Lecture 15
Access Control

ECE 422: Reliable and Secure Systems Design

Instructor: An Ran Chen
Term: 2024 Winter

Schedule for today

- Key concepts from last class
- Access Control
  - Threats, vulnerabilities and attacks
  - Types of control
  - Access control lists (ACLs)
- Models of access control
  - Discretionary access control (DAC)
  - Role-based access control (RBAC)
  - Mandatory access control (MAC)
  - Attribute-based access control (ABAC)

Confidentiality

Confidentiality

- Only the authorized user can access particular resources

Methods to achieve confidentiality:

- Encryption: encoding/decoding of the plaintext
  - E.g., Symmetric/asymmetric encryption
- Access controls: restricted access
  - E.g., Our library website
- Authentication: credentials check
  - E.g., Mobile authentication for faculty and staff

UoA's Information Services & Technology

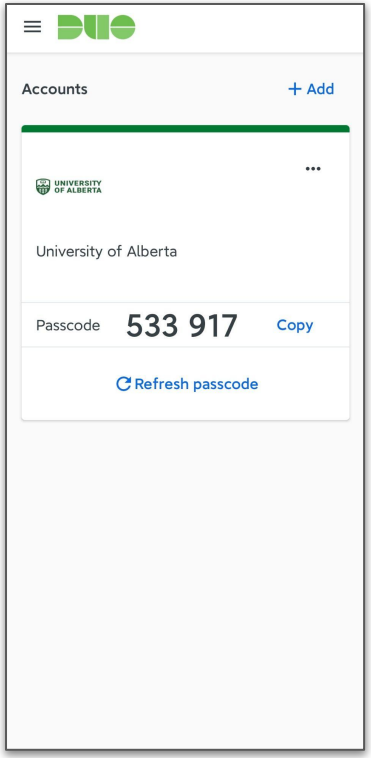
Authentication

- Password-based authentication
  - Username + password
- Magic links
  - Links through email or mobile device
- SMS-based authentication
  - Text messages
- Authenticator apps
  - Push notifications, or one-time password (OTP)
- Biometric authentication
  - Biometric data (e.g., fingerprint and face recognition)
- Multi-factor authentication (MFA)
  - Two or more independent authentication factors

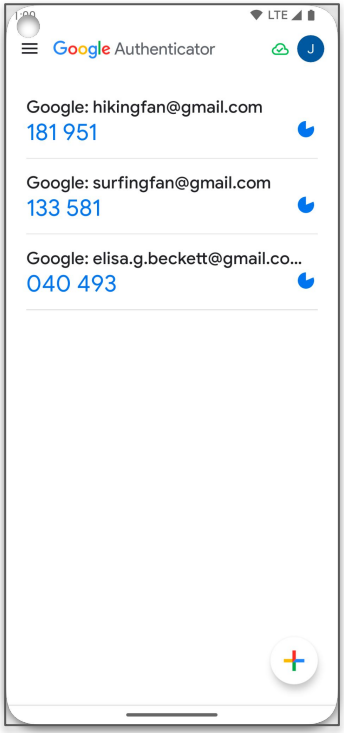
TOTP

Time-based one-time password (TOTP) uses a public algorithm to generate the one-time password.

- Generate unique passcodes based on the current interval of time
- Time interval is generally 30 seconds
- No delivery of the one-time passcode is required
    - Generation algorithm shared ahead of time
- One-time passcode generated through a shared secret key and the current time



HOTP



Google Authenticator

HMAC-based one-time passwords (HOTP) also uses a public algorithm to generate the one-time password.

- Generate unique passcodes based on the current counter
- Counter is a variable stored on the server and the application, increases each time a passcode is generated.
- No delivery of the one-time passcode is required
  - Generation algorithm shared ahead of time
- HMAC takes as input: (counter + secret key)

Multi-factor authentication (MFA)

Multi-factor authentication (MFA) requires two or more factors to verify user's identify.

