

SENG 460

PRACTICE OF INFORMATION SECURITY  
AND PRIVACY

# **Access Control**

# **ACCESS CONTROL OVERVIEW**

- **Access Control Concepts/Definitions**
- **Identification & Authentication Methods and Technologies**
- **Authorization Methods and Technologies**
- **Accountability Methods and Technologies**
- **Enterprise Access Control Solutions – IDM Systems**
- **Access Control Threats and Countermeasures**

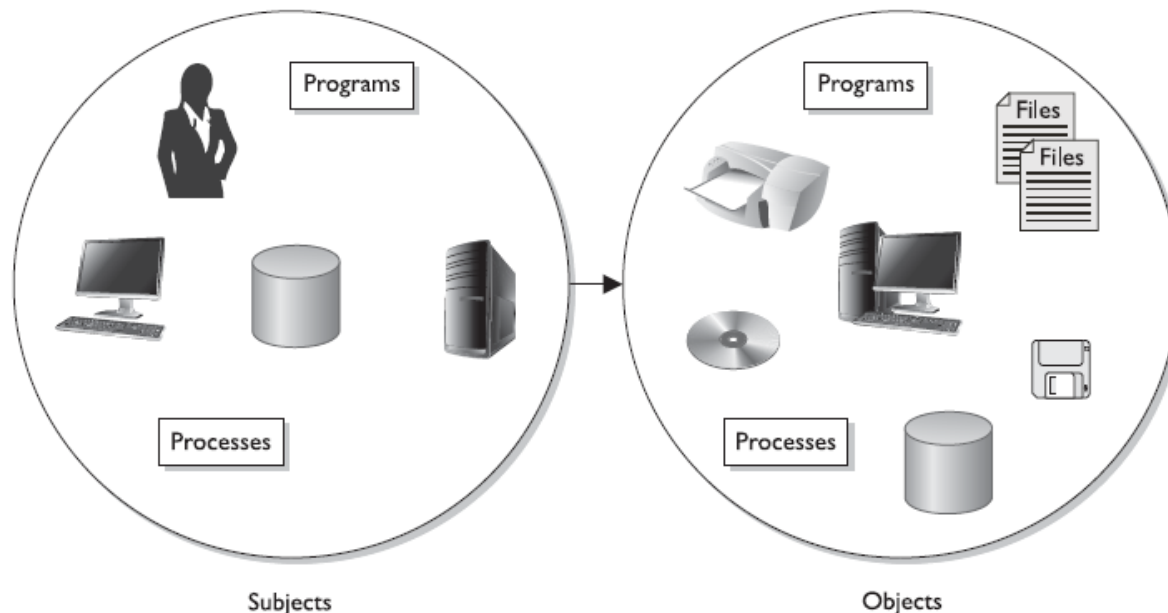
# ACCESS CONTROL CONCEPTS

## - GENERAL DEFINITIONS

**Access** is the flow of information between a subject and an object.

- A **subject** is an active entity that requests access to an object or the data within an object.
- An **object** is a passive entity that contains information or needed functionality.

**Access controls** are security measures that control how users and systems communicate and interact with other systems and resources.



# ACCESS CONTROL CONCEPTS

## - KEY ELEMENTS

- **Identification**

- A method of identifying a subject (user, program, or process). E.g. User Name, Employee ID, Account ID, etc.

- **Authentication**

- A method of ensuring a subject is the entity it claims to be. E.g. Password, Secret Token, A unique tattoo, etc.

- **Authorization**

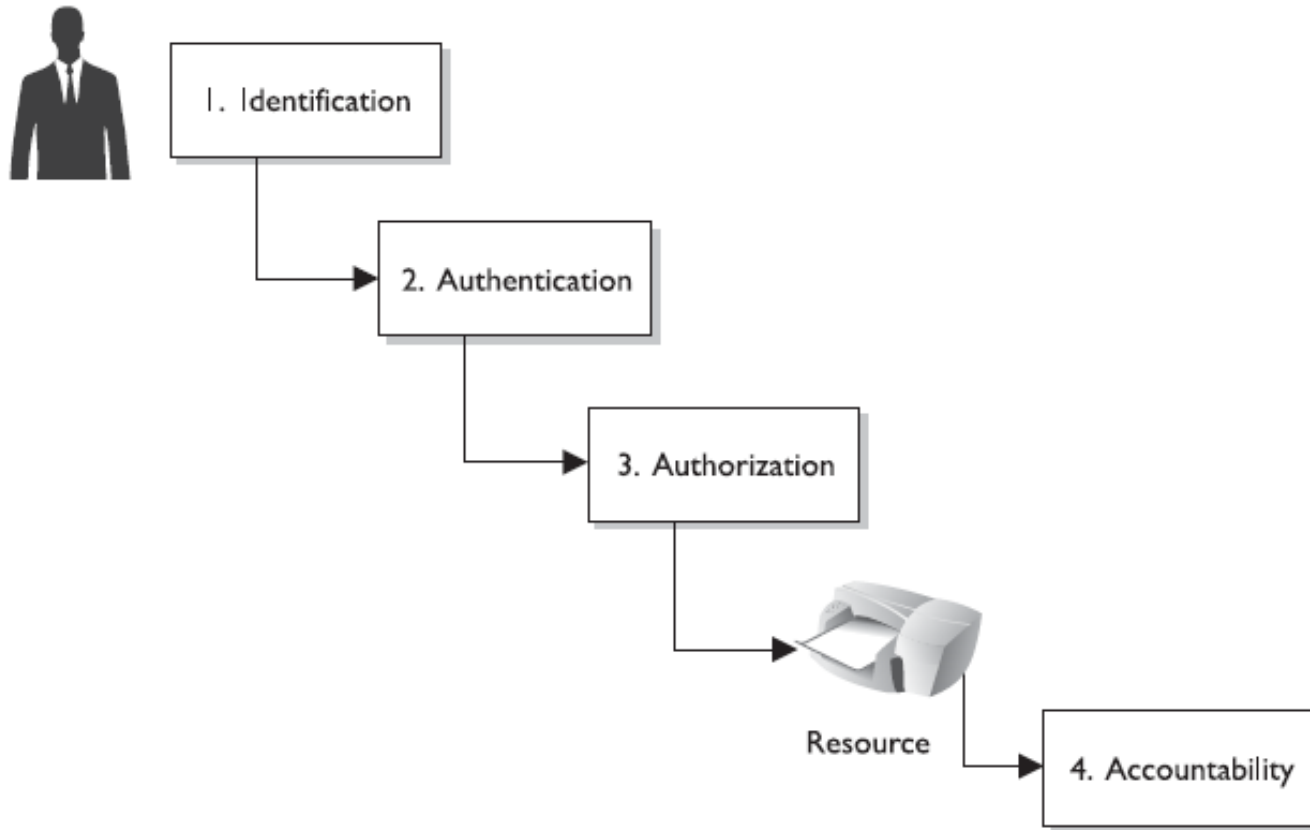
- A method to determine if this subject has been given the necessary rights and privileges to carry out the requested actions.

