ANDROID ICC
Lecture 9d

COMPSCI 702
Security for Smart-Devices

Muhammad **Rizwan** Asghar

March 18, 2021

THE UNIVERSITY OF AUCKLAND
NEW ZEALAND

ANDROID BINDER

- Binder enables Inter-Component Communication (ICC) in Android
- It is implemented as a driver in the Linux kernel
- It is a customised version of Open Binder
- It provides a simple RPC-like mechanism
- Apps use Java methods to invoke ICC
- Android then translates this in C++ invocations and system calls to the Binder driver

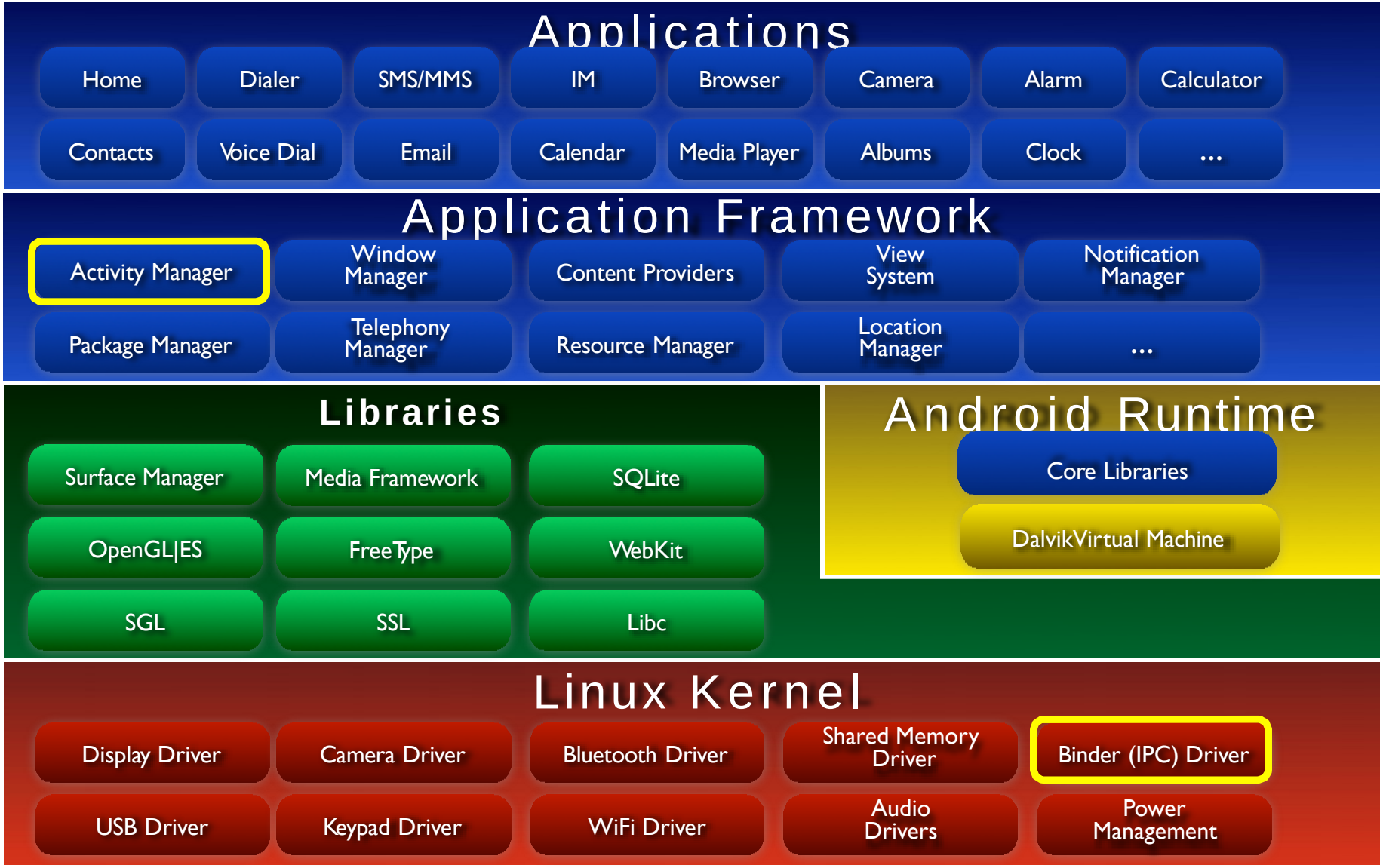
COMMUNICATION IN ANDROID

- In Linux, processes communicate and share data through
  - Pipes
  - Shared memory
  - Message queue
- In Android, app components communicate through
  - Binder

