# iOS Sandbox Escape Vulnerabilities and Exploitations

## Trainer:

Team Pangu

## Bio:

Team Pangu consists of several senior security researchers and focuses on mobile security research. Team Pangu is known for the multiple releases of jailbreak tools for iOS 7, iOS 8, and iOS 9. Team Pangu actively shares knowledge with the community and presents the latest research at well known security conferences including BlackHat, CanSecWest, SysCan, POC, and Ruxcon.

## Brief Description:

In this training we will begin with introducing some basic knowledges about iOS architecture, ARM64 basics and how to setup testing environment. Then we will talk about Mach-O format details and how to analyze dyld_shared_cache file. We also need to write some IDA scripts to help us. After that we go through the objective-C internals to get a better understanding about how to do reverse engineering. The next chapter is very important, we will discuss how Apple designs its IPC mechanisms for iOS. We have to understand how port/mach msg/XPC work. We will cover the heap management in the user space for later exploitation exercise.

Now it's time to take a look at real world vulnerabilities. We will introduce typical bug types as well as some known bugs in history and analyze details of them. Then let's see what mitigations Apple add to stop exploits. In this part, we will talk how to find ROP and JOP gadgets. In the last part of the training, we pick up three different types of bugs to develop fully functional exploits. Through all the exercises, we can see how a real exploit is developed.

## Pre-requisite:

1. Obj-C/C language programming ability
2. Familiar with ARM64 reverse engineering
3. Knowledge of typical vulnerabilities and exploits

## Outline:

1st Day:

0. Introduction

1. Basic Knowledges
    - iOS Architecture
        - Sandbox
        - Launchd
    - Attack Surface
    - ARM64 Basics
    - Environment Prepare
        - Develop
        - Debug

2. Mach-O & Caches
    - Mach-O Format
    - dyld_shared_cache

3. Runtime
    - Objective-C
    - Reverse Engineering

4. IPC
    - Mach Port
    - Mach Message
    - Bootstrap
    - XPC
    - NSXPC
    - Daemon Analysis
    - Exercise

5. Heap Management
    - Nano/Tiny/Small/Large
    - CF*/NS*/xpc*/OOL Objects
    - Exercise

6. Vulnerability
    - Bug Types

Known Bugs

7. Exploitation

    Mitigations

    ROP & JOP

    Post Exploitation

2nd Day:

8. Assetsd Logical Bug

    Bug Analysis

    Exploit Exercise

9. Backboardd Arbitrary Memory Free Bug

    Bug Analysis

    Exploit Exercise

10. Backboardd Double Free Bug

    Bug Analysis

    Exploit Exercise

11. XPC OOB Bug

    Bug Analysis

    Exploit Exercise

12. Q&A