UNIVERSITY OF WESTMINSTER

AAA & Access Control

6COSC019W- Cyber Security

Dr Ayman El Hajjar

March 26, 2024

School of Computer Science and Engineering
University of Westminster

OUTLINE

1. Access Control
2. Logical Access Control
3. Access Control principles
4. Access Control Models
5. Authentication, Authorisation & Accountability (AAA)

Access Control

Protecting Security Assets

The ultimate goal for any security practitioner is to be able to secure all assets of their organisation.

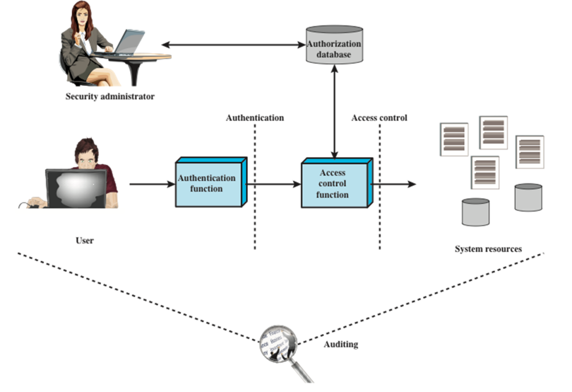
Defining Access Control

- ❏ Access Control is the process of protecting a resource so that it is used only by those allowed to.
- ❏ Mitigations put into place to protect a resource from a threat such as to prevent unauthorised use.

Access Control Functions

- **Identification**: Who is asking to access the asset?
  - Subjects supplying identification information
  - Username, user ID, account number
- **Authentication**: Can their identities be verified?
  - Verifying the identification information
  - Passphrase, PIN, biometric, password, OTP
- **Authorisation**: What can the requester access and do?
  - Using criteria to determine what the subjects can do on objects
  - ”I know who you are, I will allow you to do what you are allowed to ?”
- **Accountability**: How are actions traced to an individual to ensure the person who makes data or system changes can be identified?
  - Audit logs and/or real-time monitoring to track subject activities with objects

ACCESS CONTROL



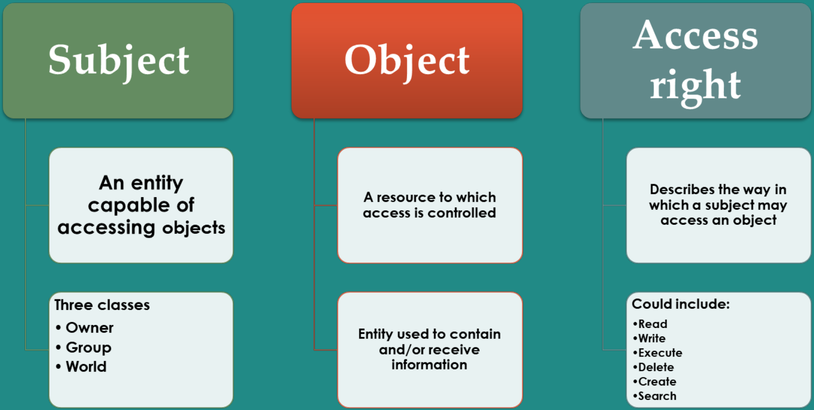
Policy Definition and Policy Enforcement Phases

- ❑ **Policy Definition phase**: We start by defining Who has access and what systems or resources they can use.
  - ❒ Tied to the authorisation phase
- ❑ Then, the policy enforcement phase Grants/Rejects requests for access based on the authorisations defined in the first phase.
  - ❒ Tied to identification, authentication, & accountability

An example

- ❑ **In the policy definition phase:** We define the following
  - ❒ Students are only authorised to see contents of their modules. They cannot edit.
- ❑ **In the policy enforcement phase:** For each student who access the system:
  - ❒ Identified by their username and authenticated by their password, they are given access to what they are authorised to see as per the policy definition phase.

