Class-Dump的使用

## Class-Dump

class dump是一个命令行工具，用来监测存储在Mach-O二进制文件理的Objective-C运行时信息。它为类(class)，分类(category)和协议(protocol)生成声明信息。这些信息与 otool -ov 命令提供的信息是一样的，但表示得更像正常的Objective-C的声明，所以它更紧凑，更易读。

class-dump-x是一个class-dump的修改版，在当时（2008年) class-dump 3.1.2不支持Objective-C 2.0 ABI). Objective-C 2.0 ABI删除了OBJC段，在data段引入了一些新的section. 并且 class/obj的布局也边了。

它不生成@property声明，因为所有的properties被映射到方法了。 不创建@property 元素，这样的源码可以与objc 1.0的编译器兼容。

class\_dump\_z 是对上面两个的改进。

## 使用步骤

### 下载、配置class-dump

前往 https://code.google.com/p/networkpx/wiki/class\_dump\_z ，下载tar包，然后解压配置到本地环境



### 解密App：

由于上传至App Store的App经苹果加密，故使用逆向工具前需解密App。

解密工具：Clutch（需越狱环境下使用）

### 使用class-dump反编译App

class-dump-z XXX（App名称）

结果如下：

typedef struct \_NSZone NSZone;

typedef struct CGPoint {

        float x;

        float y;

} CGPoint;

typedef struct CGSize {

        float width;

        float height;

} CGSize;

//...

typedef struct AQRecorder {

        unsigned long long \_field1;

        unsigned char \_field2;

        OpaqueAudioComponentInstance\* \_field3;

        AURenderCallbackStruct \_field4;

        CAStreamBasicDescription \_field5;

        unsigned char \_field6;

        ReverbEffect32 \_field7;

        Freeverb \_field8;

        bool \_field9;

        BandpassFilter \_field10;

        BandpassFilter \_field11;

        queue<short, std::deque<short, std::allocator<short>> > \_field12;

        queue<short, std::deque<short, std::allocator<short>> > \_field13;

        queue<short, std::deque<short, std::allocator<short>> > \_field14;

        CFStringRef \_field15;

        OpaqueAudioQueue\* \_field16;

        AudioQueueBuffer\* \_field17[3];

        OpaqueAudioFileID\* \_field18;

        long long \_field19;

        CAStreamBasicDescription \_field20;

        unsigned char \_field21;

        id \_field22;

} AQRecorder;

//...

typedef struct \_Crashlytics\_\_Session\_\_User {

ProtobufCMessage \_field1;

char\* \_field2;

char\* \_field3;

char\* \_field4;

unsigned \_field5;

Crashlytics\_\_CustomAttribute\*\* \_field6;

} Crashlytics\_\_Session\_\_User;

//...

@protocol EGOImageLoaderObserver <NSObject>

@optional

-(void)imageLoaderDidFailToLoad:(id)imageLoader;

-(void)imageLoaderDidLoad:(id)imageLoader;

@end

### 结论

通过class-dump可将破解后的ipa文件反编译至类（class），分类(category)和协议(protocol)的形式，可通过反编译后的文本分析App是否具有安全隐患。