Week 7: Access Control and Privilege Escalation

Ayman El Hajjar

6COSC002W - Security and Forensics

Email: a.elhajjar@westminster.ac.uk
Twitter: @azelhajjar

01 March 2021

University of Westminster

Session Overview

Key Concepts

- Access control concepts and technologies
- Formal models of access control
- How identity is managed by access control
- Developing and maintaining system access controls

Defining Access Control

- The process of protecting a resource so that it is used only by those allowed to
- Prevents unauthorized use
- Mitigations put into place to protect a resource from a threat

Access Control Components

Access Control Component	Description
Identification	Who is asking to access the asset?
Authentication	Can their identities be verified?
Authorization	What, exactly, can the requestor access? And what can they do?
Accountability	How are actions traced to an individual to ensure the person who makes data or system changes can be identified?

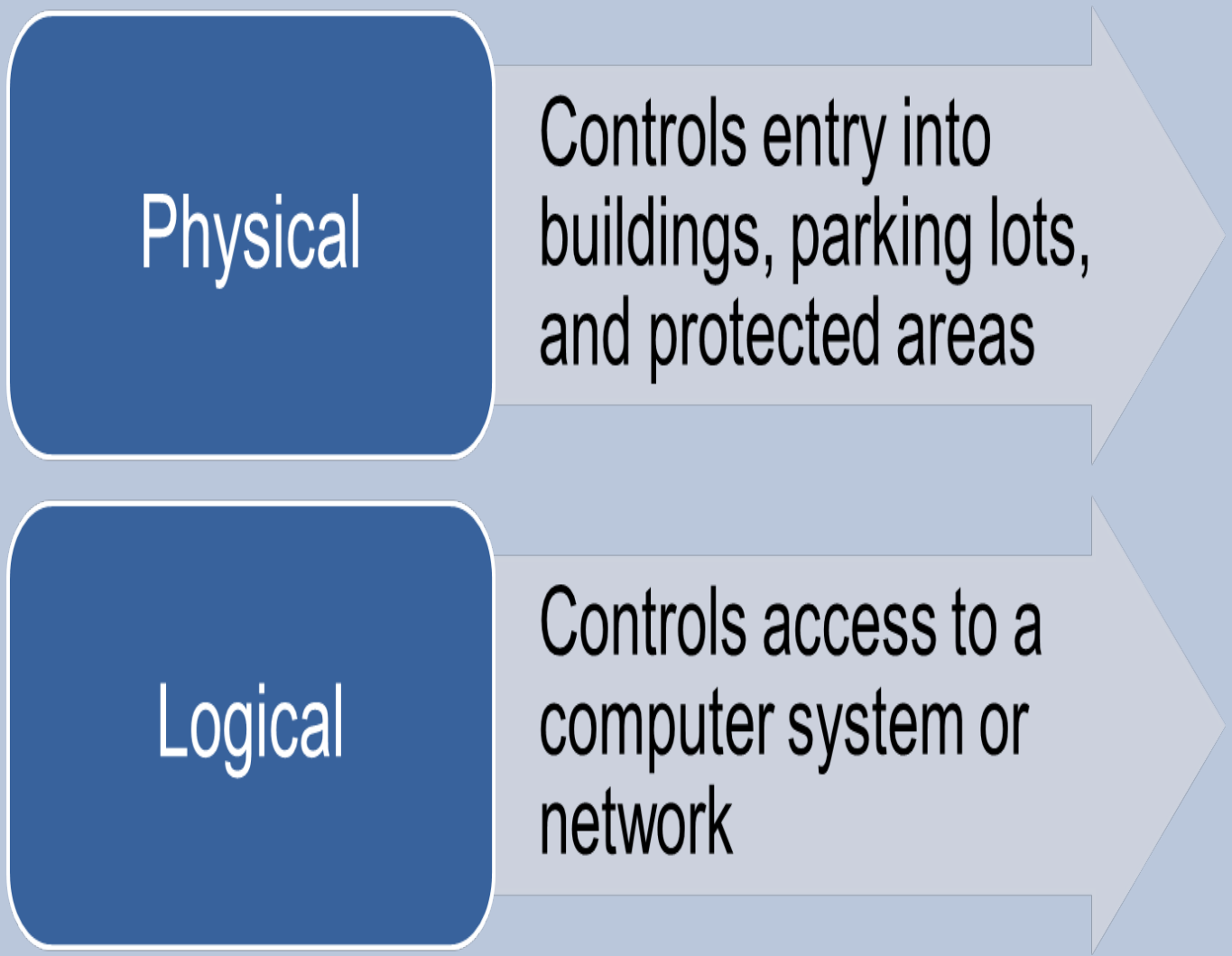
Access Control Components

- **Identification**
  - Subjects supplying identification information
  - Username, user ID, account number
- **Authentication**
  - Verifying the identification information
  - Passphrase, PIN value, biometric, one-time password, password
- **Authorization**
  - Using criteria to make a determination of operations that subjects can carry out on objects
  - "I know who you are, now what am I going to allow you to do?"
- **Accountability**
  - Audit logs and monitoring to track subject activities with objects

Policy Definition and Policy Enforcement Phases

- Policy definition phase—Who has access and what systems or resources they can use
  - Tied to the authorization phase
- Policy enforcement phase—Grants or rejects requests for access based on the authorizations defined in the first phase
  - Tied to identification, authentication, and accountability phases

Two Types of Access Control



Physical Access Control

- Smart cards are an example
- Programmed with ID number
- Used at parking lots, elevators, office doors
- Shared office buildings may require an additional after hours card
- Cards control access to physical resources

