

# Reverse Engineering in iOS

Tomasz Grynfelder  
@tgrynfelder



The goal

# The goal of apps' RE

- Deep dive into FairPlay encrypted app from AppStore in order to:
  - Inspect
  - Modify
  - Verify usage of our (licensed) products
  - Know your enemy



# Requirements

# Requirements

- Jailbroken iOS device
- Desktop tools
- Device tools

# Requirements

- Jailbroken iOS device
  - up to 7.0.6 - untethered jailbreak Evasi0n7
  - up to 7.1.1 - untethered jailbreak Pangu



# Requirements

- Desktop tools:
  - Ida Pro / Hopper
  - Reveal / Spark Inspector

# Requirements

- Device Tools
  - otool
  - gdb
  - class-dump-z
  - cycrypt



# Requirements

- Device Tools
  - otool
  - gdb
  - class-dump-z
  - cycript
  - or clutch

# App reverse engineering

# Initial analysis



# Initial analysis

```
root# cd /var/mobile/Applications/00000000-0000-0000-0000-FFFFFFFFFFFF/  
AppName.app/
```

```
root# otool -h AppName
```

```
AppName:
```

```
Mach header
```

magic	cputype	cpusubtype	caps	filetype	ncmds	sizeofcmds	flags
0xfeedface	12	9	0x00	2	47	5016	0x00218085

# Initial analysis

```
root# otool -Vl AppName  
(...)  
Load command 11  
      cmd LC_ENCRYPTION_INFO  
      cmdsize 20  
cryptoff 16394  
cryptsize 7987008  
cryptid 1  
(...)
```

# Initial analysis

```
root# otool -Vh AppName
```

```
AppName:
```

```
Mach header
```

magic	cputype	cpusubtype	caps	filetype	ncmds	sizeofcmds	flags
MH_MAGIC	ARM	9	0x00	EXECUTE	47	5016	NOUNDEFS
DYLDLINK TWOLEVEL WEAK_DEFINES BINDS_TO_WEAK PIE							



# Initial analysis

```
root# class-dump-z AppName
```

```
Warning: Part of this binary is encrypted. Usually, the result will be not  
meaningful. Try to provide an unencrypted version instead.
```

```
@protocol XXEncryptedProtocol_8436d0
```

```
-(?)XXEncryptedMethod_6d5a20;
```

```
-(?)XXEncryptedMethod_6d5a14;
```

```
-(?)XXEncryptedMethod_6d5a08;
```

```
-(?)XXEncryptedMethod_6d5a00;
```

```
(...)
```



# Decrypting

# Decrypting

- Find out starting address and data size in binary
- Find out starting address of the application in memory
- Override binary part with decrypted part of the application dumped using gdb/lldb
- Change LC\_ENCRYPTION\_INFO cryptid to 0



# Decrypting automation

# Decrypting automation

- clutch tool

```
iPhone:~ root# clutch
```

```
usage: clutch [application name] [...]
```

```
Applications available: AppName1 AppName2 AppName3 AppName4 AppName5
```

```
iPhone:~ root# clutch AppName
```

```
Cracking AppName...
```

```
  /var/root/Documents/Cracked/AppName-vX.X.X.ipa
```

