

FUSE: Beyond single-app security

Detecting Android app collusion and data exfiltration

FUSE helps security analysts identify the impact of Android apps on the security of mobile devices. FUSE operates on app binaries as distributed by app stores, so no source code is needed. Unlike other Android analysis tools, FUSE supports both single and multi-app analysis techniques.



Multi-app analysis

Android apps can collude to share access to restricted permissions. FUSE combines static analysis from multiple individual apps to quickly show where collusion or other undesirable interactions may occur.

- Examine all data flow paths possible in a collection of Android apps.
- Identify the specific methods responsible for information flows.
- Filter by customizing the visible information flow types and hiding trusted nodes to focus on potentially dangerous capabilities.



Single-app analysis

FUSE reads Android APKs and platform images, producing reports that identify:

- Potential security vulnerabilities
- Deprecated/Insecure API use.
- Suspicious behaviors
- Unnecessary permissions.

FUSE also decompiles each app and provides an interactive Dex Explorer to search and navigate the application bytecode in a web browser during detailed manual analysis.



DEX Explorer

FUSE lets analysts interactively filter, select, and zoom in for deeper looks at information flows, app components, and bytecode. The Dex Explorer offers a direct look at suspicious code for quick accept/reject decisions.



Automated policy evaluation

FUSE can also work without manual analysts once an information flow policy has been identified. Our policy evaluation engine will automatically check the information flows through a collection of apps and flag violations.