- Knowledge factor: Something only the user knows
  - Password, PIN code
- Possession factor: Something only the user has
  - Access card, key, authorized device
- Biological factor: Something only the user is
  - Physical trait: fingerprint, retinal pattern
  - Behavioral process: voice recognition, keystroke dynamics

Schedule for today

- Key concepts from last class
- Access Control
  - Threats, vulnerabilities and attacks
  - Types of control
  - Access control lists (ACLs)
- Models of access control
  - Discretionary access control (DAC)
  - Role-based access control (RBAC)
  - Mandatory access control (MAC)
  - Attribute-based access control (ABAC)

Confidentiality

Confidentiality

- Only the authorized user can access particular resources

Methods to achieve confidentiality:

- Encryption: encoding/decoding of the plaintext
  - E.g., Symmetric/asymmetric encryption
- Access controls: restricted access
  - E.g., Our library website
- Authentication: credentials check
  - E.g., Mobile authentication for faculty and staff

UoA's Information Services & Technology

Access control

Access control determines who is allowed to access certain data, apps, and resources (i.e., protects digital spaces).

Goal of access control:

- Protect confidential information
  - Customer data
  - Intellectual property
- Prevent security risks (through authentication and authorization)
  - Data exfiltration
  - Network security threats (e.g., phishing, ransomware)
- Minimize the impacts
  - Policies on access management

Access control

Assets may vary from:

- Hardware: computer systems, devices
- Software: operating system, utilities, applications
- Data: final report, class projects, emails

While hardware and software may be expensive, unique data cannot be recovered if it is lost.

Access control and authentication

Access control identifies a user based on their credentials and then, for example, authorizes the appropriate level of access once they are authenticated.

- Passwords, magic link, SMS code are all examples of credentials used to identify and authenticate a user.
- Multi-factor authentication contains an extra layer of security by having more than just one authentication factor.

Once a user's identity has been authenticated, access control policies grant specific permissions and enable the user to proceed with the resource.

Schedule for today

- Key concepts from last class
- Access Control
  - Threats, vulnerabilities and attacks
  - Types of control
  - Access control lists (ACLs)
- Models of access control
  - Discretionary access control (DAC)
  - Role-based access control (RBAC)
  - Mandatory access control (MAC)
  - Attribute-based access control (ABAC)

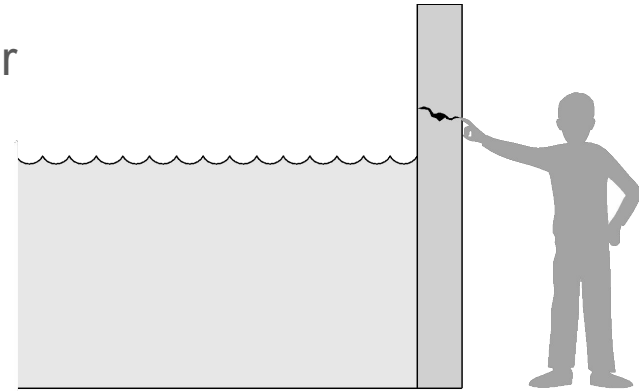
Threats, vulnerabilities and attacks

Access control is what eliminates/reduces/mitigates a vulnerability.

- Threat: an event that may cause harm to protected assets.
- Vulnerability: a weakness which could be exploited to cause harm to protected assets.
- Attack: an action that exploit a vulnerability in an attempt to cause harm.

Example: attempt to repair a fixture in a water reservoir

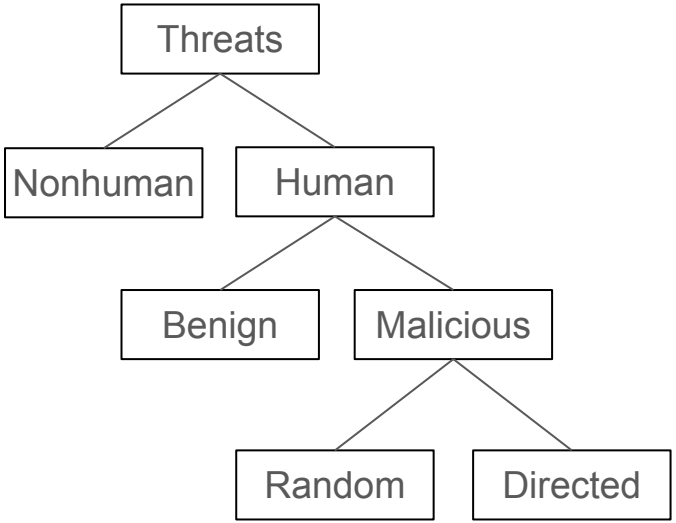
- Threat: water overflowing
- Vulnerability: crack in the reservoir
- Attack: add more water into the reservoir
- Access control: someone's finger (... for now)



Threats

Threats can be caused both by human and other sources.

