

Data Security and Privacy

Chapter 5: Access Control and User Authentication

Fall 2020-2021

Access Control

- Access control:
 - method by which systems determine whether and how to admit a user into a trusted area of the organization
- Mandatory access controls (MACs):
 - use data classification schemes
- Discretionary access controls (DACs):
 - allow users to control and possibly provide access to information/resources at their disposal
- Nondiscretionary controls(RBAC):
 - strictly enforced version of MACs that are managed by a central authority

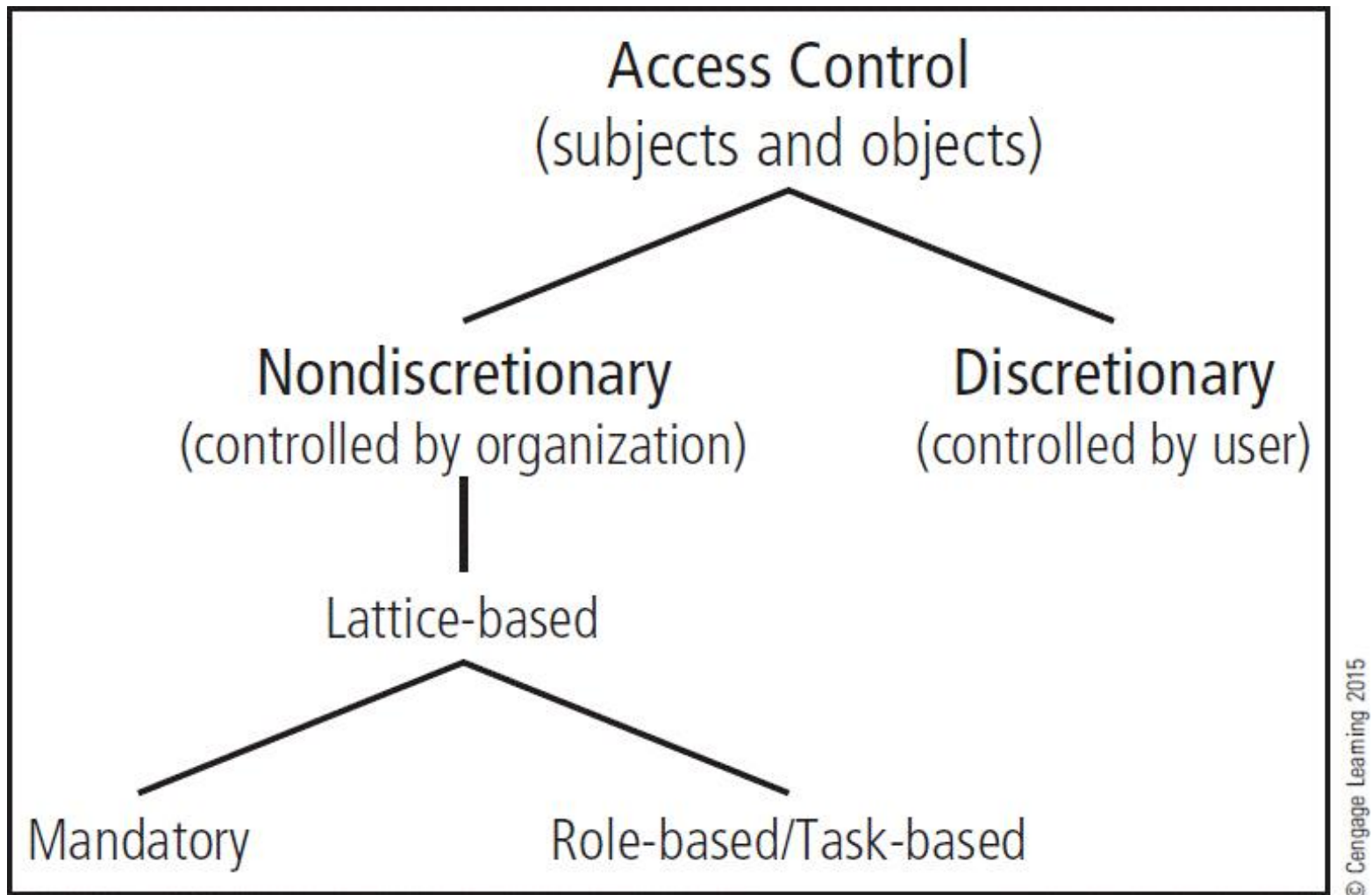


Figure 6-1 Access control approaches

Identification

- Identification:
 - mechanism whereby **unverified entities** seeking access to a resource **provide a label** by which they are **known** to the system
- Identifiers can be **composite** identifiers, **concatenating** elements—department codes, random numbers, or special characters—to make them unique.
- Some organizations generate **random numbers**.

