# System Security

## Access Control Fundamentals

Giovanni Russello

g.russello@auckland.ac.nz

**http://www.cs.auckland.ac.nz/compsci725s2c/**

# Access Control

- “The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner“
- central element of computer security
- assume have users
  - authenticated to system
  - assigned access rights to certain resources on system

# Authentication Phase

It is only concerned with correctly identifying an entity against a known set

- Assigning a unique identifier to the entity (i.e., user name)
- Using a secret (supposedly) known only to the specific entity
- Alternatively, using a unique feature that characterises the entity – identity and secret are the same

# Authorisation Phase

- Once the identity has been verified *access rights* are assigned so that the entity is able to *perform actions* within the system

# Access Control Requirements

- Reliable Input
  - Authenticated entities
  - Genuine information
- Least Privilege
  - Entities granted minimum set of access rights
- Administrative Duties
  - Only a special entity should be able to manage access rights for other entities

# Access Control Refinements

- Separation of Duty
- Fine Vs. Coarse Specifications
- Open and Closed policies
- (Automated) Conflict Resolution

# Access Control Elements

- subject - entity that can access objects
  - a process representing user/application
  - Principal is another term for referring to subject
- object - access controlled resource
  - e.g. files, directories, records, programs etc
- access right - way in which subject accesses an object
  - e.g. read, write, execute, delete, create, search

