Information Security

Lecture 1: Introduction to Information Security

Mona Taghavi

LaSalle College
Montréal

What is security?

- Security is the protection of assets from harm
  - Physical security (prevent burglary and theft of property)
  - Societal security (security of critical infrastructures)
  - National security (political stability and national integrity)
  - Safety (security of life and health)
  - Environmental security (stop pollution and invasive species)
  - Information security and data protection

What is Information Security?

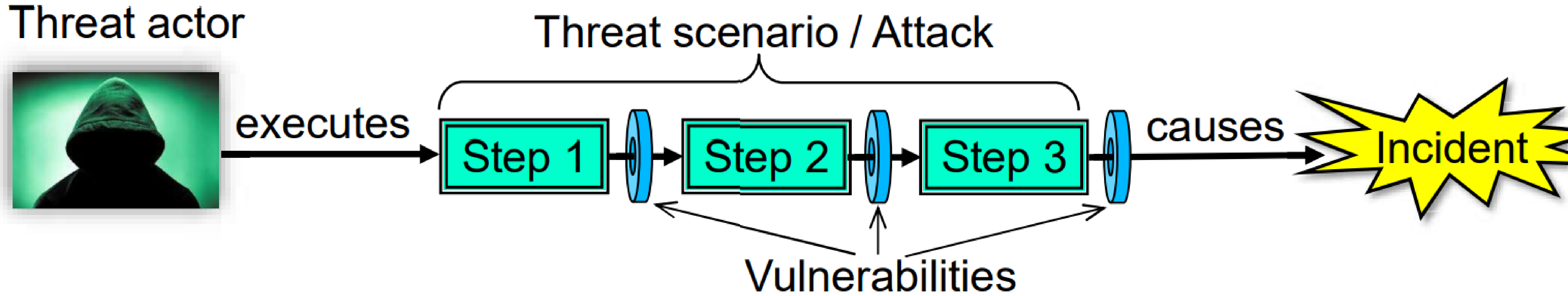
- Information Security is the protection of information assets from damage or harm
- What are the assets to be protected?
  - Example: data files, software, IT equipment and infrastructure
- Covers both intentional and accidental events
  - Threat agents can be humans or acts of nature
  - People can cause harm by accident or by intent
- Information Security defined:
  - The preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved. (ISO27000 Information Security Management Systems - Overview and Vocabulary)

Information Security Management

- IS management consists of activities to control and reduce risk of damage to information assets IS management focuses on:
  - Evaluate threats, vulnerabilities and risks Control security risks by reducing vulnerability to threats
  - Detection and response to attacks
  - Recovery from damage caused by attacks
  - Investigate and collect evidence about incidents (forensics)

