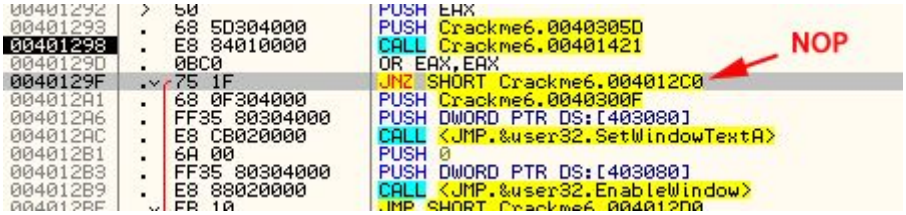
第九章续：“无相关字符串”的解决方案

一、简介

针对第九章的家庭作用，这里我提供几个解决方案。记住，有无数种方法可以破解这个程序，而这只是一个很小的例子。如果你自己找到了一个方法，那么恭喜你。如果没有的话，也别着急，我们将分多次解决它。

二、方案一

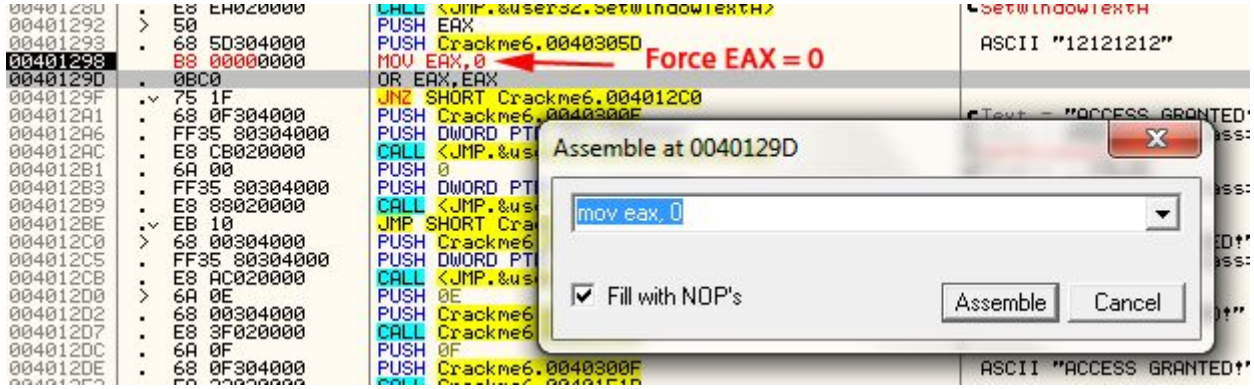
最简单的一种方法是给程序打补丁，只需要将 40129F 处的 JNZ 指令 NOP 掉就行:



这会强制程序每一次都直接空降到好消息那。

三、方案二

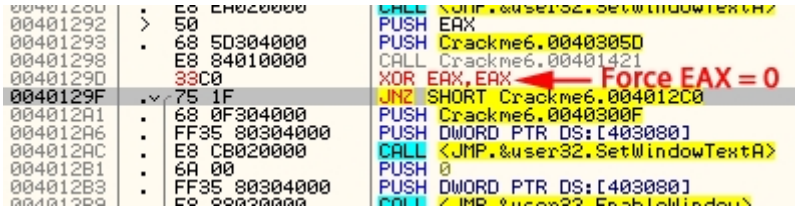
另一个可行性方案是,让 EAX 一直等于 0,将那个检测密码的 CALL 用 MOV EAX, 0 替换掉:



这个基本上将检测密码可行性的 CALL 整个删除了，程序将总是跳转到好消息那。

四、方案三

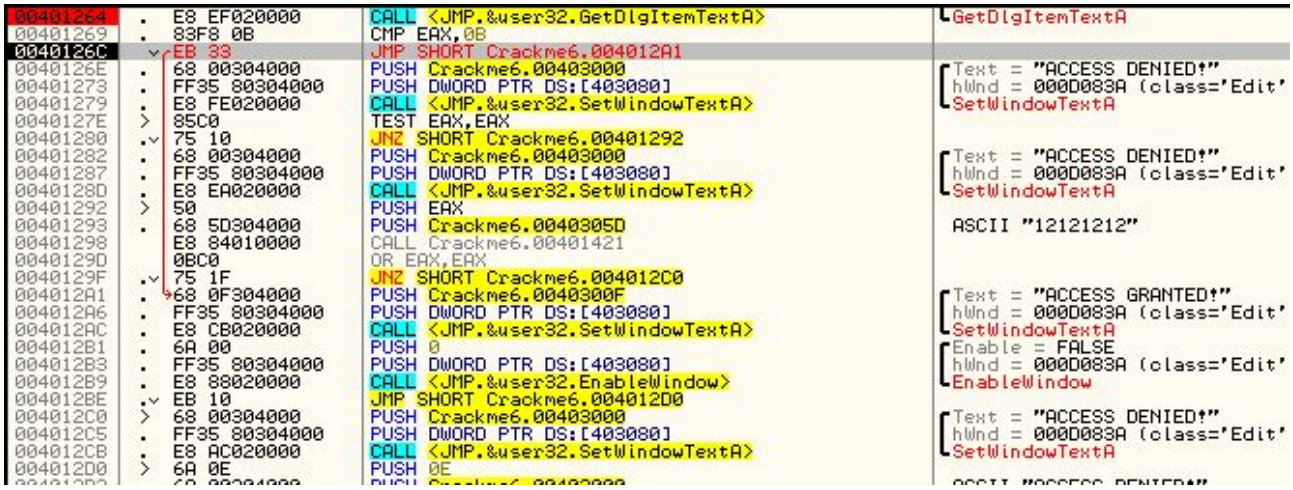
继续方案二的思想，我们将那个 CALL 留下，在它返回以后，我们再强制 EAX 等于 0。只需要将 OR EAX,EAX 替换成 XOR EAX, EAX 即可:



我喜欢这个解决方案，对此还有一定的讽刺意味（你只打了一个字节的补丁，只加了一个字母😀）。（译者注：我觉得讽刺意味应该是，一个程序的保护机制，加一个字母就搞定了，确实挺讽刺的。）

五、加分题

我希望加分题没有给你带来烦恼。移除密码长度限制的最简单的方法是替换掉原始的跳转，如果密码太长的话，就用一个直接跳转到好消息的 JMP 替换掉原始跳转。



这个相当的巧妙（在下一章中有更好的办法），不过确实有用。这样做的好处是，不仅修补了程序让它总是接受你的密码，而且和上面的方法不一样的是，它也移除了对密码的所有限制。