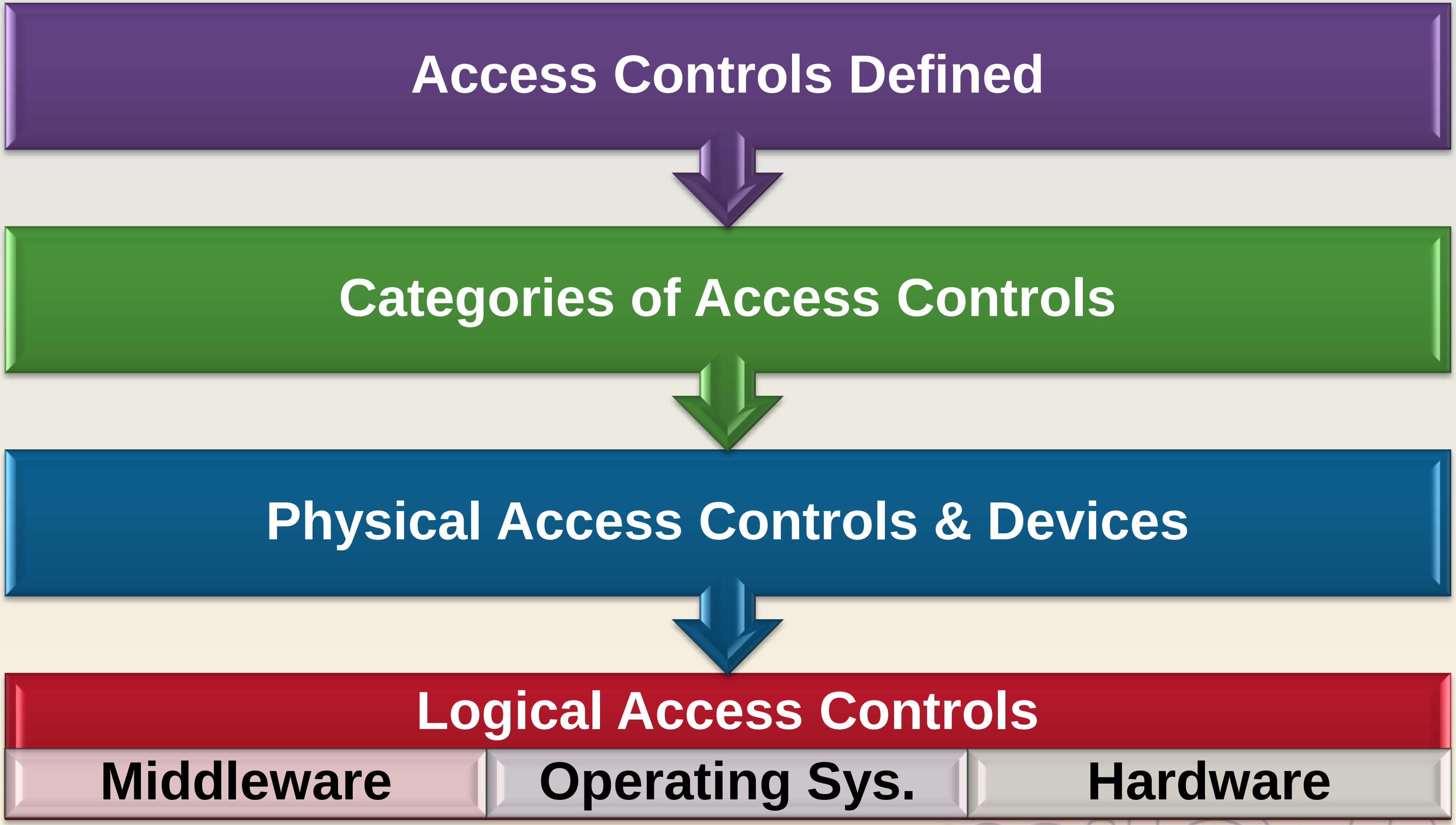
ACCESS CONTROLS

Overview



Access Controls Defined

Categories of Access Controls

Physical Access Controls & Devices

Logical Access Controls

Middleware

Operating Sys.