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 behavior on that system

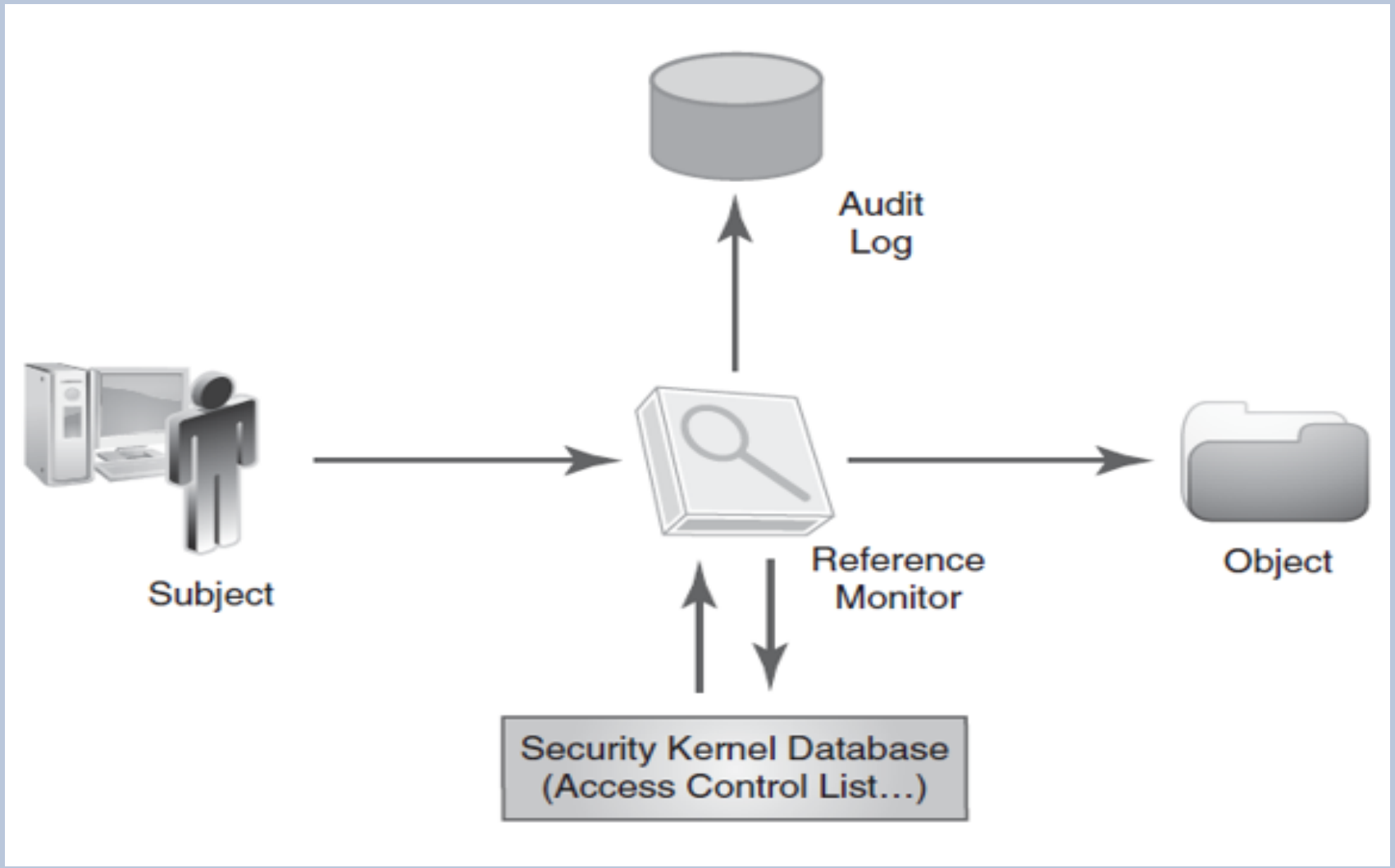
The Security Kernel

- Enforces access control for computer systems
- Central point of access control
- Implements the reference monitor concept

Enforcing Access Control

1. The subject requests access to an object. The security kernel intercepts the request.
2. The security kernel refers to its rules base, also known as the security kernel database.
   - It uses these rules to determine access rights.
   - Access rights are set according to the policies an organization has defined.
3. The kernel allows or denies access based on the defined access rules.
4. All access requests handled by the system are logged for later tracking and analysis.

Enforcing Access Control



Access Control Policies

- Four central components of access control:

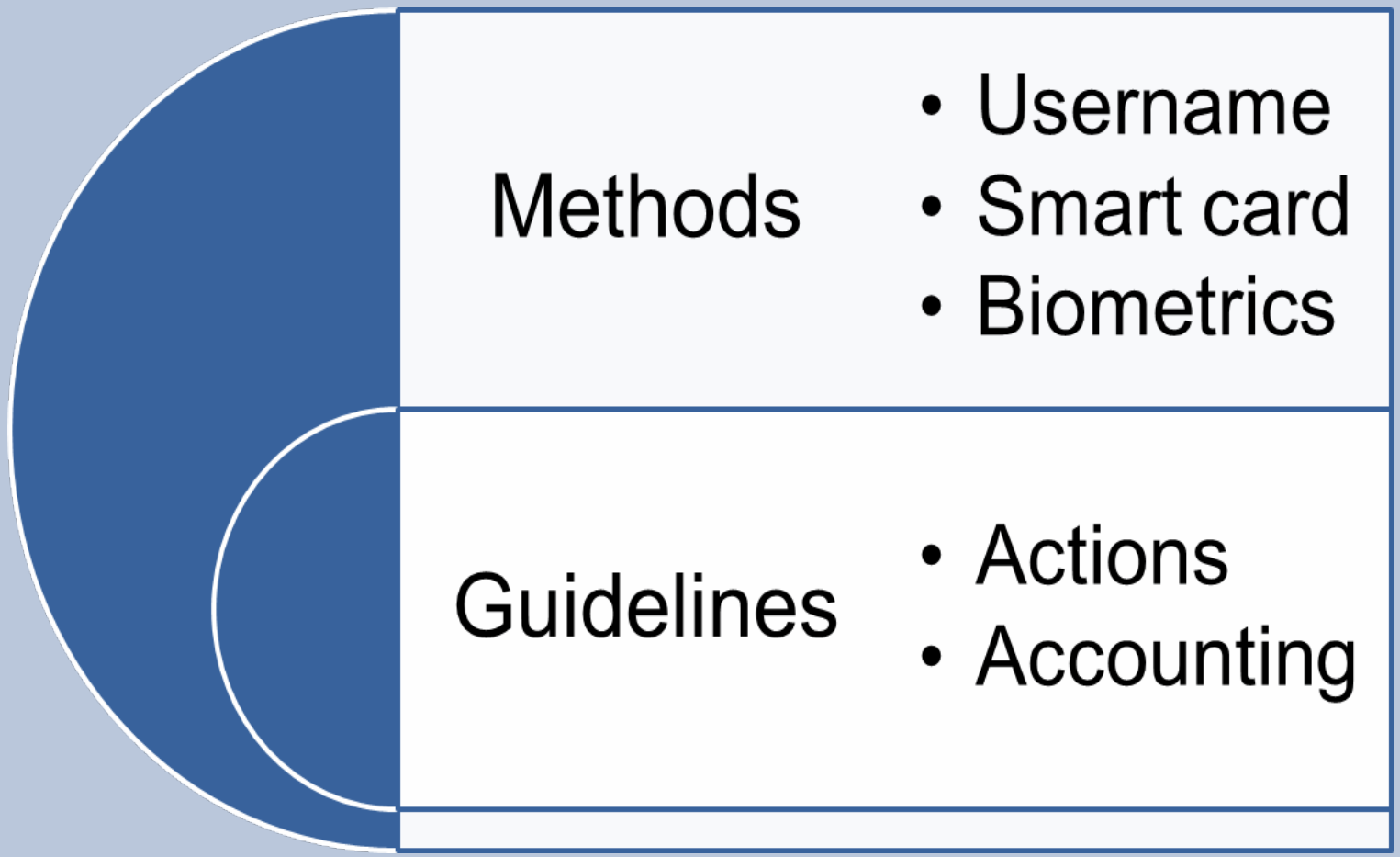
Users	People who use the system or processes (subjects)
Resources	Protected objects in the system
Actions	Activities that authorized users can perform on resources
Relationships	Optional conditions that exist between users and resources

