Secure Software Design and Engineering
(CY-321)

Security in Software Development Lifecycle (SDLC)

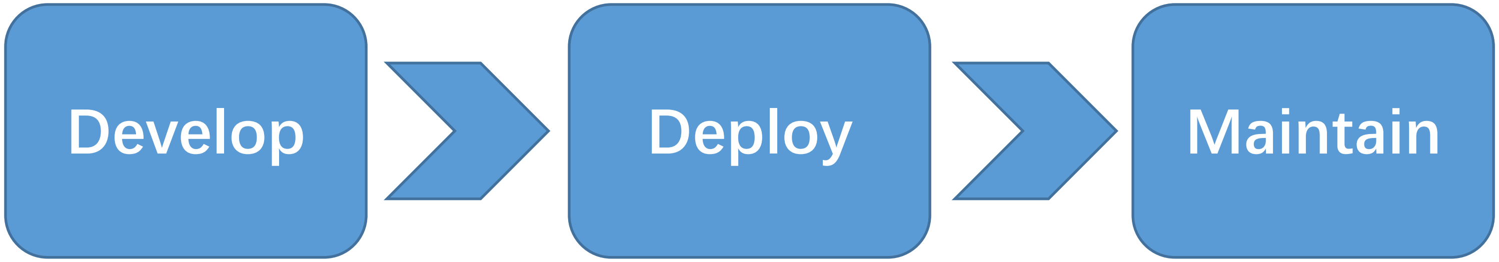
Dr. Zubair Ahmad

Text Books

Official (ISC)2 Guide to the CSSLP (latest).

Software Security: Building Security In, 1st Edition by Gary McGraw.

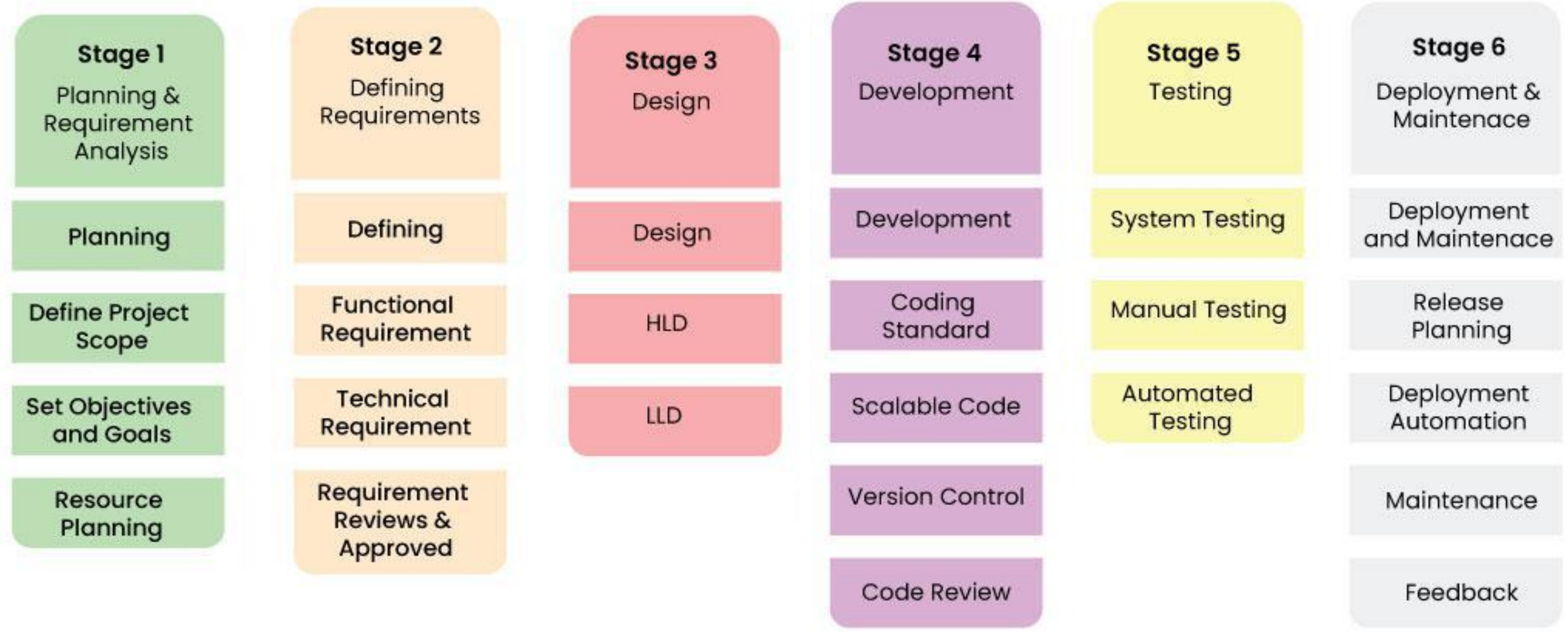
A Quick overview of SDLC



- Tasks or activities into **six to eight phases**

- **Goal:** To improve software quality by focusing on the process

A Quick overview of SDLC



Stage 1 Planning & Requirement Analysis	Stage 2 Defining Requirements	Stage 3 Design	Stage 4 Development	Stage 5 Testing	Stage 6 Deployment & Maintenace
Planning	Defining	Design	Development	System Testing	Deployment and Maintenace
Define Project Scope	Functional Requirement	HLD	Coding Standard	Manual Testing	Release Planning
Set Objectives and Goals	Technical Requirement	LLD	Scalable Code	Automated Testing	Deployment Automation
Resource Planning	Requirement Reviews & Approved		Version Control		Maintenance
			Code Review		Feedback