# Access Control Features

Auditor

User

Authentication Mechanism

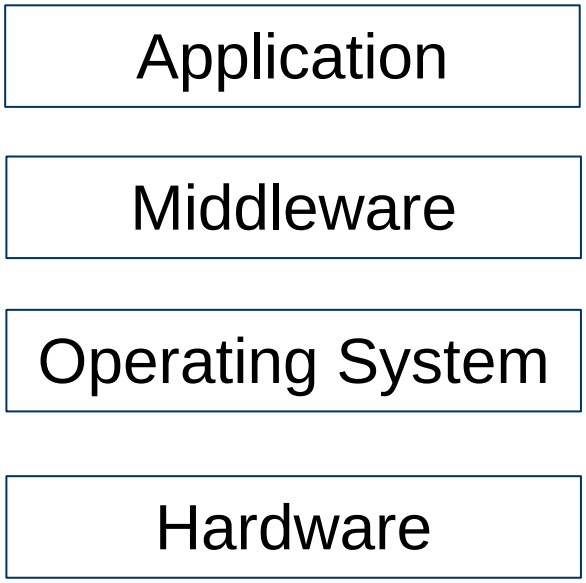
Authorisation Mechanism

Resources

Authorisations

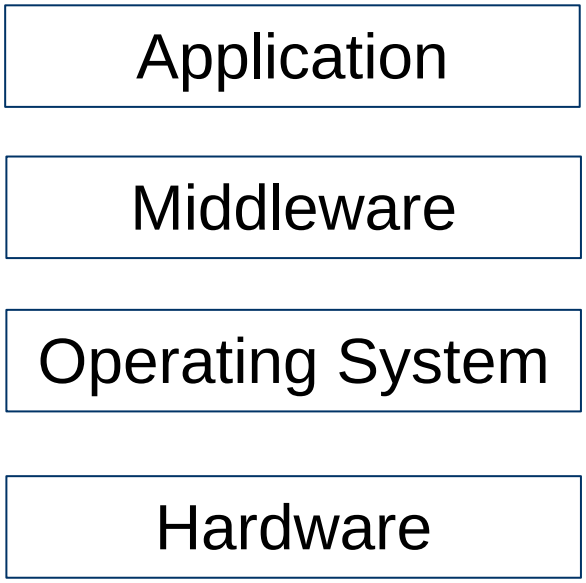
Security Administrator

# Working on Levels



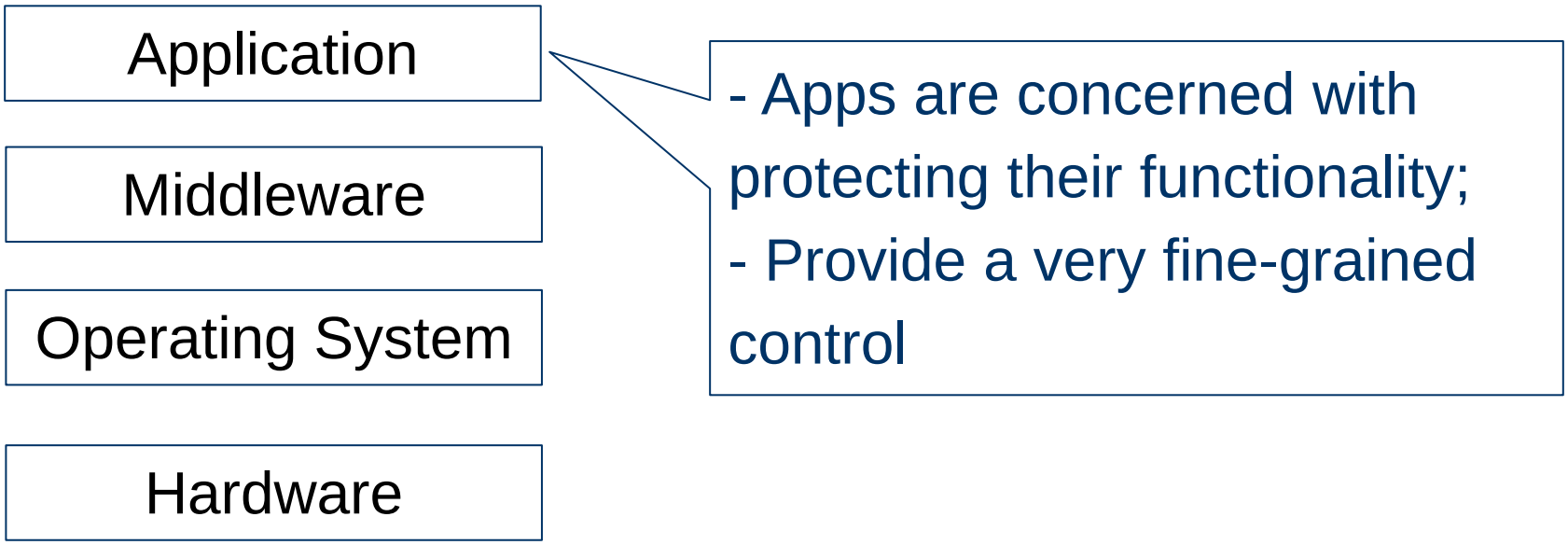

At each level, access control decisions are made for satisfying different security requirements

