# Security

## Models:

- a security model (what you're defending)
- a threat model (who's attacking & how)

## What do you mean by **"security" (CIA)**?

- C: confidentiality (privacy)
- I: integrity (avoid tampering)
- A: availability

### For example:

- confidentiality: we don't want USC student to have our grade.
- integrity: we don't want USC student to modify our grade.
- availiability: USC student just cannot be authorized to get in the system.

### Security Model:

What we need to identify in any security mode:

- assets (properties, what valueable things we want to protect)
- vulnerabilities (weakness, identify what is the weak part of your system)
- threats (plausible ways that attacker may use to attack your vulnerabilities and get your assets)