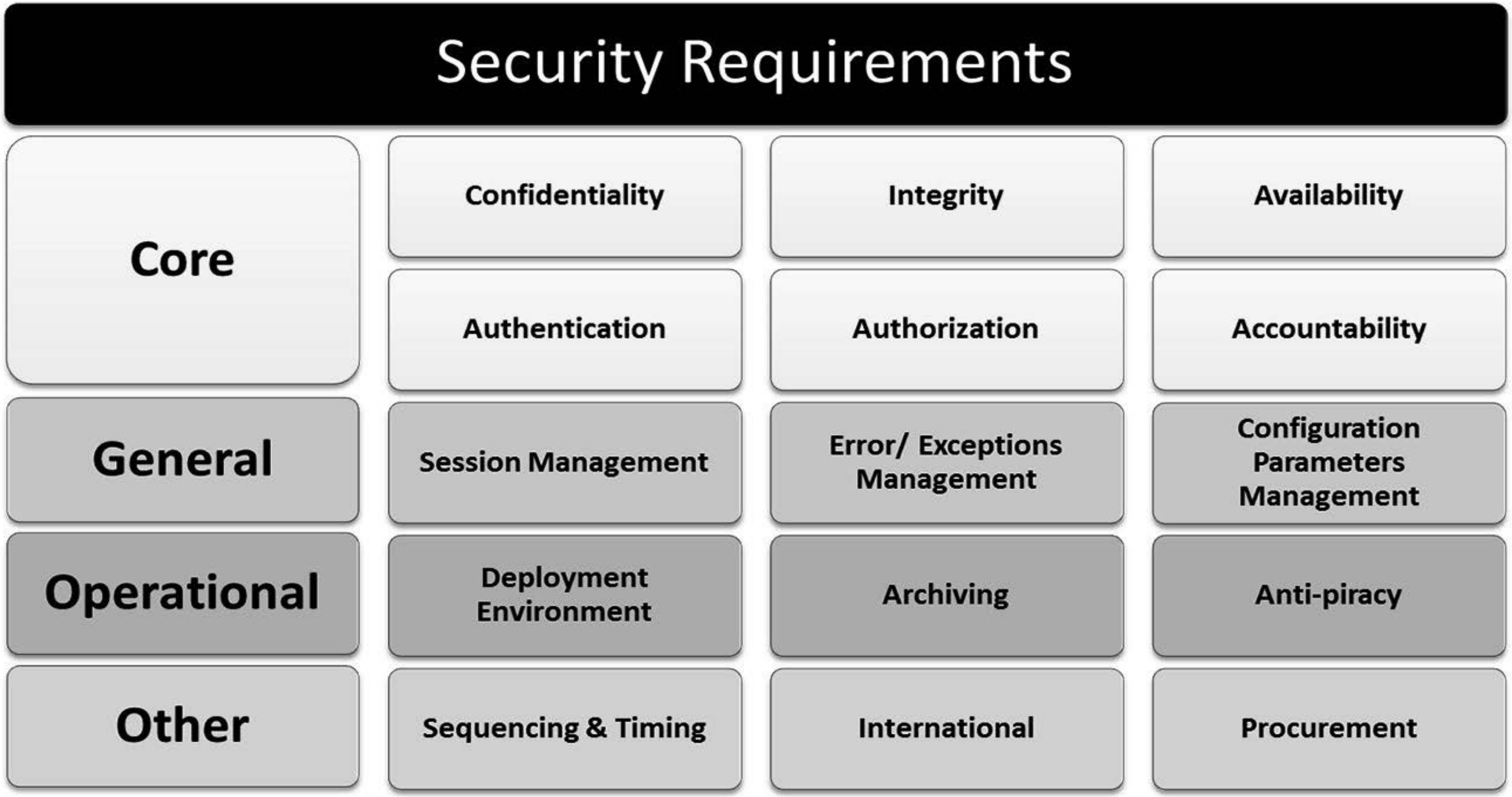
Why is Security Important in the SDLC?

Security related activities are deferred until the testing phase, which is late in the SDLC after most of the critical design and implementation has been completed

