The practice and evolution of iOS kernel hacking

Data: March 26 ~ 28

Intro:

This 3-day training is designed to introduce advanced exploitation techniques for 64-bit iOS kernel, with a special focus on teaching students to develop complete kernel exploits based on real world vulnerabilities. Students will get an in-depth analysis of iOS kernel security features, explore the evolution of kernel exploit mitigations from iOS 9 to iOS 11, and learn exploitation techniques against the most common kernel vulnerability categories such as info leaks, UAF, race condition, and heap overflows.

Agenda:

1. iOS Security and Development Basic
2. iOS Kernel Reverse Engineering
3. Kernel Exploit Mitigations
4. Common Kernel Vulnerability Categories
    A. Kernel Exploit Technologies
    B. Heap Fengshui
    C. ROP and JOP
    D. Bypass KPP
5. Exploitation Labs with Real-World Vulnerabilities
    A. Analyze and exploit bugs one-by-one
    B. Cover iOS 9, iOS 10, and iOS 11

Student Requirements:

1. Basic Knowledge of iOS architecture
2. Familiarity with ARM64 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