University of BRISTOL

Systems & Software Security

COMSM0050

2020/2021

bristol.ac.uk

University of BRISTOL

Introduction to OS security

bristol.ac.uk

Security Goals

- Will be discussed again in week 6
- **Confidentiality**: prevention of unauthorized or unintended information disclosure
- **Integrity**: ensuring that information on a system is no tampered with (addition, deletion, modified etc.)

Security Goals

- Will be discussed again in week 6
- **Confidentiality**: prevention of unauthorized or unintended information disclosure
- **Integrity**: ensuring that information on a system is no tampered with (addition, deletion, modified etc.)

Confidentiality and Integrity are interdependent:

- If I can tamper the code enforcing confidentiality, it is moot
- If no confidentiality I can steal credential, therefore gaining root privileges

Principals, subjects, objects

- Objects: (or resources) are what needs to be protected (e.g. files, devices etc.)
- Subjects: are the active agents that perform operations on objects (e.g. processes are threads)
- Principals: this is an abstraction for the “human”

DAC in Linux

- First approach protecting file access:
  - Present in virtually all OS (Discretionary Access Control)
  - UNIX model you are probably all familiar with by now:
    - e.g. drwxrwxr-x 2 accounting accounting 6 Jan 8 15:13
    - read
    - write
    - execute
- Let owner decide of access policies
- Let the applications handle more complex policies

Access Matrix

	/tmp/	/usr/lib
Alice	rwx	rwx
Bob	rwx	r-x

Access Matrix

	/tmp/	/usr/lib
Alice	rwx	rwx
Bob	rwx	r-x

Ok in principles, but how do you deal with hundred users and millions of objects?

How do you check this?

As pointed out earlier terminal and browser have the same privilege, is that really ok?

Access Matrix

	/tmp/	/usr/lib
Alice	rwx	rwx
Bob	rwx	r-x

Ok in principles, but how do you deal with hundred users and millions of objects?

How do you check this?

As pointed out earlier terminal and browser have the same privilege, is that really ok?

Would that provide sufficient security?

DAC in Linux

- Not really!
- Program access data not users
  - I trust Alice, but do I trust every program she runs?
- Confidentiality issues
  - Bob may have access to data and make it public by mistake
  - I want to flag data as confidential and not worry about getting all file permission right
- Integrity issues
  - Charles may download and execute random e-mail attachment
  - It should not compromise systems libraries

Principle of least privilege

- Saltzer and Schroeder 1975 (check course website)
- Protection domain as small as possible
  - No more access than necessary

Principle of least privilege

- Saltzer and Schroeder 1975 (check course website)
- Protection domain as small as possible
  - No more access than necessary

	/tmp/	/usr/lib
Alice	rwx	rwx
Bob	rwx	r-x