的设置，在未更改 PID 的状态下是不能进行外壳加密的。



“硬件 PID”：ET99 的产品标示，默认 8 个 F，通过种子码算法产生，种子即是在“PID 种子”中输入的。

“SO PIN 码”：管理员 PIN 码，开发商保存，可用于对 USER PIN 的解锁等，通过种子码算法产生，默认 16 个 F。

“USER PIN”：用户 PIN 码，字符限制“0-9，A-F”，外壳加密中需要验证，同时读写数据需要该 PIN 码验证通过，默认 16 个 F。

“新的 USER PIN 码”：用户根据自己的需要设置，注意字符的限制。

“PID 种子”：用于产生 PID 的种子，长度在 1-51 字节范围内。

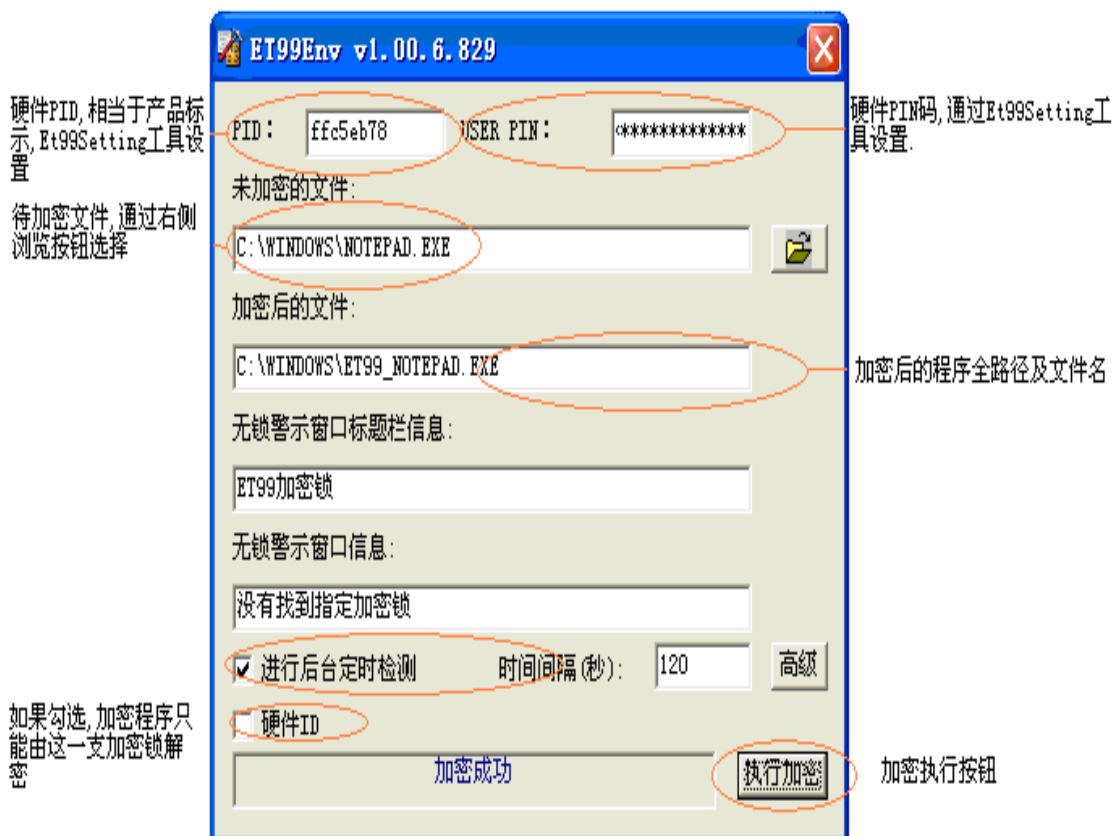
“SO PIN 种子”：用于产生 SO PIN 的种子，长度在 1-51 字节范围内。

“请选择设置项”：用户根据自己的需要，选择需要修改的属性。

“设置”：设置完成点击设置按钮，提示设置成功。

用户需要记住“新的 SO PIN”和“新的硬件 PID”。

使用外壳加密程序对待加密的程序进行外壳加密，外壳程序的界面如下：



“PID: ”：输入在步骤 1 中产生的“新的硬件 PID”。

“USER PIN: ”：输入在步骤 1 中设置的“新的 USER PIN 码”。

“未加密的文件”：用户通过右侧的浏览按钮选择待加密的文件。

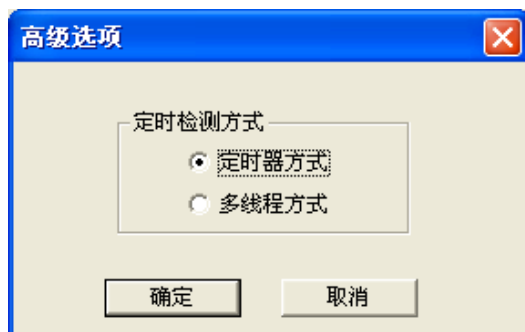
“加密后的文件”：这里显示加密后文件的输出路径和加密后文件名，用户可以根据需要修改。

“进行后台定时检测”：如果不勾选，程序启动时需要插有加密锁，运行期间可以拔掉加密锁；如果勾选，表示外壳程序会定时检测加密锁是否插在计算机上，如果不在，则会报错。

“硬件 ID”：如果不勾选，设置成相同的 PID 和 USER PIN 一批加密锁都可以解密加密之后的软件；如果勾选，加密之后的程序只能由这一支加密锁解密运

行;

“高级”：主要是提供了两种定时检测的方式，“定时器方式”和“多线程方式”。



“执行加密”：外壳加密的最后一步，设置项都填写完成之后，点击该按钮，将会提示“加密成功”。

至此，外壳加密完成，加密之后的程序在插有指定加密锁时可以运行，如果没有查加密锁，程序无法运行，提示没有找到加密锁。