Smartphones are now ubiquitous. However, the security requirements of these systems and the applications they support are still being understood. As a result, the security infrastructure available in current smartphone OS is largely underdeveloped. We consider the security requirements of smartphone applications and show how to fulfill them using Secure Application InterTaction (Saint), a modified Android OS. Saint governs install-time permission assignment and their run-time use as dictated by application provider policy. It provides necessary utility for applications to assert and control the security decisions on the platform.

### Limitation of Android

- **Android’s security is system/user centric - protects the phone from malicious applications but provides limited infrastructure for applications to protect themselves**
  - **Permission assignment policy** - Applications have limited ability to control to whom permissions for accessing their interfaces are granted, e.g., white or black-list applications.
  - **Interface exposure policy** - Android provides only rudimentary facilities for applications to control how their interfaces are used by other applications.
  - **Interface use policy** - Applications have limited means of selecting, at run-time, which application’s interfaces they use.

### Saint’s Implementation

- Install-time policies are enforced by the Saint installer based on decisions made by the AppPolicy Provider (a-c).
- Interaction policies are enforced by the Saint mediator that intercepts component IPC (1-5). The decision is made based on the policies specified by both the caller and callee applications.

### Saint’s Supported Policies

Policy tree illustrating the example policies required by applications. The double-stroke boxes indicate support by the existing platform.

### Publication


Supported by NSF