Java程序破解

现在很多应用软件都会带有licenseID，licenseID一般是固定长度的字符串，在加上版本号，过期日期等形成一格字符串（license）。

一般情况是这样的，用RSA等加密算法形成publicKey、privateKey,用私钥加密license，生成签名，将公钥和签名发给客户端，客户端利用公钥和签名vertify license是否合法。

总体步骤如下：

1. jd-gui 反编译，查询java源码，找到signature vertify代码处
2. 下载javassist.jar，javassist使用方法参考：

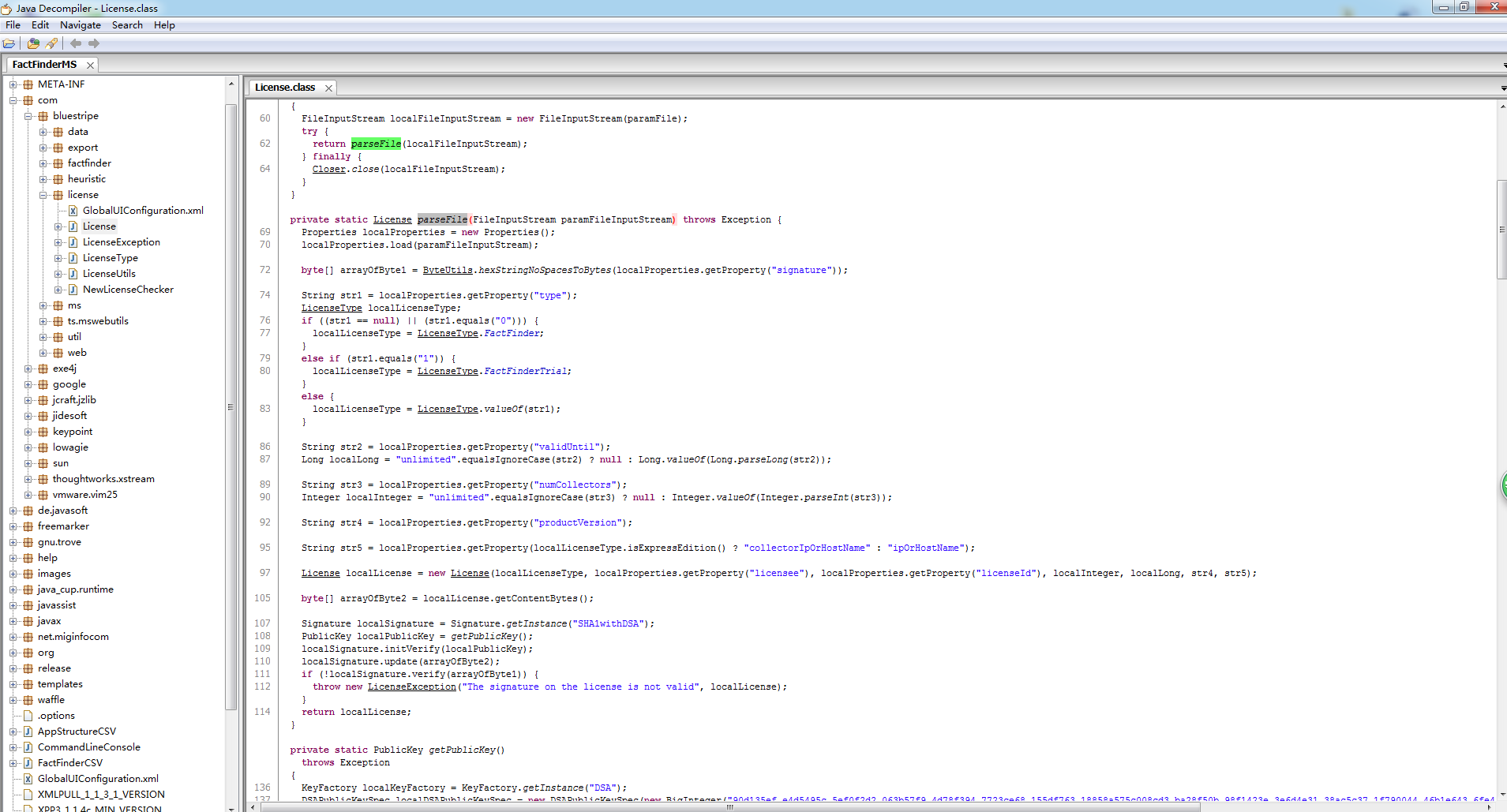
<http://blog.csdn.net/xingfeng0501/article/details/7084486>