- Nonhuman threats
  - E.g., fires, loss of electrical power
- Human threats
  - Benign (non malicious) intent
    - E.g., typo, software bugs
  - Malicious intent
    - Random (any computer/organization/individual)
      - E.g., malicious code on github
    - Directed (specific)
      - E.g., impersonation



Types of control

There are three types of access controls:

- Physical control
- Procedural control
- Technical control

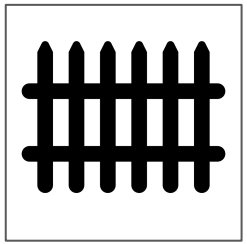
Physical control

Physical controls are implemented by physical infrastructure.

- Prevent and detect unauthorized access to physical spaces, systems or assets

Example of physical infrastructures:

- Fences
- Access cards
- CCTV



Procedural control

Procedural controls are implemented by people and practices.

- Security awareness training can also falls under procedural controls

Example of procedural control:

- Guards
- Security awareness program

October is UoA's [cyber security awareness month]

Technical control

Technical controls are implemented using systems.

- Both hardware and software mechanisms are used to protect assets

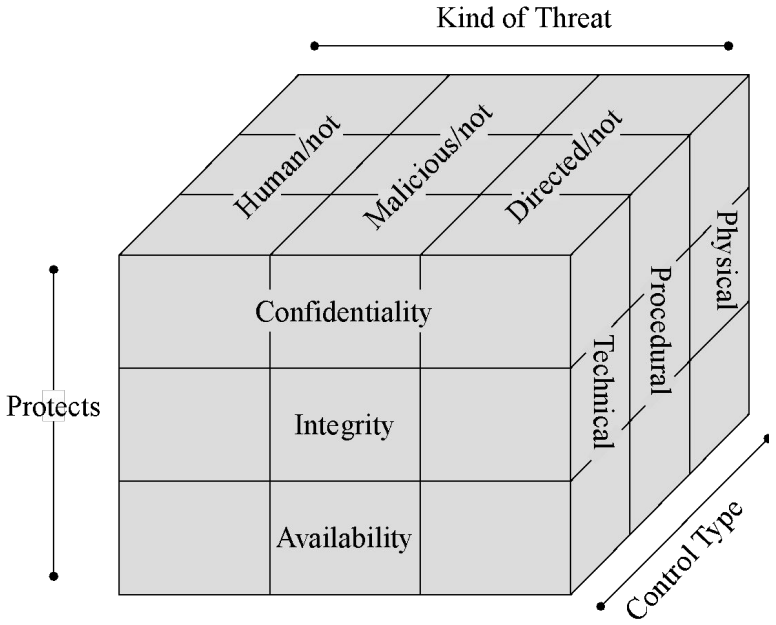
Example of technical control:

- Authentication
- Firewall
- Antivirus software

Two common forms of technical controls:

- Access control lists (ACLs)
- Encryption

Threats, vulnerabilities, and control types



- CIA are the basic security principles.
- Vulnerabilities are weaknesses in a system that affect the CIA triad.
- Threats exploit those weaknesses in the system.
- Controls protect those weaknesses from exploitation.