Hardware

Role of Access Control

Access Control

- Collection of controls to limit and control system access
  - Access to assets, information, or configuration features
- Access can be based on identity, group membership, clearance, need-to-know, physical and logical location, and more
- Controls are used to protect against unauthorized disclosure, corruption, destruction, or modification

Definitions

Subject

- Active entity that accesses an object
- Generally initiates the flow of data
- Usually changes state of system

Object

- Passive entity that is accessed by a subject
- Contains or receives data

Access

- Data that flows from an object to a subject
- Ability to “do something” with an object
  - Read, modify, delete, create, execute

Access Control

- Controlling how subjects and objects interact

More Definitions

Access Privileges

- Permissions defining the extent of access a subject has to an object
- Defines circumstances in which these permissions can be used

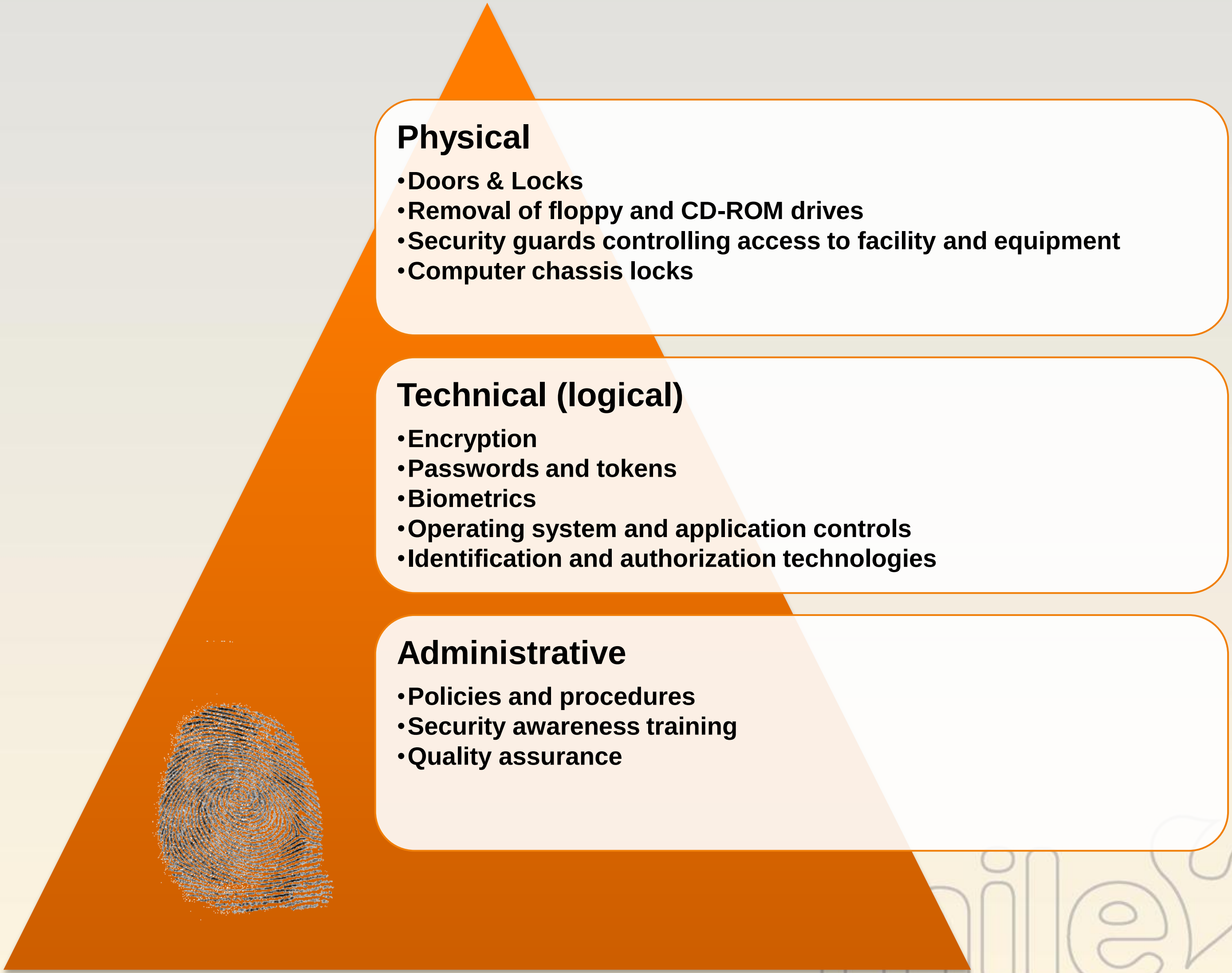
Access Rules

- Statements specifying subject’s access rights
- Enforcement of security policies and business objectives
- Collectively referred to as user profiles
- Enforced through software