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)

Authorization Policies

Methods and Guidelines for Identification



Authentication Types

Knowledge	Something you know
Ownership	Something you have
Characteristics	Something unique to you
Location	Somewhere you are
Action	Something you do/how you do it

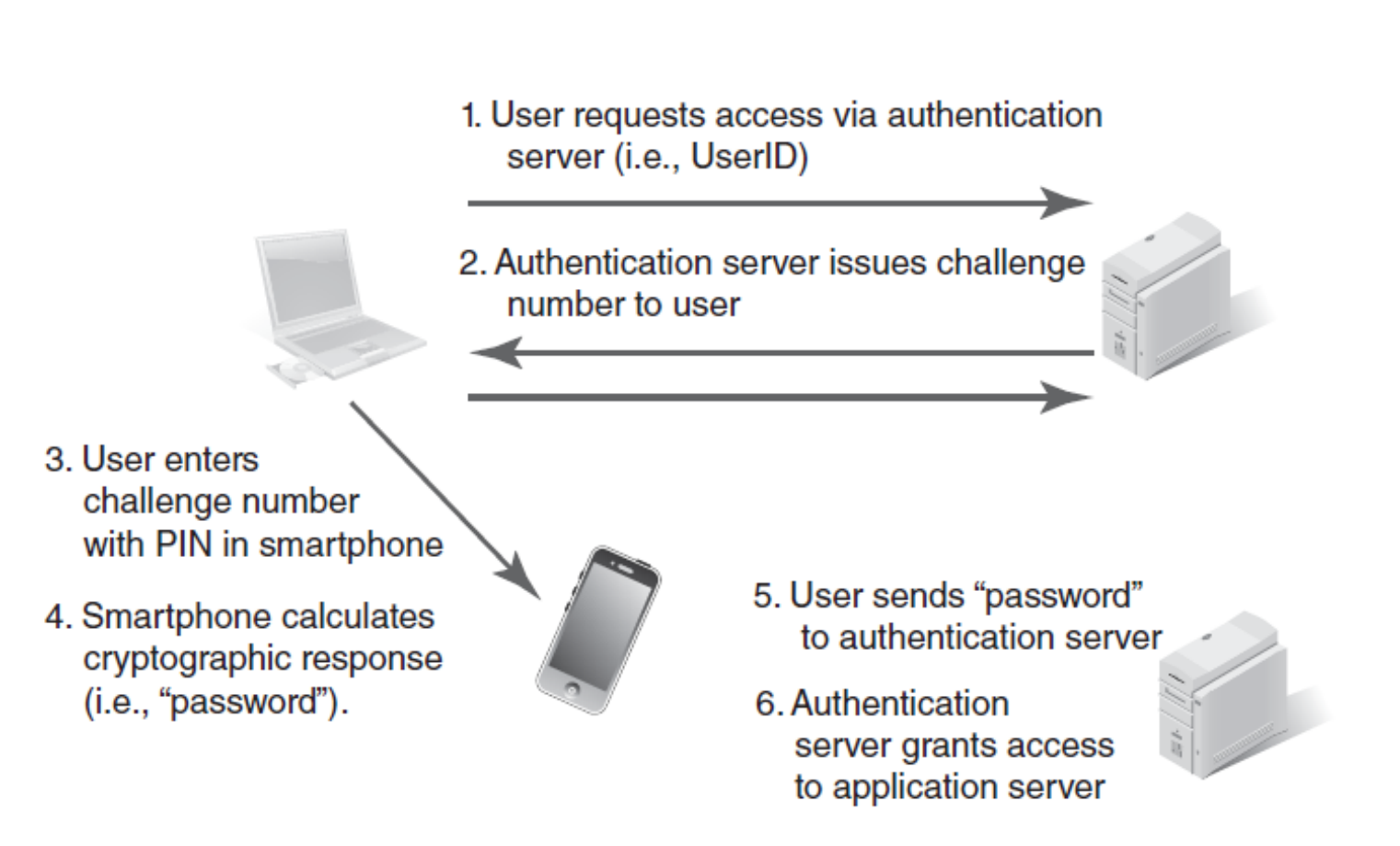
Authentication by Knowledge

- Password
  - Weak passwords easily cracked by brute-force or dictionary attack
  - Password best practices
- Passphrase
  - Stronger than a password
- Account lockout policies
- Audit logon events

