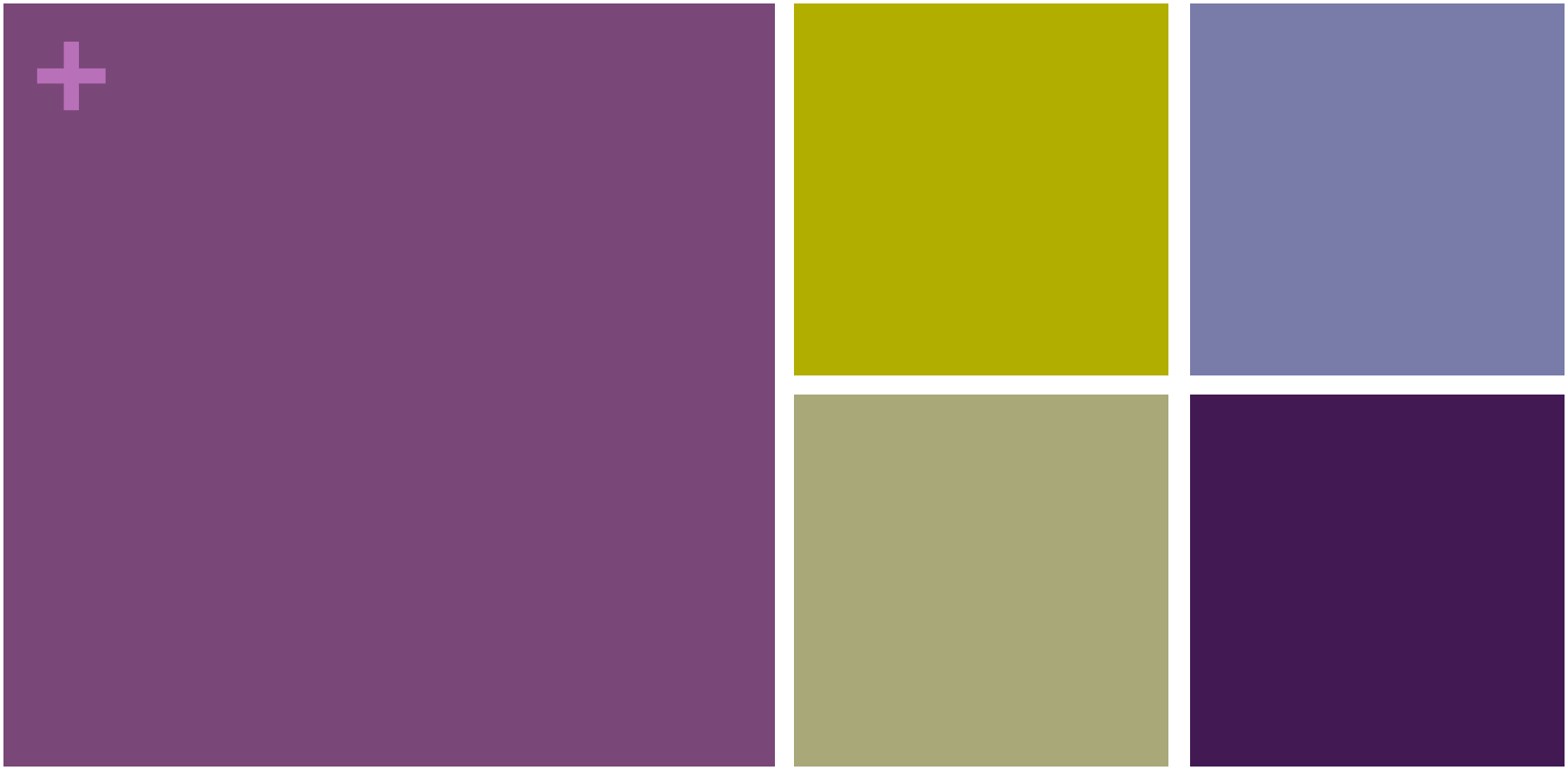


# Private API

Black App

2013/05/28

# iOS API

- Published API（Documented API）
- Unpublished API（Undocumented API）
- Private API

# How to use private API?

- We need header file.
  - Download from: https://github.com/nst/iOS-Runtime-Headers
  - Or dump by class-dump.

# How to use private API? -Dump .h File.

1. Get class-dump.
   - Download the latest version: http://stevenygard.com/projects/class-dump/
   - Drop the class-dump file to /usr/bin directory.
2. Dump the .h file.
   - Cd to /Applications/Xcode.app/Contents/Developer/Platforms/iPhoneSimulator.platform/Developer/SDKs/iPhoneSimulator6.1.sdk/System/Library/Frameworks/
   - Run the command: class-dump ./Message.framework/ > /Users/Brian/Desktop/Message_6.1.h
3. We can use the private API now!

# How to detect the use of private APIs?

1. otool -L
   - This will list all libraries the app has linked to.
2. nm –u
   - This will list all linked symbols.
   - Ex: Undocumented C functions such as _UIImageWithName.
3. Listing Objective-C selectors, or strings.
   - Objective-C selectors are stored in a special region of the binary, and therefore Apple could extract the content from there, and check if you've used some undocumented Objective-C methods, such as -[UIDevice setOrientation:].

# Get screenshot with iOS Device.

- CGImageRef screen = UIGetScreenImage();
- UIImage* image = [UIImage imageWithCGImage:screen];
- CGImageRelease(screen);

# Get screenshot with iOS Device.


A nice screenshot is now available under iPhone album

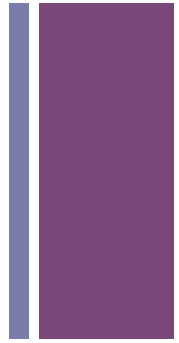
# Send messages with iPhone

- 1. We have to dump header file for a private class call CTMessageCenter

- 2. Send simple message with a static method call sendSMSWithText:

```
[[CTMessageCenter sharedMessageCenter]
sendSMSWithText:@"h3LL0 W0rlD" serviceCenter:nil
toAddress:@"0972195395"];
```

# Demo



- Use class-dump tool to dump private API.
- Get screenshot with iOS Device.
- Send messages with iPhone.