Access Path

- Path that request travels through
- Can be through different layers of software
- Mechanisms that can be bypassed in layers should also be seen as part of the path

Categories of Access Controls



Physical

- Doors & Locks
- Removal of floppy and CD-ROM drives
- Security guards controlling access to facility and equipment
- Computer chassis locks

Technical (logical)

- Encryption
- Passwords and tokens
- Biometrics
- Operating system and application controls
- Identification and authorization technologies

Administrative

- Policies and procedures
- Security awareness training
- Quality assurance

Physical Controls

Physical Controls

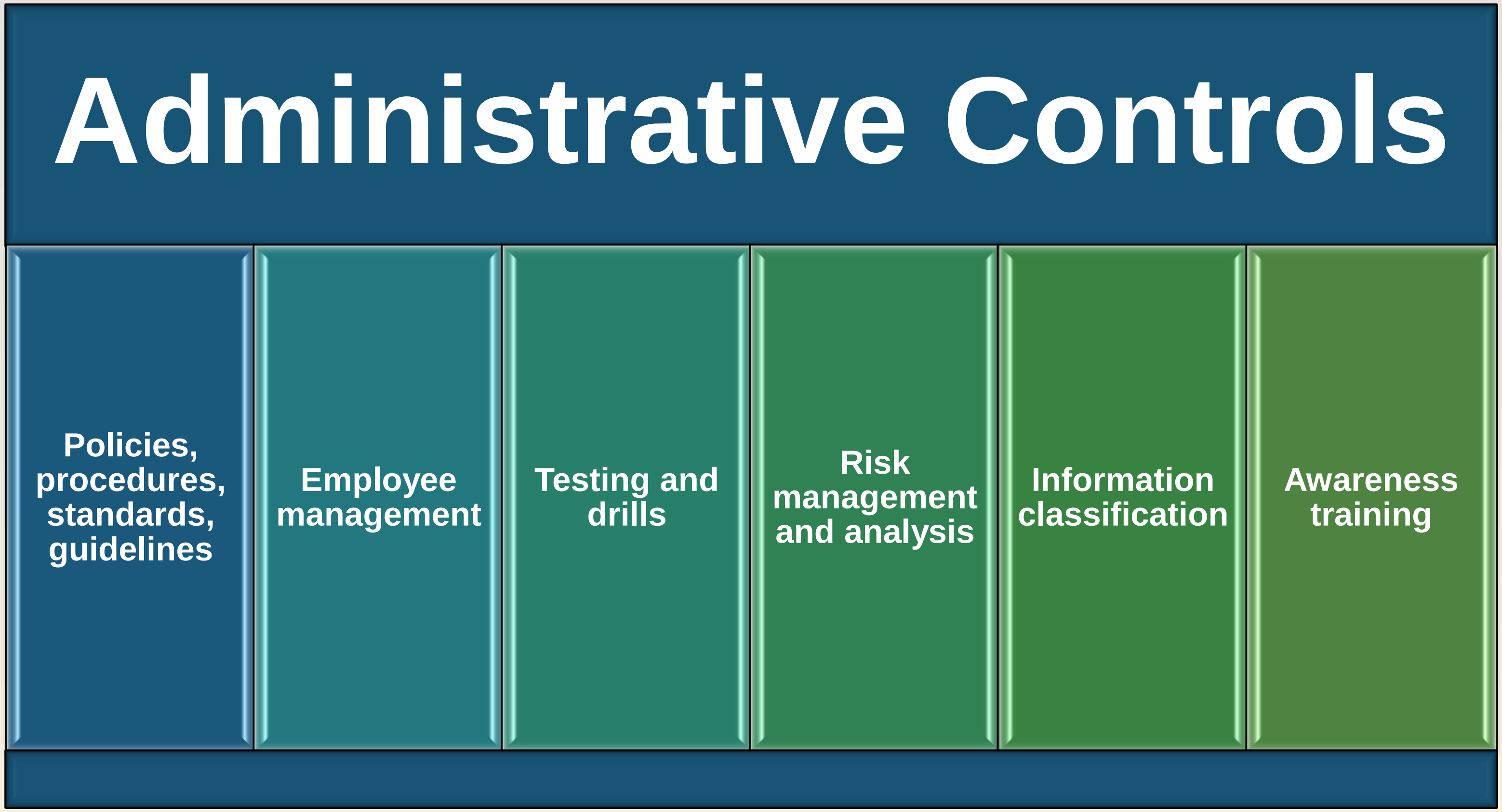
- Doors, windows, walls
- Security guards and dogs
- Fencing and lighting
- Locks
- Environmental controls
- Intrusion detection systems

