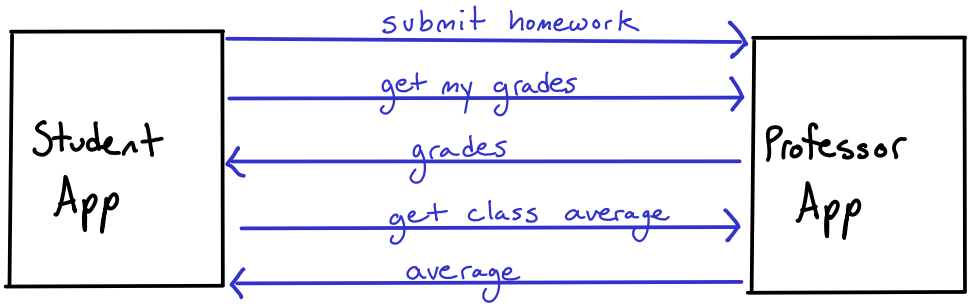
- Exam will move to earlier date
- All notes submitted so far are OK

Access Control

- ACM (Access Control Matrix)
  - capabilities
  - ACLs
- Bell-Lapudula / Biba / Lattice-Based ACs
- Role-Based Access Control (RBAC)

Homework Grading System



- Apps only communicate via messages
- OS tags each message with sender
- Only student can see own grade
- Can only submit homework once

ACM - Access Control Matrix

$$A_{d,o} = \{ r \mid d \text{ has } r \text{ access to } o \}$$

A	HW Queue	Student 1 Grade	Student 2 Grade	Avg
Professor	dequeue owner	read write	read write	read write
Student 1	enqueue	read		read
Student 2	enqueue		read	read

Owner $\in A_{d,o}$ the d can grant d' r on o.
Control $\in A_{d_1,d_2}$ then d_1 can rename r for $A_{d_1,o}$
copy bit => can delete your privileges

An access control system consists of
- access control matrix
- set of rights
- set of commands

command ($d_1, \ldots, d_n, r_1, \ldots, r_m, o_1, \ldots, o_\ell$)
if ($r_1' \in A_{d_1,o_1}$ and $r_2' \in A_{d_2,o_2}$ and ...)

op_1 :
op_2 :
⋮
} operations are adding and removing from ACM

grant (d, d_1 r_1 o)
if (owner $\in A_{d,o}$)
$A_{d,o}$ $\cup =$ $\{ r \}$

Question: Is there a sequence of commands that can result in $r \in A_{d,o}$?
Theorem: Harrison - Ruzzo - Ullman
This is undecidable

Implementing ACMs

- Capability Lists
  - store by row
  - with each domain, store a list of its access rights
  - easy to look up domain capabilities
  - file handles

- Access Control Lists
  - store by column
  - list everyone that can access an object with that object
  - easy to see who can access something
  - file permissions
  - Windows NTFS, AndrewFS, POSJX Linux
  - Positive/Negative order?
    - rules should be unordered

Bell-Lapadula (Multi-Level Security)

If o is labeled with S, the d can only access o if d is labeled with $S' \geq S$

Secrecy:
- Top Secret
- Secret
- Confidential
- Public

Compartments:
- JFK
- Area 51

If o is labeled with a $C = \{C_0, \ldots, C_n\}$ then a domain must have access to all compartments in C

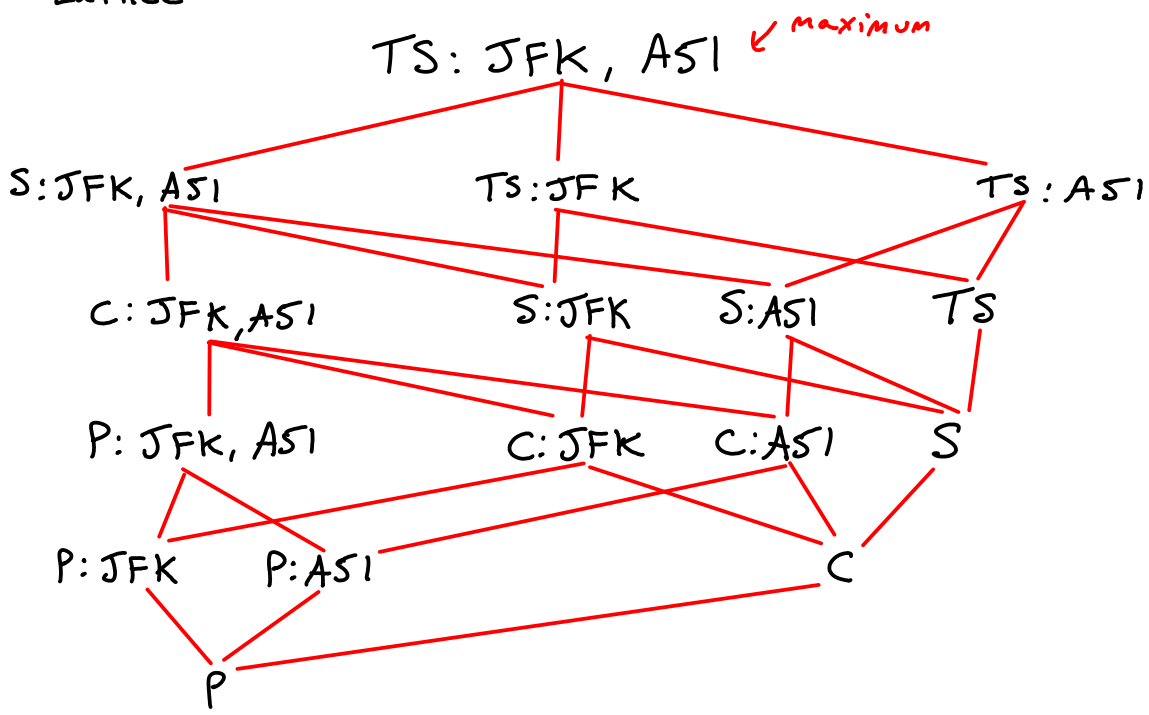
A "label" is a pair $\ell = (S, C)$ [C is a set of compartments]

we define $(S_1, C_1) \leq (S_2, C_2)$

iff $S_1 \leq S_2$

$C_1 \subseteq C_2$

Lattice



$LUB(l_1, l_2) = l$ s.t.

① $l_1 \leq l$

② $l_2 \leq l$

③ $\forall l'$ s.t. $l_1 \leq l'$ and $l_2 \leq l'$ and $l \leq l'$

What about writes?

If d has label l and o has label l',

d can write o if $l \leq l'$

and read o if $l' \leq l$