ACCESS CONTROL COMPONENTS



Subject

An entity capable of accessing objects

Three classes
- Owner
- Group
- World

Object

A resource to which access is controlled

Entity used to contain and/or receive information

Access right

Describes the way in which a subject may access an object

Could include:
- Read
- Write
- Execute
- Delete
- Create
- Search

Types of Access Control

Physical Access Control

- ❑ Cards control access to physical resources or fingerprint (less used)
- ❑ Smart cards Programmed with ID number are an example
- ❑ Used at parking lots, elevators, office doors

Logical Access Control

- ❑ Deciding which users can get into a system
- ❑ Monitoring what each user does on that system
- ❑ Restraining or influencing a user's behaviour on that system

Enforcing Access Control

The Security Kernel

❑ Enforces access control for computer systems

❑ Central point of access control

❑ Implements the reference monitor concept

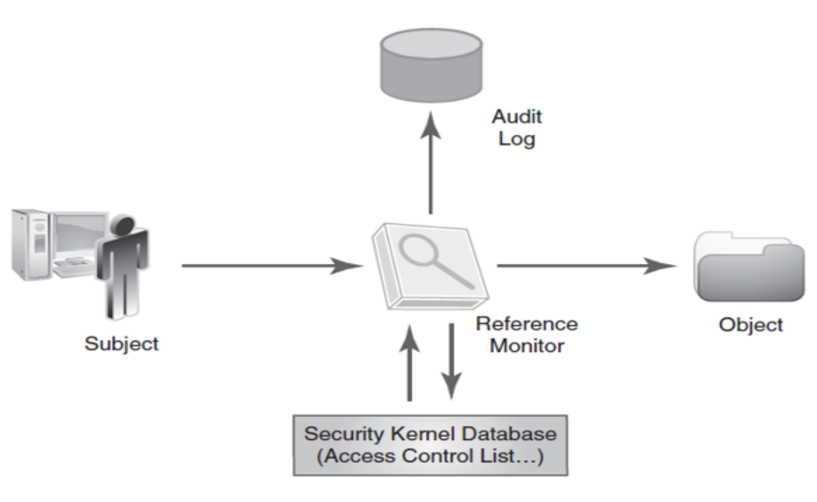
How Access Control is enforced

❑ The subject requests access to an object. The security kernel intercepts the request.

❑ The security kernel refers to its rules base, also known as the security kernel database to allow or deny access.

❑ All access requests handled by the system are logged for later tracking and analysis.

Enforcing Access Control



Logical Access Control

Logical Access Control Solutions

Logical Controls	Solutions
Biometrics	Static: Fingerprints, iris granularity, retina blood vessels, facial features, and hand geometry Dynamic: Voice inflections, keyboard strokes, and signature motions
Tokens	Synchronous or asynchronous Smart cards and memory cards
Passwords	Stringent password controls for users Account lockout policies Auditing logon events
Single sign-on	Kerberos process Secure European System for Applications in a Multi-Vendor Environment (SESAME)

Authentication Types

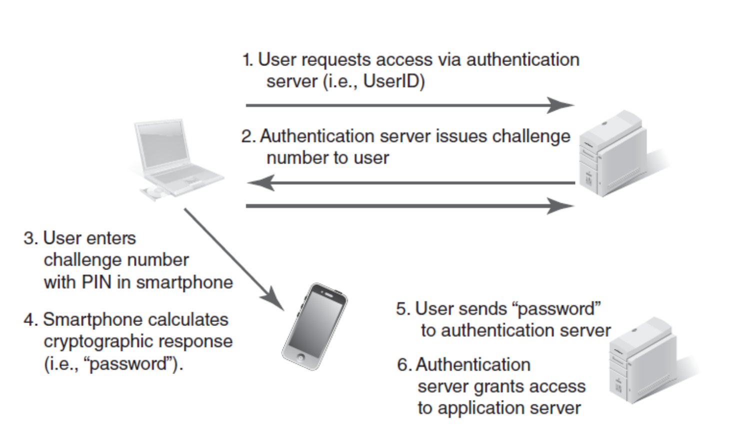
Authentication by Knowledge: Something you know

- ❒ Passwords, passphrases. PIN number

Authentication by Ownership: Something you own

- ❑ Synchronous token- Calculates a number at both the authentication server and the device
  - ❒ Time-based synchronization, i.e. software authenticator
  - ❒ Event-based synchronization, i.e. SMS one time password
- ❑ Asynchronous token: Fixed, no calculation is needed as long as you prove you physically have it, you can access
  - ❒ USB token or Smart card

ASYNCHRONOUS TOKEN CHALLENGE-RESPONSE


1. User requests access via authentication server (i.e., UserID)
2. Authentication server issues challenge number to user
3. User enters challenge number with PIN in smartphone
4. Smartphone calculates cryptographic response (i.e., “password”).
5. User sends “password” to authentication server
6. Authentication server grants access to application server

AUTHENTICATION TYPES

Authentication by Characteristics: Something unique to you

- ❒ This can be:
  - ❑ **Biometrics** Something Static, What are you

    Fingerprint, facial recognition, hand geometry, Retina scan
  - ❑ Something Dynamic such as What you do!