Logical Controls

Technical Controls

- Firewalls
- IDS
- Encryption
- Protocols
- Authentication mechanisms
- Auditing
- Access control technologies

“Soft” Controls



Administrative Controls

- Policies, procedures, standards, guidelines
- Employee management
- Testing and drills
- Risk management and analysis
- Information classification
- Awareness training

Security Roles

Data Owner

- Responsible for subset(s) of data and data classification
- Sets security requirements for data protection

System Owner

- Responsible for specific computer system(s)
- One system will have one system owner
  - Can hold data from several data owners

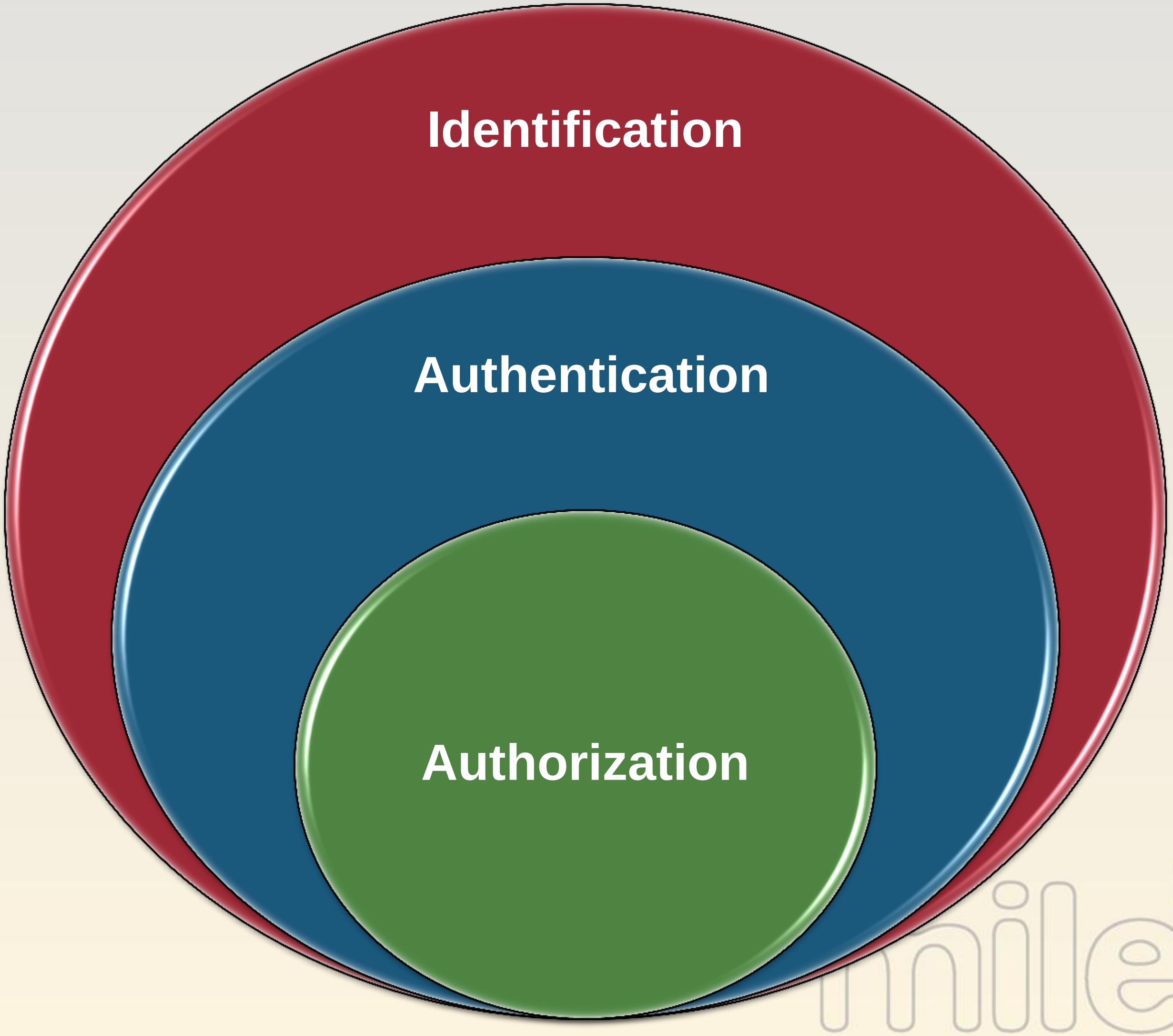
Data Custodian

- Is delegated data maintenance tasks
- Required to implement and maintain controls to provide the protection level dictated by data owner