Threat

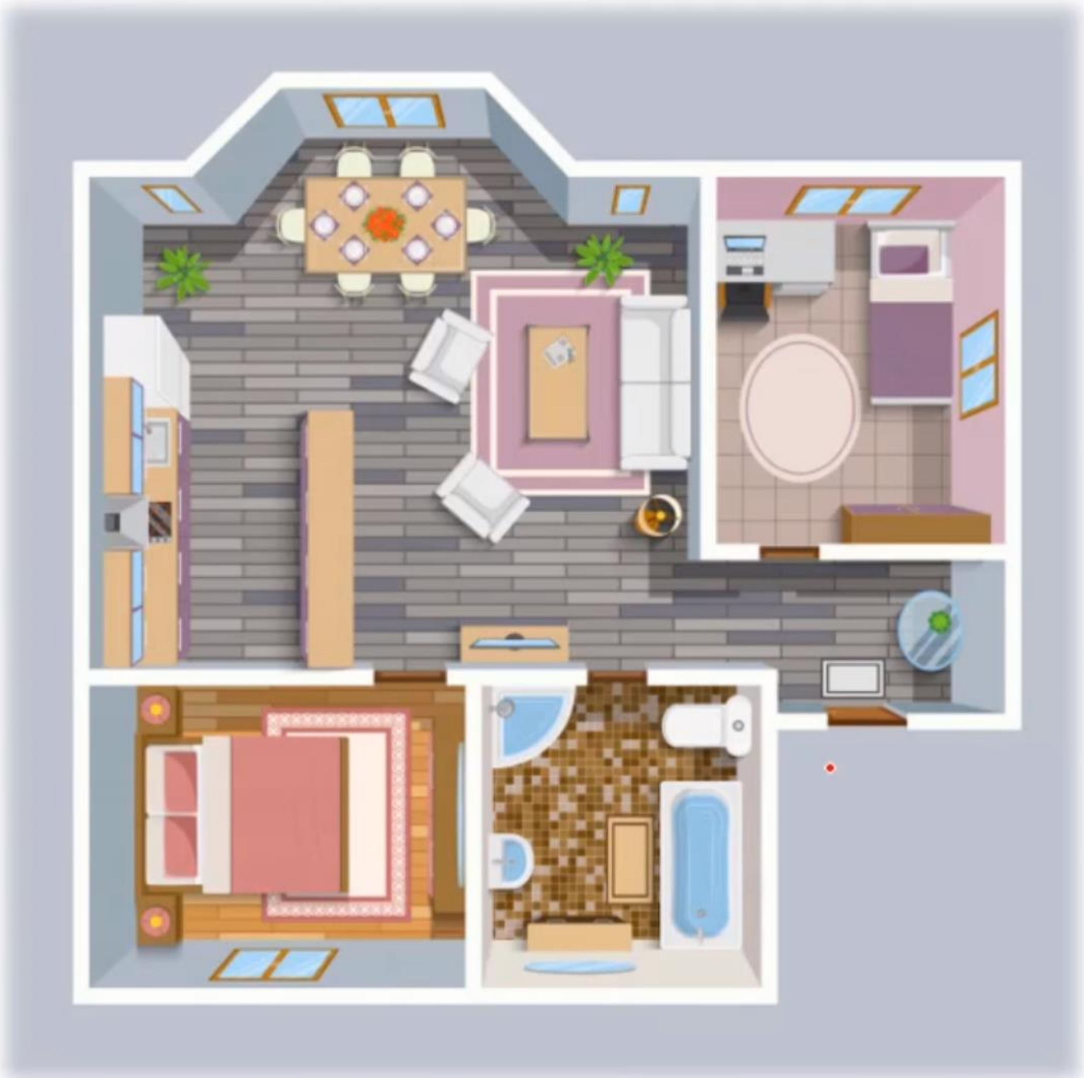
- Threat Actor: An active entity which can execute a threat scenario.
- Threat Scenario: The set of steps executed in a (potential) cyber attack.



