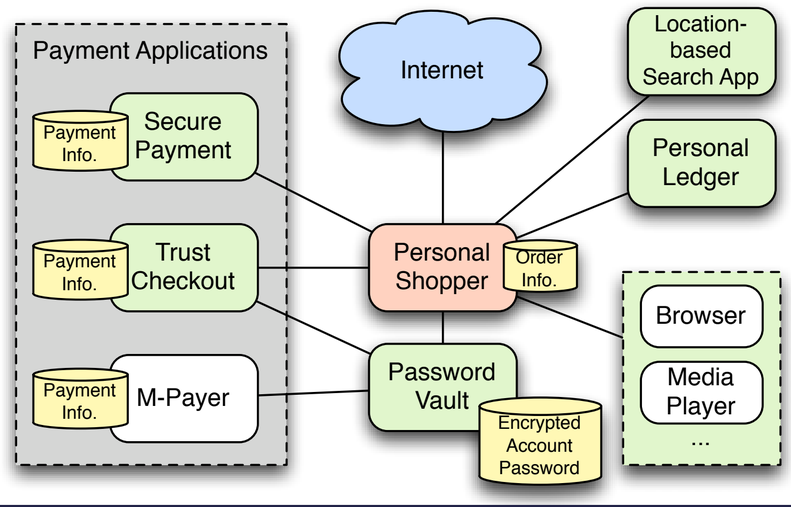
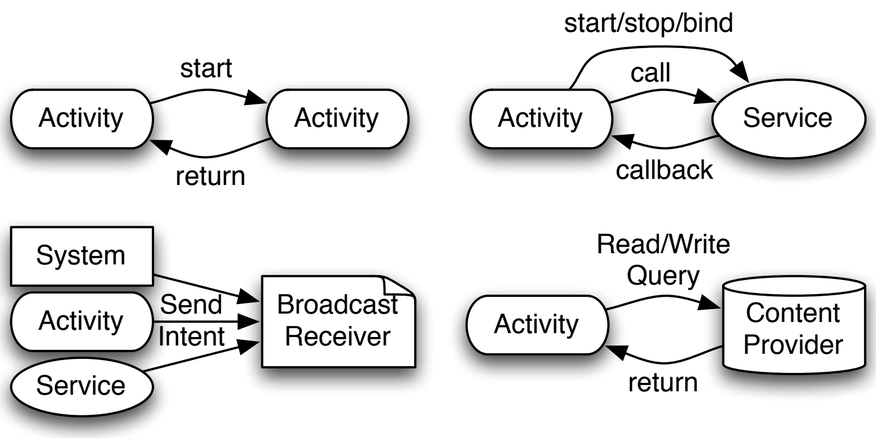
Semantically Rich Application-Centric Security in Android

Machigar Ongtang, Stephen McLaughlin, William Enck, and Patrick McDaniel

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 INTeraction (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.



Existing Applications Interactions in Android



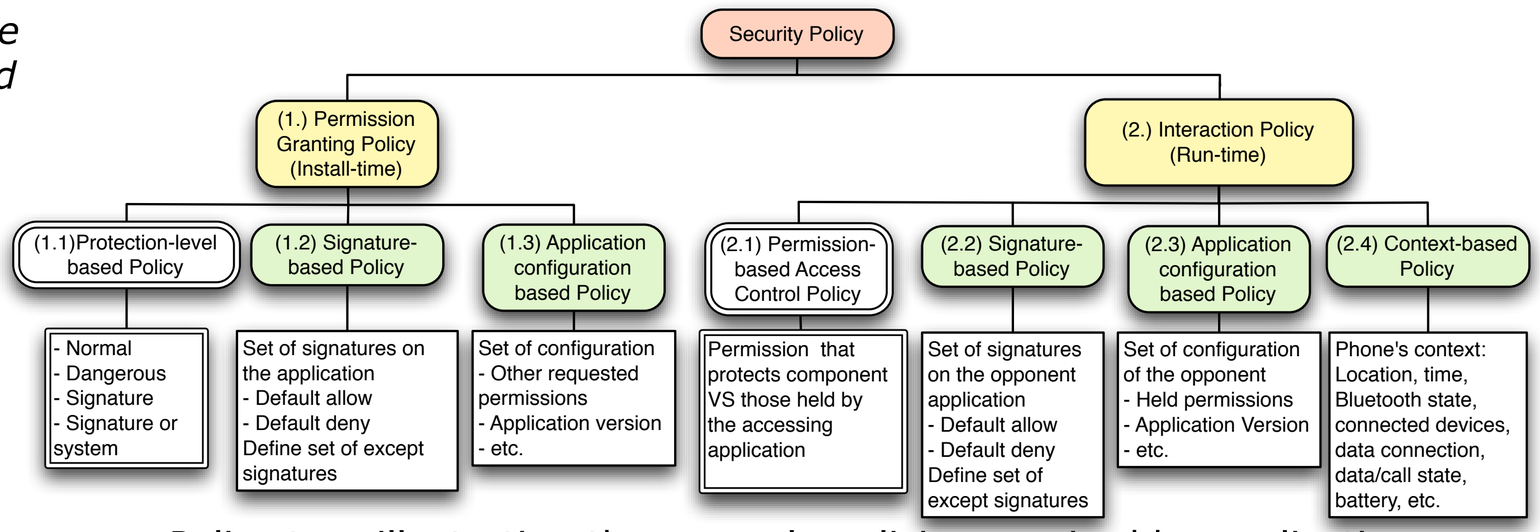
- Android's applications are comprised of components of types Activity, Service, Content Provider, and Broadcast Receiver.
- Inter-application communication passes through and is controlled by the middleware's IPC mechanism
- An application can protect its components using permission labels.
- An application may initiate IPC with a component in another or the same application if it has been assigned the permission label used to protect that component.

