ANDROID PERMISSIONS
Lecture 10b

COMPSCI 702
Security for Smart-Devices

Muhammad **Rizwan** Asghar

March 23, 2021

WHY PERMISSIONS

- Since Android apps are sandboxed, they can access only their own files and other resources on the device

- Android can grant additional, fine-grained access rights to apps in order to enable richer functionality

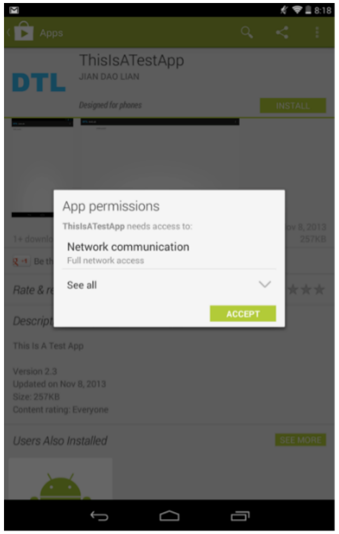
- These access rights are permissions

- Permissions can help Android to control access to resources, say Internet connectivity, data, or services

ANDROID PERMISSIONS

- Apps can request permissions by defining them in the **AndroidManifest.xml** file
- Android apps can request a set of additional permissions that are **granted at runtime**
- A user **may be asked** to grant requested permissions
- Android comes with a **built-in** list of pre-defined permissions
- **New permissions** that correspond to new features are added in each version
- Additional permissions, called **custom permissions**, can be defined by both system and user-installed apps

SOME PERMISSIONS



App permissions

ThisIsATestApp needs access to:

Network communication
Full network access

See all

This Is A Test App

Version 2.3
Updated on Nov 8, 2013
Size: 257KB
Content rating: Everyone

- CAMERA
  - Required to access the camera device
- INTERNET
  - Allows apps to open network sockets
- READ_CONTACTS
  - Allows an app to read the user's contacts data
- RECEIVE_SMS
  - Allows an app to receive SMS
- SEND_SMS
  - Allows an app to send SMS

PERMISSION EXAMPLE

- An app that wants to receive incoming SMS has to declare in its manifest

```
<uses-permission
android:name=android.permission.RECEIVE_SMS
"/>
```

- RECEIVE_SMS is considered a dangerous permission

PERMISSION MANAGEMENT

- Permissions are assigned to each app (as identified by a unique package name) by the package manager
- The package manager maintains a central database of installed packages with information about
  - Install path
  - Version
  - Certificate info
  - Assigned permissions to each package
  - A list of all permissions defined on a device
- This package database is stored in the XML file /data/system/packages.xml
- It is updated each time an app is installed, updated, or uninstalled

PERMISSION PROTECTION LEVELS

- Protection levels characterise potential risk implied in the permission

- Indicate the procedure that the system should follow when determining whether or not to grant the permission

- Four protection levels
  - Normal
  - Dangerous
  - Signature
  - SignatureOrSystem

NORMAL

- A permission that is less security-critical
- Granted without asking users
- Examples
  - ACCESS_NETWORK_STATE
    - Allows apps to access information about networks

DANGEROUS

- Permissions with the dangerous protection level give access to user data or some form of control over the device
- Involves some functionalities that can cost money
- Requires user approval
- Examples
  - READ_SMS
    - Allows an app to read SMS
  - CAMERA
    - Gives apps access to the camera device

SIGNATURE

- A signature permission is only granted to requesting apps that are signed with the same key as the app that declared the permission
- This is the “strongest” permission level because it requires the possession of a cryptographic key
- Thus, apps using signature permissions are typically controlled by the same developer
- It is decided by the system without requiring user intervention
- Built-in signature permissions are typically used by system apps that perform device management tasks
- Examples
  - NET_ADMIN
    - Configure network interfaces, IPSec, and so on