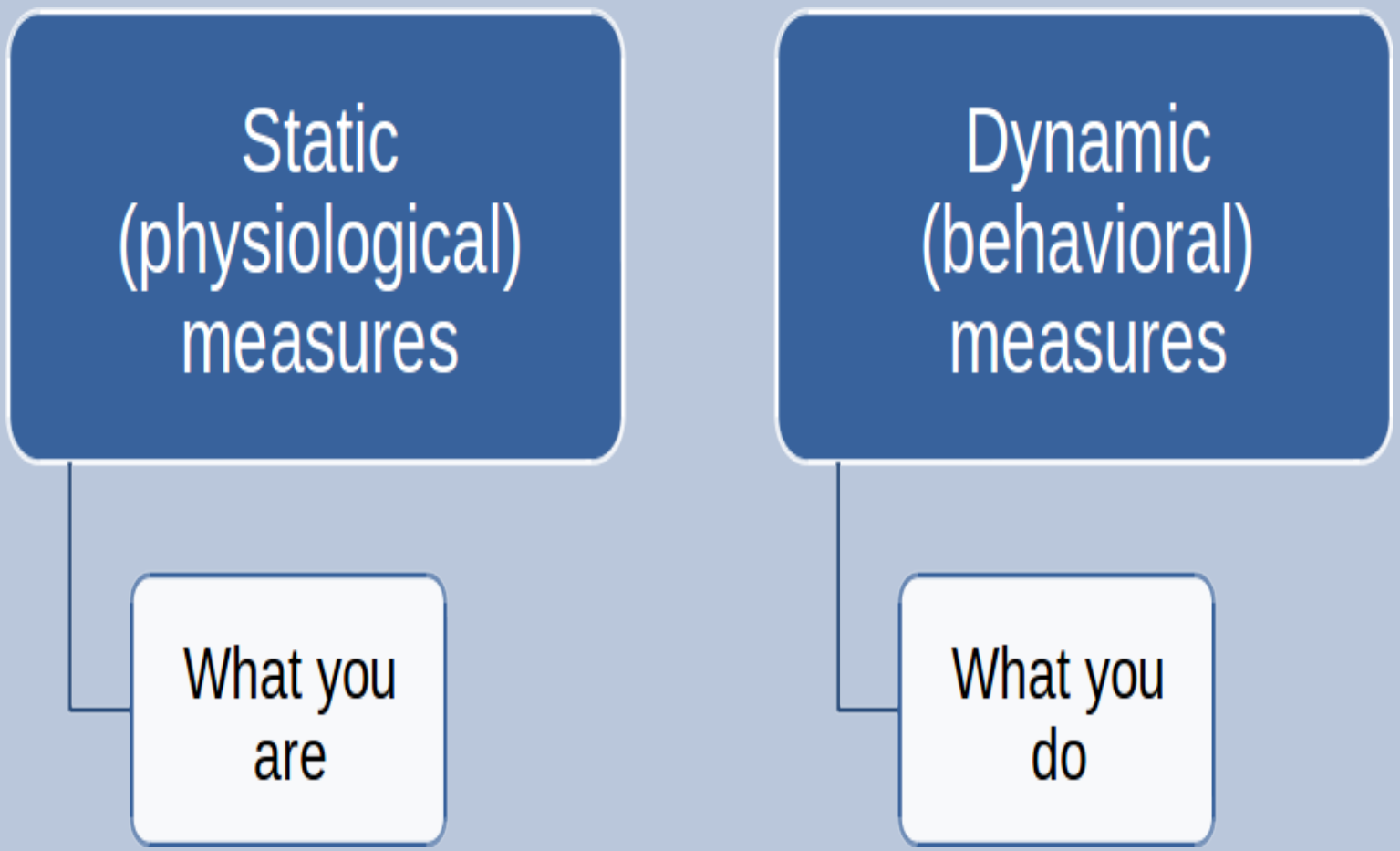
Authentication by Ownership

- Synchronous token- Calculates a number at both the authentication server and the device
  - Time-based synchronization system
  - Event-based synchronization system
  - Continuous authentication
- Asynchronous token
  - USB token
  - Smart card
  - Memory cards (magnetic stripe)

