1030 - Ghost in the Droid: Possessing Android Applications with ParaSpectre

Sunday at 10:30 in Track 4
20 minutes | Demo, Tool
chaosdata *Senior Security Consultant, NCC Group*

Modern Android applications are large and complex, and can be a pain to analyze even without obfuscation - static analysis can only get one so far, the debugger sucks, Frida doesn't give you enough access to the Java environment, and editing smali or writing Xposed hooks can be time consuming and error prone. There has to be a better way!

What if we could inject a command line REPL into an app to drive functionality? And what if we could also make writing function hooks fast and easy?

In this talk, I will introduce ParaSpectre, a platform for dynamic analysis of Android applications that injects JRuby into Android applications. It bundles a hook configuration web API, a web application interface to configure and edit hooks, and a connect-back JRuby REPL to aid application exploration from the inside-out. It supports various selectors to match classes and methods, can be reconfigured on-the-fly without requiring a device reboot, and takes the pain out of writing method hooks for Android apps.

ParaSpectre is for developers and security researchers alike. While not itself a debugger, it provides a level of access into a running application that a debugger generally won't.
chaosdata
chaosdata(aka "Jeff") is a security consultant by day, and sometimes by night. He hacks on embedded systems, mobile apps and devices, web apps, and complicated things that don't have names. He also likes exotic candies.

@chaosdatumz

#defcon25/by_track/track4/sunday #defcon25/By_Day/_Sunday