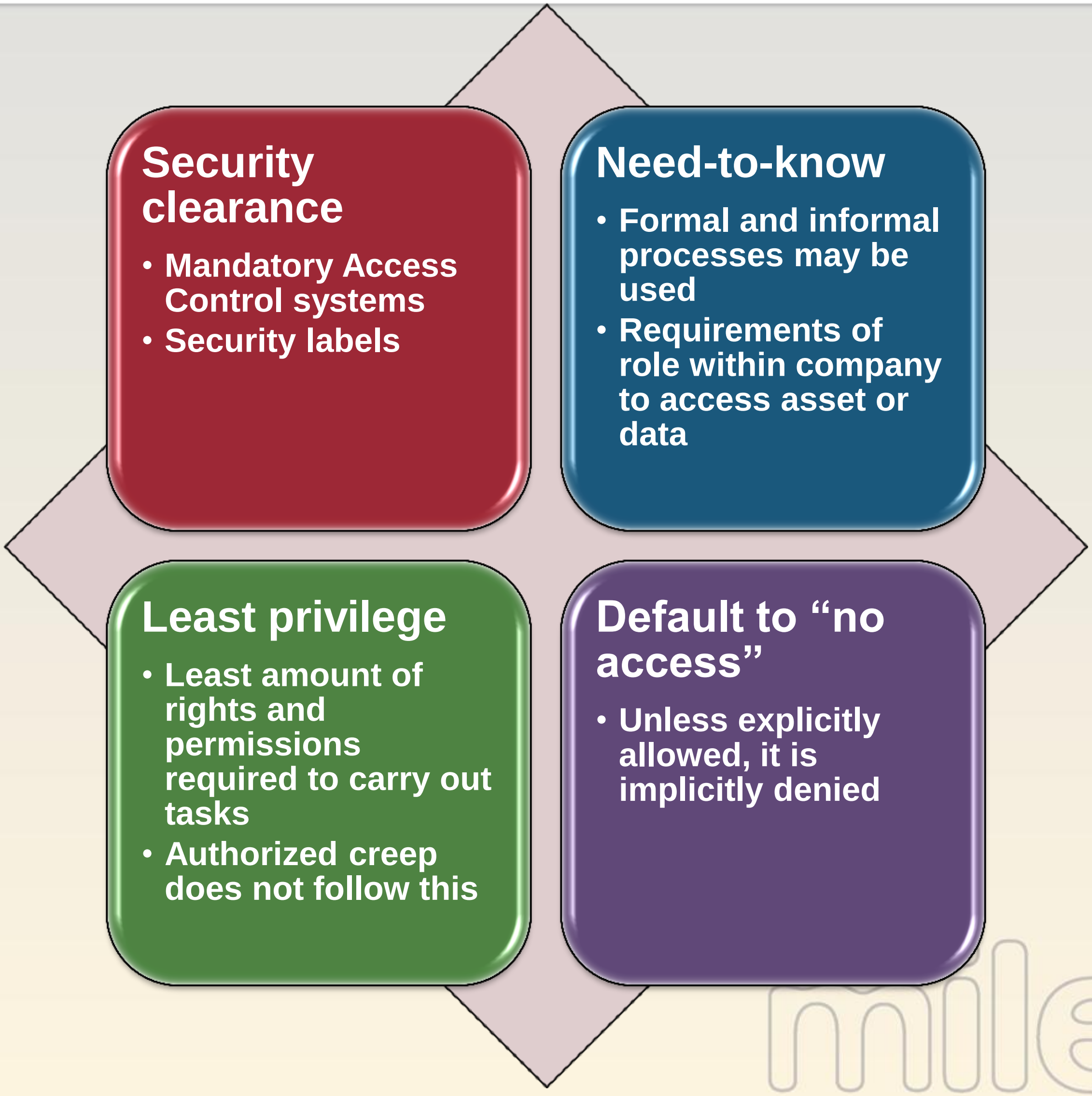
User

- Person who routinely uses company data for work-related tasks

Steps to Granting Access



Access Criteria



Security clearance

- Mandatory Access Control systems
- Security labels

Need-to-know

- Formal and informal processes may be used
- Requirements of role within company to access asset or data

Least privilege

- Least amount of rights and permissions required to carry out tasks
- Authorized creep does not follow this

Default to "no access"

- Unless explicitly allowed, it is implicitly denied

Physical Access Control Mechanisms

Mechanism	Examples
Biometrics	Retina Scan, Fingerprint, Voice Print
Token Devices	Synchronous and Asynchronous Devices
Memory Cards	ATM Cards, Proximity Card
Smart Cards	Credit Cards, Identification Card
Cryptographic Keys	Private Key

Biometric System Types

Biometric Type	Description
Fingerprint	Ridge Endings and Bifurcations = Minutiae
Finger Scan	Same as Fingerprint but extracting a smaller amount of Data
Palm Scan	All prints from Fingers and Creases, Ridges and Grooves from the Palm
Hand Geometry	Shape of (length and width) Hand and Fingers
Retina Scan	Blood Vessel Pattern of Retina on Back of Eyeball
Iris Scan	Colored portion of Eye that Surrounds the Pupil
Signature Dynamics	Captures Electrical Signals of Signature Process
Keyboard Dynamics	Captures Electrical Signals of Typing Process
Voice Print	Distinguishes Differences in Sounds, Frequencies and Patterns
Facial Scan	Bone Structure, Nose Ridges, Forehead Size and Eye Width
Hand Topology	Side-View of Hand, Reviewing Size and Width

Synchronous Token

Token Device Characteristics

- Token device and authentication service are synchronized
  - Time or event

- Device generates a password, which is displayed to the user.
- User types in value and identification data into login screen.
- One-time password is part of credential set sent to authentication server.
- Authentication server is expecting a specific value.
  - Expected value received = authenticated
  - Different value received = rejected

Asynchronous Token Device

Asynchronous One-Time Password Generator

- Based on challenge/response mechanisms
  - Random value is sent from authentication server to the user
  - User enters value into token device
  - Token device hashes or encrypts value and provides the result to the user
  - User uses this result as a one-time password and sends it to the authentication server
    - Expected value received = authenticated
    - Different value received = rejected

Memory Cards

Memory Card Characteristics

- Magnetic strip that holds data and cannot *process* data
  - Anyone with a reader can view data held on strip if not encrypted
- No microprocessor or integrated circuits
- Proximity cards, credit cards, ATM cards
- Added costs compared to other authentication technologies
  - Reader purchase
  - Card generation and maintenance