Schedule for today

- Key concepts from last class
- Access Control
  - Threats, vulnerabilities and attacks
  - Types of control
  - Access control lists (ACLs)
- Models of access control
  - Discretionary access control (DAC)
  - Role-based access control (RBAC)
  - Mandatory access control (MAC)
  - Attribute-based access control (ABAC)

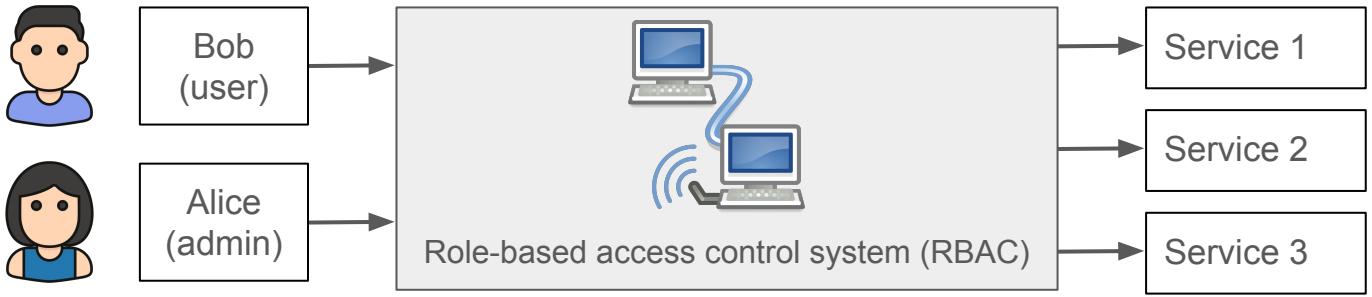
Access control list (ACL)

An access control list is a set of instructions that either allow access to a computer environment or deny it.

- Restrict access to unauthorized users
- Control traffic by limiting the number of users

It is analogous to a guest list to a wedding.

- Only those on the lists are authorized to entries



Examples of application: filesystem ACLs

Filesystem ACLs:

- Inside an operating system (e.g., Unix-based systems)
- Inform the operating system of the access privileges that a user has to a system object (e.g., what resource, what access rights)

Example: Linux access control lists using the *getfacl* command

```
[root]# getfacl /random_folder
user::rwx
group::rwx
other::---
```

Linux filesystem:
Access class: user, group, other
Types of access: read, write, execute

```
[root]# setfacl -d -m random_user:rwx
/random_folder

[root]# getfacl /random_folder
user::rwx
group::rwx
other::---
default:user::rwx
default:user:random_user:rwx
```

Examples of application: network ACLs

Network ACLs:

- For a web server, DNS server or VPN systems
- Allow to filter requests for a single or group of IP addresses
- Protect against server attack

Example: Web access control

- Block web requests that do not meet specific conditions
- Conditions can be criteria or metrics
    - Criteria: IP address origin, country of origin, size of the request
    - Metrics: number of requests in any 10-minute period

Schedule for today

- Key concepts from last class
- Access Control
  - Threats, vulnerabilities and attacks
  - Types of control
  - Access control lists (ACLs)
- Models of access control
  - Discretionary access control (DAC)
  - Role-based access control (RBAC)
  - Mandatory access control (MAC)
  - Attribute-based access control (ABAC)

Access control models

Users receive access based on access control models.

- Different systems have different access control requirements.

There are four models of access controls:

- Discretionary access control (DAC)
- Role-based access control (RBAC)
- Mandatory access control (MAC)
- Attribute-based access control (ABAC)

Discretionary access control (DAC)

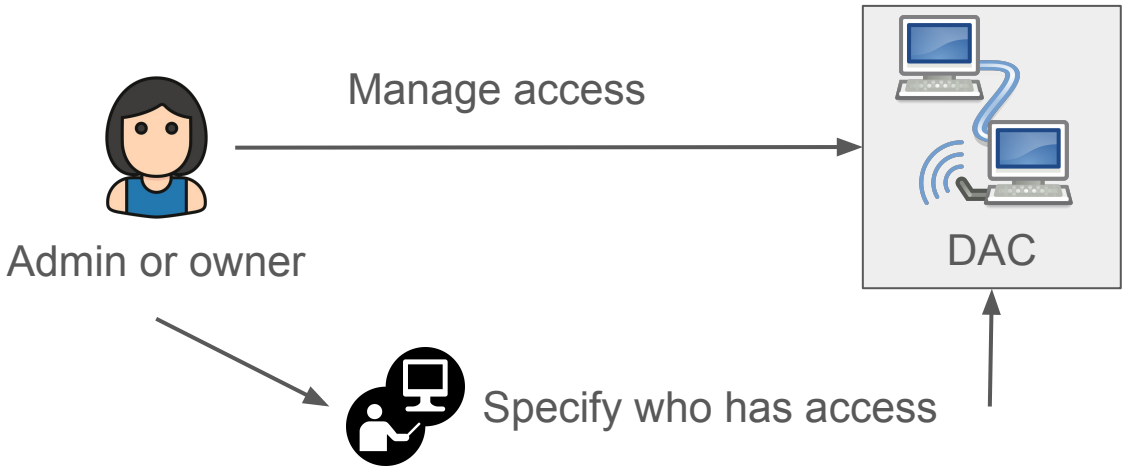
In a discretionary access control (DAC) model, each resource has an owner and owners grant access to users or user groups at their own discretion.

