ACCESS CONTROL
Lecture 3b

COMPSCI 702
Security for Smart-Devices

Muhammad **Rizwan** Asghar

March 4, 2021

THE UNIVERSITY OF AUCKLAND
NEW ZEALAND

SECURITY OBJECTIVES

- Confidentiality
  - Protection of the data
- Integrity
  - Ensuring the data is not altered by unauthorised parties
- Availability
  - Ensuring timely access to the data
- Authentication
  - Identifying whether the communicating entity is the one it claims to be
- Authorisation
  - Regulating access to the data

SECURITY MECHANIMS

- Encryption
  - Symmetric key cryptography (e.g., DES and AES)
  - Asymmetric or public key cryptography (e.g., RSA)
- Integrity
  - Digital signature (e.g., RSA)
- Authentication techniques
  - Username/password and PIN
- Access control
  - **Focus of this lecture!**

ACCESS CONTROL REQUIREMENTS

- Reliable inputs
  - Authenticated entities
    - E.g., using UPI and password
  - Genuine information
    - E.g., a student or staff member
- Least privilege
  - Principle of least privileges deals with granting the minimum set of access rights to do a job
  - For instance, accessing a single course vs all courses
- Administrative duties
  - Only a special entity should be able to manage access rights
  - For instance, granting, revoking, or update access rights

ACCESS CONTROL ELEMENTS

- Subject
  - An entity that can access objects
  - It could be a user or process representing a user/application
- Object
  - An entity that needs to be protected
  - E.g., files, directories, or other resources
- Access right
  - An access right $r \in R$ describes how a subject $s \in S$ can access an object $o \in O$
  - E.g., read, write, execute, create, delete, and search

ACCESS CONTROL SYSTEM

- Access control function f(s, o, r)
  - It looks up access right r for the combination (s, o)
  - On a successful match, it grants access, otherwise not
- Security administrator
  - An entity that manages access rights
- Auditor
  - An entity that inspects the whole authorisation system

A TYPICAL ACCESS CONTROL SYSTEM

Auditor

User

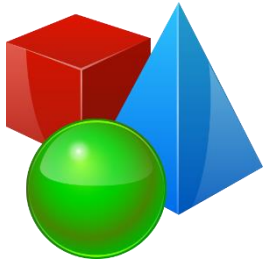
Access control function

Resources

Access Rights

Security Administrator

ACCESS CONTROL MODELS



- Discretionary Access Control (DAC)
- Mandatory Access Control (MAC)
- Role-Based Access Control (RBAC)
- *Usage Control (UCON)*
- *Policy-Based Access Control (PBAC)*

DISCRETIONARY ACCESS CONTROL

- Users can protect what they own
- The owner may grant access to subjects
- Access is granted based on identity of the requester
- These mechanisms are adequate for honest users
- Vulnerable to Trojan horses
- DAC is used in operating systems and DBMS
  - E.g., Linux file permissions: rwxr-x--x

TO BE CONTINUED

- See the next lecture

Questions?

Thanks for your attention!