- **Accountability**

- A method to ensure subjects are accountable for their actions. (***non-repudiation***)

# ACCESS CONTROL CONCEPTS

## - STEPS



# IDENTIFICATION METHODS AND TECHNOLOGIES

**When issuing identification values to users, the following should be in place:**

- Each value should be unique, for user accountability.
- A standard naming scheme should be followed.
- The value should be non-descriptive of the user's position or tasks.

**Identity examples:** user name, employee number, account number, IP address, MAC (*Media access control*) Address

A ***Federated Identity*** is a portable identity that can be used across business boundaries.

# AUTHENTICATION METHODS AND TECHNOLOGIES

## -THREE FACTORS FOR AUTHENTICATION

- **Knowledge factor authentication:** Something a person knows
  - Most popular form is password authentication. Other knowledge factors include date of birth, mother's maiden name, etc.
- **Ownership factor authentication:** Something a person has or possesses
  - A key, a token, swipe card, access card, or badge.
- **Characteristic factor authentication:** Something a person is
  - Authenticating a person's identity based on a unique physical attribute (also referred as biometrics).

***Strong authentication*** uses at least two out of these three factors.

***Mutual Authentication*** means the two communicating entities authenticate to each other.

# AUTHENTICATION METHODS AND TECHNOLOGIES

## - KNOWLEDGE FACTOR (TYPE I AUTHENTICATION FACTOR)

- **Numeric passwords:** Includes only numbers.
- **Standard word or simple passwords:** single words that include a mixture of upper- and lowercase letters.
- **Combination passwords:** a mix of dictionary words, usually two unrelated words.
- **Complex passwords:** Includes a mixture of upper- and lowercase letters, numbers, and special characters.
- **Passphrase passwords:** Requires that a long phrase be used.
- **Cognitive passwords:** A piece of information that can be used to verify an individual's identity.
- **Graphical passwords:** Uses graphics as part of the authentication mechanism.
- **Static passwords:** Remains the same for each login.
- **One-time passwords:** Only used once to log in to the system.



# AUTHENTICATION METHODS AND TECHNOLOGIES

## - OWNERSHIP FACTOR (TYPE II AUTHENTICATION FACTOR)

- A **Synchronous Token** generates a unique password at fixed time intervals.
- An **Asynchronous Token** generates the password based on a challenge/response technique with the authentication server.
- A **Memory Card** is a swipe card that is issued to valid users. The card contains user authentication information.
- A **Smart Card** accepts, stores, and sends data but can hold more data than a memory card.
  - Contact cards require physical contact with the card reader.
  - Contactless cards simply need to be in close proximity to the reader.
  - Hybrid cards allow a card to be used in both contact and contactless systems.

# AUTHENTICATION METHODS AND TECHNOLOGIES

## - CHARACTERISTIC FACTORS (TYPE III AUTHENTICATION FACTOR)

- Physiological characteristics include any unique physical attribute of the user.
  - **Fingerprint:** Scans the ridges of a finger for matching
  - **Hand geometry:** Obtains size, shape, bone length, finger length, or other layout attributes of a user's hand
  - **Hand topography:** Records the peaks, valleys, and shape of the hand
  - **Palm or hand scan:** Combines fingerprint and hand geometry
  - **Facial scan:** Records facial characteristics, including bone structure, eye width, and forehead size
  - **Retina scan:** Scans the retina's blood vessel pattern
  - **Iris scan:** Scans the colored portion of the eye, including all rifts, coronas, and furrows
  - **Vascular scans:** Scans the pattern of veins in the user's hand or face
- Behavioral characteristics measure a person's actions in a situation.
  - **Signature dynamics:** Measure stroke speed, pen pressure, and acceleration and deceleration while the user writes his signature
  - **Keystroke dynamics:** Measure the typing pattern that a user uses when inputting a password or other predetermined phrase
  - **Voice pattern or print:** Measures the sound pattern of a user stating a certain word