SIGNATUREORSYSTEM

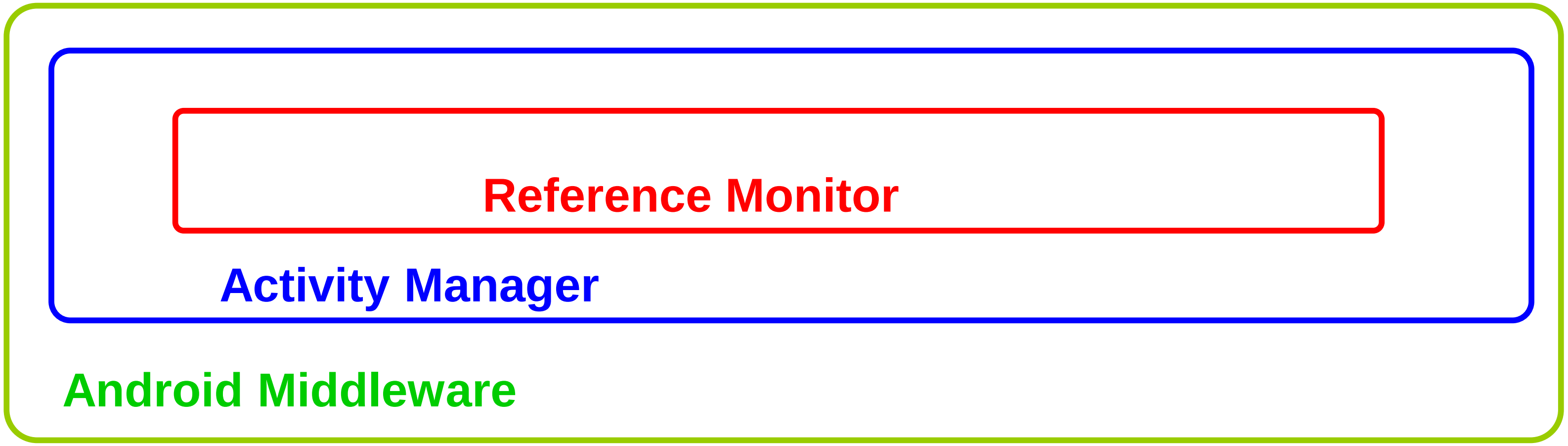
- Granted to apps that are either part of the system image or signed with the same key as the app that declared the permission

- This allows vendors that have their apps pre-installed on an Android device to share specific features that require a permission without having to share signing keys

- Until Android 4.3, any app installed in the system partition was granted signatureOrSystem permission automatically

- Since Android 4.4, apps need to be installed in the /system/priv-app/ directory in order to be granted permissions with this protection level

