Github上读一下AndFix这个项目的源码，还有xposed、dexposed。

大致原理就是将java方法通过c/c++修改属性变为public native方法，上下文携带到native层，然后根据上下文指向另一个java方法，从而“偷梁换柱”，如果是支持ART的手机，那么策略不一样，将bug method的关键信息（classloader、theadid等）保留，将修复过的方法的各种信息赋给bug method，完成“移花接木”。

另外，其实有挺多的策略改变运行时行为的，比如：

* Javasisst：字节码修改类库，依赖字节码修改和DX类库，可以完成动态替换和切面编程。
* AspectJ：依赖字节码编织器，需要按照其语法来编写，需要一点“编织”时间。
* Xposed方案，简直是一个Bug，神器般的存在，没准以后会被Android系统修复呢，不仅可以改变自己的类行为还可以hook系统的方法，root过的机器还可以hook其他App和系统进程。

http://www.trinea.cn/android/android-plugin/