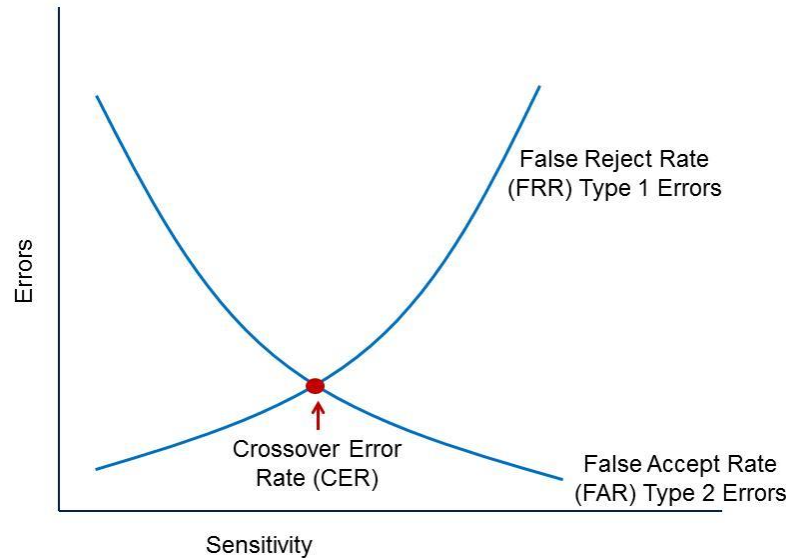
# AUTHENTICATION METHODS AND TECHNOLOGIES

## - BIOMETRIC CONSIDERATIONS

- **Enrollment time:** obtaining the sample that is used.
- **Feature extraction:** obtaining biometric information from a collected sample.
- **Throughput rate:** The rate at which the biometric system can scan characteristics and complete the analysis to permit or deny access.
- **Acceptability:** Describes the likelihood that users will accept and follow the system.
- **Accuracy:** how correct the overall readings will be.

# AUTHENTICATION METHODS AND TECHNOLOGIES

## - BIOMETRIC SYSTEM EVALUATION



**False rejection rate (FRR):** valid users that will be falsely rejected by the system.

**False acceptance rate (FAR):** invalid users that will be falsely accepted by the system.

**Crossover error rate (CER):** The point at which FRR equals FAR.

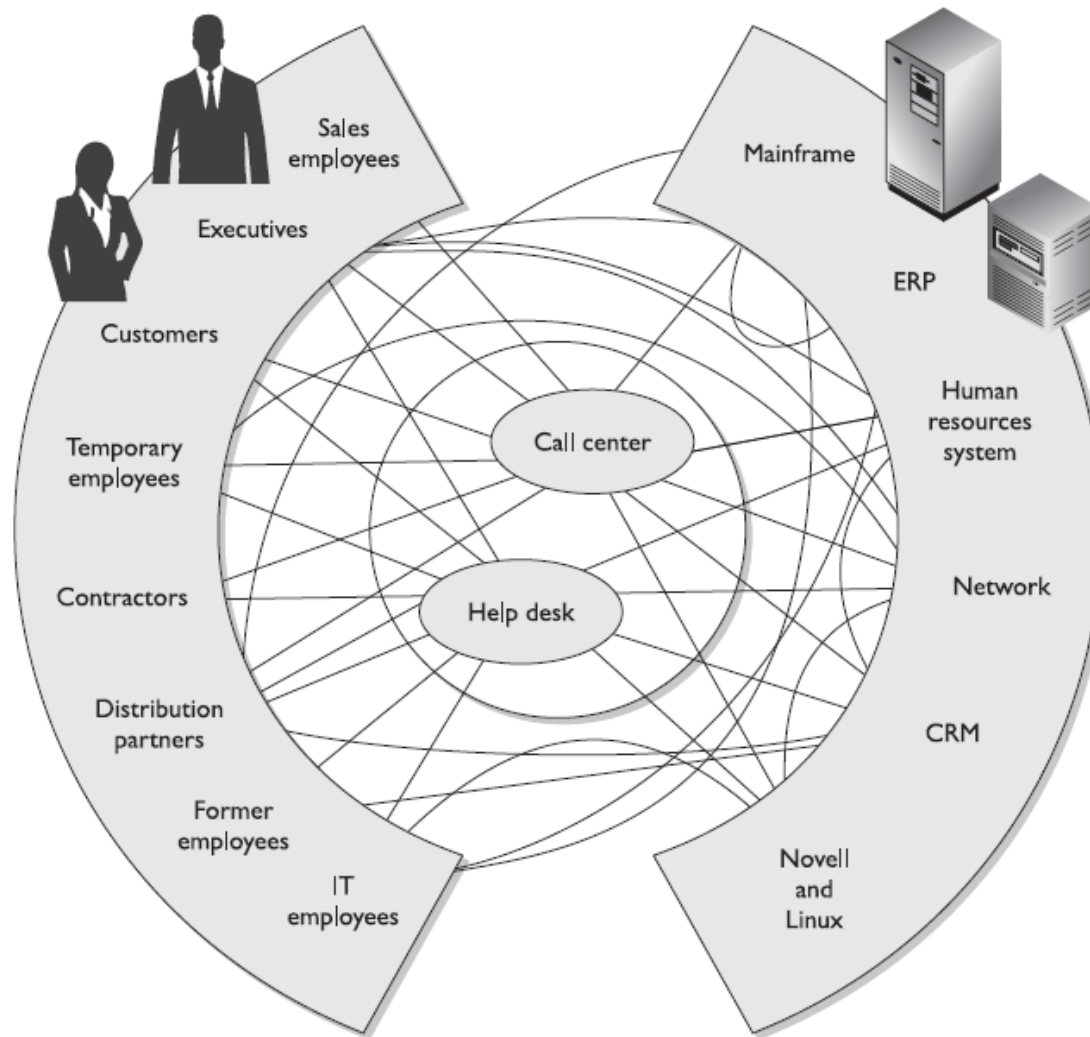
# AUTHORIZATION METHODS AND TECHNOLOGIES

## - GENERAL AUTHORIZATION PRINCIPLES

- **Formalization of Access Control Policies:** An access control policy defines the method for identifying and authenticating users and the level of user access to different user levels. An organization should ensure its access control policies implemented as formal guidelines.
- **Separation of duties:** Prevents fraud by distributing tasks and their associated rights and privileges between more than one user.
  - dual controls
  - split knowledge
- **Least privilege/need to know:** Ensure that a user or process is given only the minimum access privilege needed to perform a particular task.
- **Default to no access:** During the authorization process, you should configure an organization's access control mechanisms so that the default level of security is to default to *no access*.

