Amandroid: A Precise and General Inter-component Data Flow Analysis Framework for Security Vetting of Android Apps

Fengguo Wei, Sankardas Roy, Xinming Ou and Robby, *Kansas State University*

We propose a new approach to conduct static analysis for security vetting of Android apps, and built a general frame- work, called Amandroid for determining points-to information for all objects in an Android app in a flow and context- sensitive way across Android apps components. We show that: (a) this type of comprehensive analysis is completely feasible in terms of computing resources needed with modern hardware, (b) one can easily leverage the results from this general analysis to build various types of specialized security analyses – in many cases the amount of additional coding needed is around 100 lines of code, and (c) the result of those specialized analyses leveraging Amandroid is at least on par and often exceeds prior works designed for the specific problems, which we demonstrate by comparing Amandroid's results with those of prior works whenever we can obtain the executable of those tools. Since Amandroid's analysis directly handles inter-component control and data flows, it can be used to address security problems that result from interactions among multiple components from either the same or different apps. Amandroid's analysis is sound in that it can provide assurance of the absence of the specified security problems in an app with well-specified and reasonable assumptions on Android runtime system and its library.