Authentication

- Authentication:
 - the process of **validating** a supplicant's purported identity
- Authentication factors(Something a supplicant knows)
 - Password:
 - a private word or a combination of characters that only the user should know
 - Passphrase:
 - a series of characters, typically longer than a password

Authentication (cont'd)

- Authentication factors(Something a supplicant has)
 - Dumb card:
 - ID or ATM card with magnetic stripe
 - Smart card:
 - contains a computer chip that can verify and validate information
 - Synchronous tokens
 - Asynchronous tokens
- Something a supplicant is
 - Relies upon individual characteristics
 - Strong authentication

Authorization

- Authorization:
 - the matching of an authenticated entity to a list of information assets and corresponding access levels
- Authorization can be handled in one of three ways:
 - Authorization for each authenticated user
 - Authorization for members of a group
 - Authorization across multiple systems
- Authorization tickets

Accountability

- Accountability (auditability):
 - ensures that all actions on a system—authorized or unauthorized—can be attributed to an authenticated identity
- Most often accomplished by means of **system logs** and database journals, and the auditing of these records
- Systems logs record specific information.
- Logs have many uses.

Biometrics

- Approach based on the use of measurable human characteristics/traits to authenticate identity
- Only fingerprints, retina of eye, and iris of eye are considered truly unique.
- Evaluated on false reject rate, false accept rate, and crossover error rate
- Highly reliable/effective biometric systems are often considered intrusive by users.

