十一、 开发基于 HEV 技术的注册码验证器

实验目的

1. 实践 VT 技术相关指令
2. 实践 VT 技术中 VMX 抢占计时器技术
3. 实践 NewBluePill 的内存隐藏技术

实验概述

在前面的实验中，我们已经对虚拟化技术有了初步的了解。这个实验将展示虚拟化技术在实际生活中的运用。

如今，共享软件和大多数的商业软件都在使用注册码技术来保护自己的版权，然而，由于验证程序处于 Ring-3 特权态（少数处于 Ring-0 特权态），因此很容易通过动态分析的手段改变跳转/改变语义或者推算出算法，从而破解掉软件。

这个问题的根源在于两个：

1) 注册码验证系统的运行时空间操作系统可见
2) 注册码的验证一般只有一次[1]

引入虚拟化技术后，由于我们拥有了比操作系统更高的权限，再加上我们在 NewBluePill 中所看到的内存隐藏技术，所以我们可以尝试去解决这个问题。考虑下面的模型：

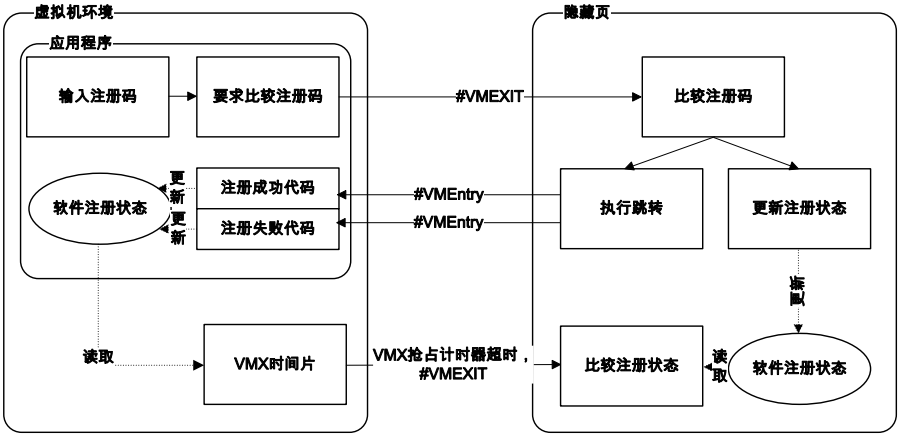

图 11.1 注册码验证器流程图

由图 11.1 所示，将比较注册码的关键部分内存隐藏，从而无法通过动态分析看到这部分内存。此外，通过 VMX 抢占计时器每过一定时间判断一次软件真实注册状态，防止破解者通过修改应用程序的注册失败代码语义而修改保存在应用程序中的软件注册状态[2]。当在

[1] 其实这个问题也与操作系统可见所有用户程序空间有关，在普通情况下，软件多次验证注册码基本不能带来任何好处。

[2] 在应用程序部分保存软件注册状态可以起到优化的作用，当其状态为未注册时，可以不必再去通过 VMX

Hypervisor 中发现应用程序的软件注册状态不等于自己保持的注册状态时，终止应用程序的运行。

实验过程

抢占计时器去陷入检查。