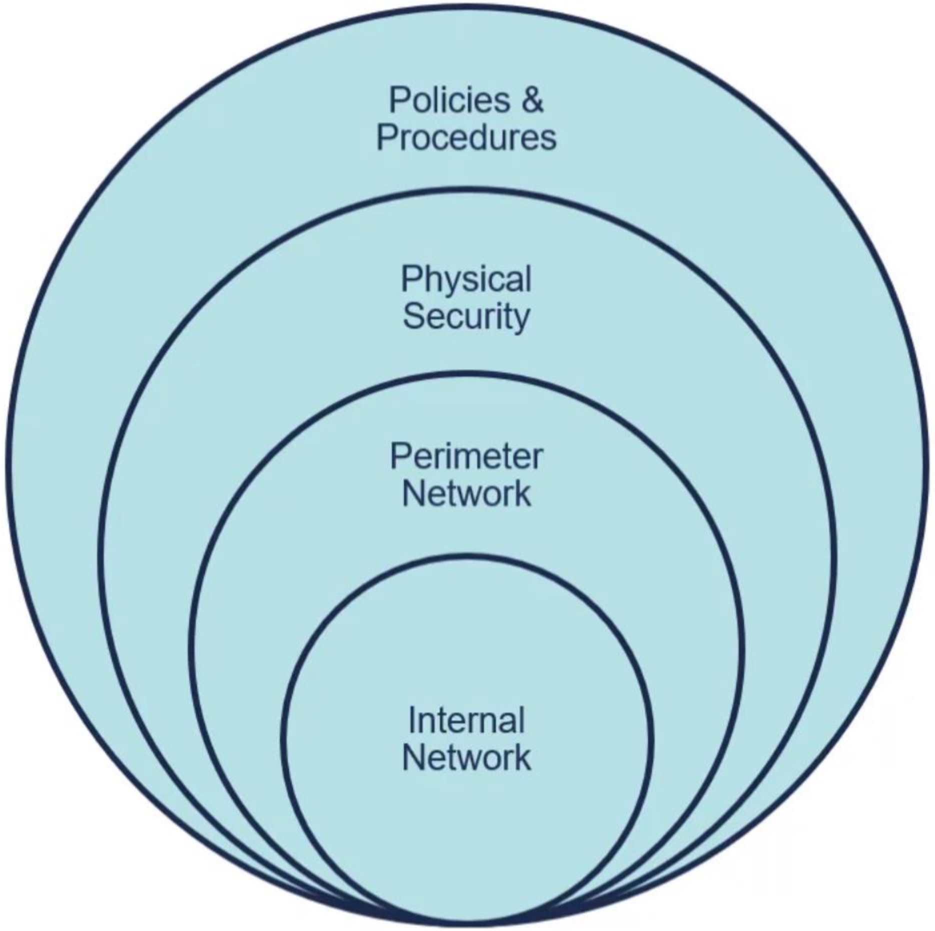
Vulnerability, Risk and Control

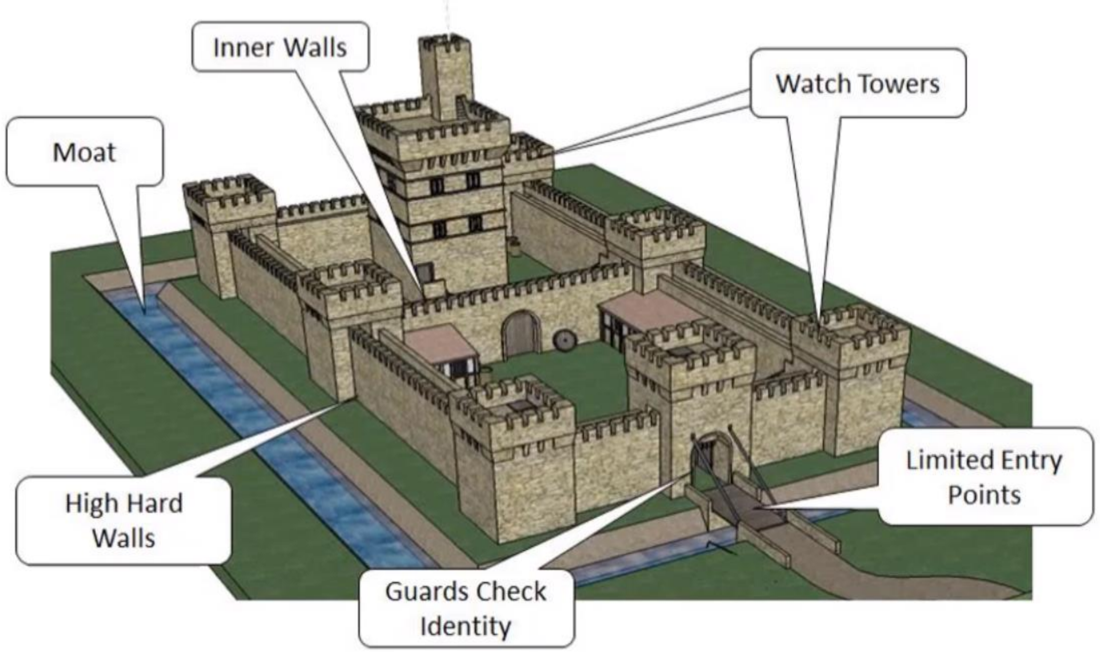
- **Vulnerabilities:** Weaknesses or opportunities allowing a threat scenario to be executed
- **Security Risk:** Likelihood (ease of executing a threat scenario), combined with the potential damage in case of an incident (successful attack)
- **Security Control:** A method for removing vulnerabilities and reducing security risk