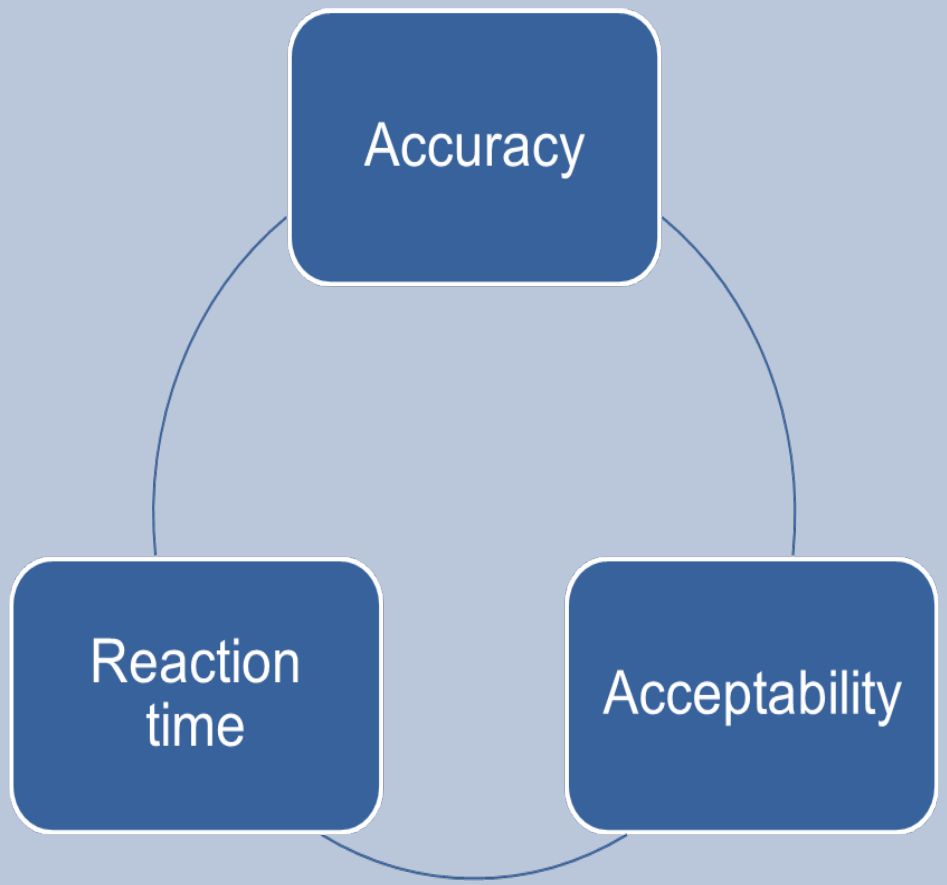
Asynchronous Token Challenge-Response



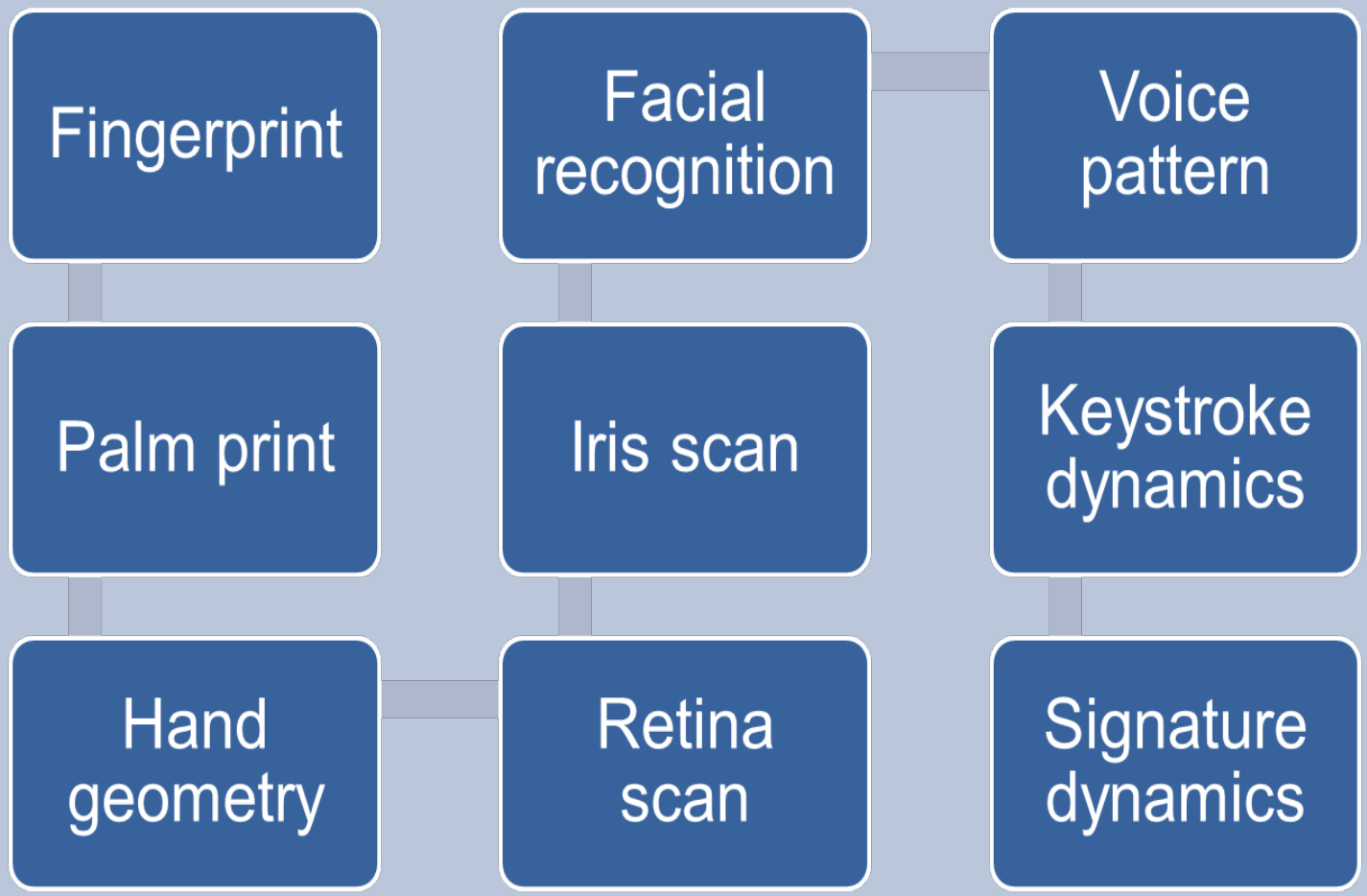
Authentication by Characteristics/Biometrics



Concerns Surrounding Biometrics



Types of Biometrics



Privacy issues in biometrics

- Biometric technologies don't just involve collecting data about a person.
- Biometrics collects information intrinsic to people.
- Every person must submit to an examination,and that examination must be digitally recorded and stored.
- Unauthorized access to this data could lead to misuse.

Authentication by Location and Action

- Location
  - Strong indicator of authenticity
  - Additional information to suggest granting or denying access to a resource
- Action
  - Stores the patterns or nuances of how you do something
  - Record typing patterns

Single Sign-On (SSO)

- Sign on to a computer or network once
- Identification and authorization credentials allow user to access all computers and systems where authorized
- Reduces human error
- Difficult to put in place

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:
  1. Discretionary
  2. Mandatory
  3. Non-Discretionary
  4. Rule Based
- Each model type uses different methods to control how subjects access objects
- Each model has its own merits and limitations.

Models of Access Control

Discretionary access control (DAC)

Mandatory access control (MAC)

Nondiscretionary access control

Rule-based access control

Access Control Models

- All access control models are built on the **security operation principles** listed below: of the model.
  - **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 duties and responsibilities** This principle ensures that sensitive functions are split into tasks performed by two or more employees.