Shift Left

Shift Right

Planning and Requirement Stage



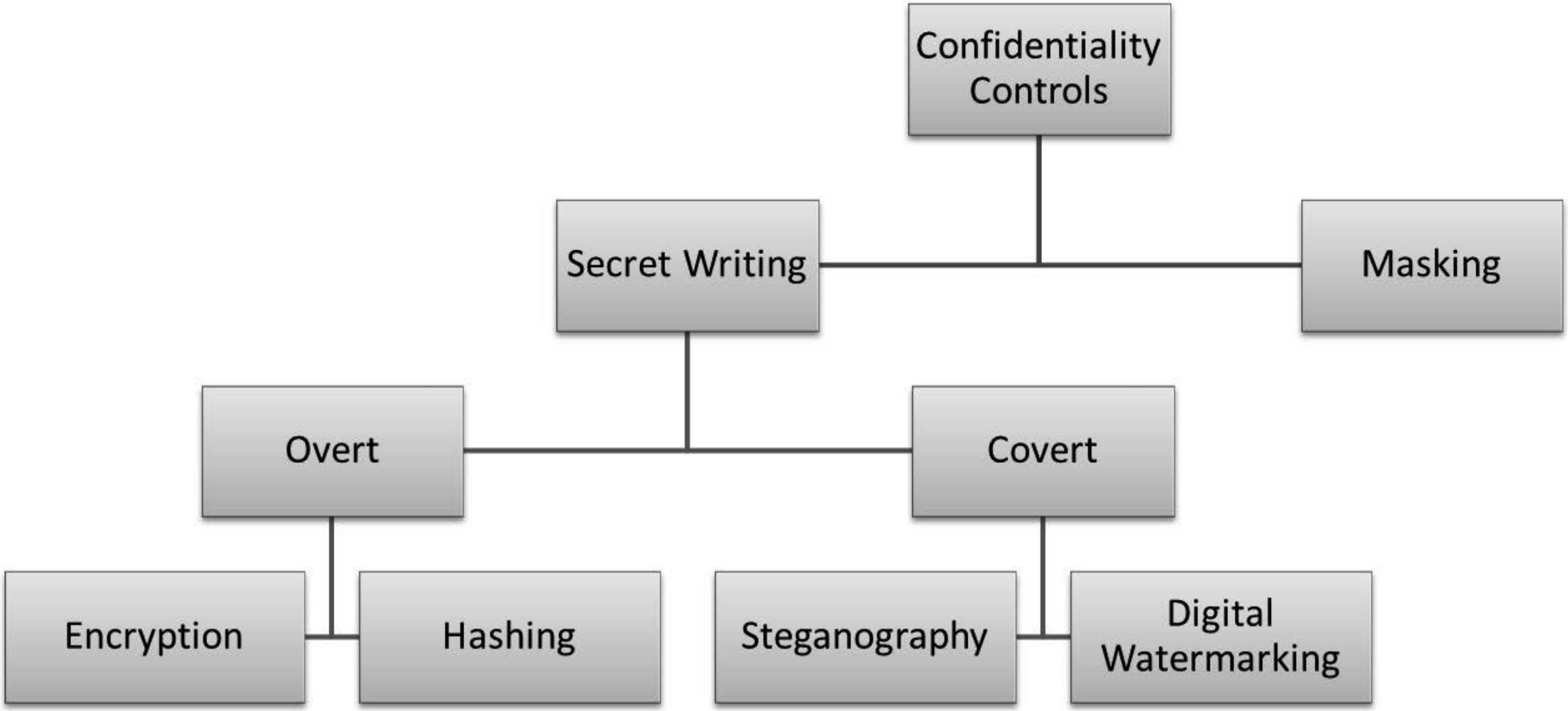
Security Requirements			
Core	Confidentiality	Integrity	Availability
	Authentication	Authorization	Accountability
General	Session Management	Error/ Exceptions Management	Configuration Parameters Management
Operational	Deployment Environment	Archiving	Anti-piracy
Other	Sequencing & Timing	International	Procurement

Confidentiality Requirements (1)

Address protection against the unauthorized disclosure of data or information that are either private or sensitive in nature

- **Data** can be broadly classified into **public** and **non-public data** or information.
- Public data is also referred to as *directory* information.

Confidentiality Requirements (2)



Confidentiality Controls

Secret Writing

Masking

Overt

Covert

Encryption

Hashing

Steganography

Digital Watermarking

Confidentiality Requirements (3)

Secret writing

The goal is to prevent the disclosure of the information deemed secret

- Includes overt cryptographic mechanisms such as encryption and hashing or covert mechanisms such as steganography and digital watermarking

Masking

The original information is either asterisked or X” ed out

- Protect against **shoulder surfing attacks**
- Input fields that take passwords
- The masking of credit card numbers or social security numbers (SSN), except for the last four digits

Confidentiality Requirements (4)

Secret writing

Overt

To make the information humanly indecipherable or unintelligible even if disclosed

- Also commonly referred to as cryptography includes Encryption and Hashing

Covert

The goal of covert secret writing is to hide information within itself or in some other media or form

- The most common forms of covert secret writing are Steganography and Digital Watermarking

Confidentiality Requirements (5)

When Confidentiality Req need to be applied?

In ***Transit***: When the data is transmitted over unprotected networks i.e., data-in-motion.

In ***Processing***: When the data is held in computer memory or media for processing

In ***Storage***: When the data is at rest, within transactional systems as well as non-transactional systems including archives i.e., data- at-rest

Confidentiality Requirements (6)

- “Personal health information must be protected against disclosure using approved encryption mechanisms.”
- “Password and other sensitive input fields need to be masked.”
- “Passwords must not be stored in the clear in backend systems and when stored must be hashed with at least an equivalent to the SHA-256 hash function.”
- “Transport layer security (TLS) such as Secure Socket Layer must be in place to protect against insider man-in-the-middle (MITM) threats for all credit card information that is transmitted.”
- “The use of non-secure transport protocols such as File Transfer Protocol (FTP) to transmit account credentials in the clear to third parties outside your organization should not be allowed.”
- “Log files must not store any sensitive information as defined by the business in humanly readable or easily decipherable form.”