# Working on Levels

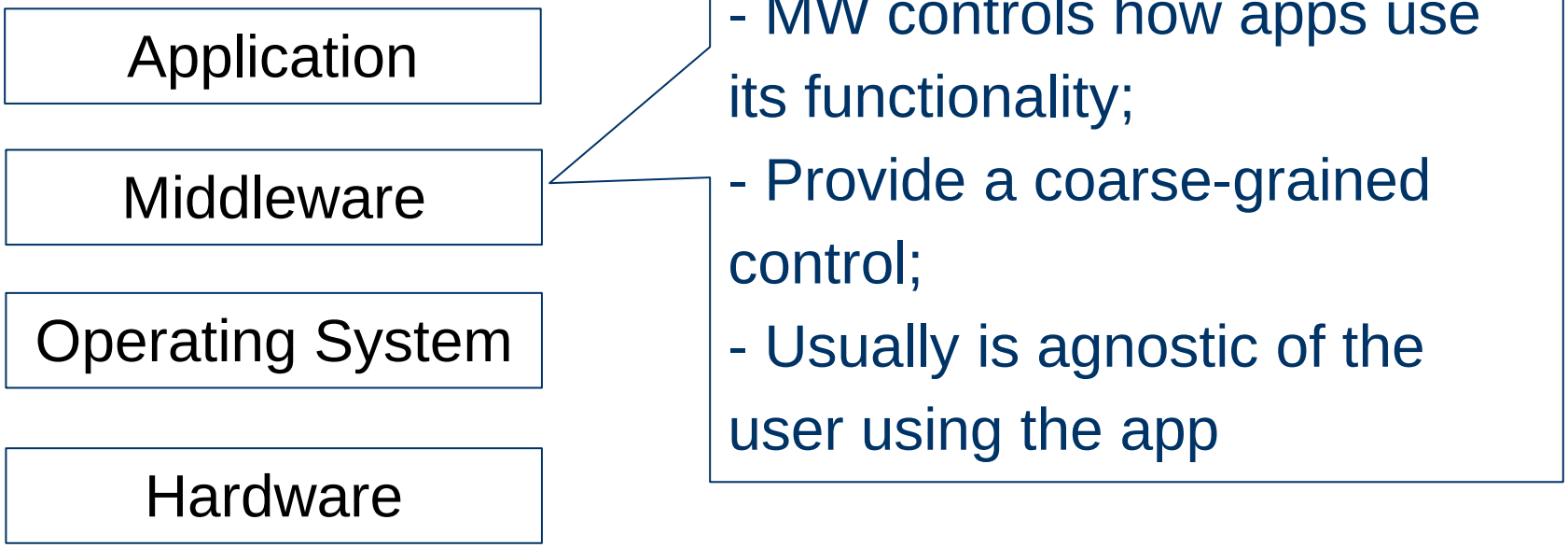



Can you give a concrete example of a system built with all these layers?

