ANDROID SECURITY WEAKNESSES

Lecture 12b

COMPSCI 702

Security for Smart-Devices

Nalin Asanka Gamagedara Arachchilage

Slides from Muhammad **Rizwan** Asghar

March 25, 2021

THE UNIVERSITY OF AUCKLAND
NEW ZEALAND

POORLY DEISNGED APPS

- If not designed properly, apps can (unintentionally)
  - Expose resources
    - Internet, location, etc.
  - Deplete resources
    - Battery, data, etc.
  - Compromise privacy
    - Location, data, etc.

PRIVILEGE ESCALATION

- An adversary tries to escalate privileges to gain unauthorised access to protected resources

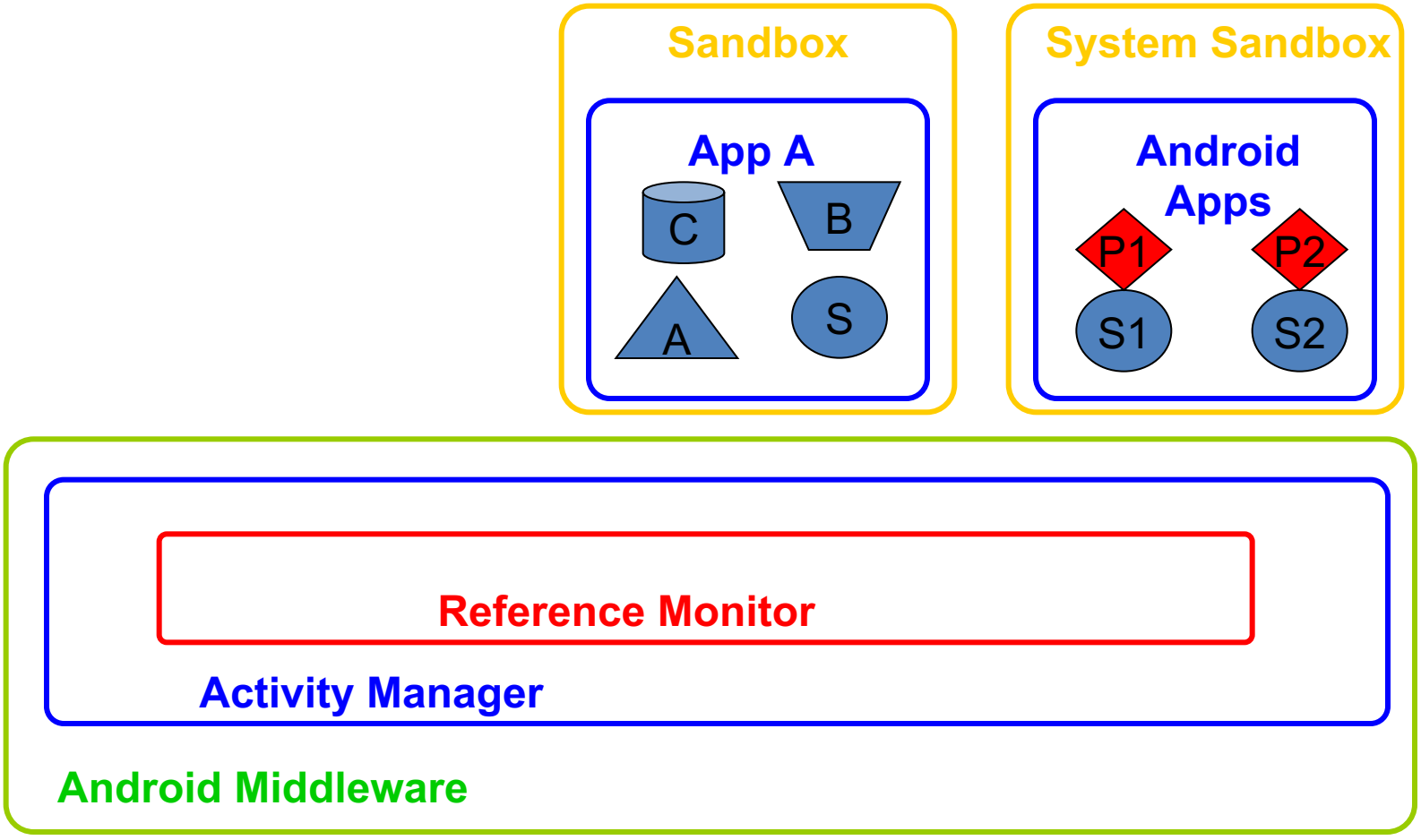
- Two major attacks
  - Confused deputy attacks
  - Collusion attacks