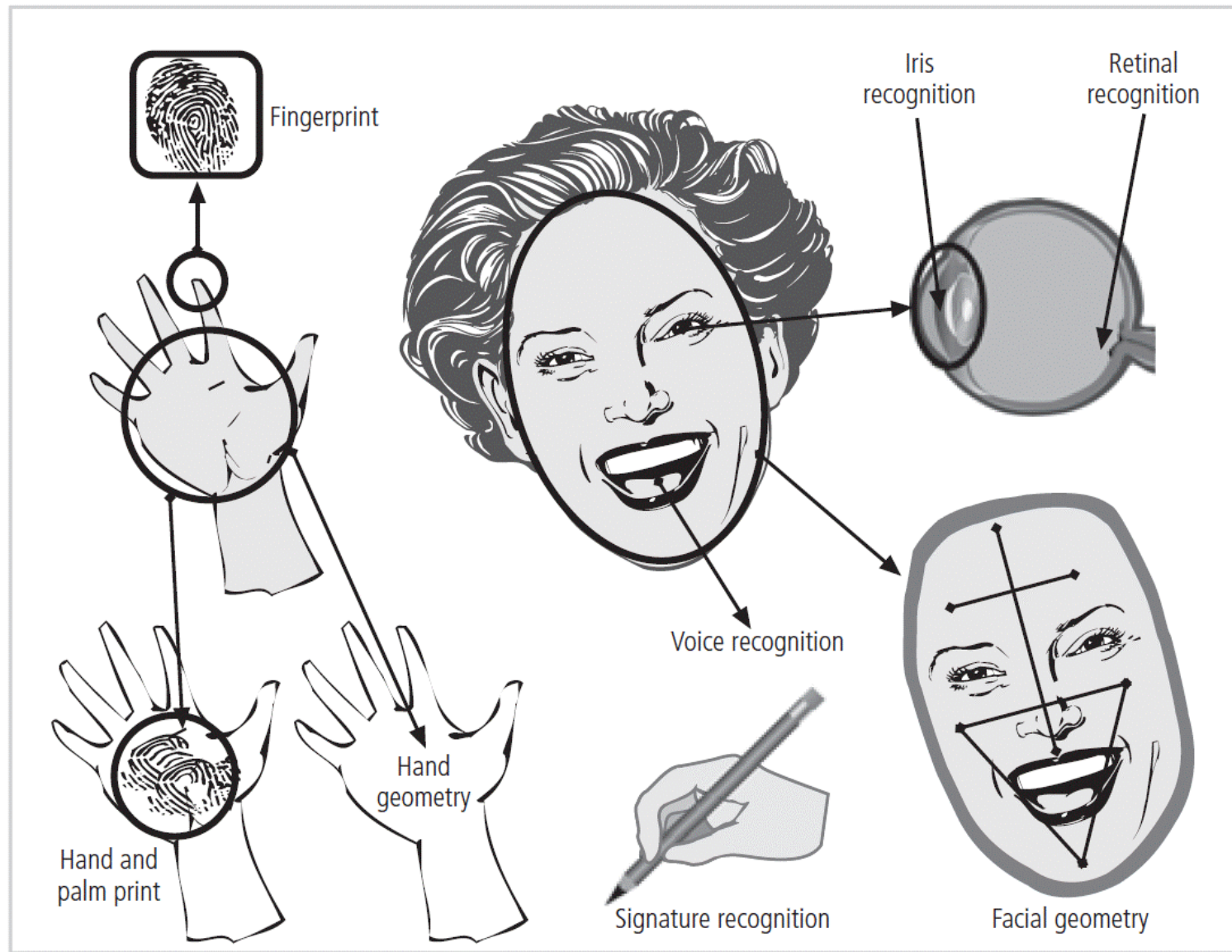


Figure 6-5 Biometric recognition characteristics

Biometrics	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	H	L	M	H	L	H	L
Facial Thermogram	H	H	L	H	M	H	H
Fingerprint	M	H	H	M	H	M	H
Hand Geometry	M	M	M	H	M	M	M
Hand Vein	M	M	M	M	M	M	H
Eye: Iris	H	H	H	M	H	L	H
Eye: Retina	H	H	M	L	H	L	H
DNA	H	H	H	L	H	L	L
Odor & Scent	H	H	H	L	L	M	L
Voice	M	L	L	M	L	H	L
Signature	L	L	L	H	L	H	L
Keystroke	L	L	L	M	L	M	M
Gait	M	L	L	H	L	H	M

Table 6-1 Ranking of Biometric Effectiveness and Acceptance

In the table, H = High, M = Medium, and L = Low.

From multiple sources.³

Access Control Implementations: *Controlling Accesses to Resources*

- Trusted computing base **TCB**(reference monitor) sees a request for a resource, how does it decide whether it should be granted?
 - **Example:**
 - ✓ Should John's process making a request to read a certain file be allowed to do so?
- **Authentication** establishes the source of a request (e.g., John's UID)
- **Authorization** or access control answers the question if a certain source of a request (User ID) is allowed to read the file

Controlling Accesses to Resources

- Access Control

- it is about who is allowed to access what.
- Two parts
 - **Part I:** Decide who should have access to certain resources (access control policy)
 - **Part II:** Enforcement – only accesses defined by the access control policy are granted.

Access Control Matrix (ACM)

- Abstracts the state relevant to access control.
- Rows of ACM correspond to users/subjects/groups
- Columns correspond to resources that need to be protected.
- ACM defines who can access what
 - ACM [U,O] define what access rights user U has for object O.

List each object in a column

List each user or subject in a row

A11	A12	A13	...	A1n
A21	A22	A23	...	A2n
A31	A32	A33	...	A3n
⋮	⋮	⋮	⋮	⋮
Am1	Am2	Am3	...	Amn

Data Confidentiality Quiz

Select the best answer to complete this sentence:

A file is created by a certain user who becomes its owner. The owner can choose to provide access to this file to other users. If file data confidentiality is desired, the owner should control who has...

☐

Read access to the file

☐

Write access to the file

☐

Both read and write access to the file

Determining Access Quiz

Select the best answer to the question:

The access control policy in a system can either define positive access for a certain subject or can specify that the subject be denied access. Consider a case where subject Alice belongs to a group All-Students. The system specifies that members of the group All-Students be able to read file foo but Alice is denied access for it. In such a case, what should the system do?

☐

Alice has access because she is member of All-Students so she must be allowed to read foo

☐

Negative access should take precedence and Alice's request must be denied

Implementing Access Control

- **Access control matrix is large**
- How do we represent it in the system?
 - Column for object O_i is $[(ui_1, rights_1), (ui_2, rights_2), \dots]$
 - Called **access control list or ACL**
 - Associated with each resource
 - For user u_i , a row in the matrix is $[(oi_1, rights_1), (oi_2, rights_2), \dots]$.
 - Called a **capability-list or C-list**.
 - Such a C-list stored for each user

Implementing Access Control

	X	Y	Z
A	rwX	r	
B		rw	rx
C		rw	rx

ACLs
 $X \rightarrow [(A, rwX)]$
 $Y \rightarrow [(A, r)(B, rw)(C, rw)]$
 $Z \rightarrow [(B, rx)(C, rx)]$

C-lists
 $A \rightarrow [(X, rwX)(Y, r)]$
 $B \rightarrow [(Y, rw)(Z, rx)]$
 $C \rightarrow [(Y, rw)(Z, rx)]$

- Where should an ACL be stored?

- In trusted part of the system
- Consists of access control entries, or, ACEs

- Where do C-lists go?

- User catalogue of capabilities defines what a certain user can access
- Can be stored in objects/resources themselves

ACE Quiz

Select the best answer:

Alice goes to a movie theater and purchases a ticket for her favorite movie. She is allowed access to the movie because she has the ticket. The ticket is more like a...