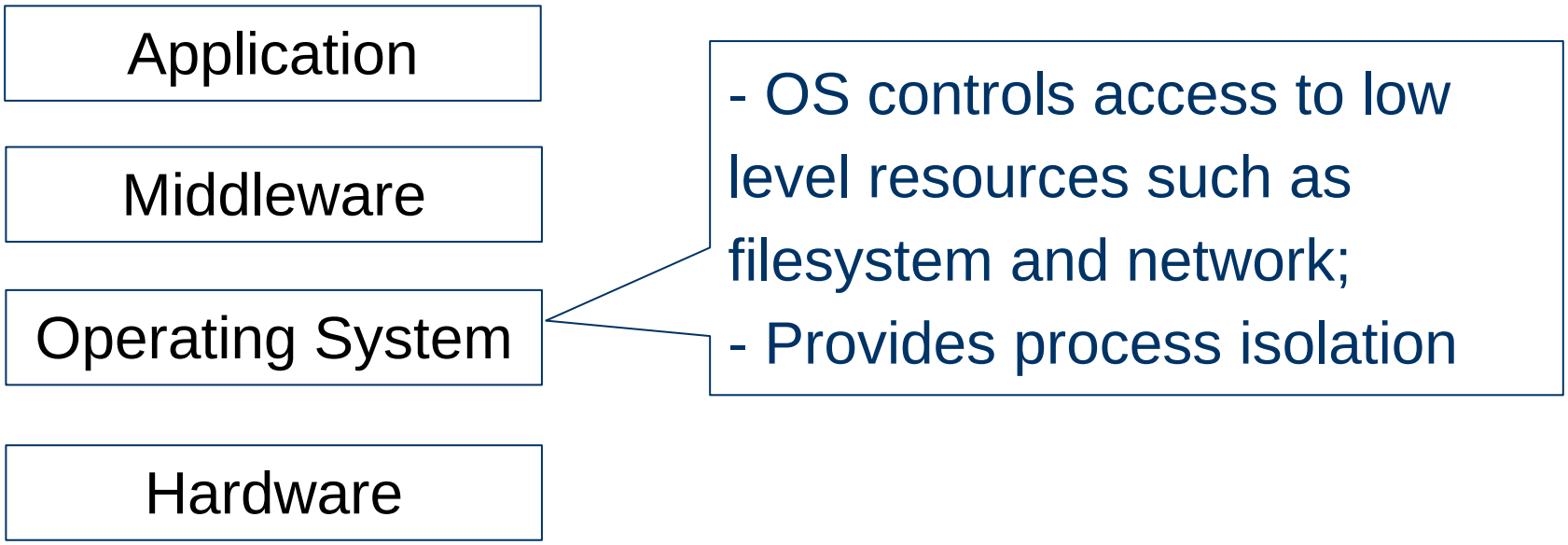
# Working on Levels: Application



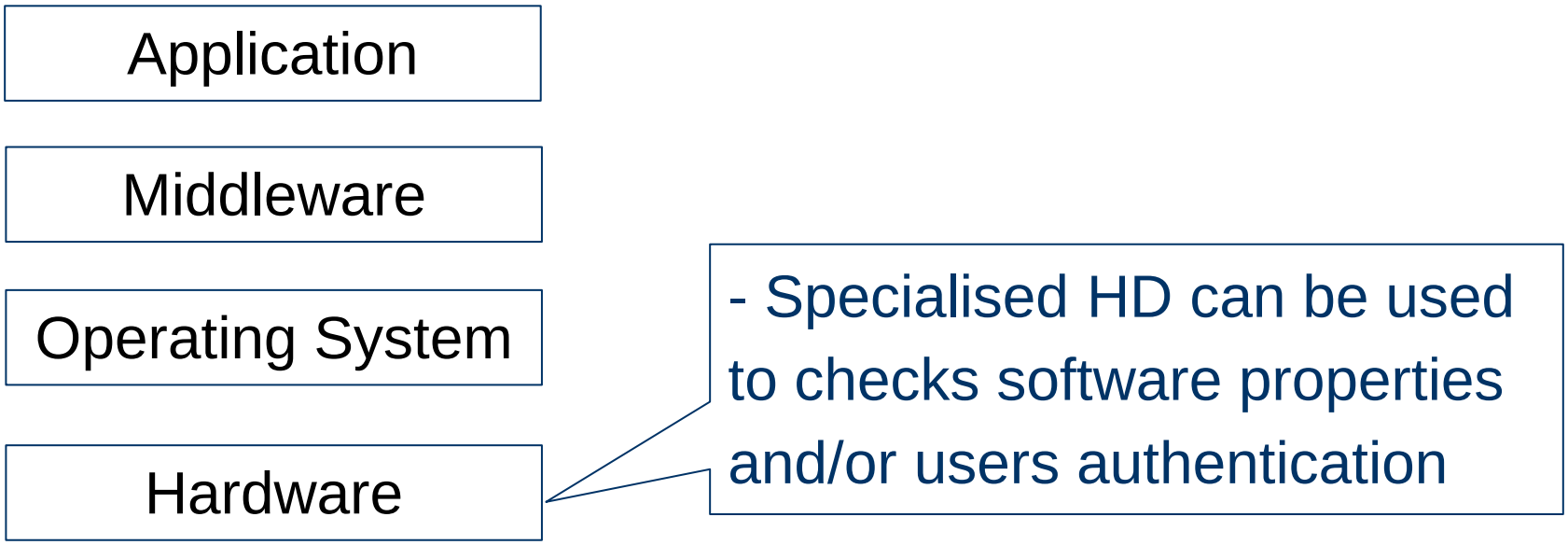
# Working on Levels: Middleware



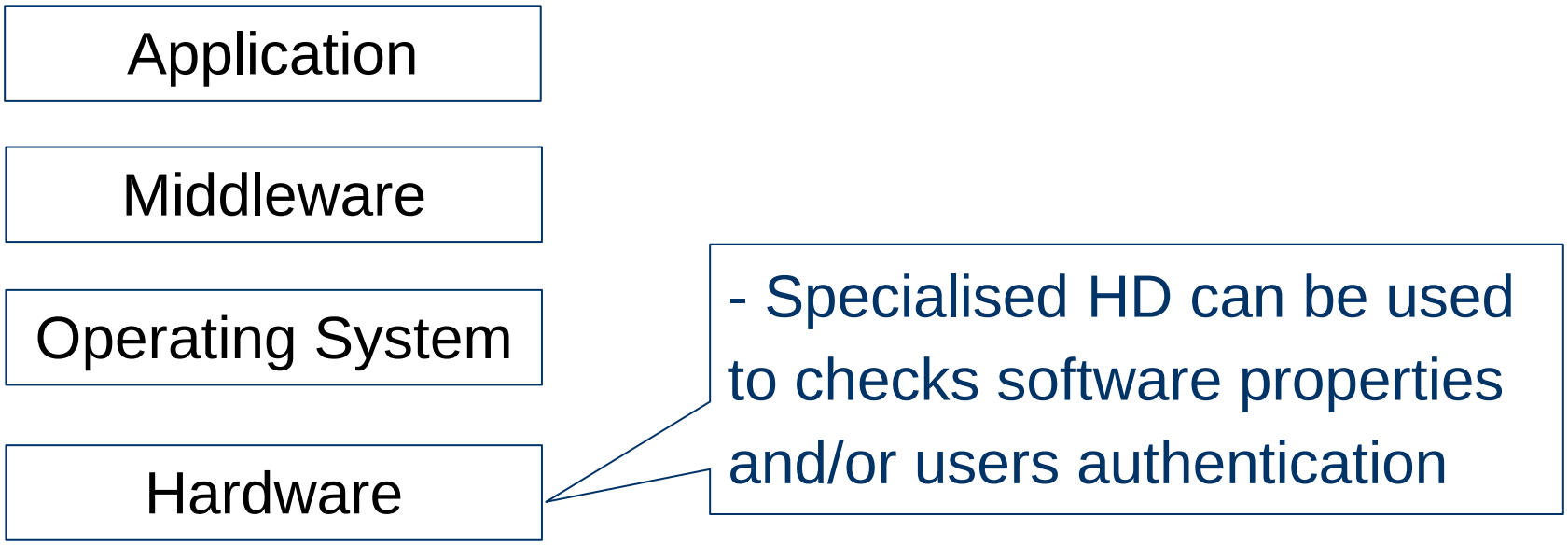
# Working on Levels: OS



# Working on Levels: HW



# Managing Security Policies



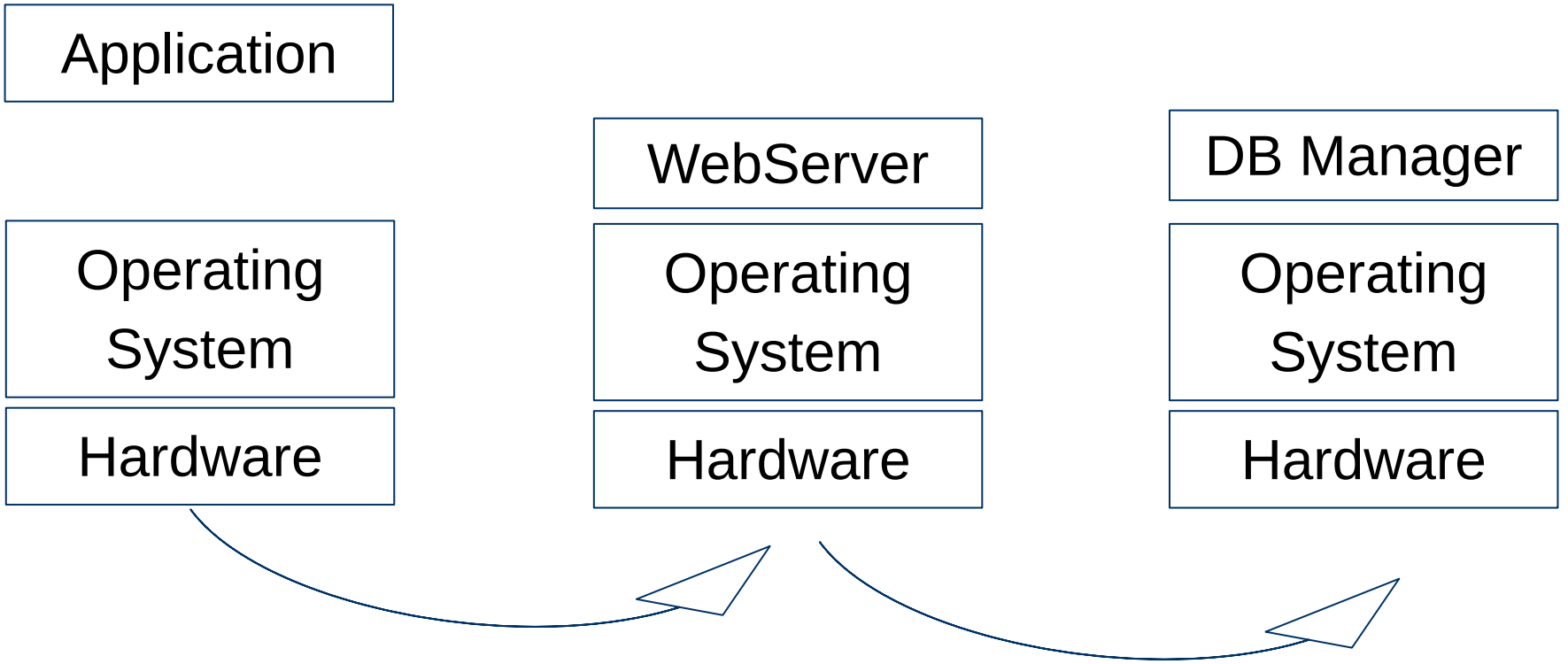
# Managing Security Policies

- Each layer requires specialised policies
- It might be required different Admins for each layer
- Ideally, the Admin of each layer should define security policies without knowing the security requirements of the other layers
- In reality, things are always more complicated!