# Analysis of IPA

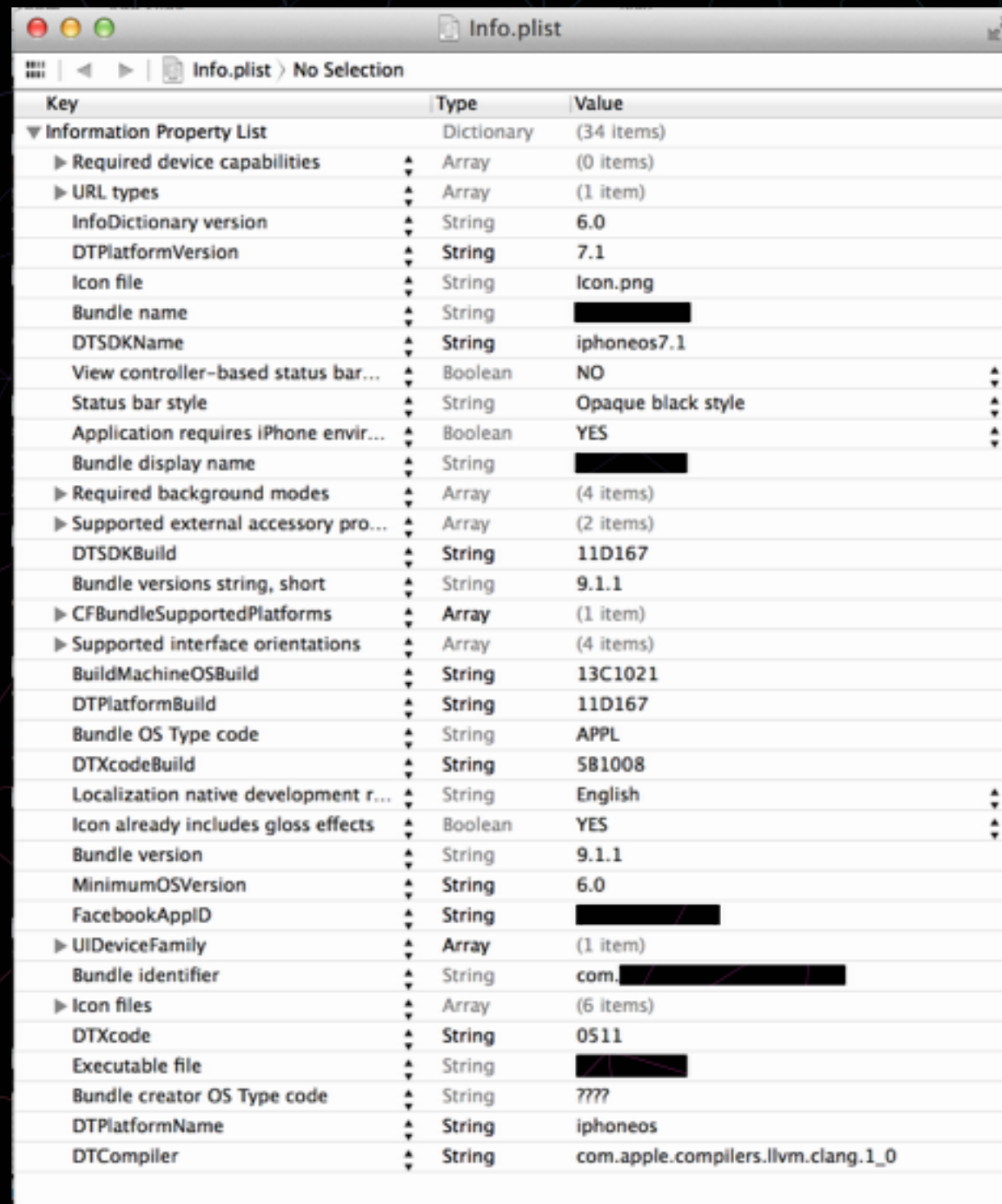


# Analysis of IPA

- Info.plist
- strings in binary
- class interfaces
- resource files

# Analysis of IPA

- Info.plist

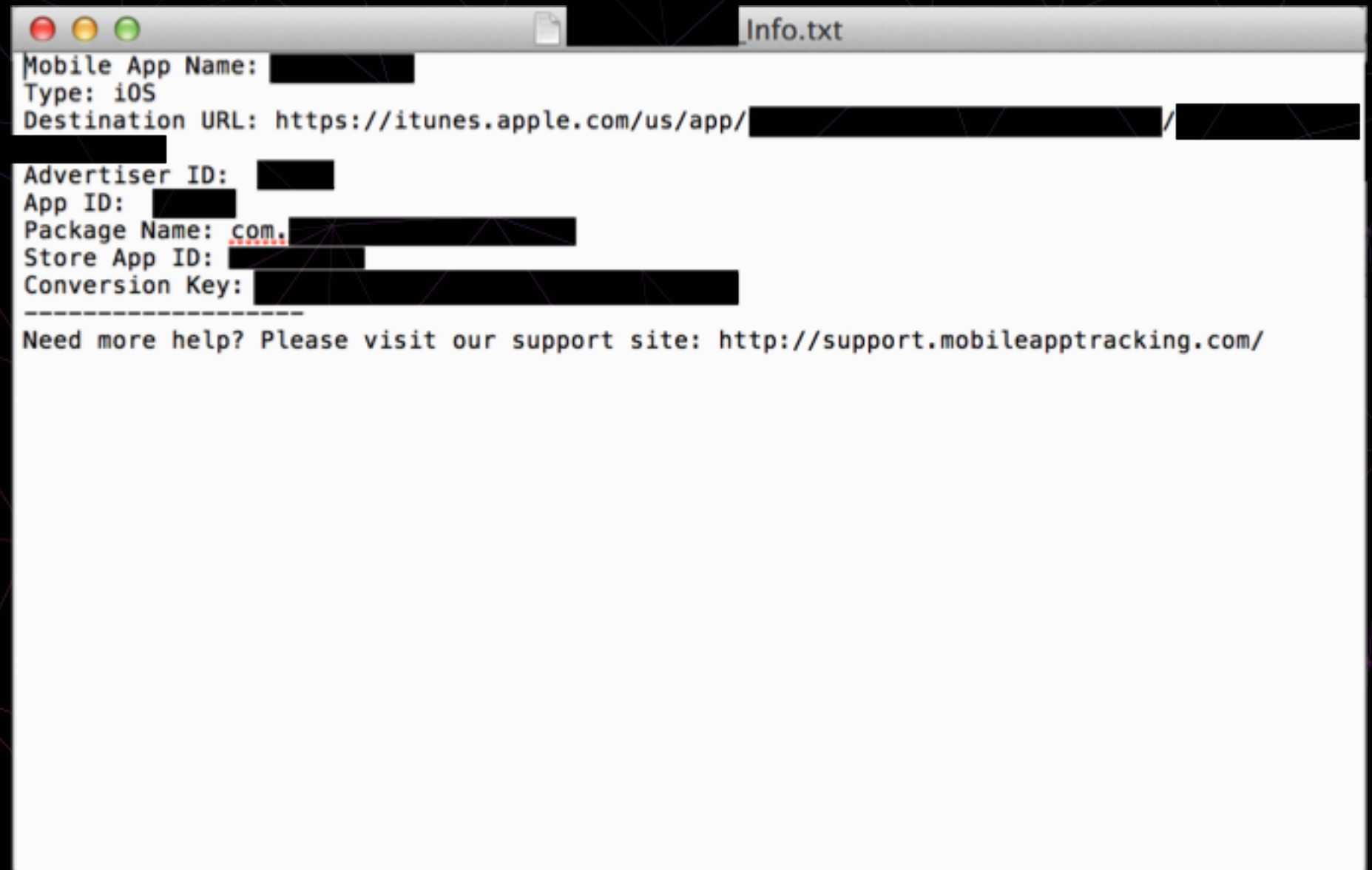


The screenshot shows a code editor window titled 'Info.plist' with a table of keys and values. The table has three columns: Key, Type, and Value. The keys are organized into sections, with some expanded to show their contents. The values are mostly strings, arrays, and booleans, with some redacted with black boxes.

Key	Type	Value
▼ Information Property List	Dictionary	(34 items)
▶ Required device capabilities	Array	(0 items)
▶ URL types	Array	(1 item)
InfoDictionary version	String	6.0
DTPlatformVersion	String	7.1
Icon file	String	Icon.png
Bundle name	String	[REDACTED]
DTSDKName	String	iphoneos7.1
View controller-based status bar...	Boolean	NO
Status bar style	String	Opaque black style
Application requires iPhone envir...	Boolean	YES
Bundle display name	String	[REDACTED]
▶ Required background modes	Array	(4 items)
▶ Supported external accessory pro...	Array	(2 items)
DTSDKBuild	String	11D167
Bundle versions string, short	String	9.1.1
▶ CFBundleSupportedPlatforms	Array	(1 item)
▶ Supported interface orientations	Array	(4 items)
BuildMachineOSBuild	String	13C1021
DTPlatformBuild	String	11D167
Bundle OS Type code	String	APPL
DTXcodeBuild	String	5B1008
Localization native development r...	String	English
