

Static Analysis – Exemplified on Vulnerable Android Code

Gabriel Voaideş, absolvent master 2015, Spiru Haret University

Abstract:

Android applications have the potential to cause personal damage by allowing cyber-criminals to steal personal information from the user's devices. That personal information could be anything from a phone number, contacts list, conversations, Internet IP address, GPS location, to banking data.

The methods for stealing such information vary wildly, but the mal-intended usage of vulnerable or malicious code within the applications themselves is the one we are going to focus on.

Testing applications for identifying potentially dangerous code through static analysis will improve overall security and guide developers to write safer code.

We are going to show some cases of vulnerable and/or malicious use of code, some stand-alone static analysis tools, some tools embedded within IDEs that allow for static analysis, what is possible to do with them at the moment (possibilities and limitations) and what's planned for the future.

Keywords: Android security, privilege escalation, information leak, static analysis, IDE tools