Identify vulnerabilities, risk and control:

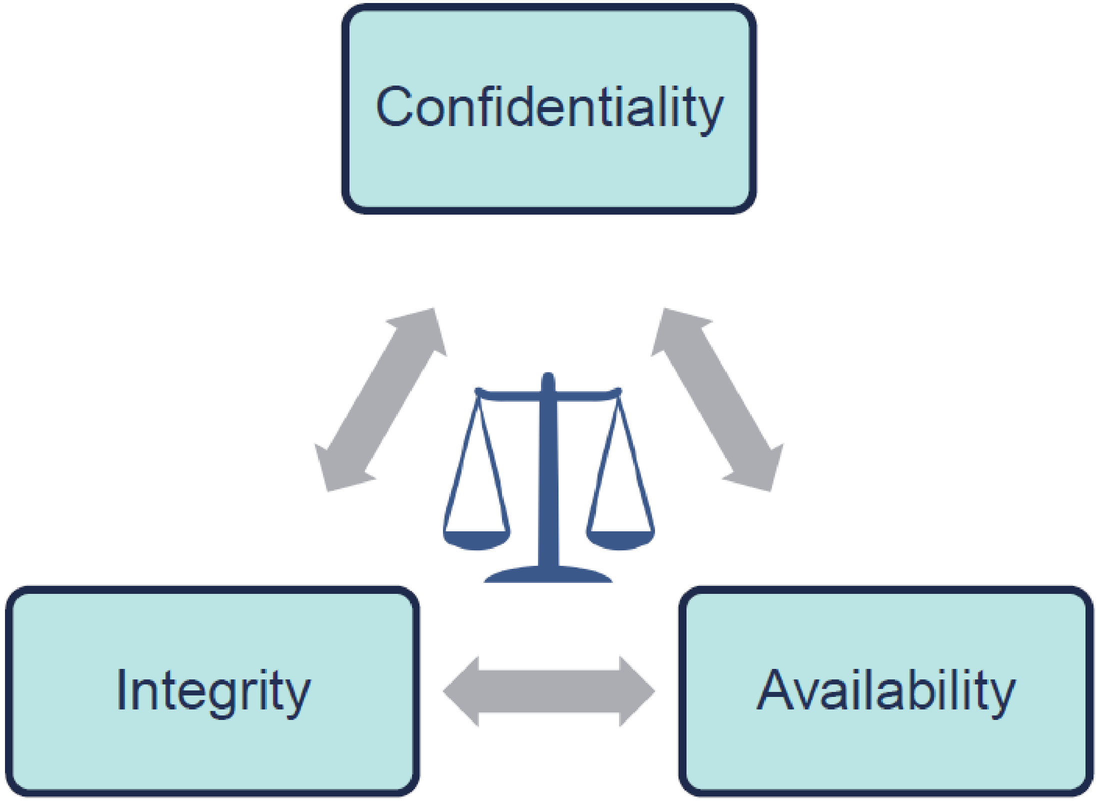


Defense in Depth





The CIA Triad



Information security consists:

- Provision of the following three services
    - Confidentiality
        - concealment of data from unauthorized parties
    - Integrity
        - assurance that data is genuine
    - Availability
        - system still functions efficiently after security provisions are in place

Attacks

- Compromise systems in ways that affect services of information security
  - attack on confidentiality:
    - unauthorized disclosure of information
  - attack on integrity:
    - destruction or corruption of information
  - attack on availability:
    - disruption or denial of services

Prevention, detection, response

- proper planning reduces risk of attack and increases capabilities of detection and response if an attack does occur

Prevention

- Establishment of policy and access control
  - who: identification, authentication, authorization
  - what: granted on “need-to-know” basis
- Implementation of hardware, software, and services
  - users cannot override, unalterable (attackers cannot defeat security mechanisms by changing them)
  - examples of preventative mechanisms
    - passwords - prevent unauthorized system access
    - firewalls - prevent unauthorized network access
    - encryption - prevents breaches of confidentiality
    - physical security devices - prevent theft
- Maintenance

Prevention is not enough!