# AUTHORIZATION METHODS AND TECHNOLOGIES

## - COMPLEXITY OF AUTHORIZATION



# AUTHORIZATION METHODS AND TECHNOLOGIES

## - ACCESS CONTROL MODELS

An **access control model** is a framework that dictates how subjects access objects. There are three main types of access control models:

- **Discretionary Access Control Model:** The owner of the object specifies which subjects can access the resource.
  - Most of the operating systems you may be used to dealing with are based on DAC such as Linux, and Macintosh systems, and most flavors of Unix.
- **Mandatory Access Control Model:** Subject authorization is based on security labels.
  - This type of model is used in environments where information classification and confidentiality is of utmost importance, such as military institutions, government agencies, and government contract companies.
- **Role-based Access Control Model:** Each subject is assigned to one or more roles.
  - A role is defined in terms of the operations and tasks the role will carry out.
  - Organizations with high turnover rates are moving more toward role-based access models in recent years.

# AUTHORIZATION METHODS AND TECHNOLOGIES

## - AUTHORIZATION MECHANISMS

**Rule-Based Control:** uses specific rules that indicate what can and cannot happen between a subject and an object.

**Constrained User Interfaces:** restrict users' access abilities by not allowing them to request certain functions or information, or to have access to specific system resources.

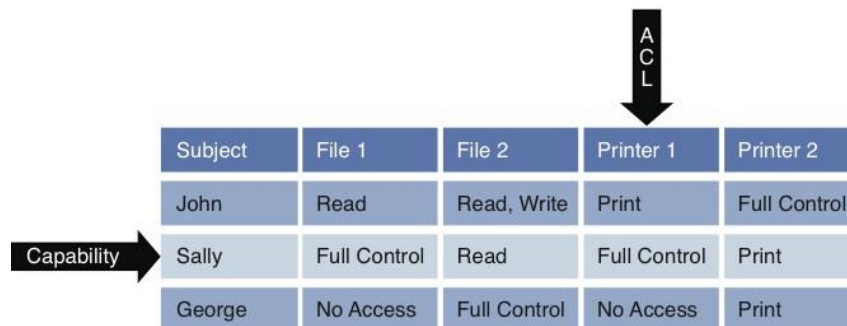
**Content-Dependent Control:** access decision is determined by the content within the object.

**Context-Dependent Control:** access decisions is based on the context of a collection of information such as subject or object attributes or environmental characteristics.

**Access Control Matrix:** An access control matrix is a table that consists of a list of subjects, a list of objects, and a list of the actions that a subject can take upon each object.

**Capabilities table:** A capability table lists the access rights that a particular subject has to objects.

**Access control list:** An ACL lists all the access rights that subjects have to a particular object.



Subject	File 1	File 2	Printer 1	Printer 2
John	Read	Read, Write	Print	Full Control
Sally	Full Control	Read	Full Control	Print
George	No Access	Full Control	No Access	Print



# ACCOUNTABILITY METHODS AND TECHNOLOGIES

## - ACCOUNTABILITY MECHANISMS

Accountability is tracked by recording user, system, and application activities (**Audit Trails/Logs**). Audit trails need to ensure the following:

- Store the audits securely.
- The right audit tools will keep the size of the logs under control.
- The logs must be protected from any unauthorized changes in order to safeguard data.
- Train the right people to review the data in the right manner.
- Make sure the ability to delete logs is only available to administrators.
- Logs should contain activities of all high-privileged accounts (root, administrator).

# **ACCOUNTABILITY METHODS AND TECHNOLOGIES**

## **- ITEMS AND ACTIONS TO BE AUDITED**

Auditing and reporting ensure that users are held accountable for their actions, but an auditing mechanism can report only on events that it is configured to monitor.

### **System-level events**

- System performance
- Logon attempts (successful and unsuccessful)
- Logon ID
- Date and time of each logon attempt
- Lockouts of users and terminals
- Use of administration utilities
- Devices used
- Functions performed
- Requests to alter configuration files

### **Application-level events**

- Error messages
- Files opened and closed
- Modifications of files
- Security violations within application

### **User-level events**

- Identification and authentication attempts
- Files, services, and resources used
- Commands initiated
- Security violations

# ACCOUNTABILITY METHODS AND TECHNOLOGIES

## - AUDIT LOG REVIEW

Audit trails can be reviewed manually or through automated means.

- Periodically Review: periodically review logs for unusual behavior of users or systems.
- Event-oriented Review: triggered by a security breach, unexplained system action, or system disruption.
- Real-time Review: monitor logs with automatic systems in real time.

**Security event management (SEM)** systems, also called **security information and event management (SIEM)** systems can gather logs from various devices (servers, firewalls, routers, etc.) and attempt to correlate the log data and provide analysis capabilities.

