Setting: shared lab with printer
- Imagine a scenario similar to CSE Labs
  - Computer labs used by many people, with administrators
  - Target for modeling: software system used to manage printing
    - Similar to real system, but use your imagination for unknown details

Example functionality
- Queue of jobs waiting to print
  - Can cancel own jobs, admins can cancel any
- Automatically converting documents to format needed by printer
- Quota of how much you can print

STRIDE threat taxonomy
- Spoofing (vs authentication)
- Tampering (vs integrity)
- Repudiation (vs. non-repudiation)
- Information disclosure (vs. confidentiality)
- Denial of service (vs. availability)
- Elevation of privilege (vs. authorization)

STRIDE examples
- S: make your jobs look like a different student's
- T: insert mistakes in another student's homework
- R: claim you don't know why your quota is used up
- I: read another student's homework
- D: break printing before an assignment deadline
- E: student performs administrator actions

Reminder: what is shellcode
- Machine code that does the attacker's desired behavior
- Just a few instructions, not a complete program
- Usually represented as sequence of bytes in hex
Reminder: basic attack sequence

- Make the program do an unsafe memory operation
- Use control to manipulate control-flow choice
  - E.g.: return address, function pointer
- Make the target of control be shellcode

Overflow example hands-on

- Steps of overflow-from-file example

Side-effects example

- A second example with a new wrinkle