Integrity Requirements (1)

System Integrity

Reliability assurance and protection

- Injection attacks such as SQL injection that makes the software act or respond in a manner not originally designed to is a classic example of system integrity violation

Data Integrity

Prevention against unauthorized modifications

- *Parity bit checking* is useful in the detection of errors or changes made to data when it is transmitted

- *Input validation* provides a high degree of protection against injection flaws and provides both system and data integrity

Integrity Requirements (2)

“All input forms and Querystring inputs need to be validated against a set of allowable inputs before the software accepts it for processing.”

“Software that is published should provide the recipient with a computed checksum and the hash function used to compute the checksum, so that the recipient can validate its accuracy and completeness.”

“All non-human actors such as system and batch processes need to be identified, monitored and prevented from altering data as it passes on systems that they run on, unless explicitly authorized to.”

Availability Requirements (1)

Maximum Tolerable Downtime (MTD)

Measure of the maximum amount of time that the software can be in a state of not providing expected service

Recovery Time Objective (RTO)

Amount of time by which the system or software needs to be restored back to the expected state of business operations

- MTD are sometimes are referred to as Maximum Tolerable Period of Disruption (MTPD)

- Adverse effects of software downtime through **Business Impact Analysis (BIA**)

Availability Requirements (2)

“Software and data should be replicated across data centers to provide load balancing and redundancy.”

“Mission critical functionality in the software should be restored to normal operations within 1 hour of disruption; mission essential functionality in the software should be restored to normal operations within 4 hours of disruption; and mission support functionality in software should be restored to normal operations within 24 hours of disruption.”

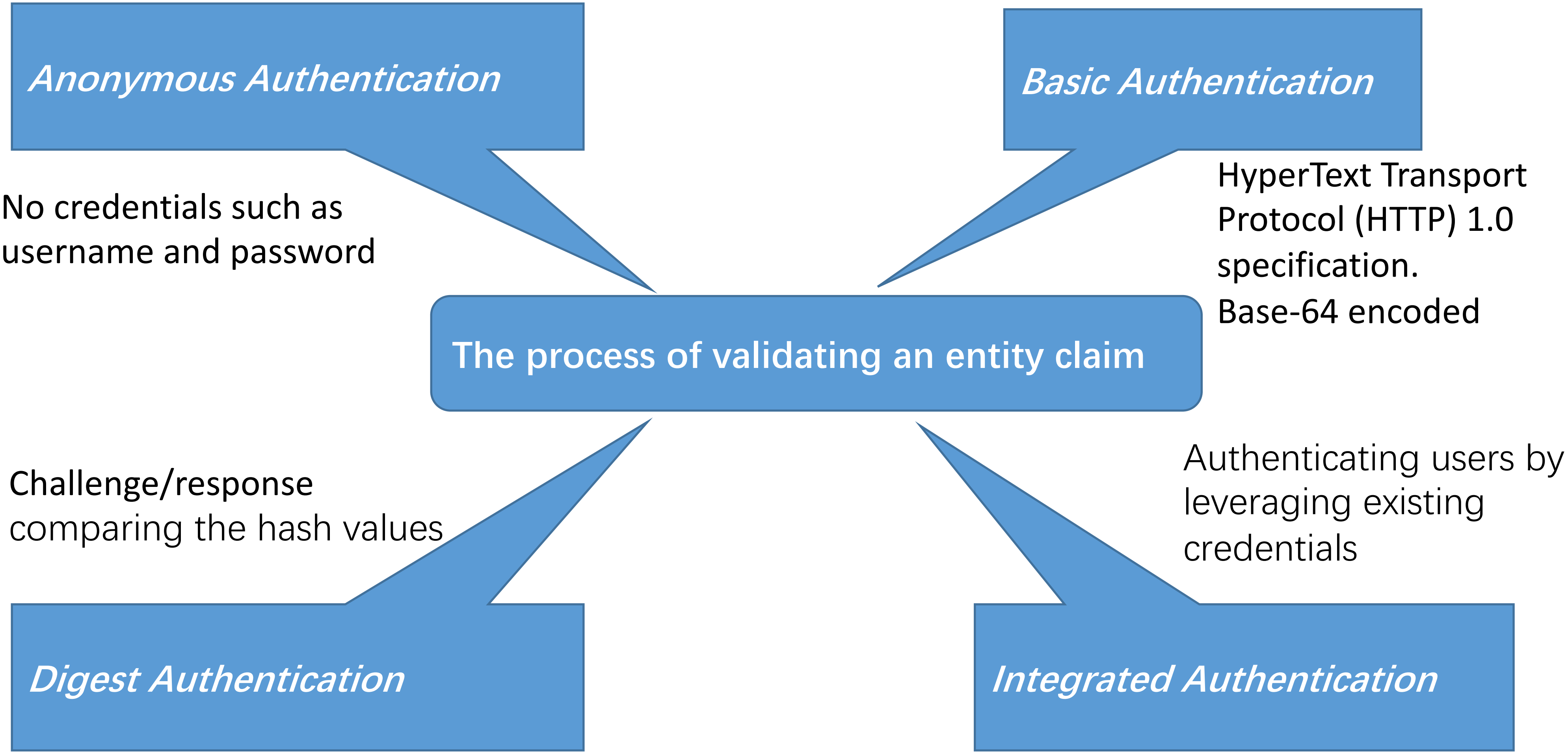
“The software shall ensure high availability of five nines (99.999%) as defined in the SLA.”