# ACCOUNTABILITY METHODS AND TECHNOLOGIES

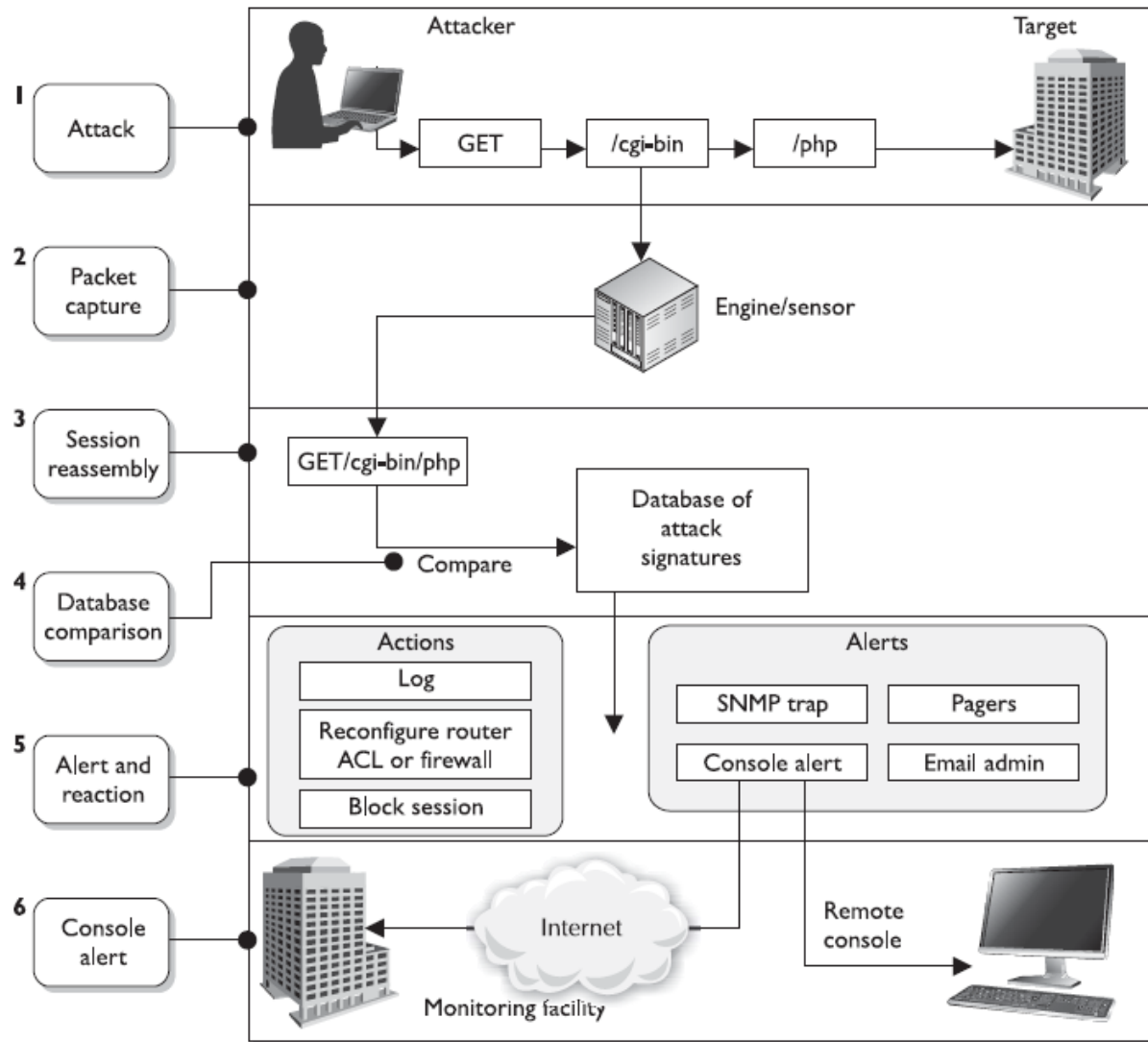
## - INTRUSION DETECTION SYSTEM

An IDS is a system responsible for detecting unauthorized access or attacks against systems and networks.

- **Signature-based:** Pattern matching, similar to antivirus software, Signatures must be continuously updated, Cannot identify new attacks
  - **Pattern matching** Compares packets to signatures
  - **Stateful matching** Compares patterns to several activities at once
- **Anomaly-based:** Behavioral-based system that learns the “normal” activities of an environment, Can detect new attacks, Also called behavior- or heuristic-based
  - **Statistical anomaly-based** Creates a profile of “normal” and compares activities to this profile
  - **Protocol anomaly-based** Identifies protocols used outside of their common bounds
  - **Traffic anomaly-based** Identifies unusual activity in network traffic
- **Rule-based:** Use of IF/THEN rule-based programming within expert systems, Use of an expert system allows for artificial intelligence characteristics. The more complex the rules, the more demands on software and hardware processing requirements. Cannot detect new attacks