Prevention systems are never perfect.

No bank ever says: "Our safe is so good, we don't need an alarm system."

No museum ever says: "Our door and window locks are so good, we don't need night watchmen.“

Detection and response are how we get security in the real world, and they're the only way we can possibly get security in the cyberspace world.

Bruce Schneier,
Counterpane Internet Security, Inc.

Detection

- Determine that either an attack is underway or has occurred and report it
- Real-time monitoring
  - or, as close as possible
  - monitor attacks to provide data about their nature, severity, and results
- Intrusion verification and notification
  - intrusion detection systems (IDS)
  - typical detection systems monitor various aspects of the system, looking for actions or information indicating an attack
    - example: denial of access to a system when user repeatedly enters incorrect password

Response

- Stop an attack
    - must be timely!
        - incident response plan developed in advance
- Assess and repair any damage
- Resumption of correct operation
- Evidence collection and preservation
    - very important
        - identifies vulnerabilities
        - strengthens future security measures

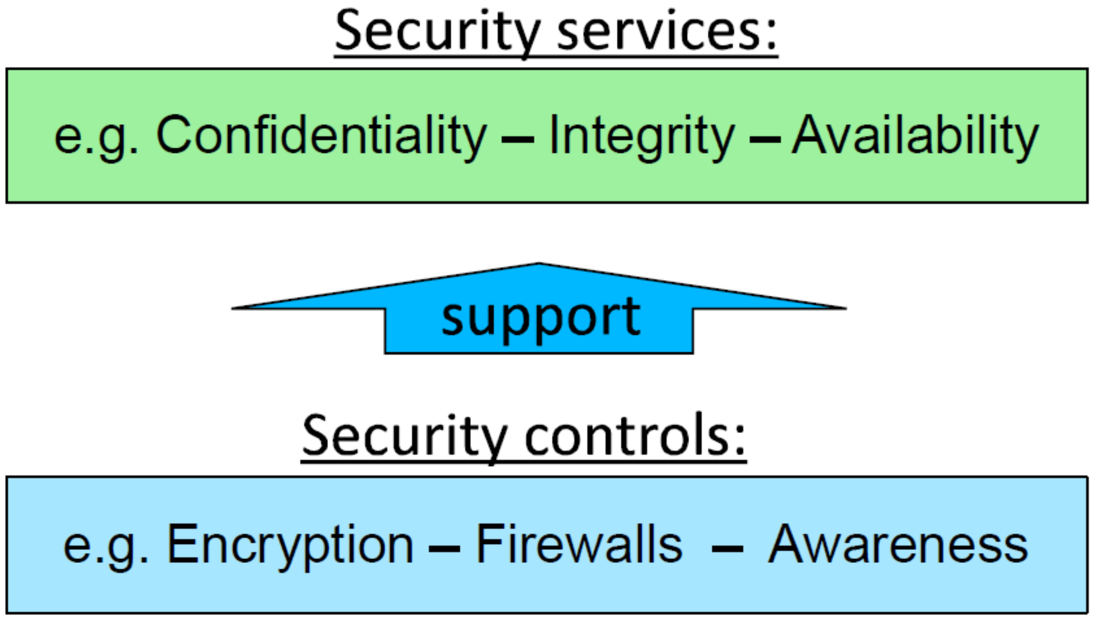
Exercise

Classify each of the following as an attack on confidentiality, integrity, and/or availability (more than one may apply). Justify your answers.

1. John copies Mary's homework
2. Paul crashes Linda's system
3. Carol changes the amount of Angelo's check from $100 to $1,000
4. Gina forges Roger's signature on a deed
5. Rhonda registers the domain name "AddisonWesley.com" and refuses to let the publishing house buy or use that domain name
6. Jonah obtains Peter's credit card number and has the credit card company cancel the card and replace it with another card bearing a different account number
7. Henry spoofs Julie's IP address to gain access to her computer

Security Services and Controls

- Security services (aka. security goals or properties) are
  - implemented independently
  - supported by specific controls
- Security controls (aka. mechanisms) are Practical mechanisms, actions, tools or procedures that are used to provide security services.



