1000 - macOS/iOS Kernel Debugging and Heap Feng Shui

Friday at 10:00 in 101 Track
20 minutes

Min(Spark) Zheng*Security Expert @ Alibaba Inc. Ph.D of CUHK.*

Xiangyu Liu*Security Engineer @ Alibaba Inc. Ph.D of CUHK.*

Kernel bug is always very difficult to reproduce and may lead to the entire system panic and restart. In practice, kernel debugging is the only way to analyze panic scenes. However, implementing such a technique in real world is not an easy task since kernel code cannot be executed in the debugger, thus is hard to be tracked. Luckily, macOS has provided a very powerful kernel debugging mechanism, KDK (Kernel Development Kit), to assist people to analyze and develop kernel exploits. While for iOS, although there is no official kernel debugger, it is also possible for us to achieve kernel debugging by leveraging some tricks.

In this talk, we will share some kernel debugging techniques and their corresponding tricks on the latest iOS/macOS. In addition, we will also introduce the new kernel heap mitigation mechanisms on iOS 10/macOS 10.12 and two heap feng shui techniques to bypass them. Finally, we will demonstrate how to debug a concrete kernel heap overflow bug and then leverage our new heap feng shui techniques to gain arbitrary kernel memory read/write on the iOS 10.2/macOS 10.12.
Min(Spark) Zheng
Min(Spark) Zheng, Security Expert @ Alibaba Inc. Ph.D of CUHK.

#defcon25/by_track/101/Friday #defcon25/By_Day/_Friday