CONFUSED DEPUTY ATTACK

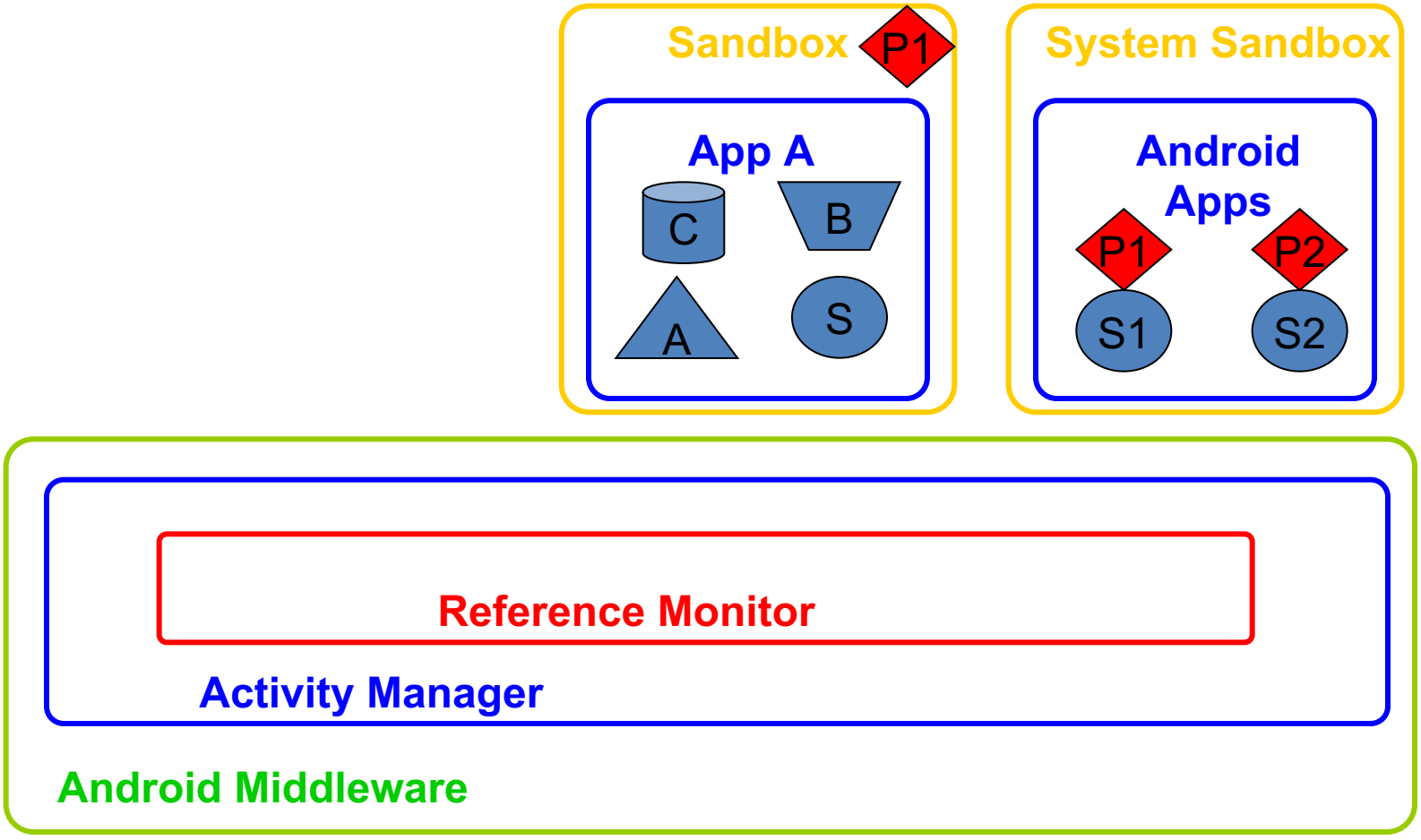
- If an app does not have a permission, it can ask its neighbour
- Confused deputy attack leverages the vulnerability in a benign app