    Voice patterns, keystroke dynamics, signature dynamics

Authentication by Location: Somewhere you are

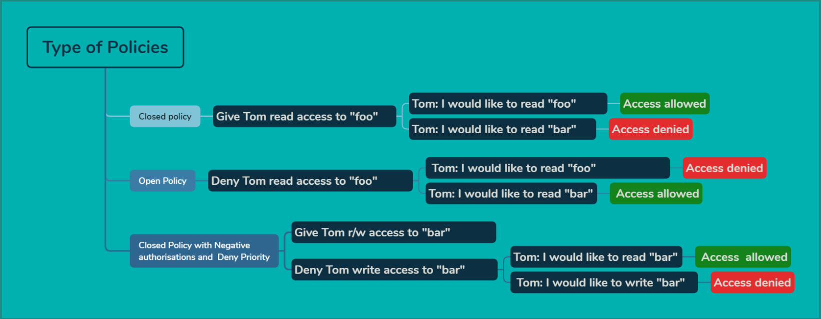
- ❑ Location
  - ❒ Strong indicator of authenticity

Access Control principles

General Principles

- Files and folders are managed by the operating system
- Applications, including shells, access files through an API
- Access control entry (ACE)
  - Allow/deny a certain type of access to a file/folder by user/group
- Access control list (ACL)
  - Collection of ACEs for a file/folder
- A file handle provides an opaque identifier for a file/folder
- File operations
  - Open file: returns file handle
  - Read/write/execute file
  - Close file: invalidates file handle
- Hierarchical file organisation
  - Tree (Windows)
  - DAG (Linux)

Access Policies



Type of Policies
Closed policy
Give Tom read access to "foo"
Tom: I would like to read "foo"
Access allowed
Tom: I would like to read "bar"
Access denied
Open Policy
Deny Tom read access to "foo"
Tom: I would like to read "foo"
Access denied
Tom: I would like to read "bar"
Access allowed
Closed Policy with Negative authorisations and Deny Priority
Give Tom r/w access to "bar"
Deny Tom write access to "bar"
Tom: I would like to read "bar"
Access allowed
Tom: I would like to write "bar"
Access denied

ACCESS CONTROL MATRIX EXAMPLE

❒ Each entry in the matrix indicates the access rights of a particular subject for a particular object

		Objects			
		File 1	**File 2**	**File 3**	**File 4**
Subjects	**User A**	Own Read Write		Own Read Write	
	User B	Read	Own Read Write	Write	Read
	User C	Read Write	Read		Own Read Write

Access Control Models

Access Control Models

❑ All access control models are built on the **security operation principles** listed below:

- ❐ **Need to know** This principle ensures that subjects are granted access only to what they need to know for their work tasks and job functions.
- ❐ **Least privilege** This principle ensures that subjects are granted only the privileges they need to perform their work tasks and job functions.
- ❐ **Separation of privileges** This principle ensures that sensitive functions are split into tasks performed by two or more employees.

ACCESS CONTROL MODELS

❑ An access control model is a framework that dictates how subjects access objects.

❑ It uses access control technologies and security mechanisms to enforce the rules and objectives of the model.

❑ There are three main types of access control models:

- ❒ Discretionary
- ❒ Mandatory (Sometimes called Non-Discretionary)
- ❒ Rule Based
- ❒ Attribute-based access control (ABAC)

❑ Each model type uses different methods to control how subjects access objects

❑ Each model has its own merits and limitations.

Discretionary access control (DAC)

Controls access based on the identity of the requester and on access rules (authorisations) stating what requestors are (or are not) allowed to do

Mandatory access control (MAC)

Controls access based on comparing security labels with security clearances

Role-based access control (RBAC)

Controls access based on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles

Attribute-based access control (ABAC)

Controls access based on attributes of the user, the resource to be accessed, and current environmental conditions

DISCRETIONARY ACCESS CONTROL (DAC)

❑ The principle of discretionary access control (DAC) dictates that the information owner is the one who decides who gets to access the system(s)

❑Scheme in which an entity may be granted access rights that permit the entity, by its own violation, to enable another entity to access some resource

❑ Most of the common operating systems on the market today (Windows, Macintosh, UNIX and others) rely on DAC principles for access and operation

