Security

Provisioning

- Provisioning Profile
- Entitlements
- Code Signature

Jailbreaking

- Altering the operating system to allow operations not permitted by default.
- Requires an exploit of the OS.
- Removes security measures (sandboxing, code signing).

Objective-C Runtime

- object oriented, dynamic, runtime oriented, strict superset of C
- objects communicate by sending messages to each other
- applicable to Swift

Objective-C Runtime

```
typedef struct objc_class *Class;

struct objc_object {
    Class isa;
};
typedef struct objc_object *id;

typedef struct objc_selector *SEL;
```

Objective-C Runtime

```
[self printMessageWithString:@"Hello World!"];
objc_msgSend(self,@selector(printMessageWithString:),@"Hello World!");
```

Objective-C Runtime

```
Ivar *class_copyIvarList(Class cls, unsigned int *outCount)
Ivar class_getInstanceVariable(Class cls, const char *name)
Ivar class_getClassVariable(Class cls, const char *name)

void objc_setAssociatedObject(id object, const void *key, id value, objc_AssociationPolicy policy)
id objc_getAssociatedObject(id object, const void *key)
void objc_removeAssociatedObjects(id object)
```

Objective-C Runtime

```
Method *class_copyMethodList(Class cls, unsigned int *outCount)
Method class_getInstanceMethod(Class cls, SEL name)

BOOL class_addMethod(Class cls, SEL name, IMP imp, const char *types)
IMP class_replaceMethod(Class cls, SEL name, IMP imp, const char *types)

void method_getArgumentType(Method m, unsigned int index, char *dst, size_t dst_len)
void method_getReturnType(Method m, char *dst, size_t dst_len)

IMP method_getImplementation(Method m)
IMP method_setImplementation(Method m, IMP imp)
void method_exchangeImplementations(Method m1, Method m2)
```

Reverse Engineering