Authentication Requirements (1)

The process of validating an entity claim

- Anonymous
- Basic
- Digest
- Integrated
- Client certificates
- Forms
- Token
- Smart cards
- Biometrics

Authentication Requirements (2)



Anonymous Authentication

No credentials such as username and password

Basic Authentication

HyperText Transport Protocol (HTTP) 1.0 specification.

Base-64 encoded

The process of validating an entity claim

Challenge/response comparing the hash values

Digest Authentication

Authenticating users by leveraging existing credentials

Integrated Authentication

Authentication Requirements(3)

Client Certificate-Based Authentication

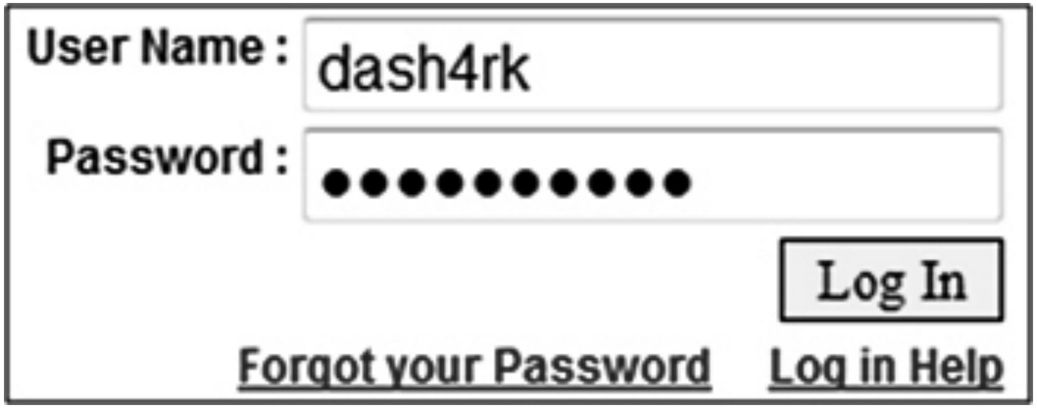
- By validating the identity of the certificate holder
- A trusted Certificate Authority (CA) issues a **client certificate** to the client.
- The certificate contains the client public key and identity information, and it is signed by the CA

- These certificates are usually in the form of digital certificates and the current standard for digital certificates is ITU X.509 v3

Authentication Requirements (4)

Forms Authentication

- Requires the user to supply a username and password



User Name : dash4rk

Password : ●●●●●●●●●●

Authentication Requirements (5)

Token-Based Authentication

- Used in conjunction with Forms authentication where a username and password is supplied for verification
- Upon verification, a token is issued to the user who supplied the credentials
- This is particularly useful in single sign on (SSO) situations

Authentication Requirements (6)