Discretionary Access Control

- Operating systems-based DAC policy considerations
  - Access control method
  - New user registration
  - Periodic review
- Application-based DAC
- Permission levels

Mandatory Access Control

- Determine the level of restriction by how sensitive the resource is (classification label)
- System and owner make the decision to allow access
- Temporal isolation/time-of-day restrictions
- MAC is stronger than DAC

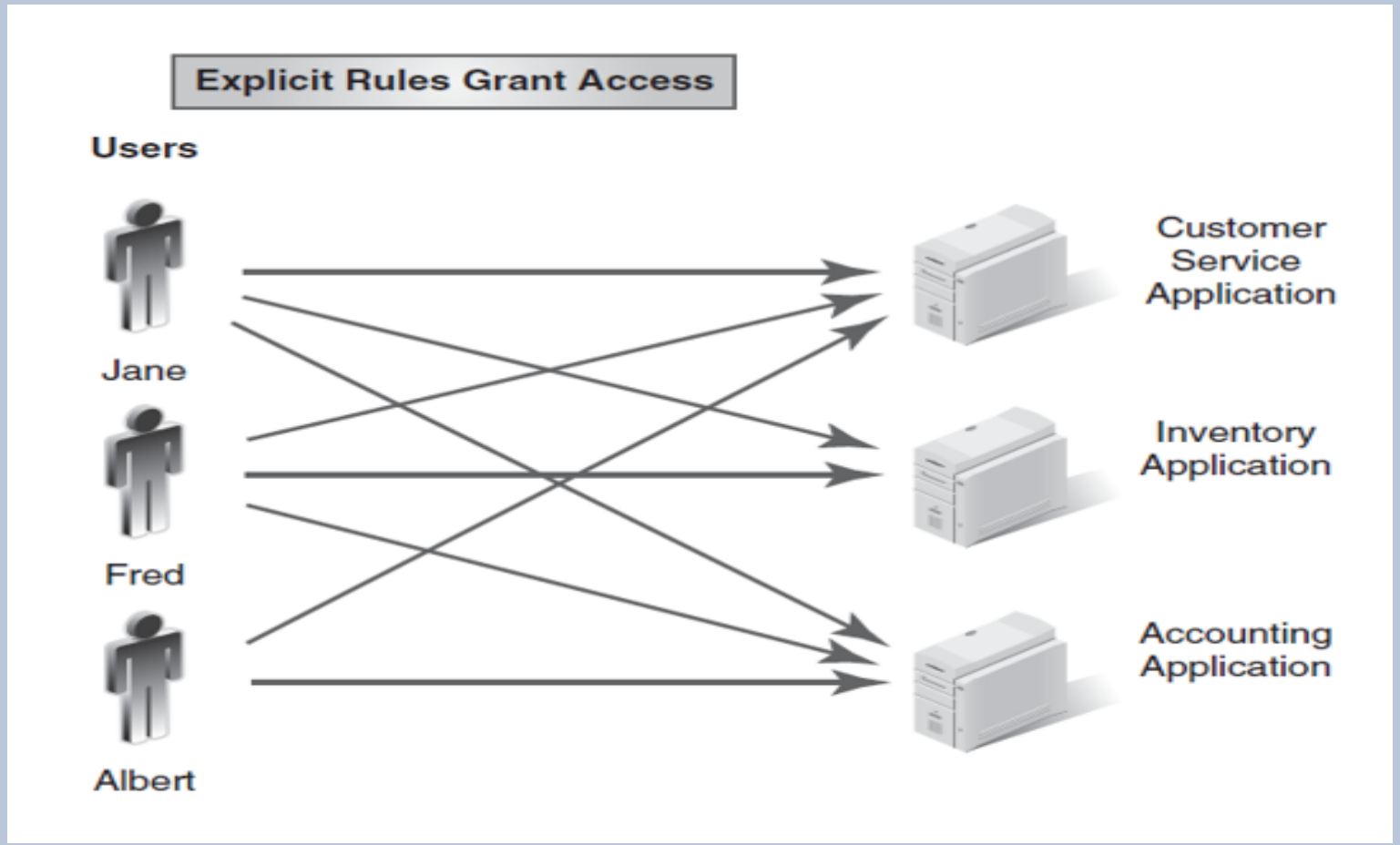
Nondiscretionary Access Control

- 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 authorized users
- More secure than discretionary access control
- Ensures that system security is enforced and tamperproof

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



Authentication,Authorization, 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 centralized 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 Access Control Administration

- A centralised access control administration method is:
- one entity (department or individual) is responsible for overseeing access to all corporate resources.
  - It configures the mechanisms that enforce access control
  - Processes any changes that are needed to a user's access control profile;
  - Provides a consistent and uniform method of controlling users' access rights.
  - Supplies strict control over data because only one entity (department or individual) has the necessary rights to change access control profiles and permissions.
- Centralised Access control provides for a more consistent and reliable environment, it can be a slow one, because all changes must be processed by one entity.

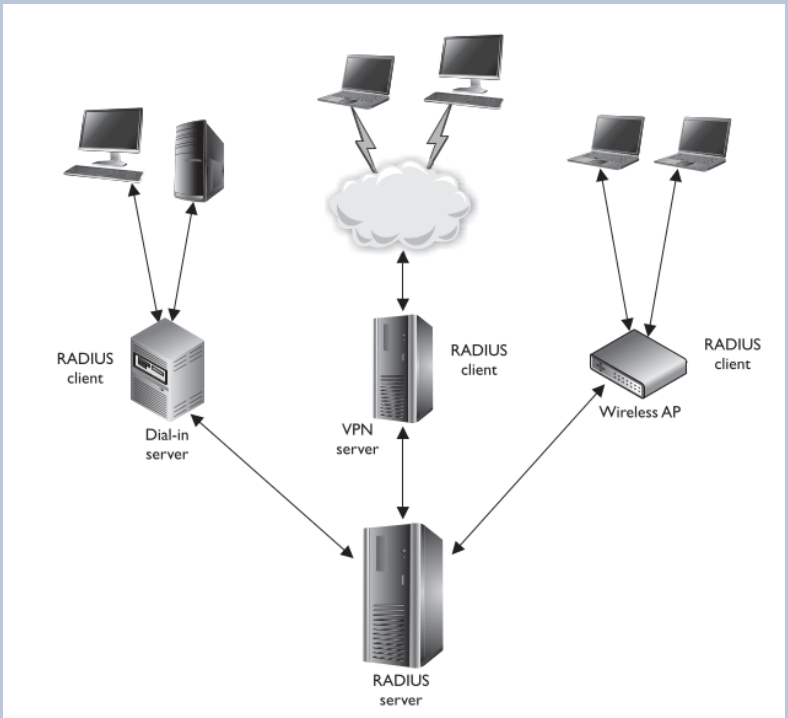
Radius

- **Remote Authentication Dial-In User Service (RADIUS)** is a network protocol that provides client/server authentication and authorization, and audits remote users.
- Many **Internet service providers (ISPs)** use RADIUS for authentication.
- Users can access the ISP from anywhere and the ISP server then forwards the user's connection request to the RADIUS server.
- Allows servers access for remote users.
- Allows users to maintain user profiles in a central database.
- Uses the User Datagram Protocol (UDP) and encrypts only the exchange of the password.
- Additional protocols can be used to encrypt the data session.