假如验证license是否合法的方法名称为parseFile（我破解的FactFinderMS）。

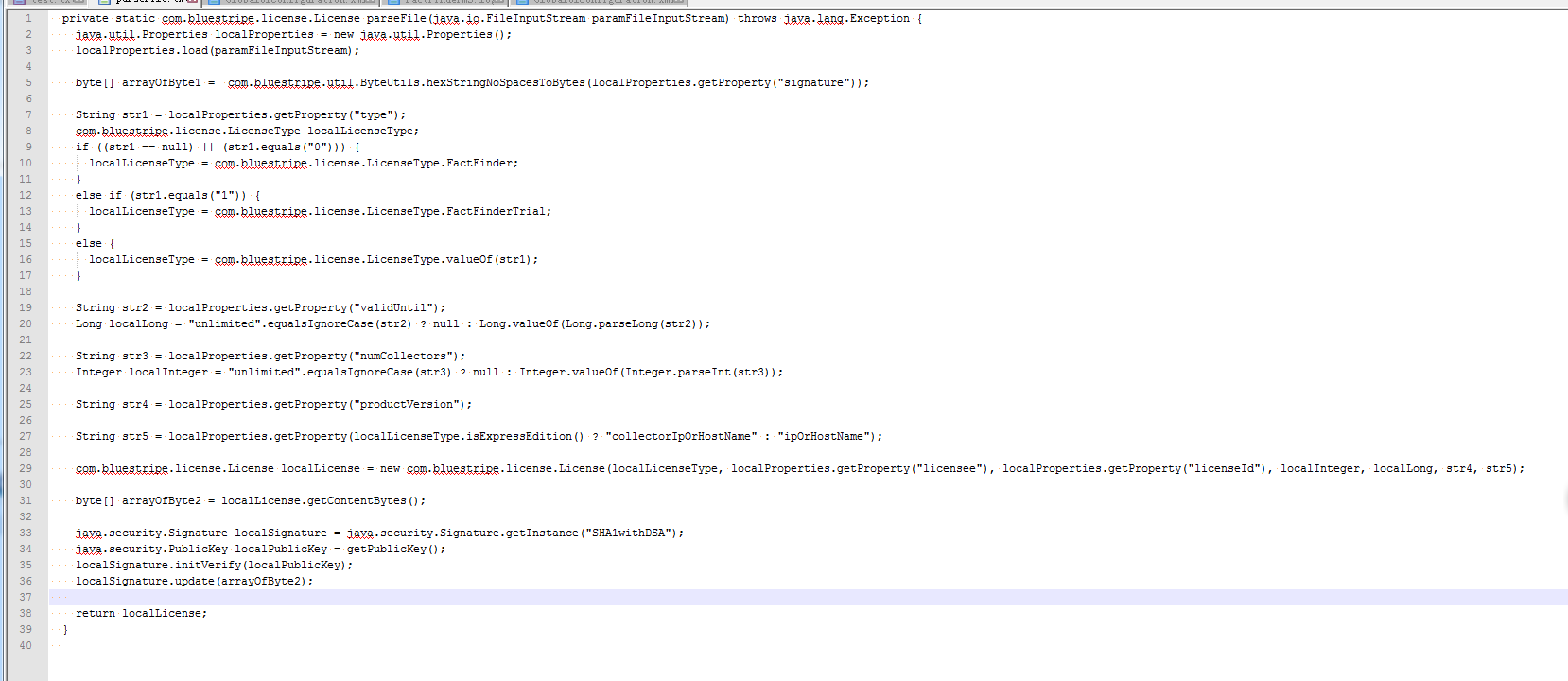
将parseFile反编译的Java代码，拷贝出来，删除vertify代码，保存到一个文件中，在cracker代码首先加载找到parseFile所在的类，删除parseFile，然后添加parseFile方法。

具体解决方法如下：

1.jd-gui打开jar包或class文件，找到vertify License代码

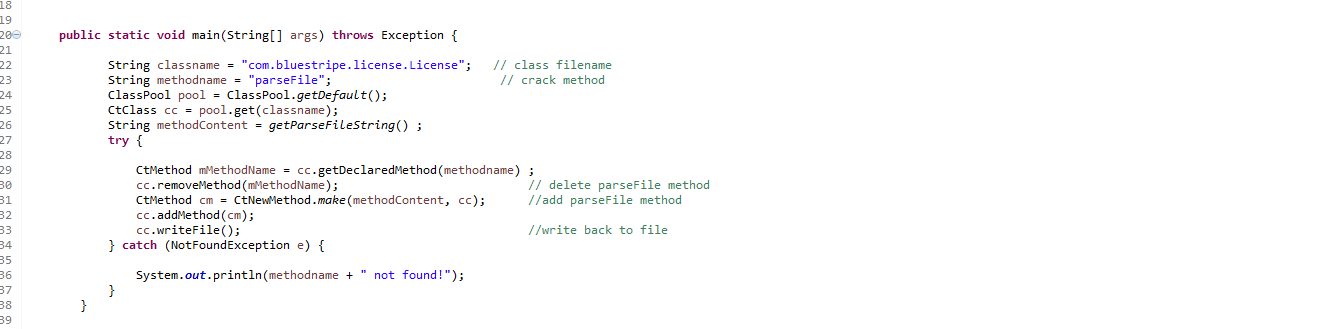


将parseFile代码拷贝到文件中



注意代码中License，FileInputStream等类需要加上包路径

1. 利用javassist修改字节码，然后写回文件



4、将写回的class文件拷贝到jar包所在的路径

此时jar 的license vertify已经被破解