# ACCOUNTABILITY METHODS AND TECHNOLOGIES

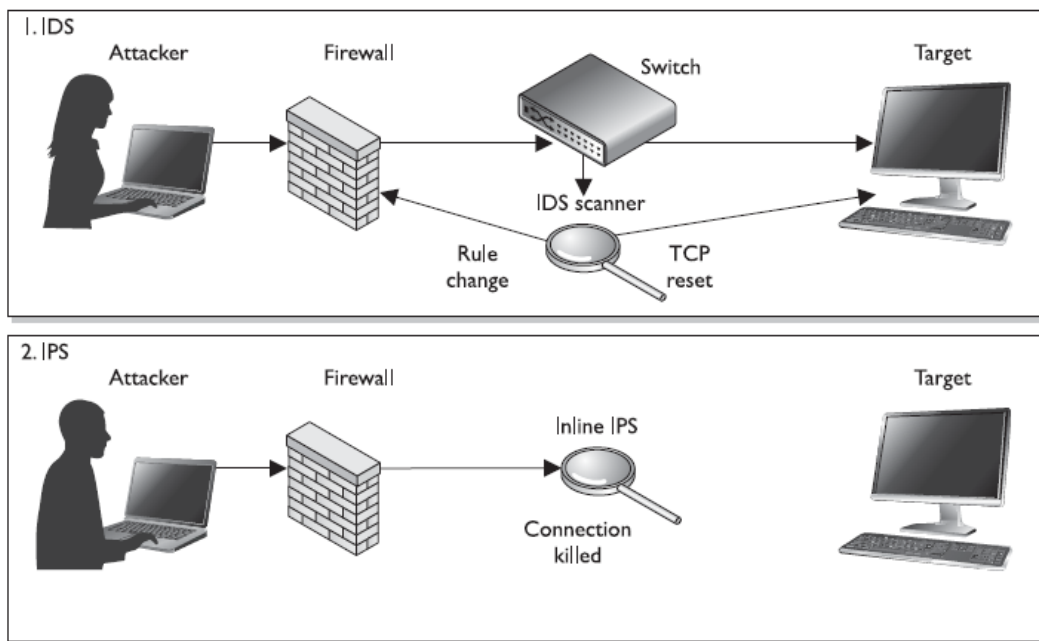
## - INTRUSION DETECTION SYSTEM



# ACCOUNTABILITY METHODS AND TECHNOLOGIES

## - INTRUSION DETECTION SYSTEM

An IPS is a system responsible for preventing attacks.



A **honeypot** is a computer or a small network segment set up as a sacrificial lamb on the network. The system is not locked down and has open ports and services enabled. This is to entice a would-be attacker to this computer instead of attacking authentic production systems on a network.

Note: **enticement** is legal but **entrapment** is illegal.

# ENTERPRISE ACCESS CONTROL SOLUTIONS – IDM SYSTEMS

Identity Management (IDM) System is a broad and loaded term that encompasses the use of different products to identify, authenticate, and authorize users through automated means.

IDM system main functionalities include:

- Directory Service
- Web Access Management
- Password Management
- Account Management
- Single Sign-on Service

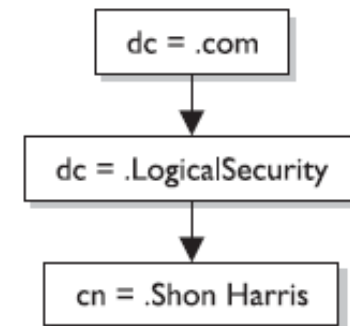
# ENTERPRISE ACCESS CONTROL SOLUTIONS – IDM SYSTEMS

## - DIRECTORY SERVICE

Most enterprises have some type of **Directory** (a kind of database) that contains information pertaining to the company's network resources and users. The **directory service** allows an administrator to configure and manage how identification, authentication, authorization, and access control take place within the network and on individual systems.

- In databases based on the X.500 standard, the directory service assigns distinguished names (DNs) to each object. Each DN represents a collection of attributes about a specific object, and is stored in the directory as an entry.

dn: cn=Shon Harris,dc=LogicalSecurity,dc=com

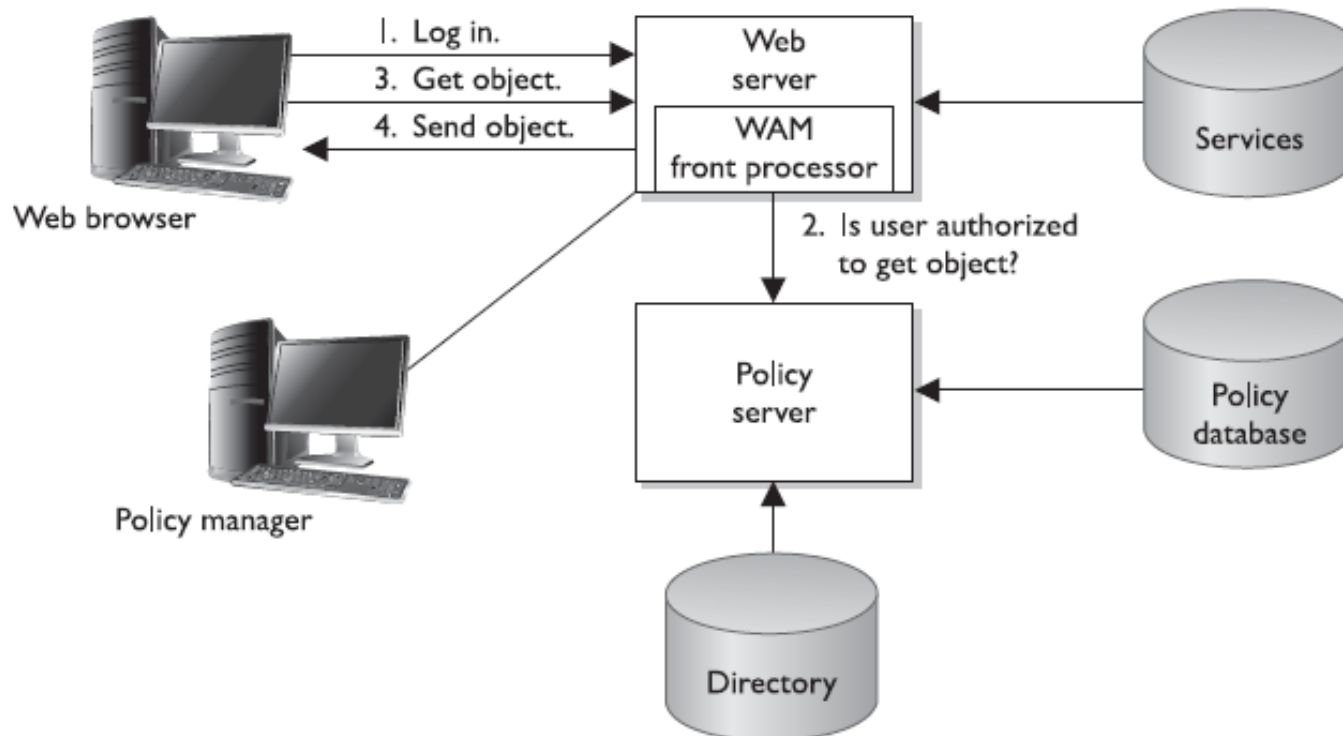




# ENTERPRISE ACCESS CONTROL SOLUTIONS – IDM SYSTEMS

## - WEB ACCESS MANAGEMENT

Web Access Management (WAM) software controls what users can access when using a web browser to interact with web-based enterprise assets.