❑ Often provided using an access matrix

☞ One dimension consists of identified subjects that may attempt data access to the resources

☞ The other dimension lists the objects that may be accessed

DAC Terms and concepts

- ❑ Access Control Lists
  - ❒ A list or a file of users who are given the privilege of access to a system or resource (a database, for example)
  - ❒ Within the file is a user ID and an associated privilege or set of privileges for that user and that resource
  - ❒ Privileges typically include Read, Write, Update, Execute, Delete, or Rename
  - ❒ The other dimension lists the objects that may be accessed
- ❑ User Provisioning
  - ❒ Granting access to new employees
  - ❒ Include checking management approvals for grating access

NON-DISCRETIONARY ACCESS CONTROL

❑ Access rules are closely managed by security administrator, not system owner or ordinary users

❑ Sensitive files are write-protected for integrity and readable only by authorised users

❑ More secure than discretionary access control

❑ Ensures that system security is enforced and tamper-proof

MANDATORY ACCESS CONTROL (MAC)

❑ Determines the level of restriction by how sensitive the resource is

❑ The system decides who gains access to information based on the concepts of subjects, objects, and labels

❑ Often used in military and government systems with labels given to objects and access is given to subject based on security clearance level.

- ❒ Subjects: The people or other systems that are granted a clearance to access an object within the information system
- ❒ Objects: The elements within the information system that are being protected from use or access
- ❒ classification label: The mechanism that binds objects to subjects. A subject's clearance permits access to an object based on the labelled security protection assigned to that object such as Top Secret, Secret, Confidential and unclassified

Rule Based Access Control (RBAC)

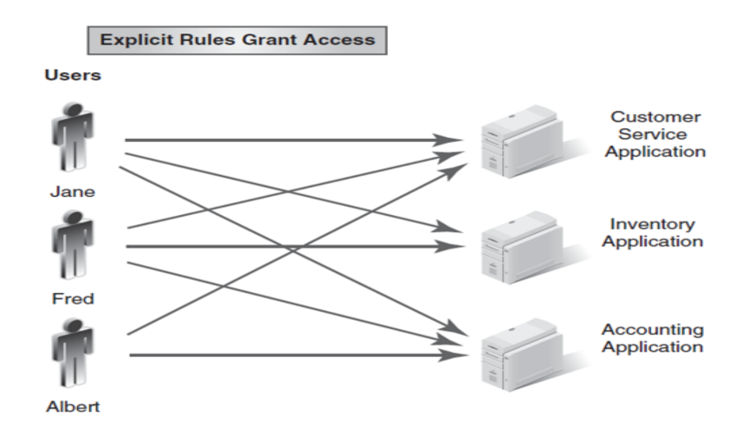
❑ Rule-based access control uses specific rules that indicate what can and cannot happen between a subject and an object.

❑ It is based on the simple concept of ”if X then Y” programming rules, which can be used to provide finer-grained access control to resources.

❑ Before a subject can access an object in a certain circumstance, it must meet a set of predefined rules.

- ❒ An example can be as simple as ”If the user's ID matches the unique user ID value in the provided digital certificate, then the user can gain access.
- ❒ or a complex example such as ”If the user is accessing the system between Monday and Friday and between 8 A.M. and 5 P.M., and if the user's security clearance equals or dominates the object's classification, and if the user has the necessary need to know, then the user can access the object.

RULE-BASED ACCESS CONTROL



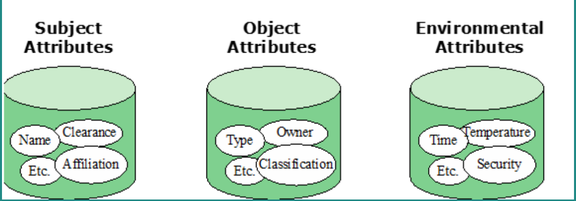
ATTRIBUTE-BASED ACCESS CONTROL (ABAC)

❑ Can define authorisations that express conditions on properties of both the resource and the subject

❑ Strength is its flexibility and expressive power

❑Main obstacle to its adoption in real systems has been concern about the performance impact of evaluating predicates on both resource and user properties for each access

❑ There is considerable interest in applying the model to cloud services



Authentication, Authorisation & Accountability (AAA)

AUTHENTICATION,AUTHORISATION, AND ACCOUNTING (AAA)

❏ AAA protocols are commonly used with remote access systems such as virtual private networks (VPNs) and other types of network access servers to provide centralised access control.