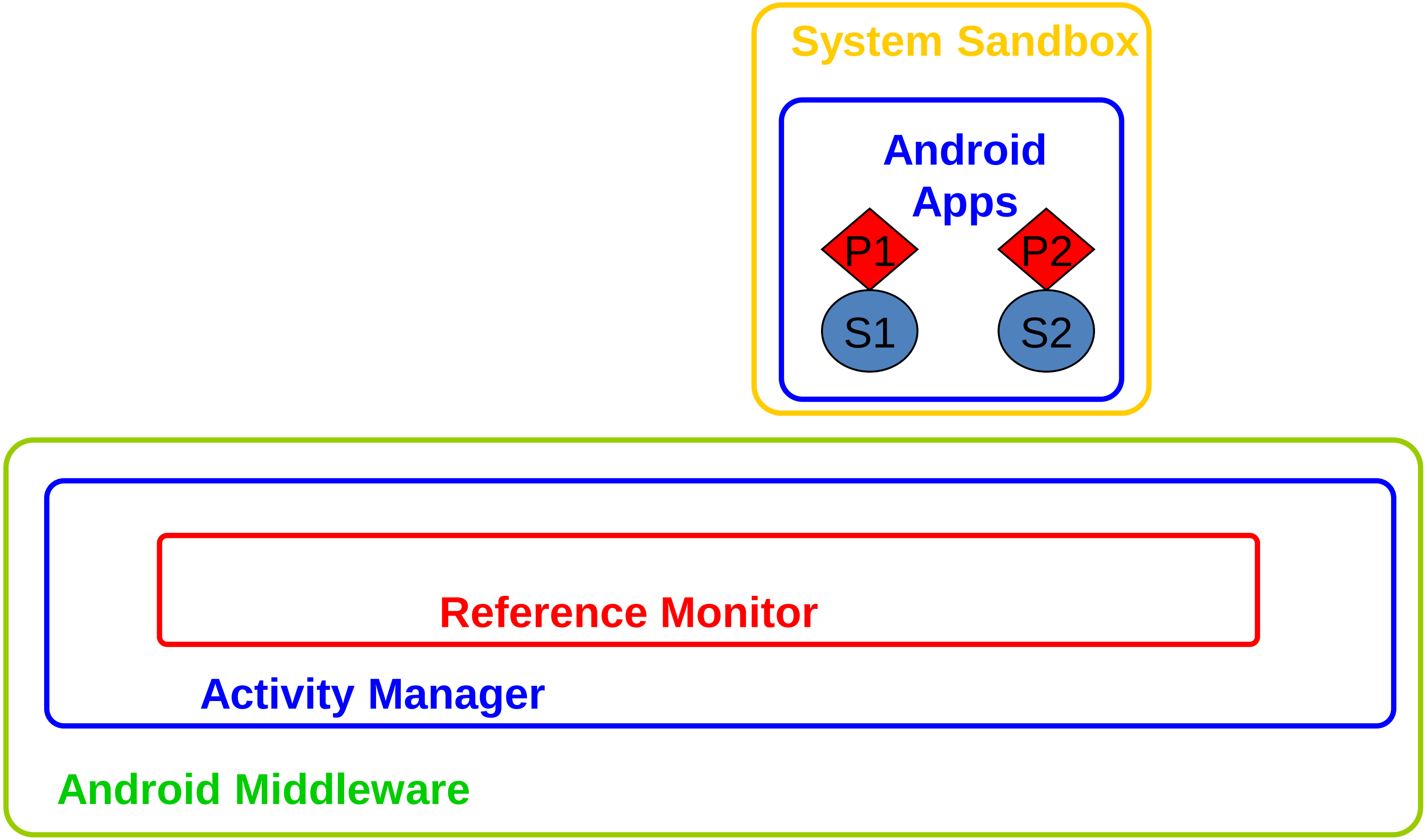
ANDROID MAC MODEL



PROTECTION DOMAIN

S1 = Location Service

P1 = LOCATION_PERMISSION



System Sandbox

Android Apps

P1

P2

S1

S2