# ENTERPRISE ACCESS CONTROL SOLUTIONS – IDM SYSTEMS

## - PASSWORD MANAGEMENT

- **Password Synchronization** Reduces the complexity of keeping up with different passwords for different systems.
- **Self-Service Password Reset** Reduces help-desk call volumes by allowing users to reset their own passwords.
- **Assisted Password Reset** Reduces the resolution process for password issues for the help desk. This may include authentication with other types of authentication mechanisms (biometrics, tokens).

# **ENTERPRISE ACCESS CONTROL SOLUTIONS – IDM SYSTEMS**

## **- ACCOUNT MANAGEMENT**

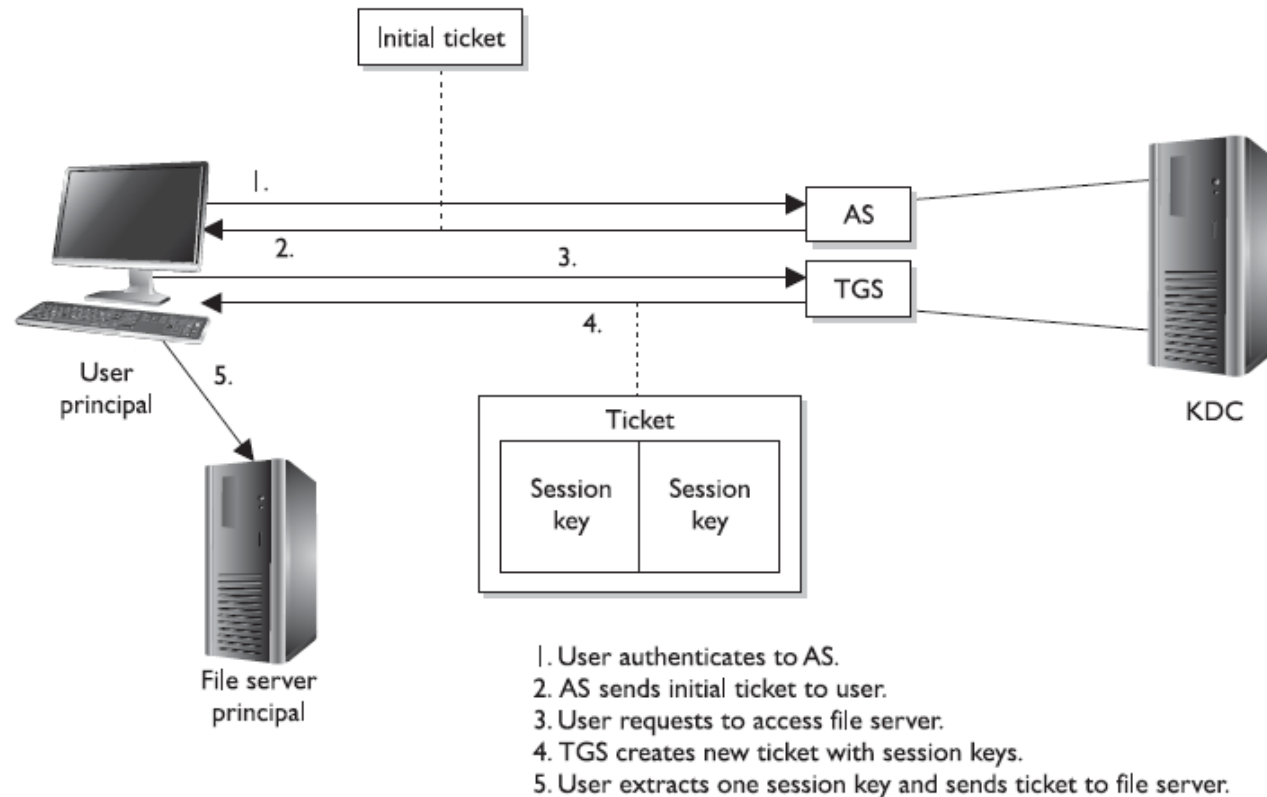
Account management deals with creating user accounts on all systems, modifying the account privileges when necessary, and decommissioning the accounts when they are no longer needed.

- Identity Provisioning service
  - A business process for creating and managing access to resources in an information technology (IT) system.
- Identity Administration service
  - Change propagation
  - self-service workflow
  - Consolidated user administration
  - Delegated user administration
  - Federated change control

