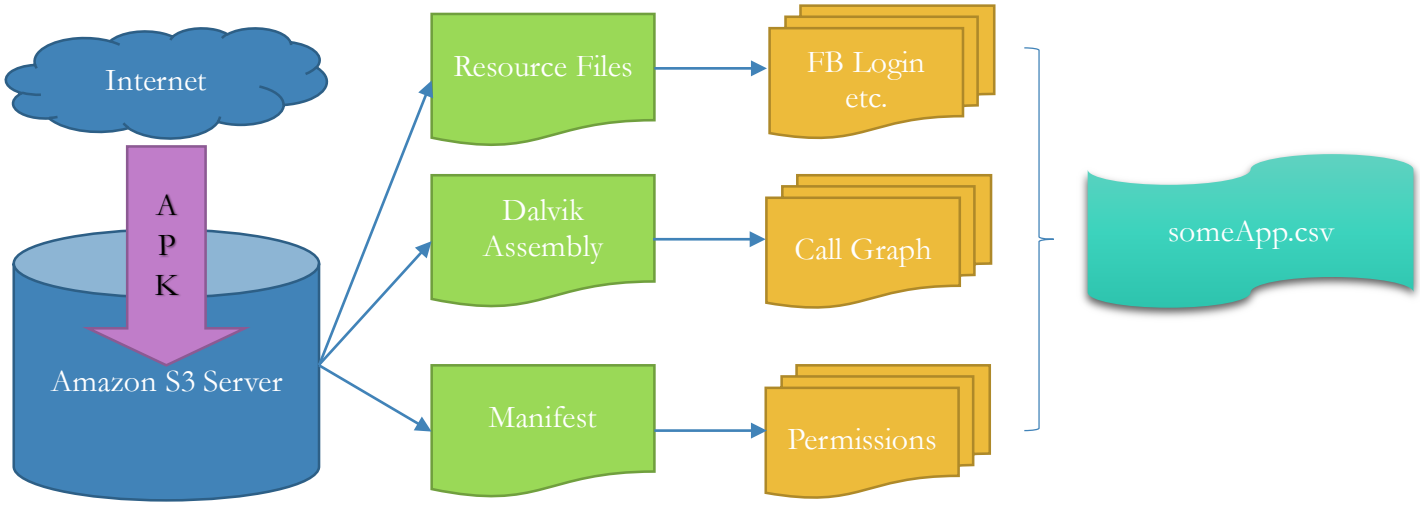
STATIC ANALYSIS FRAMEWORK FOR ANDRORD PLATFORM TO PROTECT YOUR PRIVACY



What problem does it solve? - Mobile apps might leak your login credentials, contacts, geographic locations, etc. to remote servers without permission from the user. Leaked information could be exploited for targeted advertisement or user activity analysis. Our framework detects existence of such leakage before an app is even installed!

How does it work? – After crawling app installation files from a trusted provider, our static analysis framework inspects "sensitive" features embedded inside the program and its resource files. A report is generated after the inspection to provide a general overview on the app's privacy practice.

What does it detect? – The framework is entirely extensible. Currently it detects the sharing/collection of location, contacts, device identifiers (e.g. IP, MAC, IMEI), Facebook login email, and third party software in the app's bundle.

More details? – Check out our latest publications and results here: https://www.usableprivacy.org/publications

Presented by Carnegie Mellon Mobile Commerce Lab
Privacy Day 2017