☐

Access control entry

☐

Capability

Discretionary Access Control Quiz

In discretionary access control, access to a resource is at the discretion of its owner. Let us assume **owner Alice of file foo** can choose to **grant read access** to foo to another user Bob but can prevent Bob from propagating this access right to others. **Does this ensure that a third user, Charlie, can never read the data from foo?**

☐

Yes, Charlie is not granted access so cannot read

☐

No, there may be another way for Charlie to access the data from foo

Mandatory Access Control (MAC)

- In this method, **access is determined by the system, not by the owner**
 - Systems that contain **highly sensitive data** such as government or **military based systems** use this access control type
- In this control, all users (subjects) and resources (Objects) should have a label assigned to them
 - It is a **security label** and specifies the **level of trust**
- To access the resource, the user **must have equal or higher sensitivity** level than the level of the required resource
 - **For example**, if the user requires accessing a secret file, he should have a secret clearance or a higher clearance to access the resource

Role-Based Access Control (RBAC)



- In enterprise setting, **access may be based on job function or role of a user**
 - Payroll manager, project member etc.
 - Access rights are associated with roles
- **Users authenticate themselves** to the system
- **Users then can activate one or more roles** for themselves

RBAC Benefits

- Policy **need not be updated when a certain person with a role leaves** the organization
- New employee **should be able to activate the desired role**
- **Revisiting least privilege**
 - User in one role has access to a subset of the files
 - Switch roles to gain access to other resources

Access Control Quiz

Alice has some sensitive data that she only wants to share with Bob and not Charlie. Alice will need to...

☐

Fully trust Bob to not share the data with Charlie for her to ensure that Charlie does not gain access to it.

☐

Does not need to trust Bob because access control will stop Charlie from accessing it.

RBAC Benefits Quiz

In systems that do not support RBAC but allow user groups to be defined, benefits of RBAC can be realized with groups.

☐

True

☐

False

TOKEN-BASED AUTHENTICATION

- Objects that a user possesses for the purpose of user authentication are called tokens.
- we examine two types of tokens that are widely used; these are cards that have the appearance and size of bank cards.

Memory Cards

- Can store but do not process data
- The most common is the magnetic stripe card
- Can include an internal electronic memory
- Can be used alone for physical access
 - Hotel room
 - ATM
- Provides significantly greater security when combined with a password or PIN
- Drawbacks of memory cards include:
 - Requires a special reader
 - Loss of token
 - User dissatisfaction

Smart Tokens

- **Physical characteristics:**

- Include an embedded microprocessor
- A smart token that looks like a bank card
- Can look like calculators, keys, small portable objects

- **User interface:**

- Manual interfaces include a keypad and display for human/token interaction

- **Electronic interface**

- A smart card or other token requires an electronic interface to communicate with a compatible reader/writer
- Contact and contactless interfaces

- **Authentication protocol:**

- Dynamic password generator
- Challenge-response

Smart Cards

- **Most important category of smart token**
 - Has the appearance of a credit card
 - Has an electronic interface
 - May use any of the smart token protocols
- **Contain:**
 - An entire microprocessor
 - Processor
 - Memory
 - I/O ports
- **Typically include three types of memory:**
 - Read-only memory (ROM)
 - Stores data that does not change during the card's life
 - Electrically erasable programmable ROM (EEPROM)
 - Holds application data and programs
 - Random access memory (RAM)
 - Holds temporary data generated when applications are executed

Types of Data Security Controls

1. Access Control

- offers authentication and permission. Systems of access control may include:
 - **Role-based access control** that allows users to access unique information based on their organizational position.
 - **Automatic access control**, allowing a network administrator to manage access to all information strictly.

Types of Data Security Controls

2. Encryption

- improves data security through the use of an algorithm (called an encryption key) to convert regular text into encrypted ciphertexts.
- Ciphared data is unreadable for an unauthorized user.
- Only users with an approved key can decrypt these details.
- Encryption is used to protect the data you hold and data between databases, mobile devices, and the cloud (so-called transit data).
- Your encryption keys must be handled carefully.

Types of Data Security Controls

3. Tokenization

- Tokenization eliminates random, non-algorithmically reversible sensitive data. Instead of being generated and decrypted by a mathematical algorithm, the relationship between data and token values are stored on a secure database survey table.
- The real data token is used as a substitute across multiple networks while the **original data** is saved on a different and **protected network**.

Types of Data Security Controls

4. Authentication

- to strengthen data safety and defend against data abuse, along with authorization.
- It tests whether the credentials of a user suit the databases.
- Standard authentication protocols nowadays require the combination of verification methods for an authorized user such as passwords, access tokens, swipe card or biometrics.
- Single sign-on technology allows authenticated user access to many devices, networks, and applications with one security token.
- Authorization technology defines the authorization of an authorized user to do or to access your site or server.