Icon already includes gloss effects	Boolean	YES
Bundle version	String	9.1.1
MinimumOSVersion	String	6.0
FacebookAppID	String	[REDACTED]
▶ UIDeviceFamily	Array	(1 item)
Bundle identifier	String	com.[REDACTED]
▶ Icon files	Array	(6 items)
DTXcode	String	0511
Executable file	String	[REDACTED]
Bundle creator OS Type code	String	????
DTPlatformName	String	iphoneos
DTCompiler	String	com.apple.compilers.llvm.clang.1_0

# Analysis of IPA

- resource files





# Analysis of IPA

- strings in binary

```
user@mbp:~/AppName/Payload/AppName.app$ strings AppName
```

# Analysis of IPA

- strings in binary

```
user@mbp:~/AppName/Payload/AppName.app$ strings AppName
```

```
filename
```

```
type
```

```
(...)
```

```
SELECT instruction, speed, altitude, verticalAccuracy, heartRate FROM trackpoints  
WHERE workoutKey = ? ORDER BY tpIndex ASC;
```

```
UPDATE workouts SET hasAnyTrackPointsWithValidSpeed = 1, maxSpeed = ? WHERE pk  
= ?;
```

```
UPDATE workouts SET numTrackPointsWithHeartRate = ?, heartRateSum = ?,  
averageHeartRate = ?, maxHeartRate = ? WHERE pk = ?;
```

```
(...)
```

```
itms-apps://itunes.apple.com/WebObjects/MZStore.woa/wa/viewContentsUserReviews?  
id=APP_ID&onlyLatestVersion=true&pageNumber=0&sortOrdering=1
```

```
(...)
```

```
-[FacebookManager _getUserData]
```

```
-[FacebookManager logOut]
```

```
publish_actions
```

```
userName
```

```
(...)
```