Radius

- 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.
- Used within corporate environments to provide users access to network resources.
- Organizations often implements RADIUS with callback security for an extra layer of protection.
  - Users call in, and after authentication, the RADIUS server terminates the connection and initiates a call back to the user's predefined phone number.
  - If a user's authentication credentials are compromised, the callback security prevents an attacker from using them.

Radius- architecture example



Environments can implement different RADIUS infrastructures.

1. The RADIUS protocol defines a set of fields called attribute value pairs (AVPs) that will accept certain values.
2. The user's system is given an IP address and connection parameters, and is allowed access to the Internet.
3. The access server notifies the RADIUS server when the session starts and stops.

Terminal Access Controller Access Control System

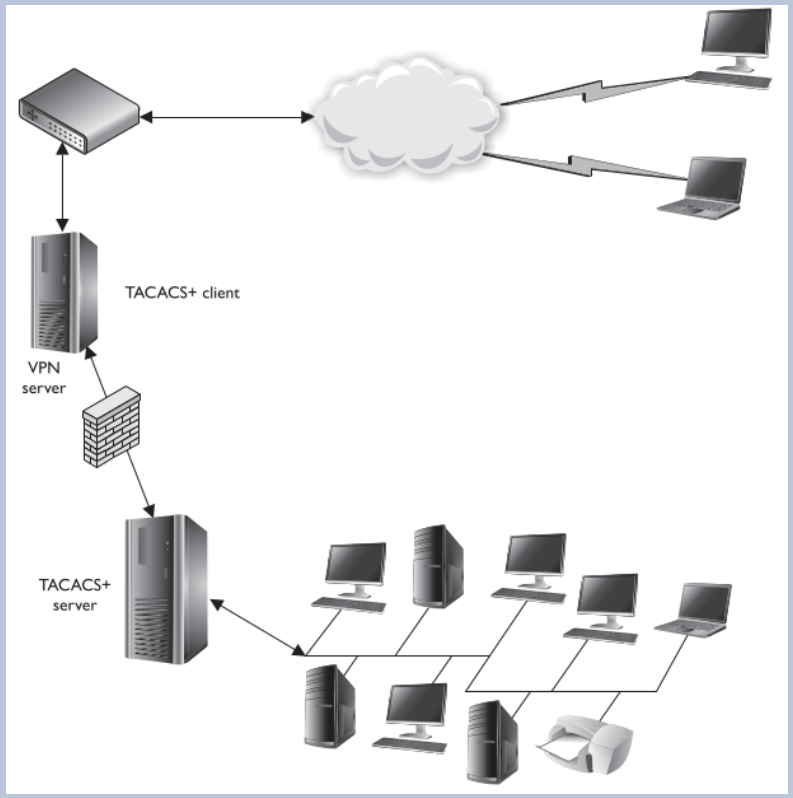
- **Terminal Access Controller Access Control System (TACACS)** has been through three generations: TACACS, Extended TACACS (XTACACS), and TACACS+.
- **TACACS** combines its authentication and authorization processes;
- **XTACACS** separates authentication, authorization, and auditing processes.
- **TACACS+** is XTACACS with extended two-factor user authentication.
- TACACS uses fixed passwords for authentication, while TACACS+ allows users to employ dynamic (one-time) passwords, which provides more protection.

TACACS+ functionality:

- TACACS+ provides basically the same functionality as RADIUS with a few differences in some of its characteristics.
  1. TACACS+ uses TCP as its transport protocol, while RADIUS uses UDP.
  2. TACACS+ software does not need to have the extra code to look for and deal with these transmission problems.
  3. TCP is a connection-oriented protocol, and that is its job and responsibility.
- What does the use of TCP means for us
  - Any software that is developed to use UDP as its transport protocol has to be "fatter" with intelligent code that will look out for the items that UDP will not catch.
  - RADIUS must have the necessary code to detect packet corruption, long timeouts, or dropped packets.

TACACS+ architecture:

- 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 authorization activities,
- TACACS+ works in a client/server environment and allows more control.



TACACS+ works in a client/server model.

Diameter

- Diameter is a protocol that has been developed to build upon the functionality of RADIUS and overcome many of its limitations.
- It provides the same type of functionality as RADIUS and TACACS+
- Traditional AAA protocols cannot keep up with our wireless devices and smart phones..
- Before Mobile and wireless communications:
  - all remote communication took place over PPP
  - Users authentication was done using either PAP or CHAP authentication protocols.
- Diameter also provides more flexibility and capabilities to meet the new demands of today's complex and diverse networks.

Diameter

- Diameter can deal with issues such as mobile IP.
- Diameter protocol consists of two portions.
  - The first is the base protocol, which provides the secure communication among Diameter entities, feature discovery, and version negotiation.
  - The second is the extensions, which are built on top of the base protocol to allow various technologies to use Diameter for authentication.
- Diameter provides several functionalities in addition to AAA functionality such as roaming operations and replay attack protection.

