Secure Software Systems

CYBR 200 | Fall 2018 | University of the Pacific | Jeff Shafer

Policy and Aspects

Content adapted from CS 5430 (System Security), Cornell University, Dr. Michael Clarkson

Schedule

This Week

- Tue August 28
  - Intro lecture
- Thur August 30
  - Project 1 Discussion
  - Security Policy & Aspects

Next Week

- Tue September 4
  - Threats, Harm, and Vulnerabilities
  - Goals and Requirements
- Thur September 6
  - Assurance

Project 1 Discussion

Security Policy and Aspects


SECURITY

What is COMPUTER Security?

- A computer system is *secure* when it
  1. Does what it should
  2. And nothing more
- A security *policy* stipulates what should and should not be done
- A good policy will cover the three *aspects* of security

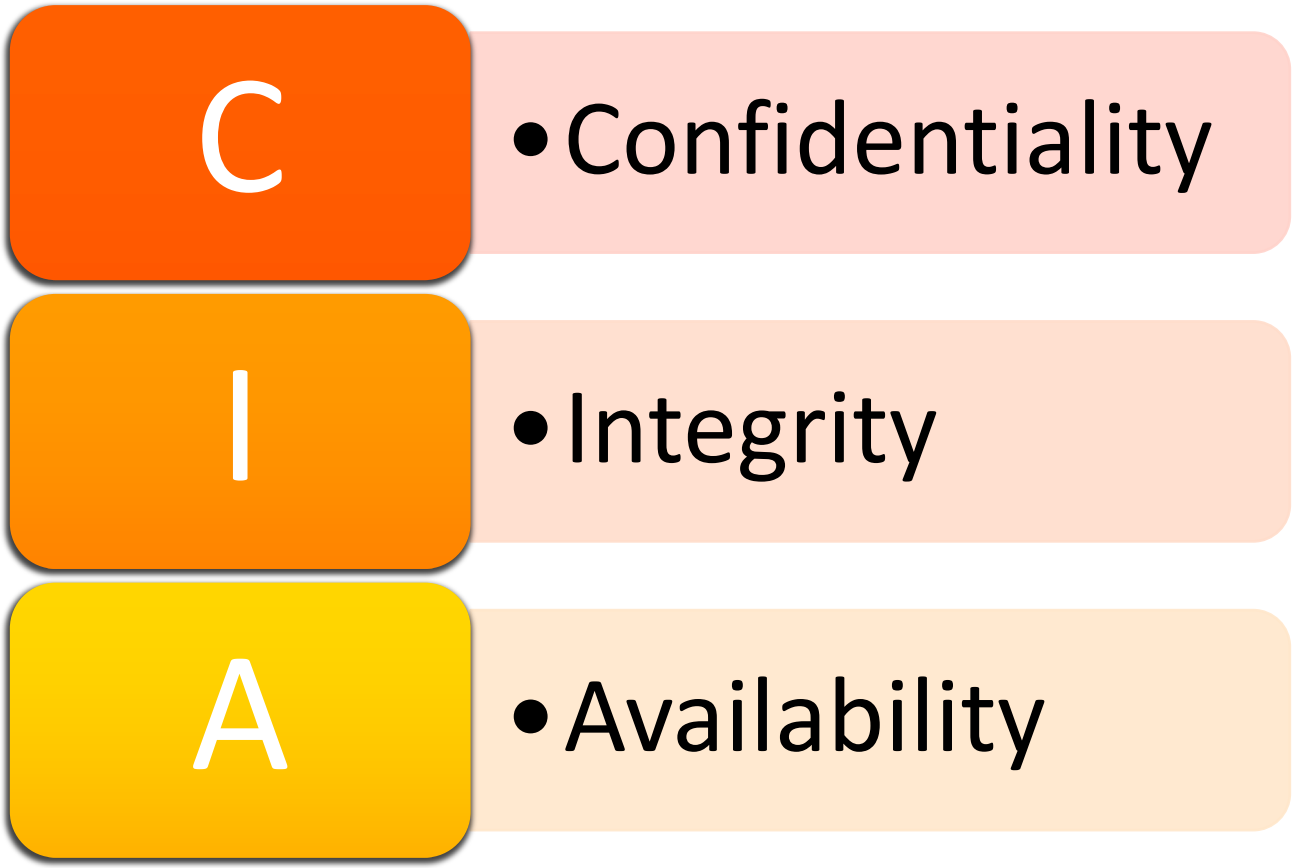
Aspects of Security

C

I

A

Aspects of Security



Aspects of Security

- **Confidentiality**
  - Protection of assets from unauthorized *disclosure*
- **Integrity**
  - Protection of assets from unauthorized *modification*
- **Availability**
  - Protection of assets from *loss of use*

Confidentiality

- **Confidentiality**
  - Protection of *assets* from unauthorized *disclosure*

Asset? Information, resource, ….

Disclosure to whom? Person, program, system, …

Synonym for person/program/system
-> ***Principal*** *(entity who can take actions)*

Confidentiality Policy Examples

- Prevent file contents from being read
  - *Access Control*
- Keep information secret
  - *Information Flow*

Integrity

- **Integrity**
  - Protection of assets from unauthorized modification

What changes are allowed to the system?

What inputs and outputs are allowed?

Integrity Policy Examples

- Output is correct according to mathematical specification
- No exceptions are thrown
- Only certain principals may write to file *(access control)*
- Data is not corrupted or tainted by new programs *(information flow)*

Availability

- **Availability**
  - Protection of assets from loss of use

Example: Denial of Service attack compromises availability

Availability Policy Examples

- Operating system must accept inputs at periodic intervals
- Program must output result of computation by specified time
- Requests must be processed in fair manner (in order of arrival, in order of priority, …)
- All requests at specified priority level must be processed

Q&A

- Attack: Malory copies Alice's homework

- **What is an example *policy* that this attack violates?**

- **What *aspect* of security does that policy cover?**