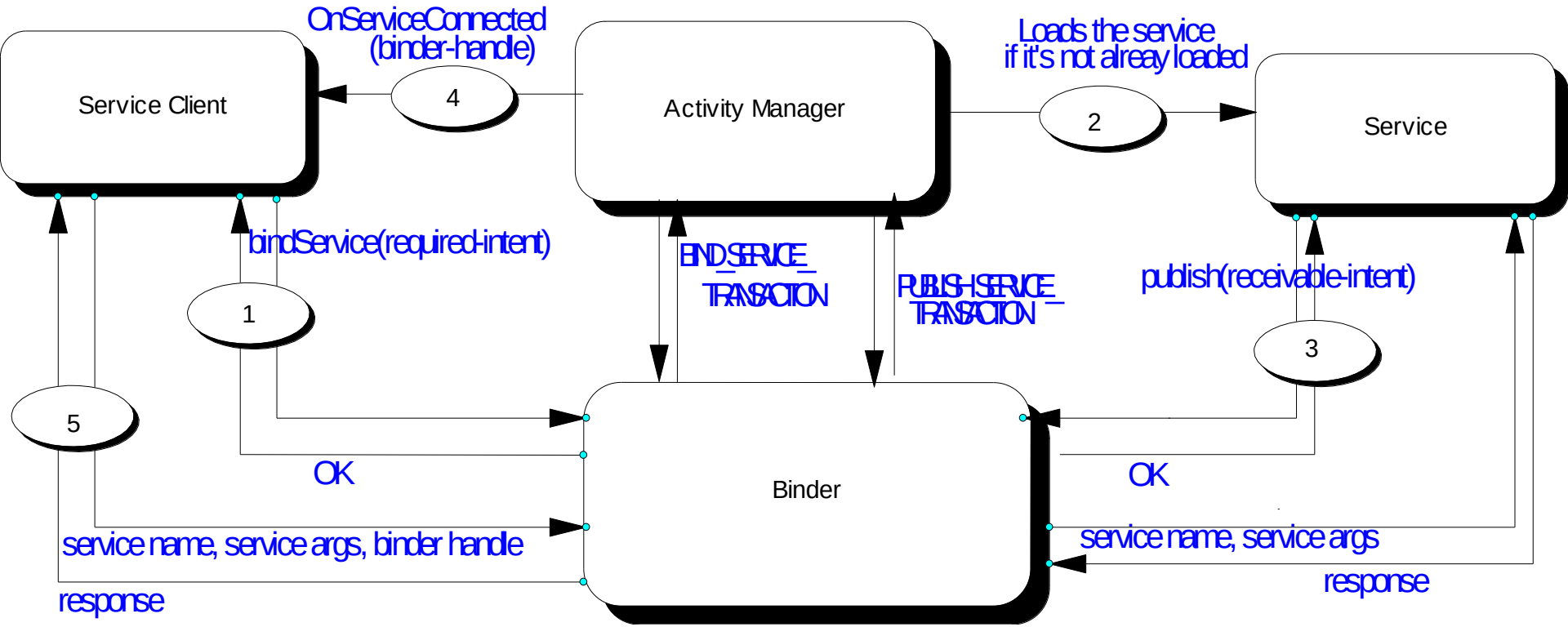
ACTIVITY MANAGER

- The Activity Manager is a special service that apps use for ICC
- It provides more than 100 methods
- Most common methods include
  - startActivity
  - sendBroadcast
  - startService
  - bindService
- Apps can export services by “publishing” them through the Activity Manager