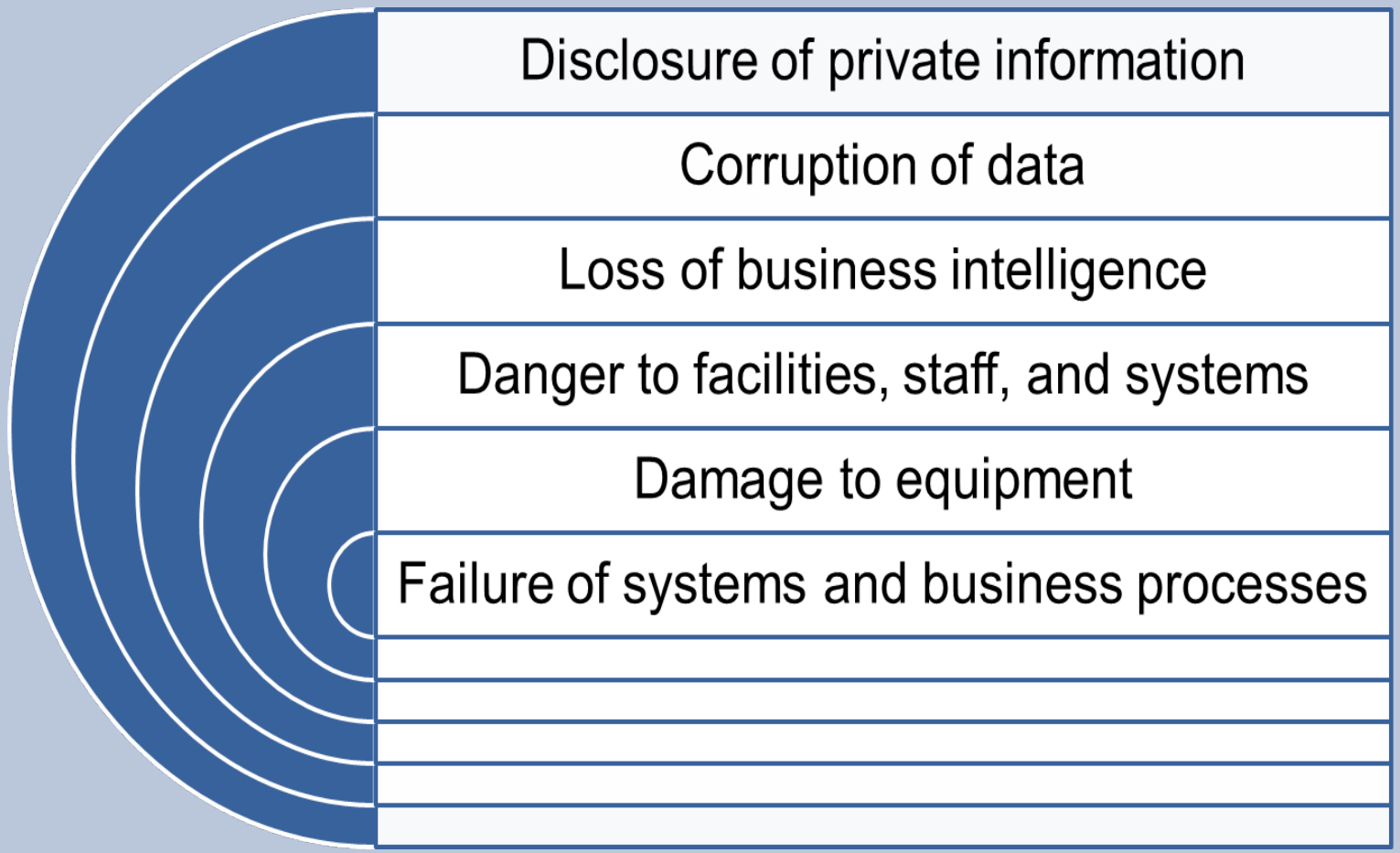
Decentralised Access Control Administration

- A **decentralized access control administration** method gives control of access to the people closer to the resources
  - The people who may better understand who should and should not have access to certain files, data, and resources.
- It is often the functional manager who assigns access control rights to employees.
- Changes can happen faster through this type of administration because not just one entity is making changes for the whole organisation.

Decentralised Access Control Administration disadvantages

- Because no single entity controls access as a whole
  - Different managers and departments can practice security and access control in different ways.
  - This does not provide uniformity and fairness across the organisation.
  - One manager can let everyone have full control over all the systems in the department another department may practice a stricter.
  - Certain controls can overlap.

Effects of Breaches in Access Control



Threats to Access Controls

- Gaining physical access
- Eavesdropping by observation
- Bypassing security
- Exploiting hardware and software
- Reusing or discarding media
- Electronic eavesdropping
- Intercepting communication
- Accessing networks
- Exploiting applications

Effects of Access Control Violations

Credential and Permissions Management

- Systems that provide the ability to collect, manage, and use the information associated with access control
- Microsoft offers Group Policy and Group Policy Objects (GPOs) to help administrators manage access controls

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 organization
  - Tree (Windows)
  - DAG (Linux)

Closed vs. Open Policy

- Closed policy
  - Also called "default secure"
- Give Tom read access to "foo"
- Give Bob r/w access to "bar"
- 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"
- Deny Bob r/w access to "bar"
- Tom: I would like to read "foo"
  - Access denied
- Tom: I would like to read "bar"
  - Access allowed

Closed Policy with Negative Authorizations 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
- Policy is used by Windows to manage access control to the file system

Access Control Entries and Lists

- An Access Control List (ACL) for a resource (e.g., a file or folder) is a sorted list of zero or more Access Control Entries (ACEs)
- An ACE refers specifies that a certain set of accesses (e.g., read, execute and write) to the resources is allowed or denied for a user or group
- Examples of ACEs for folder "Bob's 6COSC002W Grades"
  - Bob; Read; Allow
  - TAs; Read; Allow
  - TWD; Read, Write; Allow
  - Bob; Write; Deny
  - TAs; Write; Allow

Privacy

- Communicate expectations for privacy in acceptable use policies (AUPs) and logon banners
- Monitoring in the workplace includes:
  - Opening mail or email
  - Using automated software to check email
  - Checking phone logs or recording phone calls
  - Checking logs of web sites visited
  - Getting information from credit-reference agencies
  - Collecting information through point-of-sale (PoS) terminals
  - Recording activities on closed-circuit television (CCTV)

Summary

- Access control concepts and technologies
- Formal models of access control
- How identity is managed by access control
- Developing and maintaining system access controls