- Implemented using access control lists
- Case-by-case control over resources

Discretionary access control (DAC)

Administrator or owner of the resource controls the access:

- Defines a profile for each resource (i.e., resource profile)
- Updates the access control list for the profile



Benefits of DAC

- Flexible (decentralized control)
  - Owners may grant/remove access to resources at any time
- Simple (access control via ACLs)
  - An ACL defines the user privilege
- With fine-granularity
  - Access based on individual needs

However, with decentralization and simplicity:

- Difficult to tell how the resources are accessed and interconnected
- Problems: possible to have over-privileged users or conflicting permissions

Role-based access control (RBAC)

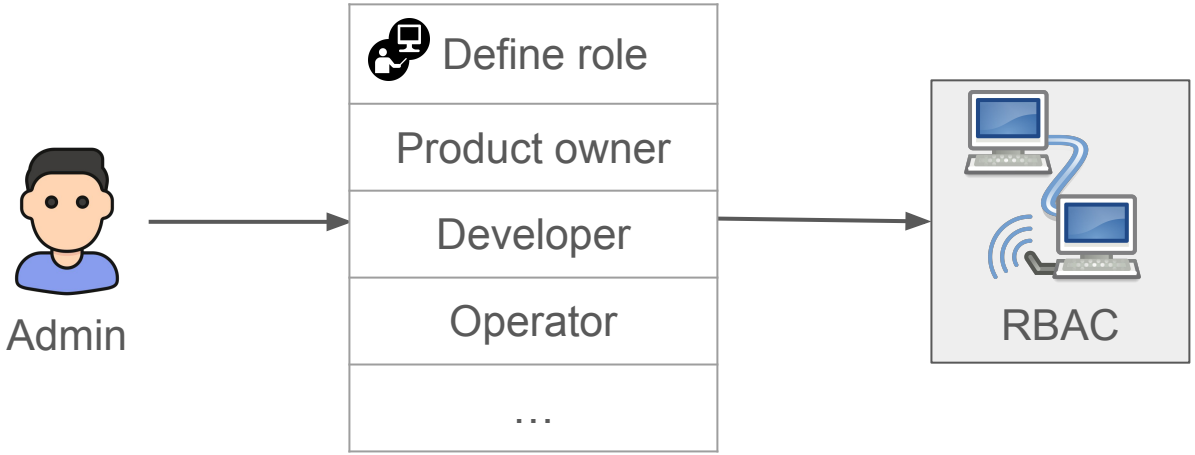
In a role-based access control (RBAC) model, the system restricts access to users based on their role(s).

- Normally within an organization
- Users are given minimum access to fulfill their job requirements

Role-based access control (RBAC)

Administrator controls the access based on the role of the user:

- Defines a role for each user
- Users can only access the resource when their role entitles the access



Benefits of RBAC

- Secure
  - Principle of least privilege
- Easy to use
  - Mapping users to data, minimal overhead in authorization management
- Compliance ready
  - Easy to handle the security and confidentiality standards

However, it requires collaboration between departments:

- Difficult to assign roles, organization is constantly growing
- Problems: new roles may contradict to existing policies, or privilege creep (unnecessary accumulation of privileges that happens during role change)

Mandatory access control (MAC)