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*

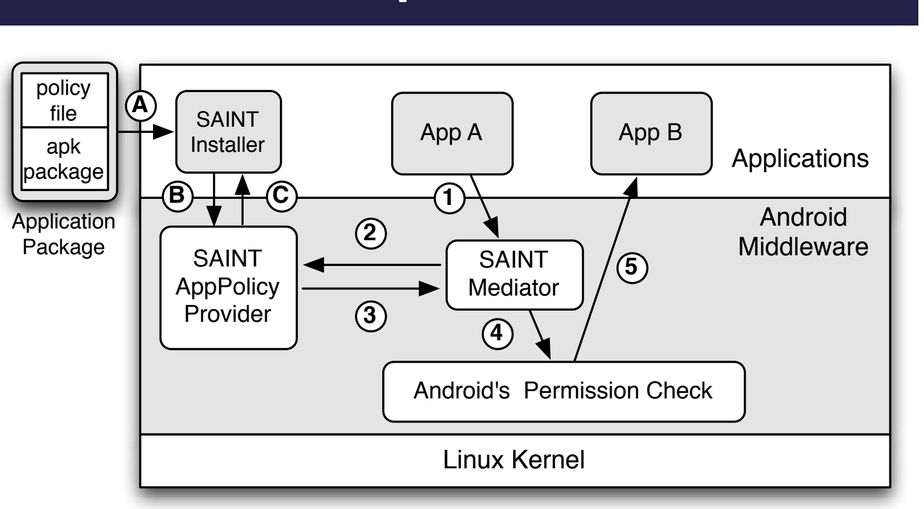
- Permission assignment policy- Applications have limited ability to control to whom permissions for accessing their interfaces are granted, e.g., white or black-list applications.
- Interface exposure policy- Android provides only rudimentary facilities for applications to control how their interfaces 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 Supported Policies

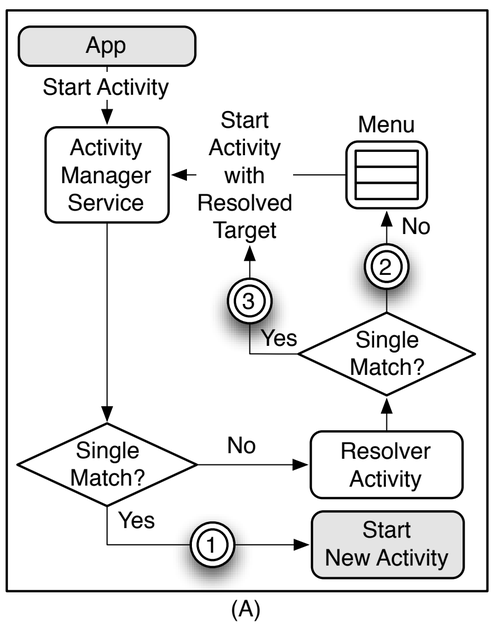


Policy tree illustrating the example policies required by applications. The double-stroke boxes indicate support by the existing platform.

Saint's Implementation

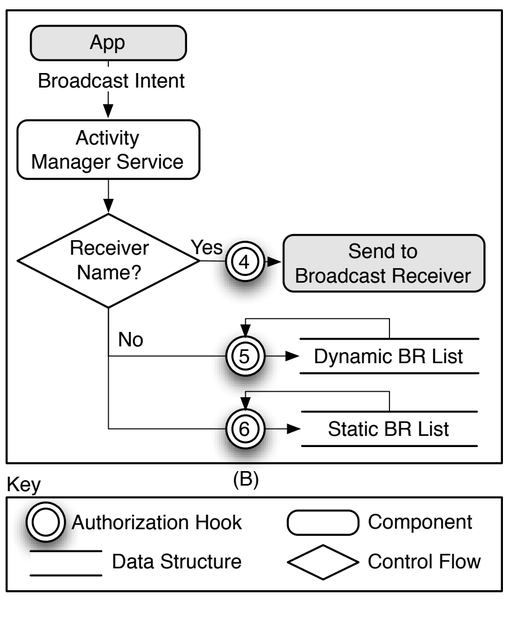


- Install-time policies are enforced by the Saint installer based on decisions made by the AppPolicy Provider (a-c)
- Interaction policies are enforced by the Saint mediator that intercepts component IPC (1-5). The decision is made based on the policies specified by both the caller and callee applications.



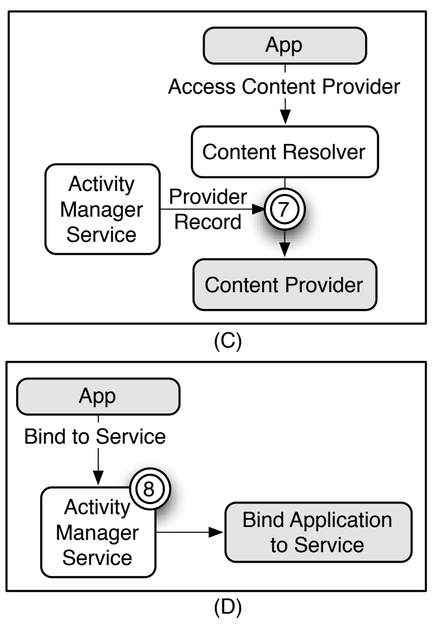
(A)

Hook mediating "starting Activity"



(B)

Hook mediating "receiving Intent broadcasts"



(C)

(D)

Hook mediating "accessing Content Provider" and "binding to Service"

Publication

Ongtang M., McLaughlin S., Enck W., McDaniel P., Semantically Rich Application-Centric Security in Android, in Proceedings of Annual Computer Security Applications Conference (ACSAC 2009), December 2009

Supported by NSF