Smart Cards-Based Authentication

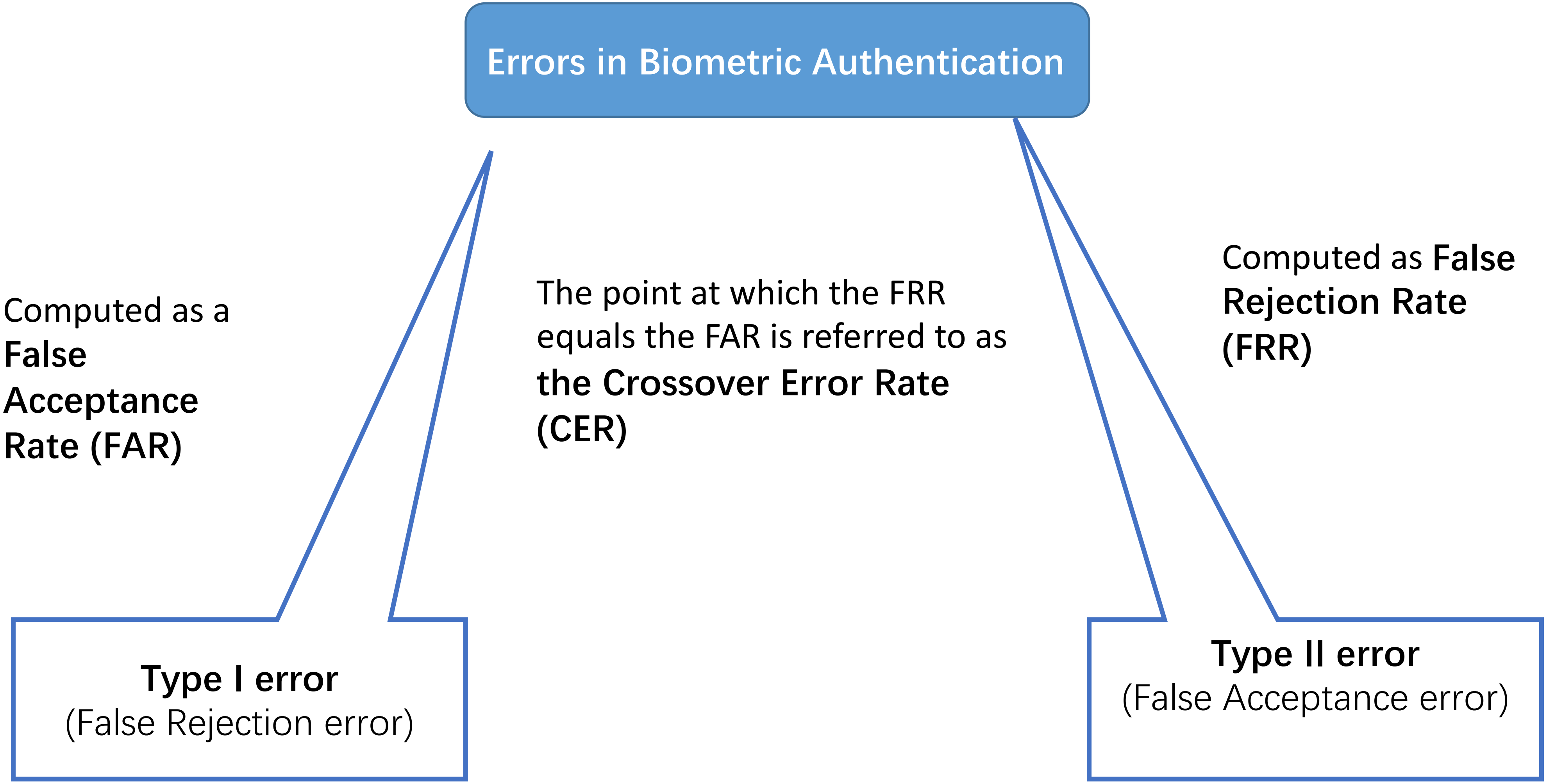
- Smart cards provide ownership (something you have)
- Major Advantage??
- Serious Disadvantage??

Authentication Requirements (7)

Biometric Authentication

- Uses biological characteristics (something you are) for providing the identity credentials
- biometric authentication requires physical access which limits its usage in remote access settings
- one of the major drawbacks of biometric based authentication implementation is that the original enrollment may no longer be valid

Authentication Requirements (8)



Errors in Biometric Authentication

Computed as a **False Acceptance Rate (FAR)**

The point at which the FRR equals the FAR is referred to as **the Crossover Error Rate (CER)**

Computed as **False Rejection Rate (FRR)**

Type I error
(False Rejection error)

Type II error
(False Acceptance error)

Authentication Requirements

“The software will be deployed only in the intranet environment and the authenticated user should not have the need to provide username and password once they have logged on to the network.”

“The software will need to support single sign on with 3rd party vendors and suppliers that are defined in the stakeholder list.”

“Both intranet and Internet users should be able to access the software.”

“The authentication policy warrants the need for two- or multi- factor authentication for all financially processing software.”

Authorization Requirements

Layered upon authentication, authorization requirements are those that confirm that an authenticated entity has the needed rights and privileges to access and perform actions on a requested resource

- CRUD operations, which stand for **Create, Read, Update or Delete** data

Authorization Requirements

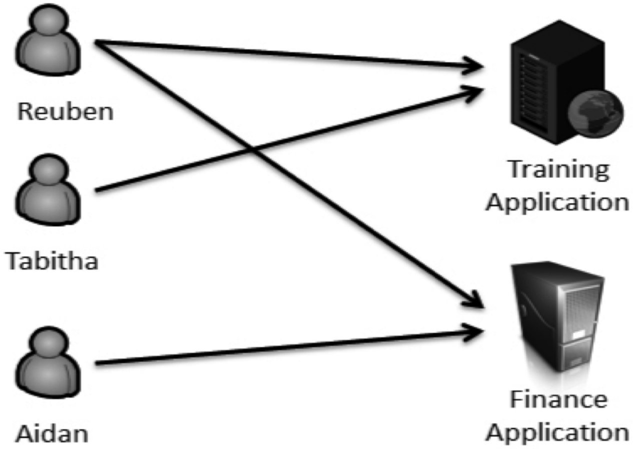
Access control models are primarily of the following types:

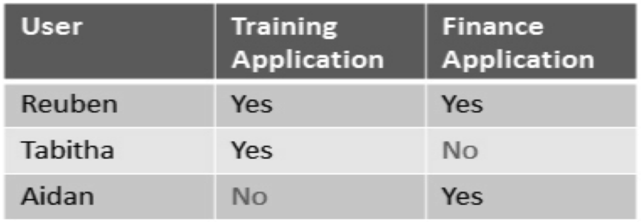
- Discretionary Access Control (DAC)
- Non-Discretionary Access Control (NDAC)
- Mandatory Access Control (MAC)
- Role-Based Access Control (RBAC)
- Resource-Based Access Control

Authorization Requirements

Discretionary Access Control (DAC)