ACTIVITY MANAGER AND BINDER



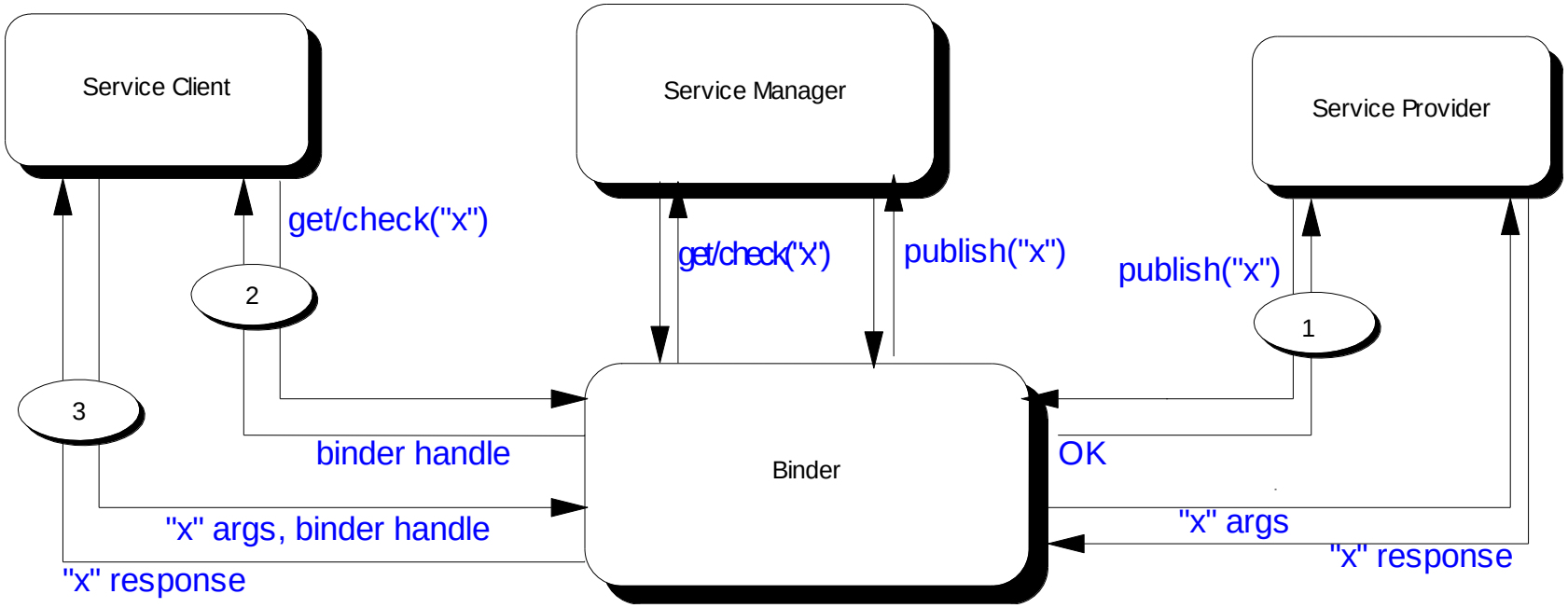
ACTIVITY MANAGER AND BINDER



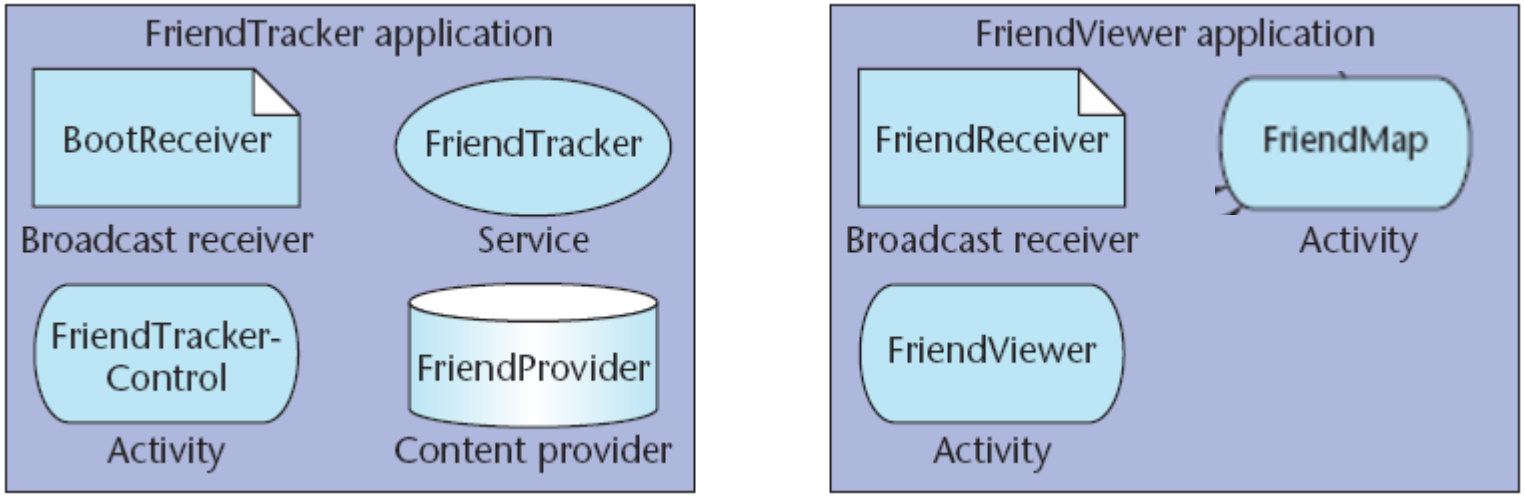
SERVICE MANAGER

- The Service Manager is a special system service to keep track of available services
- An app that wants to provide a service to others can publish its service through the Service Manager
- Communication to the Service Manager takes place through Binder
- The Service Manager accepts the following commands
  - **Publish:** Takes two arguments – service name and address – used for publishing a service within the Service Manager
  - **Get/check:** Takes one argument – service name – returns an address of the service in the form of a handler
  - **List:** Lists the service names registered with the Service Manager

