

Advanced 64-bit iOS Kernel Exploitation

Pangu Team

* The contents may be updated.

Overview

This 3-day training is designed to teach advanced exploitation techniques for 64-bit iOS kernel. Equipped with seven real world kernel vulnerabilities that most are directly exploitable inside the container sandbox, students will benefit from an in-depth analysis of iOS kernel security features, and learn how to write complete exploits on iOS 9 and iOS 10 for most common kernel vulnerability categories such as info leaks, UAF (Usef-After-Free), race condition, and heap overflows. Some of the vulnerabilities were privately fixed by Apple without public disclosure.

Agenda

1. iOS Security and Development Basic
2. iOS Kernel Reverse Engineering
3. Kernel Exploit Mitigations
4. Common Kernel Vulnerability Categories
 - *Kernel Exploit Technologies
 - *Heap Fengshui
 - *ROP and JOP
 - *Bypass KPP
5. Exploitation Labs with Seven Real-World Vulnerabilities
 - *Analyze and exploit the bugs one-by-one
 - *Including several privately fixed vulnerabilities
 - *Including the kernel vulnerabilities exploited by Pangu jailbreak tools
 - *Step-by-step courses

Student Requirements

1. Knowledge of iOS architecture
2. Familiarity with ARM32/64 assembly
3. Experience of development on jailbroken devices

4. Bring mac laptop with latest Xcode installed
5. Prepare IDA Pro or Hopper for disassembly

Price

\$4,000 per person

Language

English