- Means of restricting access to objects based on the identity of subjects and/or groups to which they belong
- Subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject





User	Training Application	Finance Application
Reuben	Yes	Yes
Tabitha	Yes	No
Aidan	No	Yes

Authorization Requirements

Non-Discretionary Access Control (DAC)

- System enforcing the security policies
- Does not rely on the subject compliance with security policies. it is unavoidably imposed on all subjects
- The system security policies and mechanisms configured by the systems or security administrators are enforced and tamperproof

Authorization Requirements

Mandatory Access Control (MAC)

- Access to objects is restricted to subjects based on the sensitivity of the information contained in the object
- The sensitivity is represented by a label
- MAC requires sensitivity labels for all the objects and clearance levels for all subjects and access is determined based on matching a subject clearance level with the object sensitivity level

Rule-based access control.

the access decision is based on a list of rules that are created or authorized by system owners who specify the privileges (i.e., read, write, execute, etc.) that the subjects (users) have on the objects (resources).

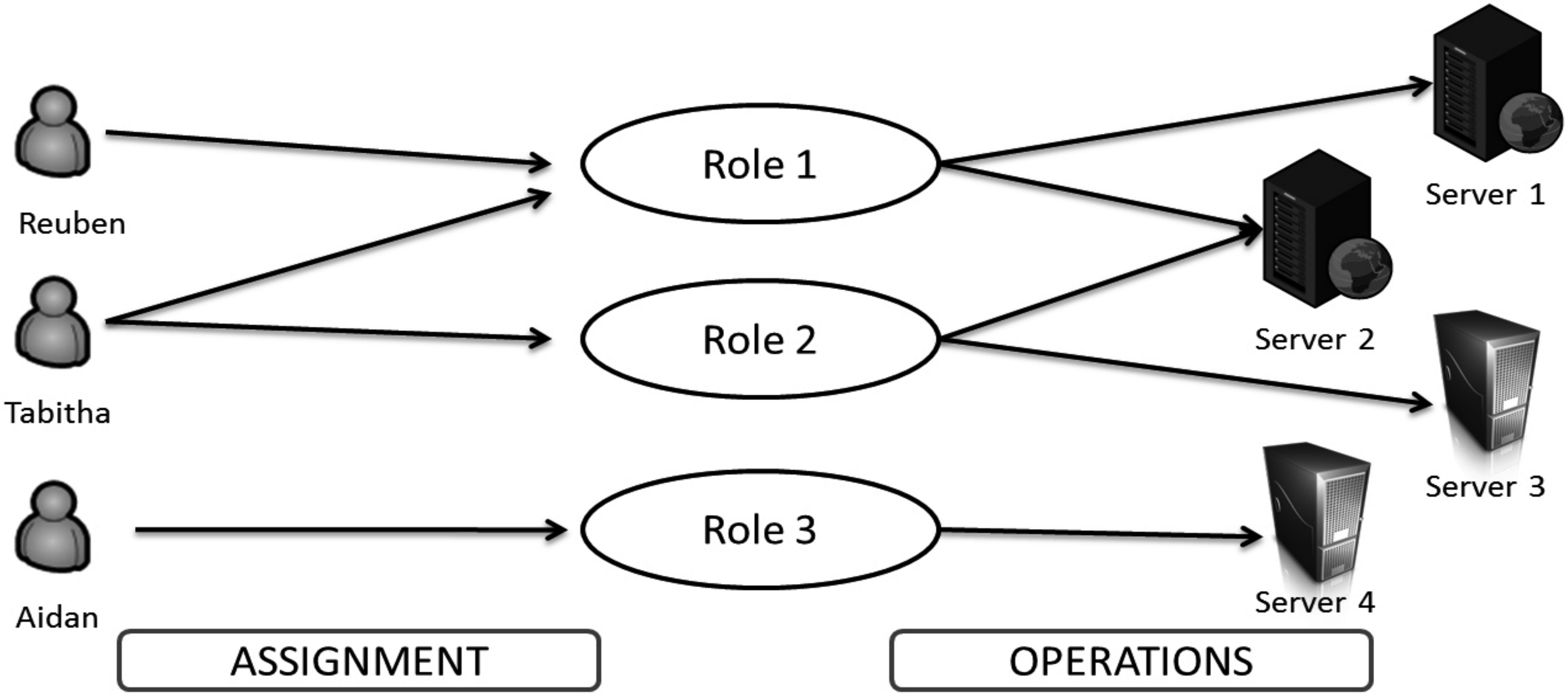
Authorization Requirements

Role-Based Access Control (RBAC)

- Individuals (subjects) have access to a resource (object) based on their assigned role
- Roles are defined by job function which can be used for authorization decisions.
- Roles define the trust levels of entities to perform desired operations. These roles may be user roles or service roles.