ASSIGNMENT OF PERMISSIONS

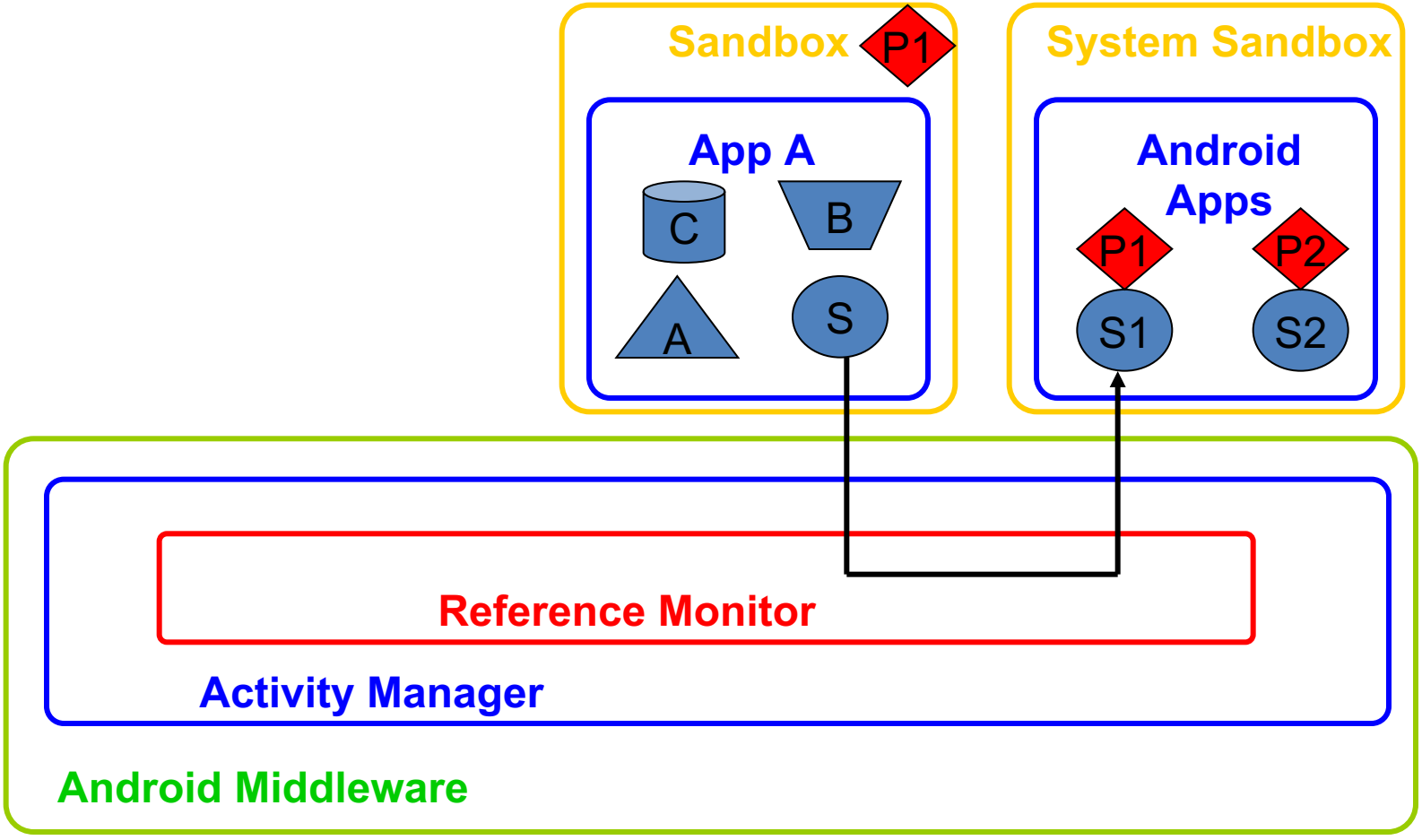
Runtime: Uses Permission = P1?