# Analysis of IPA

- class interfaces

```
user@mbp:~/AppName/Payload/AppName.app$ class-dump-z AppName
```



# Analysis of IPA

- class interfaces

```
user@mbp:~/AppName/Payload/AppName.app$ class-dump-z AppName
```

```
typedef struct _NSZone NSZone;
(...)
__attribute__((visibility("hidden")))
@interface FacebookManager : XXUnknownSuperclass {
@private
(...)
    NSString* _accessToken;
    FBSession* _session;
}
@property(assign, nonatomic) FBSession* session;
@property(copy, nonatomic) NSError* lastError;
@property(copy, nonatomic) NSString* accessToken;
-(void)processProfileDeviceResponse:(id)response;
-(void)askForPublishPermission;
-(bool)havePublishPermission;
-(void)logout;
-(bool)isLoggedIn;
```

# Runtime Analysis

# Runtime Analysis

- Bypass code sign verification on a device with AppSync7+
- Remove original app
- Install decrypted app with ipainstaller



# Runtime Analysis

- cypriat
- modify ivars
- instantiate object
- invoke methods
- swizzle methods

# Runtime Analysis

- `cycrypt`

```
iPhone:~ root# ps -ax | grep AppName
3212 ??          0:09.42 /var/mobile/Applications/00000000-0000-0000-0000-
FFFFFFFFFFFFFF/AppName.app/AppName
3230 ttys001      0:00.02 grep AppName
iPhone:~ root# cycrypt -p 3212
cy# [UIApplication sharedApplication]
#"<UIApplication: 0x17ddc650>"
cy# [[UIApplication sharedApplication] setHidden:YES withAnimation:YES]
```

# Runtime Analysis

- Reveal - view hierarchy inspection
- Integration with app:
  - copy Reveal.framework and libReveal.dylib to proper directories on a device
  - create file plist with bundle ID in proper directory





# Prevention & Protection

# Prevention & Protection

- Read:
  - Secure coding guide
  - iOS Security White Paper

# Prevention & Protection

- Look for:
  - logged data
  - Cache.db data
  - NSUserDefaults
  - credentials in .plist



# Prevention & Protection

- Use:
  - Data protection
  - Core Data encryption
  - Keychain
  - Obfuscation

# Prevention & Protection

- Use:
  - Binary integrity check
  - Strings obfuscation (XOR, encrypting with code tables)
  - SSL certificates validation

# Prevention & Protection

- Deny attaching GDB
  - `ptrace(PT_DENY_ATTACH, 0, 0, 0);`
- Check for encryption info in Mach-O header
  - `LC_ENCRYPTION_INFO`
- iTunes Metadata check



# Prevention & Protection

- Jailbreak detection
  - write to reserved paths
  - fork()
  - canOpenURL:
  - running processes

# Prevention & Protection

- Obfuscation
  - LLVM Obfuscator
    - code flow flattening
    - bogus branches of code
    - functions merging
    - result equals original app(?)

# Prevention & Protection

- Obfuscation
- iOS Class Guard
  - methods, protocols, properties
  - supports Storyboards and XIBs
  - supports CocoaPods
  - code logic



# iOS Class Guard

Let's fork and contribute!

<https://github.com/Polidea/ios-class-guard>



Q&A

One more thing....






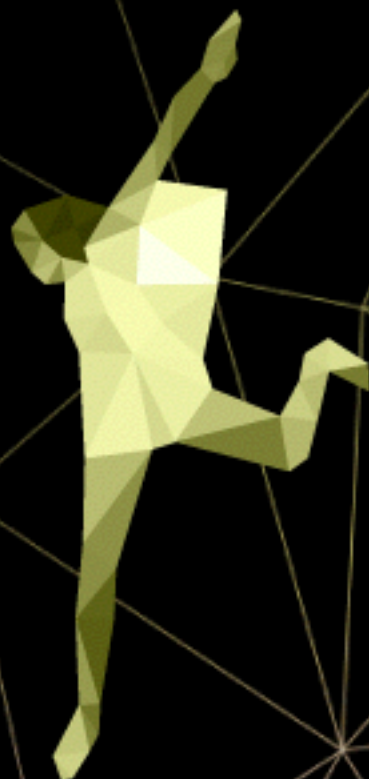


# MCE 2015

MOBILE WITH HUMAN TOUCH

FEBRUARY 4-6, 2015  
WARSAW, POLAND

[mceconf.com](http://mceconf.com)

 [mceconf](https://twitter.com/mceconf)





# Thanks!

@tgrynfelder