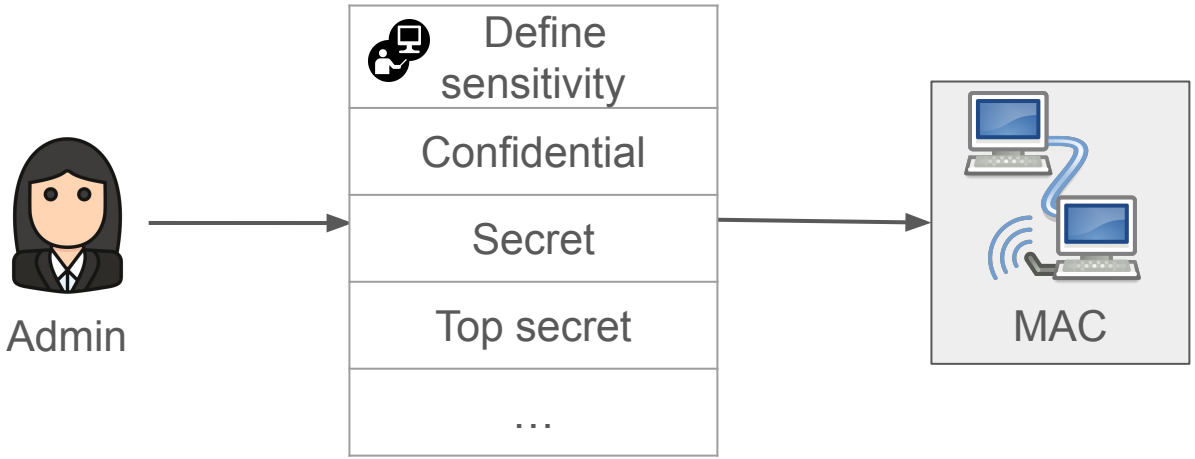
In mandatory access control (MAC), the system restricts access based on the sensitivity (or security clearance) levels of the resource.

- Commonly used in government and military contexts
- Label each resources with sensitivity levels (e.g., confidential, secret or top secret)
- Each user has a sensitivity level access
  - Defined by the administrator
  - Only the administrator can change and see the sensitivity level access

Mandatory access control (MAC)

Administrator controls the access based on the sensitivity of each resource:

- Define the sensitivity of each resource
- Users can only access the resource when their security labels entitles the access



Benefits of MAC

- Secure (most secure among the models)
  - Security levels cannot be changed
- Control over one authority
  - Centralized control
- Privacy
  - Only the administrator can see the access control (i.e., list of users and their privileges)

However, the access control at resource-level:

- Difficult to maintain the access control when data are being added and deleted constantly
- Problems: less flexible, thus the system requires regular updates

Attribute-based access control (ABAC)

In attribute-based access control (ABAC), the system restricts access based on a combination of attributes and environmental conditions.

- Attributes such as role, sensitivity level, or resource properties (e.g., ownership, types of resource)
- Environmental conditions such as time or location

Administrator or owner of the resource controls the access based on the attributes and environmental conditions:

- Assign role and sensitivity attributes to each resource
- Users can only access the resource when both their role and sensitivity label entitle them to access

Benefits of ABAC

- With fine-granularity (most precise among the models)
  - Create precise attributes without the need of additional roles
- Flexible
  - When there is a resource or user change, re-assign the attributes
- Secure
  - Security without requiring any collaboration

However, it requires time, effort and resources to implement:

- Difficult to define good attributes
- Problems: time-consuming, something that we implement over time

Access control models

Q1) What access control model is where an owner can assign permissions to users for resources they control?

Answer: ?

Q2) What access control model is where a user's clearance must exceed a resource's sensitivity label?

Answer: ?

Q3) For access control, what does authentication mean?

Answer: ?

Access control models

Q1) What access control model is where an owner can assign permissions to users for resources they control?

Answer: Discretionary access control (DAC)

Q2) What access control model is where a user's security clearance must exceed a resource's sensitivity label?

Answer: Mandatory access control (MAC)

Q3) For access control, what does authentication mean?

Answer: The credential of the user has been verified. Specific permissions are granted based on this credential.