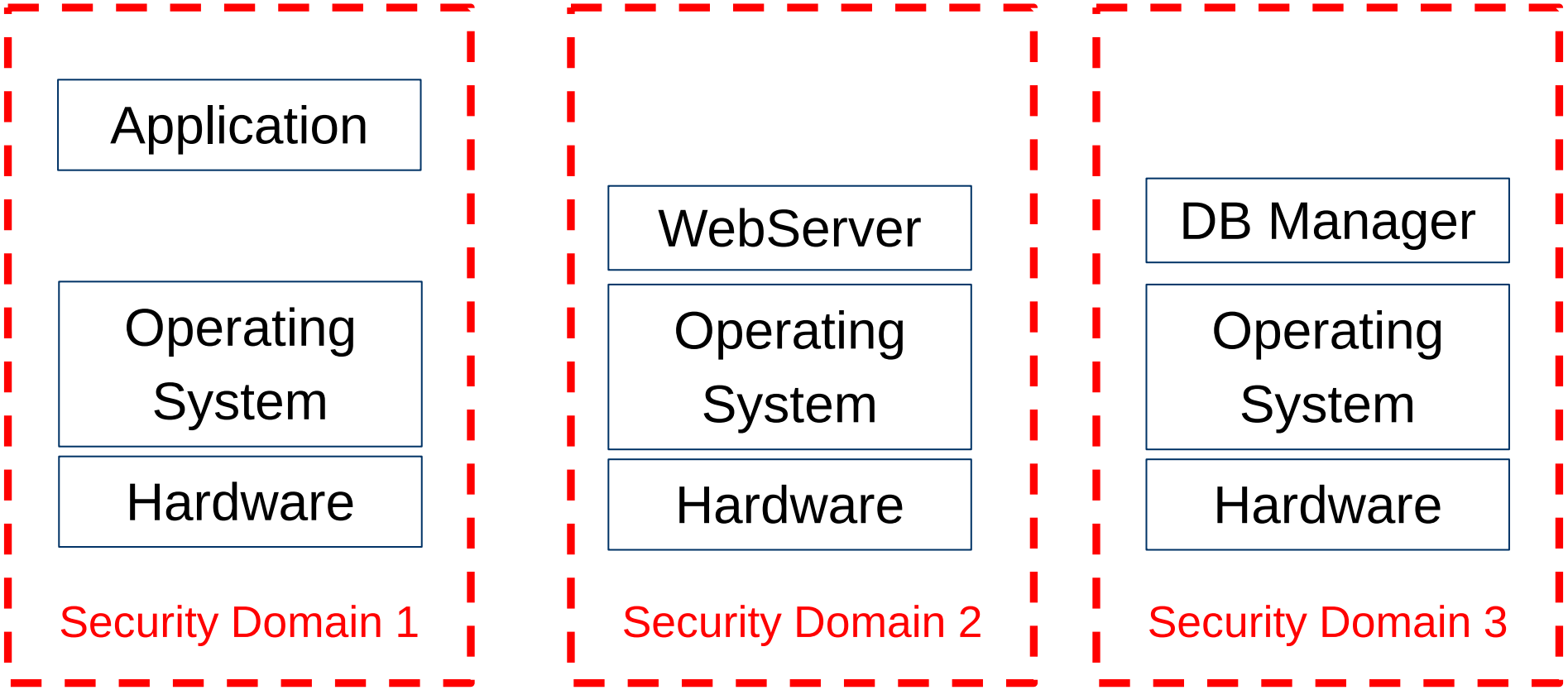
# Going Distributed!