SERVICE MANAGER IN ACTION



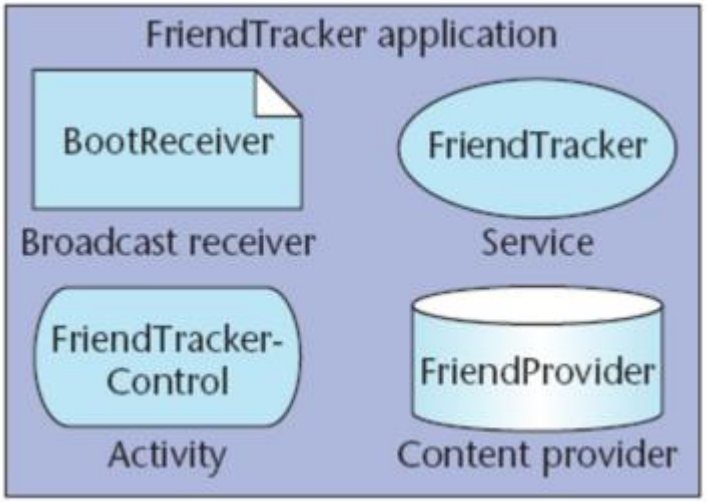
EXAMPLE: ANDROID APPLICATION



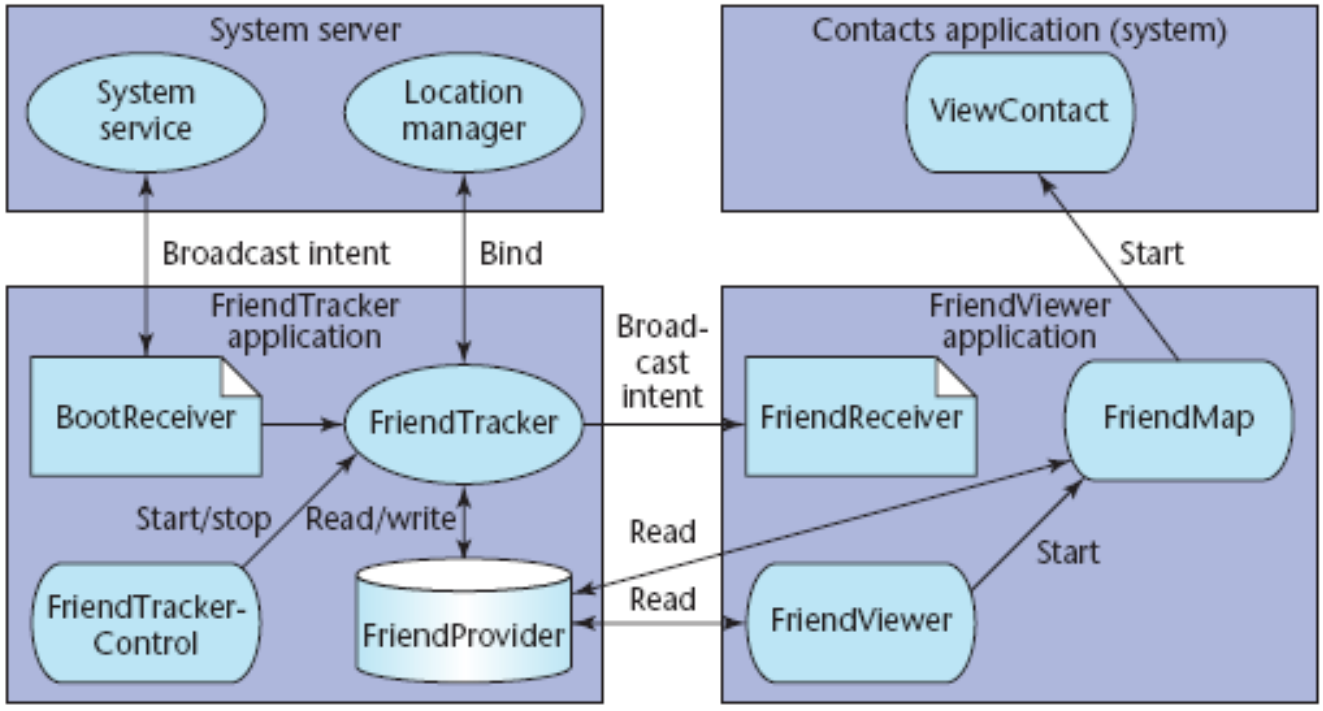
- The FriendTracker and FriendViewer applications: users can discover and view their friends' locations

FRIENDTRACKER APPLICATION

- FriendTracker (*Service*) polls an external service to discover friends' locations
- FriendProvider (*Content provider*) maintains the most recent geographic coordinates of friends
- FriendTrackerControl (*Activity*) defines a user interface for starting and stopping the tracking functionality
- BootReceiver (*Broadcast receiver*) gets a notification from the system once it boots
  - The application uses this to automatically start the FriendTracker service