Smart Card

Smart Card Characteristics

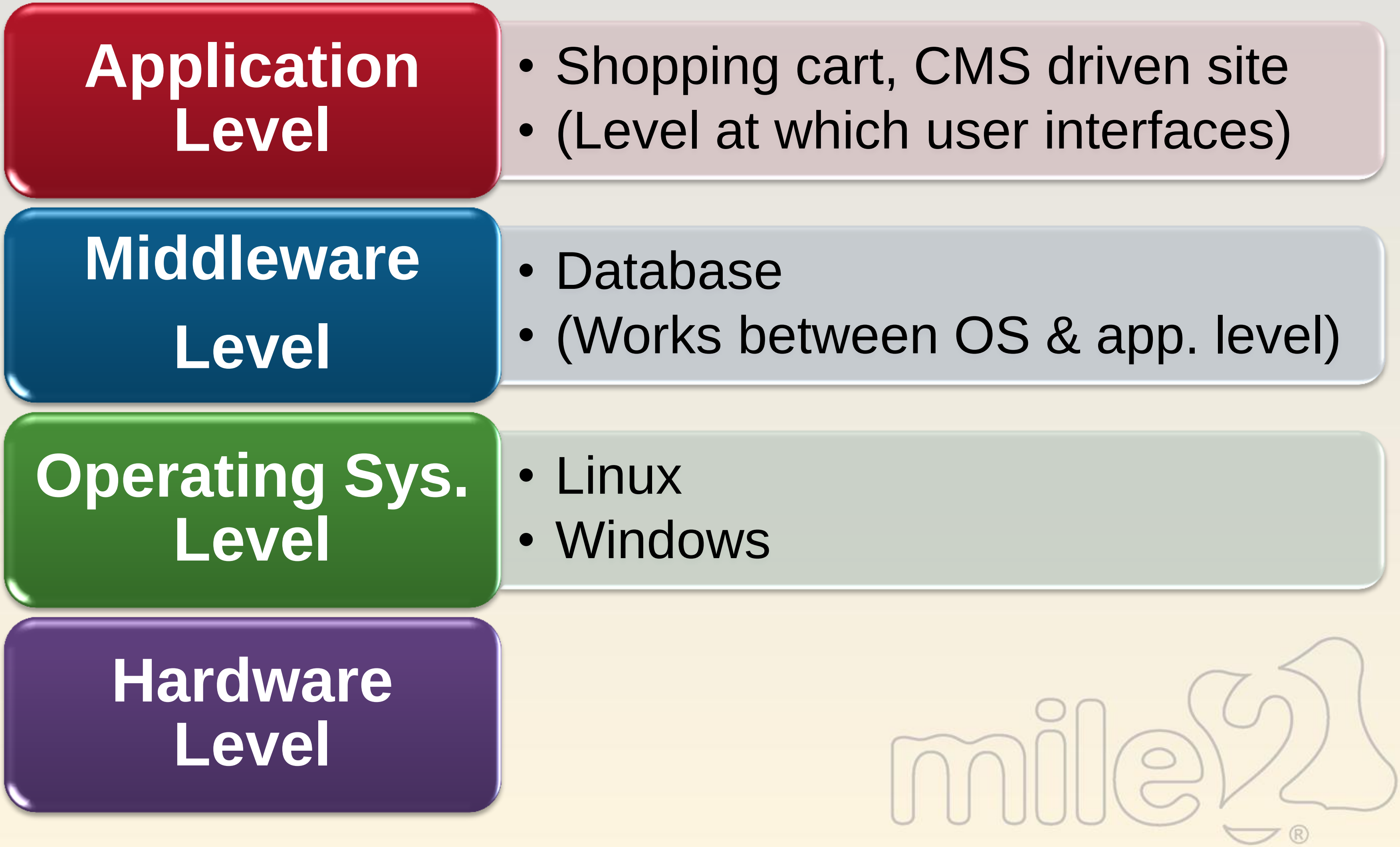
- Microprocessor and integrated circuits
  - Holds and processes data
- Tamperproof device
  - After a threshold of failed login attempts, it can render itself unusable
- PIN or password “unlocks” smart card functionality
- Smart card could be used for:
  - Holding biometric data in template
  - Responding to challenge
  - Holding private key
  - Holding user work history, medical information, money, etc.
- Added costs compared to other authentication technologies
  - Reader purchase
  - Card generation and maintenance

Cryptographic Keys

Authentication Through Cryptographic Mechanisms

- Asymmetric keys are used for authentication in some implementations
  - Private key
  - Digital signature = encrypting a hash value with the private key
- No secret information has to be shared between entities
- Challenge can be sent to user, which is encrypted with her private key for authentication

Logical Access Controls



Application Level

- Shopping cart, CMS driven site
- (Level at which user interfaces)

Middleware Level

- Database
- (Works between OS & app. level)

