android平台clang-ollvm编译器安装及使用说明

1. clang-ollvm安装

1）下载并编译项目: https://github.com/obfuscator-llvm/obfuscator

$ git clone -b llvm-4.0 <https://github.com/obfuscator-llvm/obfuscator.git>

$ mkdir build

$ cd build

$ cmake -DCMAKE\_BUILD\_TYPE=Release ../obfuscator/

$ make -j7

2）替换ndk安装包中的llvm目录

从<https://developer.android.com/ndk/downloads/?hl=zh-cn>下载最新的ndk安装包，然后执行如下命令：

$ unzip android-ndk-r16b-linux-x86\_64.zip

$ cd android-ndk-r16b/toolchains

# 备份llvm文件夹

$ cp -r llvm llvm.backup

# llvm/prebuilt/linux-x86\_64/bin下所有文件、文件夹换成1步骤中build/bin

# llvm/prebuilt/linux-x86\_64/lib下所有文件、文件夹换成1步骤中build/lib

$ rm -rf llvm/prebuilt/linux-x86\_64/bin

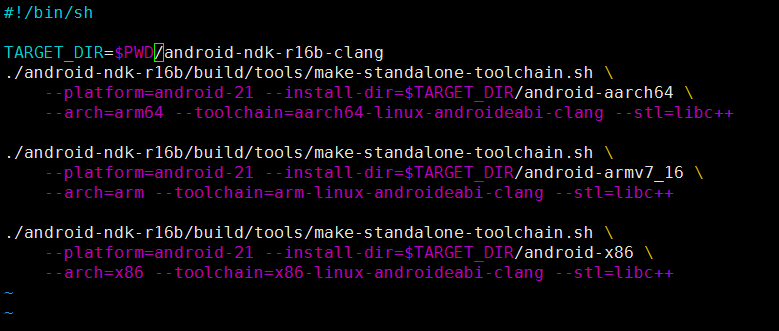
$ cp -r /path/to/ollvm-build/bin llvm/prebuilt/linux-x86\_64/

$ rm -rf llvm/prebuilt/linux-x86\_64/lib

$ cp -r /path/to/ollvm-build/lib llvm/prebuilt/linux-x86\_64/

3）创建ndk独立工具链

参考Android NDK的官方文档，安装独立工具链<https://developer.android.com/ndk/guides/standalone_toolchain?hl=zh-cn>，注意要指定--stl=libc++来选择安装llvm版的 C++ 标准模板库实现的副本：



当前目录下会生成android-ndk-r14b-clang（包含android-armv7, android-aarch64和android-x86三个toolchain子目录），将android-ndk-r14b-clang拷贝至/opt下

1. 如何开启clang-ollvm的代码混淆功能：

1）Obfuscator-llvm支持三种混淆模式分别是：

Instructions Substitution： -mllvm -sub

Bogus Control Flow： -mllvm -bcf

Control Flow Flattening： -mllvm -fla

具体原理参考<https://github.com/obfuscator-llvm/obfuscator/wiki/Features>，

2）在CMake脚本中指定相应混淆模式的编译器选项

通过设置CMAKE\_CXX\_FLAGS变量，可以达到效果，例如：

SET(CMAKE\_CXX\_FLAGS "${CMAKE\_CXX\_FLAGS} -mllvm -fla")

3）只混淆特定函数：

有的时候，由于效率或其它原因的考虑，我们只想给指定的函数混淆，OLLVM也提供了对这一特性的支持。比如，想对函数func()使用bcf混淆，只需要给函数func()增加bcf属性即可。

int func() \_\_attribute((\_\_annotate\_\_(("bcf"))));

fla，sub和bcf三个属性可以搭配使用。如果不想对func()函数使用bcf属性，那标记为“nobcf”即可。

参考下图：