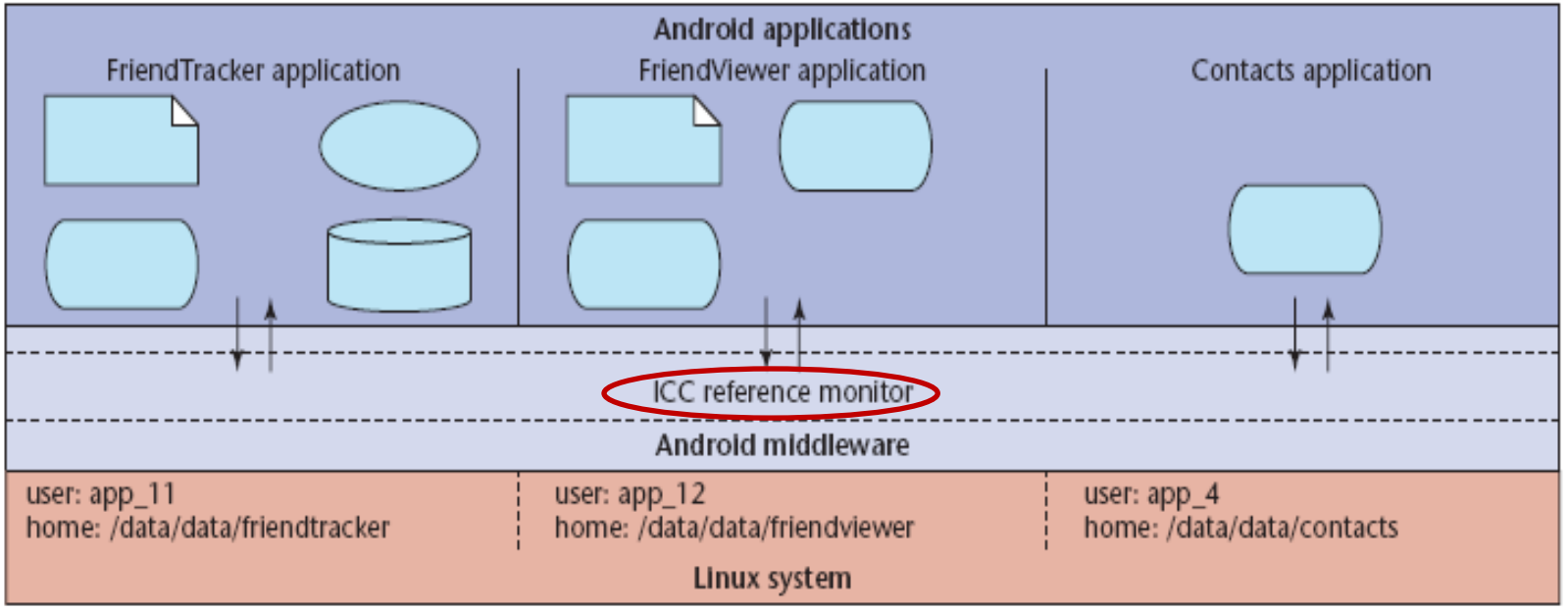


COMPONENT INTERACTION



- Service components support start, stop, and bind actions so the FriendTrackerControl (*Activity*) can start and stop the FriendTracker (*Service*) that runs in the background

REFERENCE MONITOR

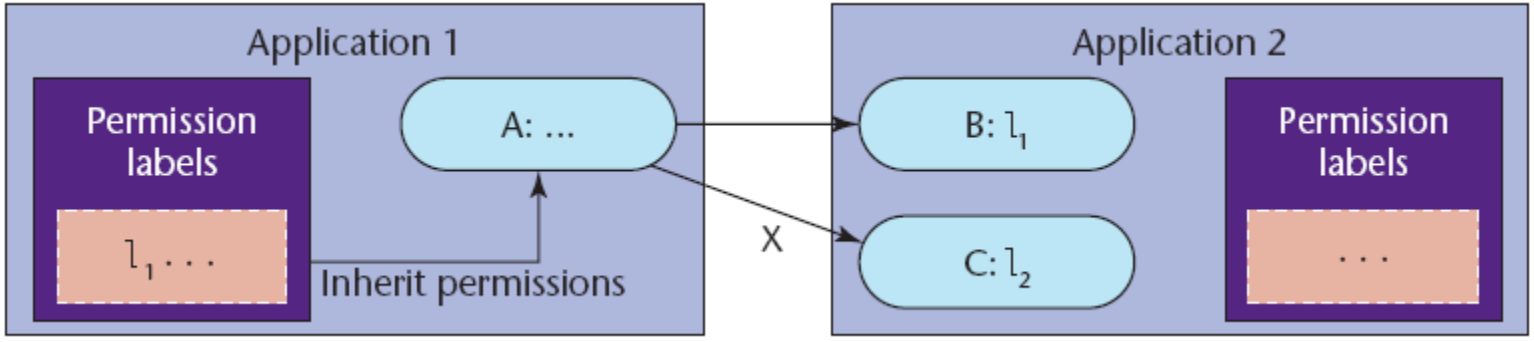


- Android middleware contains a reference monitor that mediates the establishment of ICC
- Reference monitor is part of the Activity Manager

MAC SECURITY ENFORCEMENT

- The core idea of Android security enforcement - label assignment to applications and components
- A reference monitor enforces MAC for regulating access to app components
- Access to each component is restricted by assigning it an access permission label
- Applications are assigned collections of permission labels
- When a component initiates ICC, the reference monitor checks whether its permission label is same as the target component's access permission label

PERMISSION LABELS



- The Android middleware implements a reference monitor providing MAC enforcement about how applications access components

- Component A's ability to access components B and C is determined by comparing the access permission labels on B and C with the collection of labels assigned to Application 1

SECURITY ENFORCEMENT

- Assigning permission labels to an application specifies its protection domain

- Android's policy enforcement is mandatory: permission labels cannot be changed until the application is re-installed

- Android's permission label model only restricts access to components and does not currently provide information flow guarantees

ACKNOWLEDGEMENT

- The first half of this topic is based on the slides presented by Giovanni Russello, thanks to him!

- The second half of this presentation is based on slides of Yinshu Wu, which is further based on the following:
  Enck, William, Machigar Ongtang, and Patrick McDaniel
  Understanding Android Security
  IEEE Security & Privacy 1 (2009): 50-57

Questions?

Thanks for your attention!