# ENTERPRISE ACCESS CONTROL SOLUTIONS – IDM SYSTEMS

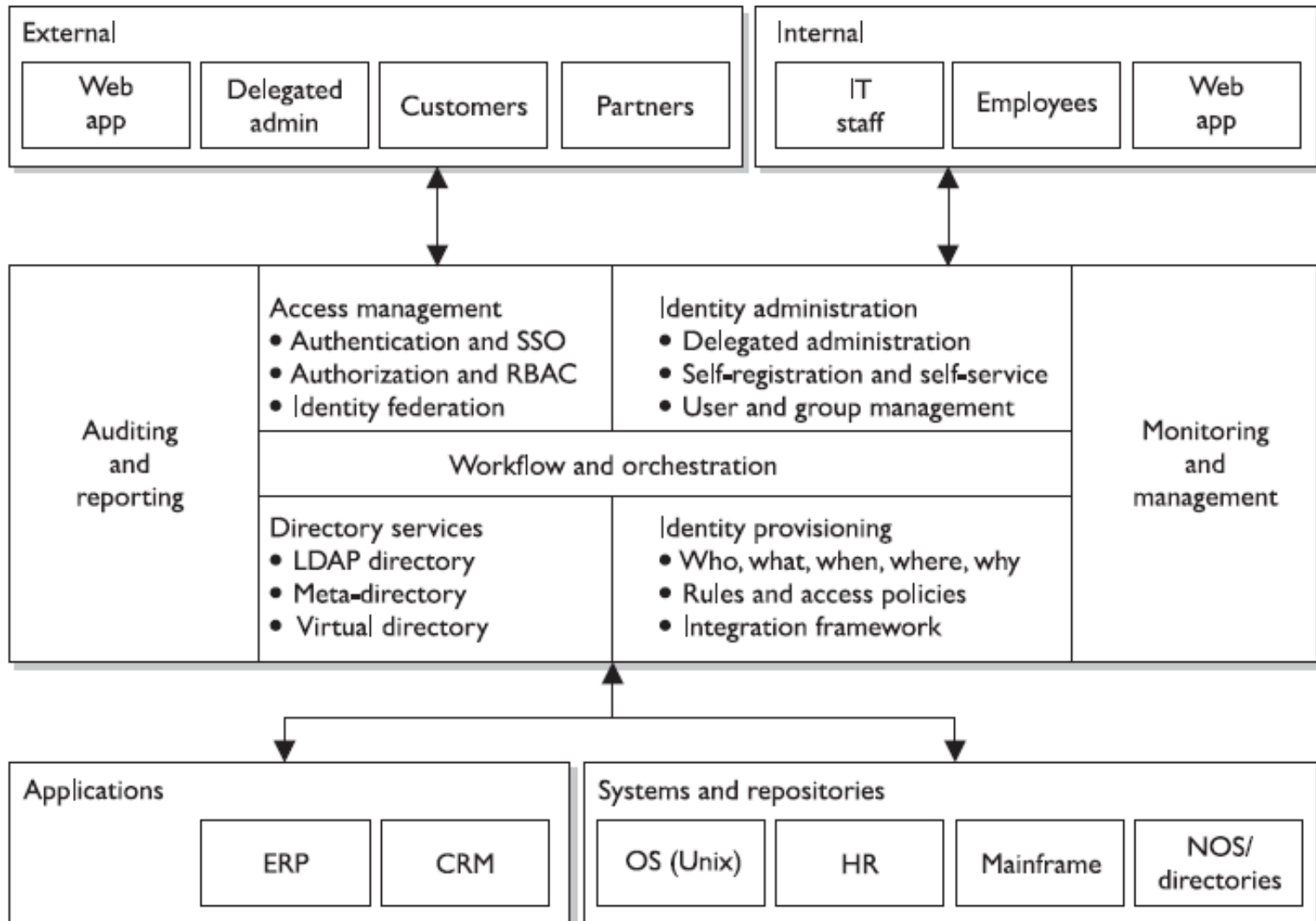
## - SINGLE-SIGN ON

Single sign-on (SSO) capabilities would allow a user to enter credentials one time and be able to access all resources in the same network domains. (Kerberos and SESAME protocols are commonly used for single sign on)



Single-Sign on using Kerberos protocol

# ENTERPRISE ACCESS CONTROL SOLUTIONS – IDM SYSTEMS



# Access Control Threats and Countermeasures

## - Password Threats

Any attack that attempts to discover user passwords. Two most popular password threats follow:

- **Dictionary attack:** Occurs when attackers use a dictionary of common words to discover passwords.
  - Complex Your Password
- **Brute force attack:** Are more difficult to carry out because they work through all possible combinations of numbers and characters.
  - Reasonable length of Password

# Access Control Threats and Countermeasures

## - Social engineering threats

Occur when attackers use believable language and user gullibility to obtain user credentials or some other confidential information.

- **Phishing/pharming:** Phishing is when attackers try to learn personal information by implementing a fake website that very closely resembles a legitimate website. Pharming pollutes the contents of a computer's DNS cache so that requests to a legitimate site are actually routed to an alternate site.
  - Be smart and be aware
- **Shoulder surfing:** When an attacker watches when a user enters login or other confidential data.
  - Watch your back
- **Identity theft:** When someone obtains personal information and uses that information to assume an identity of the individual whose information was stolen.
  - Don't give your personal information for free
- **Dumpster diving:** When attackers examine garbage contents to obtain confidential information.
  - Shredding, shredding

# Access Control Threats and Countermeasures

## - Malicious software

Malicious software, also called malware, is any software designed to perform malicious acts.

- **Virus:** Any malware that attaches itself to another application to replicate or distribute itself.
- **Worm:** Any malware that replicates itself, meaning that it does not need another application or human interaction to propagate.
- **Trojan horse:** Any malware that disguises itself as a needed application while carrying out malicious actions.
- **Spyware:** Any malware that collects private user data, including browsing history or keyboard.

*Be careful what you have clicked, and installed!*



# Access Control Threats and Countermeasures

## - Other Threats

**DoS/DDoS** : occurs when attackers flood a device with enough requests to degrade the performance of the targeted device.

- Firewall, Intrusion Detection

**Buffer overflow**: occurs when the amount of data that is submitted to the application is larger than the buffer can handle.

- Watch the legacy components/systems

**Mobile code**: Any software that is transmitted across a network to be executed on a local system.

- Scripts are dangerous

**Spoofing**: Also referred to as masquerading, occurs when communication from an attacker appears to come from trusted sources.

- Secure your communications

# Access Control Threats and Countermeasures

## - Other Threats

**Sniffing:** occurs when an attacker inserts a device or software into the communication medium that collects all the information transmitted over the medium.

- Secure your communications

**Emanating:** electromagnetic signals that are emitted by an electronic device.

- Prevent **Cover Channel** leaking

**Backdoor/trapdoor:** gives the user who uses the backdoor unlimited access to the device or application.

- Secure Software Development & Intrusion detections