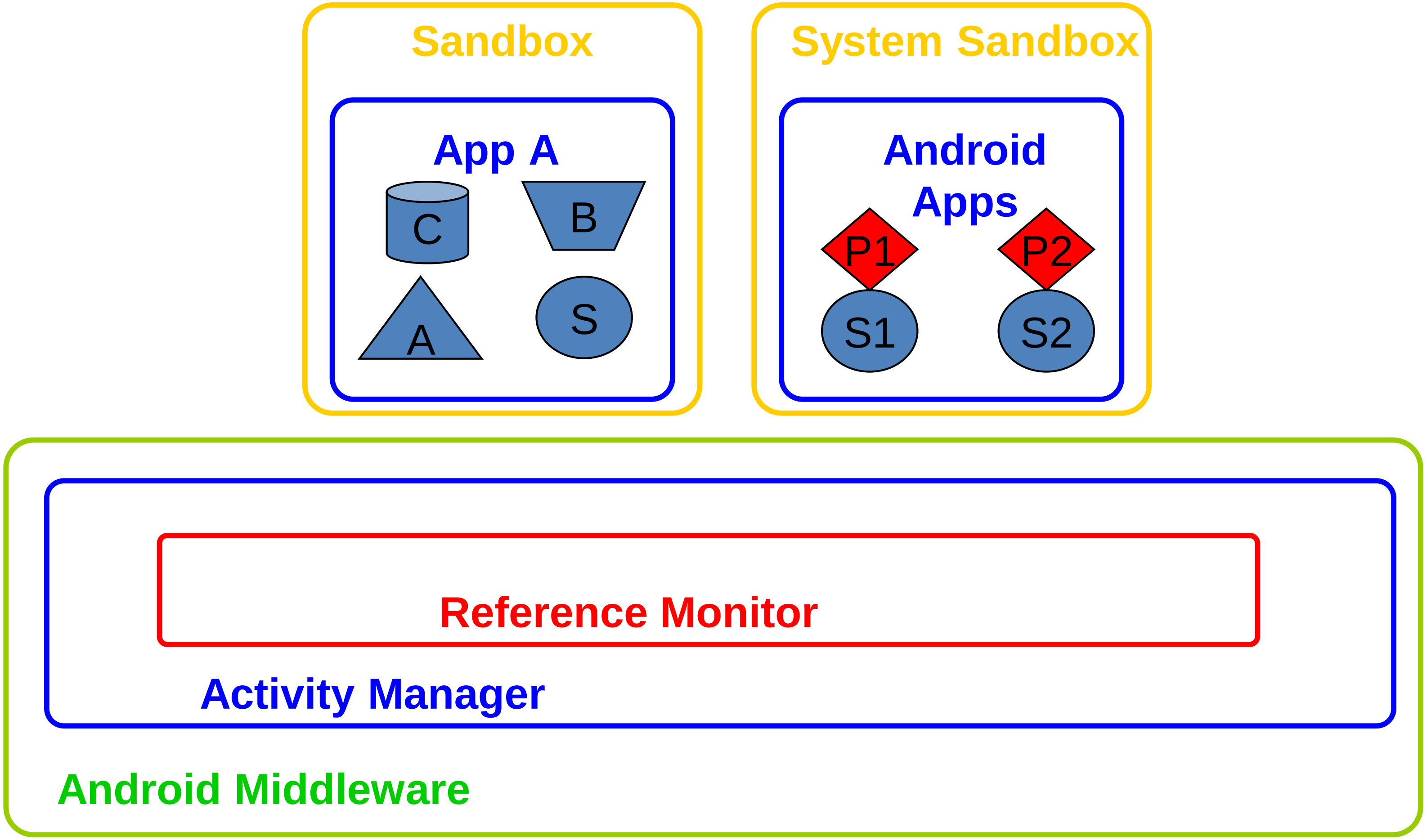
Reference Monitor

Activity Manager

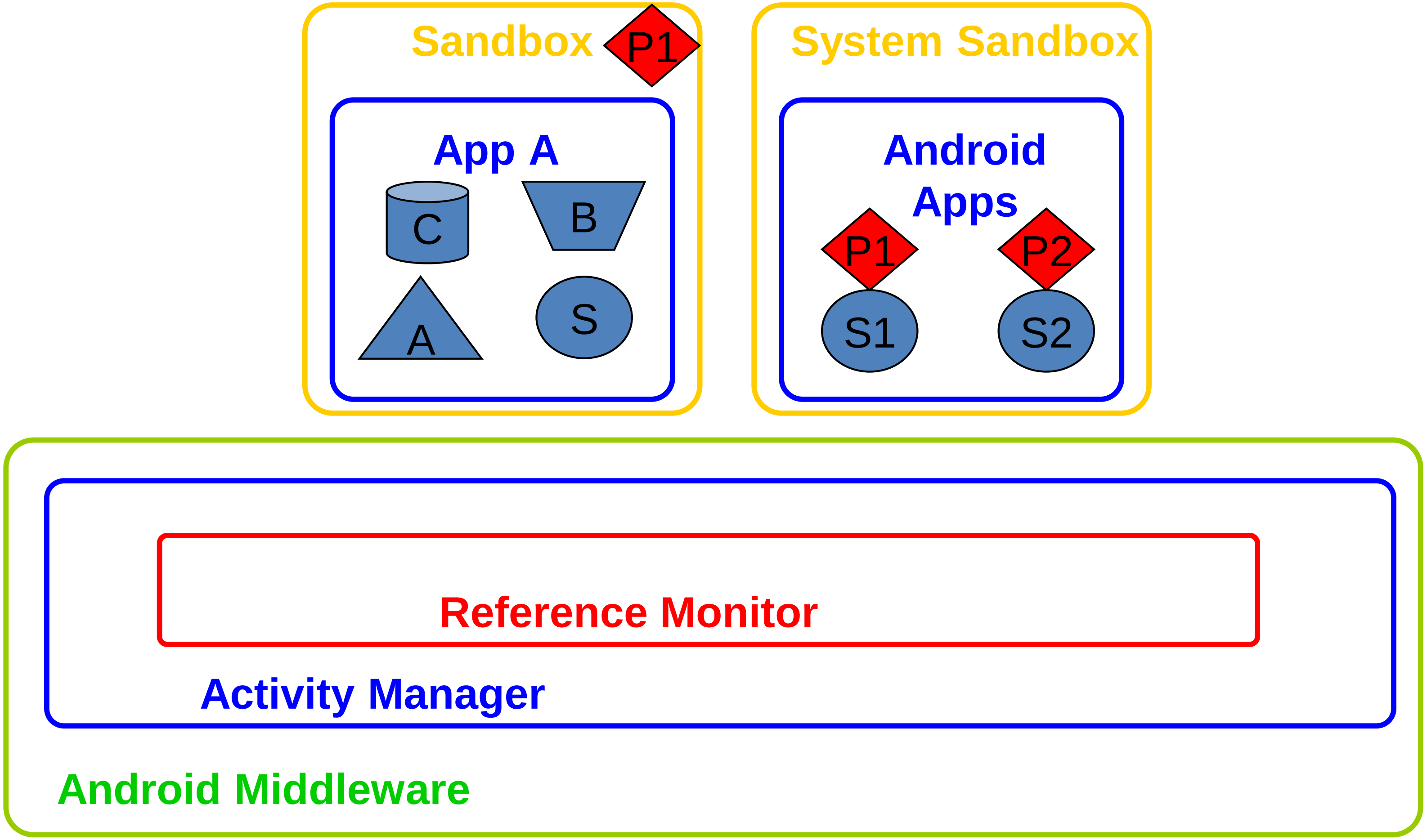
Android Middleware

ASSIGNMENTS OF PERMISSIONS

Runtime: Uses Permission = P1?