❏ They prevent internal LAN authentication systems and other servers from being attacked remotely.

❏ When a separate system is used for remote access, only the remote access users are affected if this system is successfully attacked.

❏ The AAA protocols are also commonly used for mobile IP, which provides access to mobile users with smart phones.

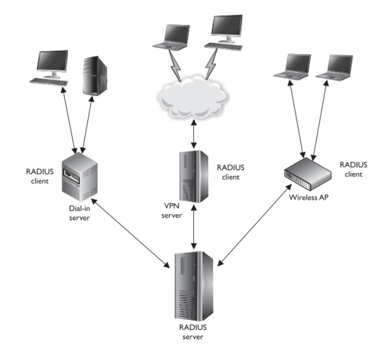
Centralised and Decentralised AAA

- ❑ Additional access control mechanisms are required because of the use of insecure networks to create a connection to the corporate local area network
- ❑ Centralised authentication, authorization, and accounting (AAA) servers
  - ❐ RADIUS
  - ❐ TACACS+
  - ❐ DIAMETER
- ❑ Decentralised Access Control: Access control is in the hands of the people closest to the system users
  - ❐ Password Authentication Protocol (PAP)
  - ❐ Challenge-Handshake Authentication Protocol (CHAP)
  - ❐ Mobile device authentication, Initiative for Open Authentication (OATH). For example One-Time Password (OTP)

Remote User Access and Authentication (RADIUS)

❑ RADIUS is a client/server protocol and software that enables remote access users to communicate with a central server to authorise their access to the requested system or service

❑ It allows companies to have a single administered entry point, which provides standardization in security and a simplistic way to track usage and network statistics.

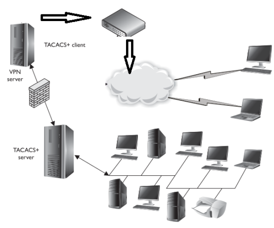


TACACS+ ARCHITECTURE:

- ❑ TACACS+ provides the same functionality as RADIUS with a few differences in some of its characteristics.
- ❒ TACACS+ uses TCP as its transport protocol, while RADIUS uses UDP.
- ❑ If compared with RADIUS, TACACS+ is the better choice for complex environments such as corporate networks that require
  - ❒ More sophisticated authentication steps
  - ❒ Tighter control over more complex authorisation activities,

What does the use of TCP means for us?

- ❒ Any software that uses UDP as its transport protocol has to be ”fatter” with intelligent code. TACAS+ will be faster to transmit.



DIAMETER

❏ Diameter is a protocol that has been developed to build upon the functionality of RADIUS and overcome many of its limitations.

❏ Diameter uses TCP as its transport protocol

❏ It provides the same type of functionality as RADIUS and TACACS+ in addition to wireless networks access.

❏ Diameter also provides more flexibility and capabilities to meet the new demands of today's complex and diverse networks.

❏ Diameter can deal with issues such as mobile IP.

❏ Diameter provides several functionalities in addition to AAA functionality such as roaming operations and replay attack protection.

SINGLE SIGN-ON (SSO)

- ❏ In an SSO system, users have one password for all corporate and back-office systems and applications they need to perform their jobs
- ❏ One password can be remembered and used, thus increasing the security of the overall system of access controls
- ❏ Single Sign-On mechanisms include
  - ❐ Kerberos
  - ❐ Federated Identities

KERBEROS

❑Kerberos is designed to provide authentication for client/server applications by using symmetric-key cryptography

❑ A free implementation available from MIT

❑ Works by assigning a unique key, called a ticket, to each user

❑ User logs in once and then can access all resources based on the permission level associated with the ticket

FEDERATED IDENTITIES

- ❑ Sites have an arrangement with a service so users can log in with the service credentials and don’t have to create a new unique user name and password
  - ❐ Facebook
  - ❐ Google

REFERENCES

- The lecture notes and contents were compiled from my own notes and from various sources.
- Figures and tables are from the recommended books
- **The lecture notes are very detailed. If you attend the lecture, you should be able to understand the topics.**
- **You can use any of the recommended readings! You do not need to read all the chapters!**
- **Recommended Readings note:** Focus on what was covered in the class.
    - Chapter 14, Security Architecture and Design, CEH v11 Certified Ethical Hacker Study Guide
    - Chapter 6, Access Controls, Fundamentals of Information Systems Security
    - Chapter 14, Authentication, Authorisation & Accountability CyBOK, The Cyber Security Body of Knowledge