- Interactions between layers can be implemented over a network
- In this case, different ***security domains*** are traversed
- Security Domain: HW + SW managed under
  - Same authority
  - A uniform set of security policies

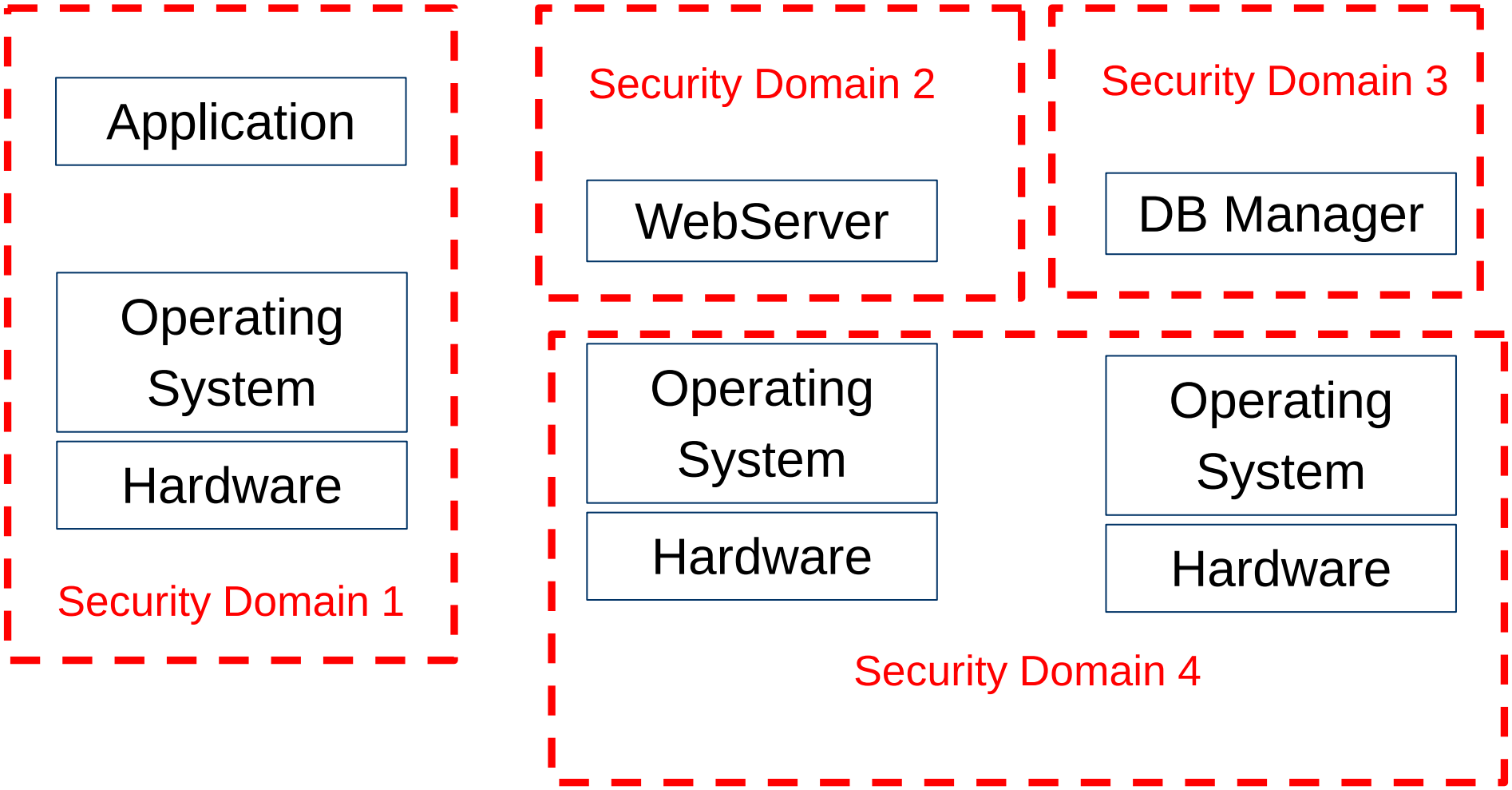
# Levels and Security Domains



# Levels and Security Domains



# Levels and Security Domains



# Dealing with Security Domains

- Each Security Domain enforces “localised” decisions
- It requires a certain level of “Trust” as a basis of extra-domain interactions
- Mapping subjects/groups/resources from different domains not always simple task
  - A different layer of abstraction is needed

# Coming up next week

- Monday: AC Models
- Tuesday: Smartphone Security
- Thursday: Guest lecture by Chris Pearce from Mozilla, NZ - http://pearce.org.nz

# Resources

- Security Engineering – Ross Anderson
  - Available from the web
- Chapter 3: http://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c03.pdf