USING THE PERMISSION



REFERENCE MONITOR

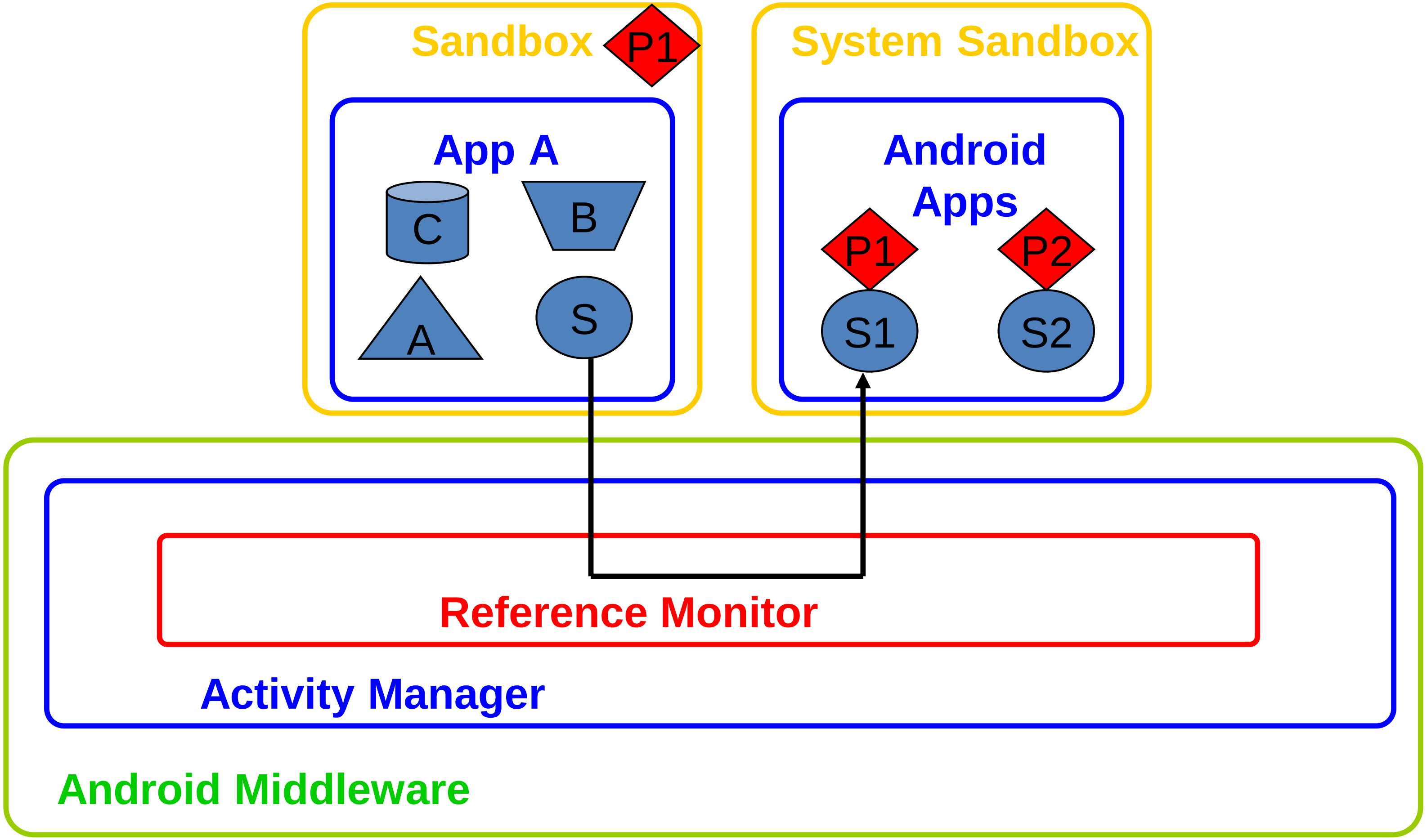


Image source: Lecture delivered by Giovanni Russello

RESOURCES

- **Chapter 2** of
  Android Security Internals: An In-Depth Guide to Android's Security Architecture
  Elenkov, Nikolay
  First Edition
  No Starch Press 2014
  ISBN:1593275811 9781593275815

- **Android permissions**
  http://developer.android.com/reference/android/Manifest.permission.html

- Enck, William, Machigar Ongtang, and Patrick McDaniel
  Understanding Android Security
  IEEE Security & Privacy 1 (2009): 50-57

Questions?

Thanks for your attention!