Operating Sys. Level

- Linux
- Windows

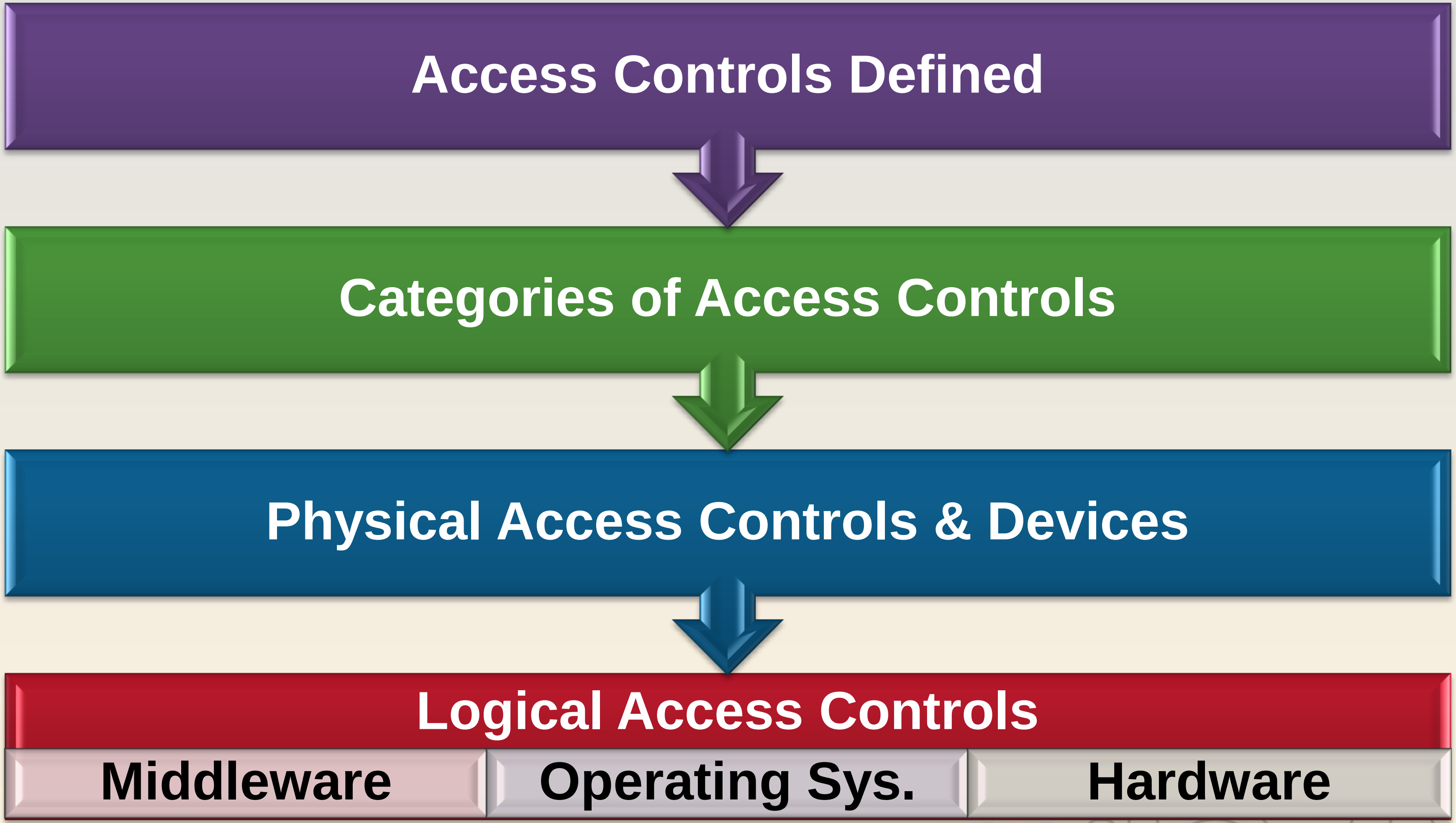
Hardware Level

OS Access Controls

Operating systems maintain access controls by means of:

- **Groups**
- **Roles**
- **Access Control Lists (ACL)**

Review



Access Controls Defined

Categories of Access Controls

Physical Access Controls & Devices

Logical Access Controls

Middleware | Operating Sys. | Hardware