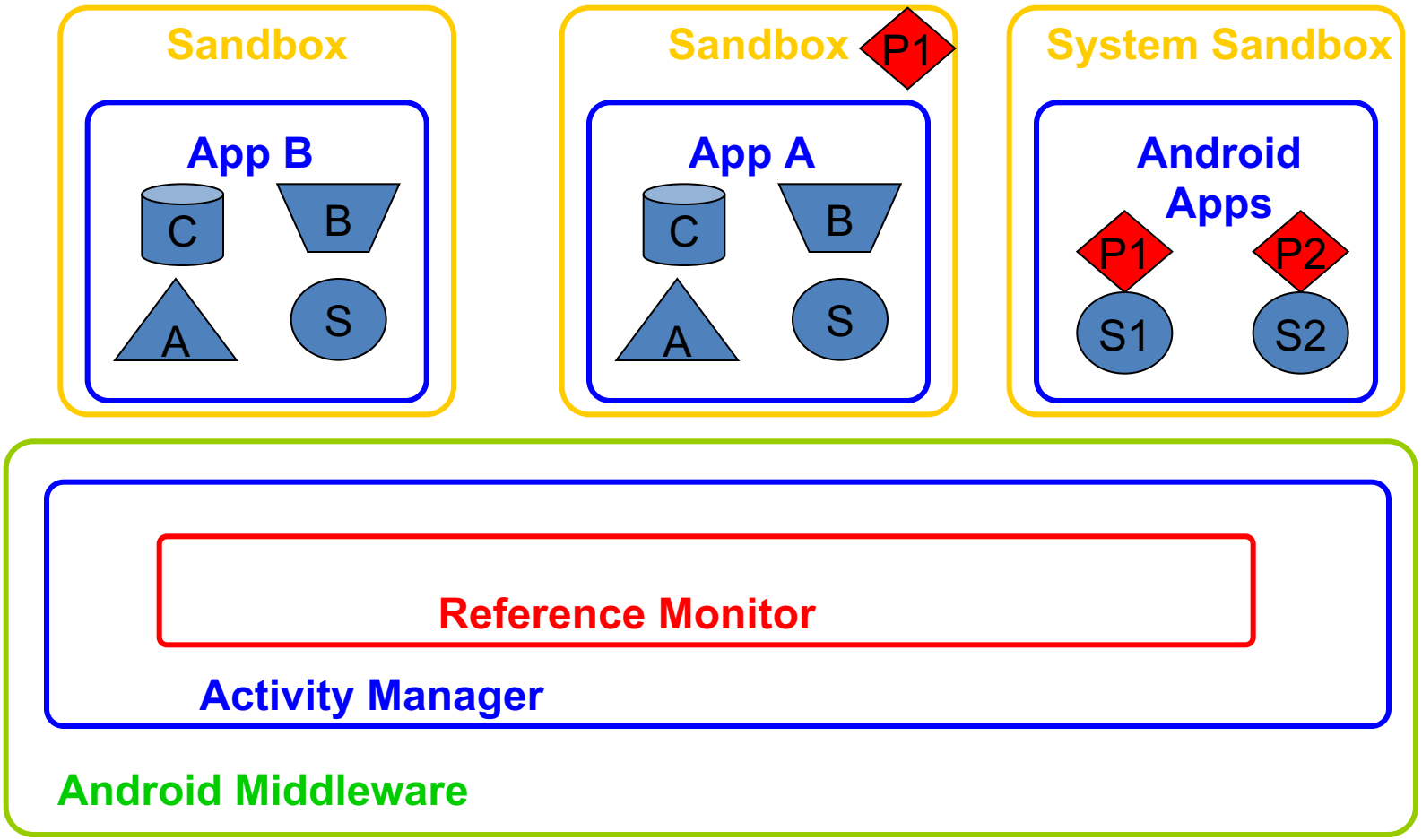
USING THE PERMISSION



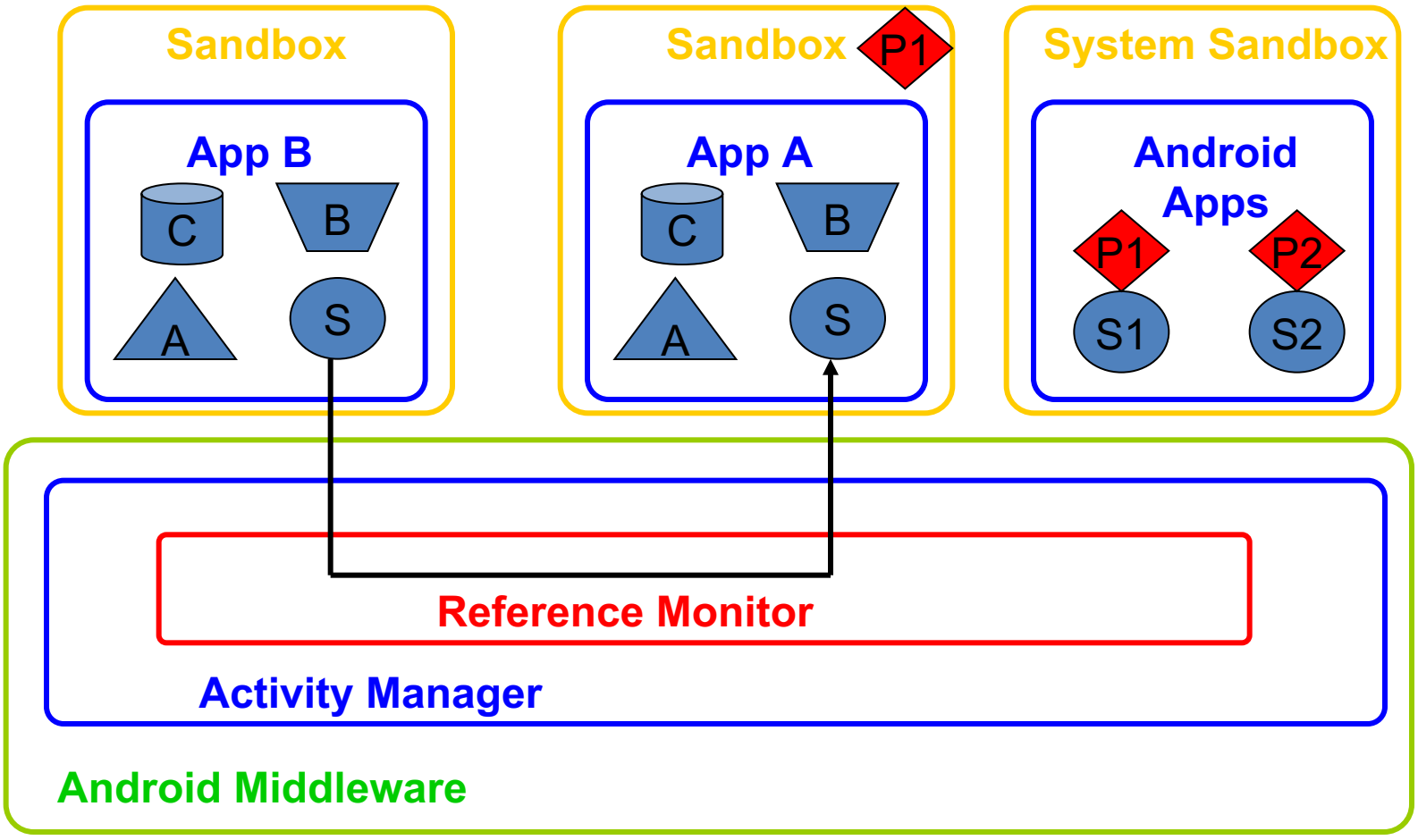
REFERENCE MONITOR



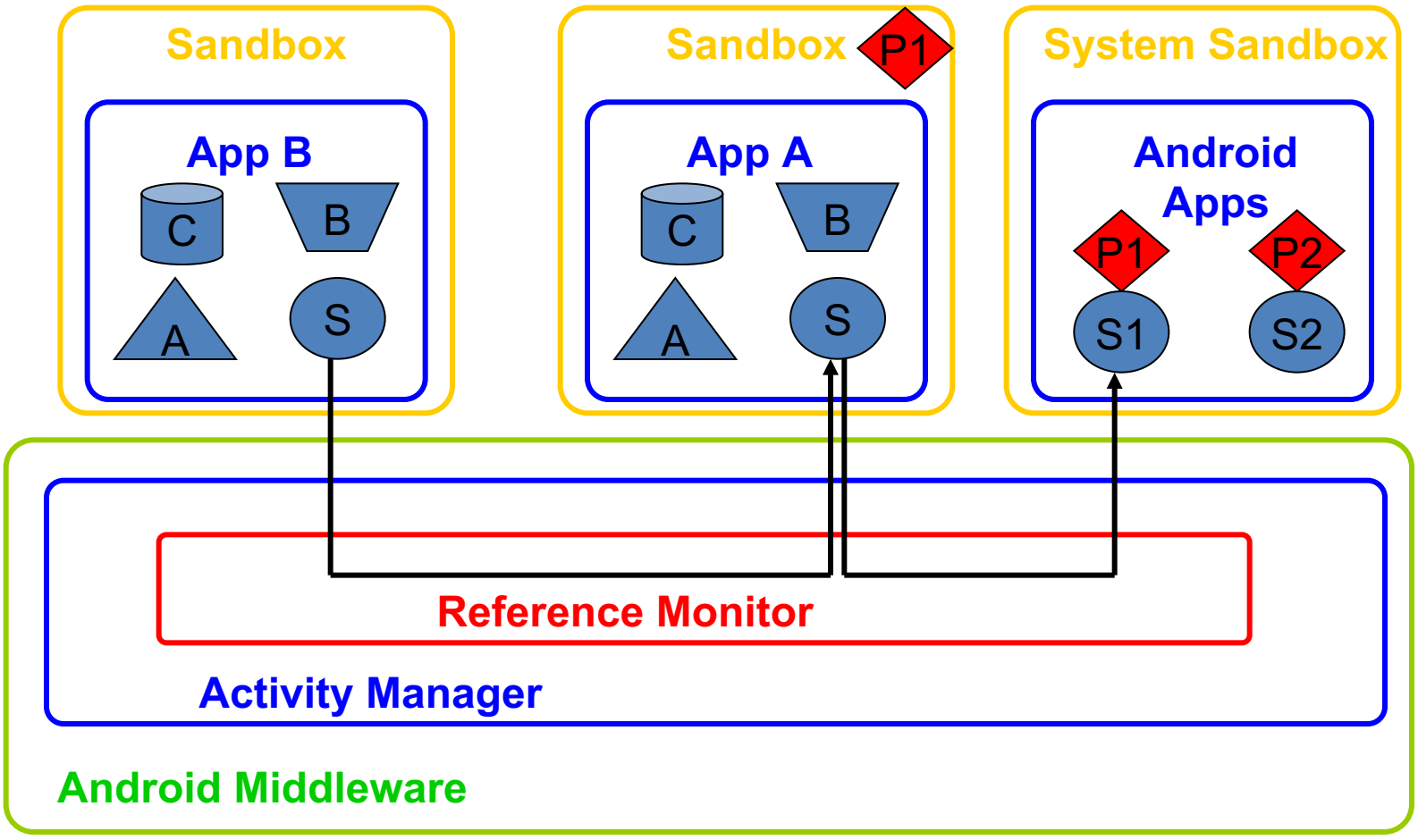
ANOTHER APPLICATION



CONSUMING A SERVICE



REFERENCE MONITOR



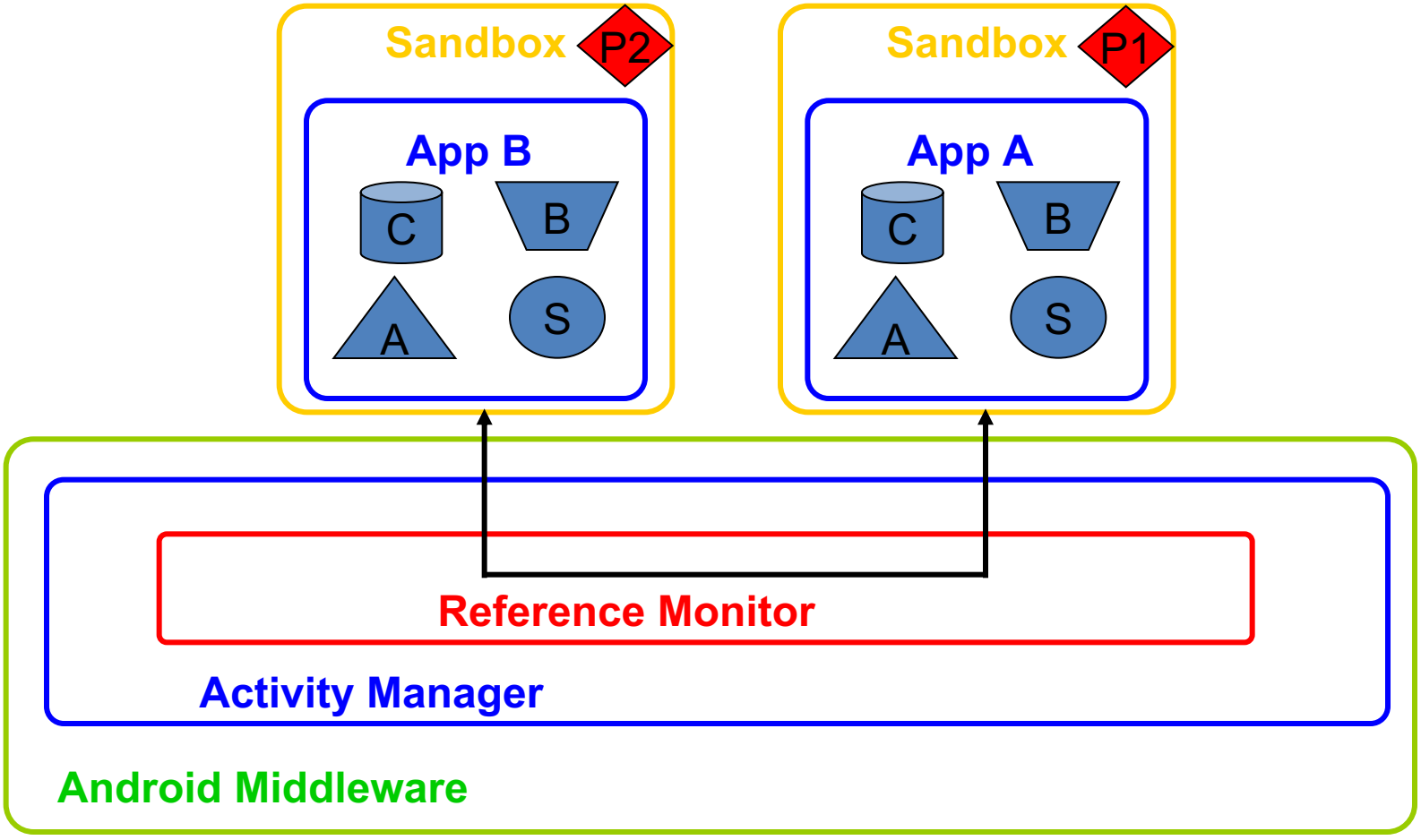
COLLUSION ATTACK

- Multiple apps can collaborate to get permissions, which each of them cannot get otherwise

- Example
  - An app has access to user location
  - Another app has access to the Internet
  - Both apps collude together in order to expose user location on the Internet

REFERENCE MONITOR

P1 = LOCATION_PERMISSION, P2 = INTERNET_PERMISSION



ANDROID ACCESS CONTROL MODEL

- Android supports all-or-nothing access
- It does not offer fine-grained access control
- Example
  - Let's assume that an app has access to the Internet and contacts
  - It is okay if the app uses contacts
  - It is also okay if the app uses the Internet
  - However, it is not okay to publish contacts through the Internet, which can lead to leaking sensitive information!
- Information flow techniques could help to prevent information disclosure

ACKNOWLEDGEMENT

- Some slides are based on the lecture delivered by Giovanni Russello, thanks to him!

Questions?

Thanks for your attention!