Authorization Requirements

Role-Based Access Control (RBAC)



Authorization Requirements

RBAC in Relation to Least Privilege and Separation of Duties

- Roles support the principle of least privilege, since roles are given just the needed privileges to undertake an operation against a resource

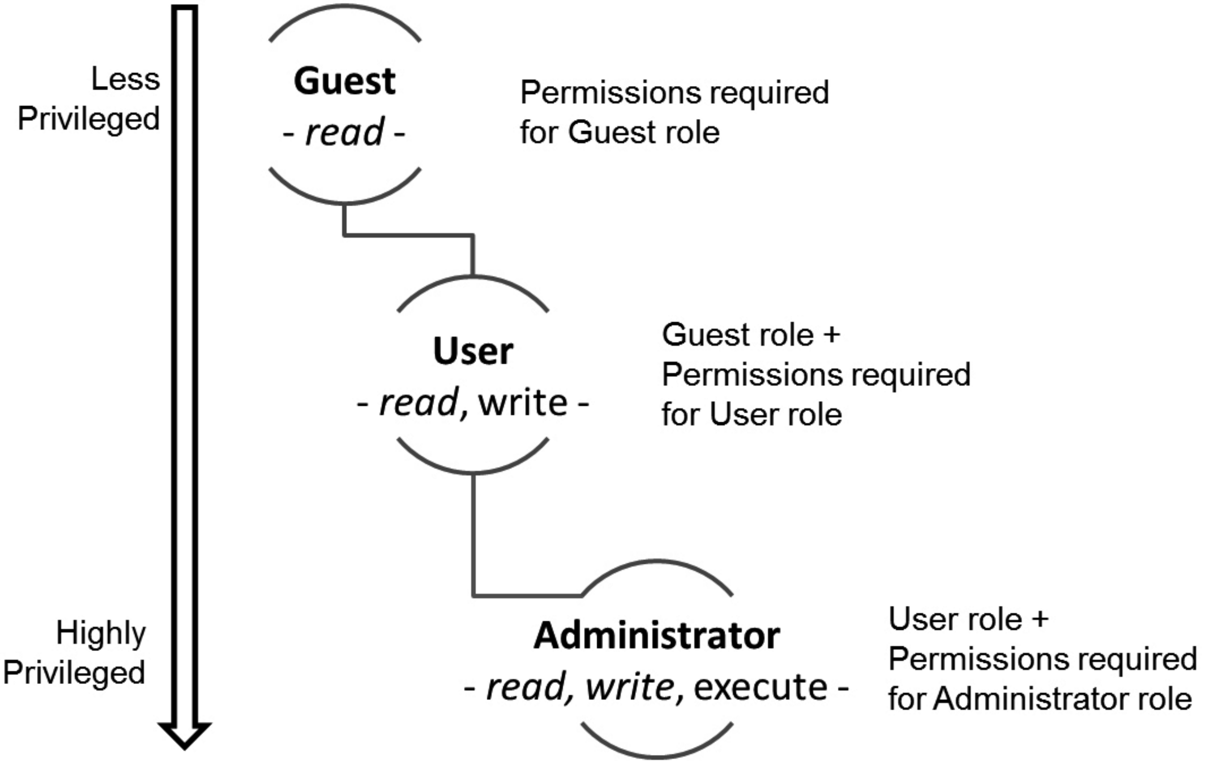
- No individual can be assigned to two roles that are mutually exclusive in their permissions to perform operations

The real benefit of RBAC over other access control methods includes the following:

- Simplified subjects and objects access rights administration
- Ability to represent the organizational structure
- Force enterprise compliance with control policies more easily and effectively.

Authorization Requirements

Role Hierarchies



Authorization Requirements

Resource-Based Access Control

- When the list of all users of your software are not known in advance, access can also be granted based on the resources

- Impersonation and Delegation Model
- Trusted Subsystem Model

Authorization Requirements

Impersonation and Delegation Model

- Allowing a secondary entity to act on one’s behalf is the principle of delegation.
- The secondary entity is considered to impersonate the identity of the primary entity when the complete sets of permissions of the primary entity are assigned to it
- **Kerberos** uses the delegation and impersonation model where the user upon successful authentication is granted a Kerberos ticket and the ticket is delegated the privileges and rights (sets of permission

Trusted Subsystem Model

- Access request decisions are granted based on the identity of a resource that is trusted instead of user identities
- A user logs into their bank account using a web browser to transfer funds from one account to another. The web application identity calls the database to first authenticate the user supplied credentials. It is not the user identity that is checked but the web application identity that is trusted and that can invoke the call to the database

Authorization Requirements

Access to highly sensitive secret files will be restricted to users with secret or top secret clearance levels only.”

“User should not be required to send their credentials each and every time once they have authenticated themselves successfully.”

“All unauthenticated users will inherit read-only permissions that are part of guest user role while authenticated users will default to having read and write permissions as part of the general user role. Only members of the administrator role will have all rights as a general user in addition to having permissions to execute operations.”

Accountability Requirements

Accountability Requirements

- The identity of the subject (user or process) performing an action (who)
- The action (what)
- The object on which the action was performed (where)
- The timestamp of the action (when)

Accountability Requirements

“All failed logon attempts will be logged along with the timestamp and the Internet Protocol address where the request originated.”

“A before and an after snapshot of the pricing data that changed when a user updates the pricing of a product must be tracked with the following auditable fields – identity, action, object and timestamp.”

“Audit logs should always append and never be overwritten.”

“The audit logs must be securely retained for a period of 3 years.”

Questions??

zubair.ahmad@giki.edu.pk

Office: G14 FCSE lobby