Security services:

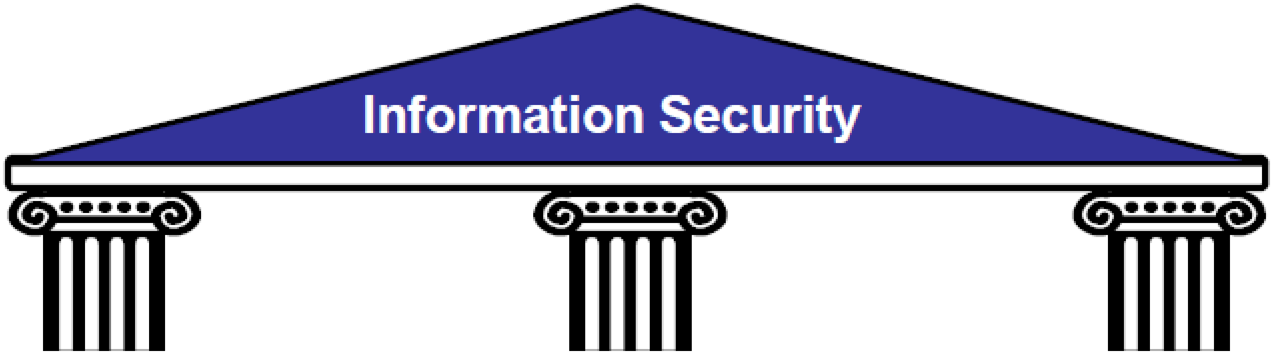
e.g. Confidentiality – Integrity – Availability

support

Security controls:

e.g. Encryption – Firewalls – Awareness

Security control categories



Information Security

Physical controls

- Facility protection
- Security guards
- Locks
- Monitoring
- Environmental controls
- Intrusion detection

Technical controls

- Logical access control
- Cryptographic controls
- Security devices
- User authentication
- Intrusion detection
- Forensics

Administrative controls

- Policies & standards
- Procedures & practice
- Personnel screening
- Awareness training
- Secure System Dev.
- Incident Response

Security Controls by Functional Types

- Preventive controls:
  - prevent attempts to exploit vulnerabilities
  - Example: encryption of files

- Detective controls:
  - warn of attempts to exploit vulnerabilities
  - Example: Intrusion detection systems (IDS)

- Corrective controls:
  - correct errors or irregularities that have been detected.
  - Example: Restoring all applications from the last known good image to bring a corrupted system back online
- Use a combination of controls to help ensure that the organizational processes, people, and technology operate within prescribed bounds.

Controls by Information States

- Information security involves protecting information assets from harm or damage. Information is considered in one of three possible states:
- During storage
  - Information storage containers
  - Electronic, physical, human

- During transmission
  - Physical or electronic

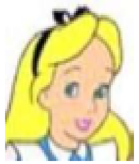
- During processing (use)
  - Physical or electronic

- Security controls for all information states are needed

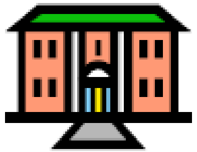
AAA’s Framework (Authentication, Authorization & Accounting)

- AAA is an information security framework for controlling access to data and system resources, enforcing policies, and auditing actions.
- **Authentication**
  - Verifies a user’s identification via the process of logging into a system.
- **Authorization (Access Control)**
  - Determines what a user has the authority to do and have access to.
- **Accounting**
  - Tracks and records user access and actions with system logs.

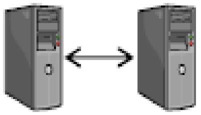
Authentication types



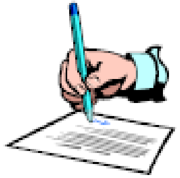
- User authentication:
  - The process of verifying a claimed identity of a (legal) user when accessing a system or an application.



- Organization authentication:
  - The process of verifying a claimed identity of a (legal) organization in a session

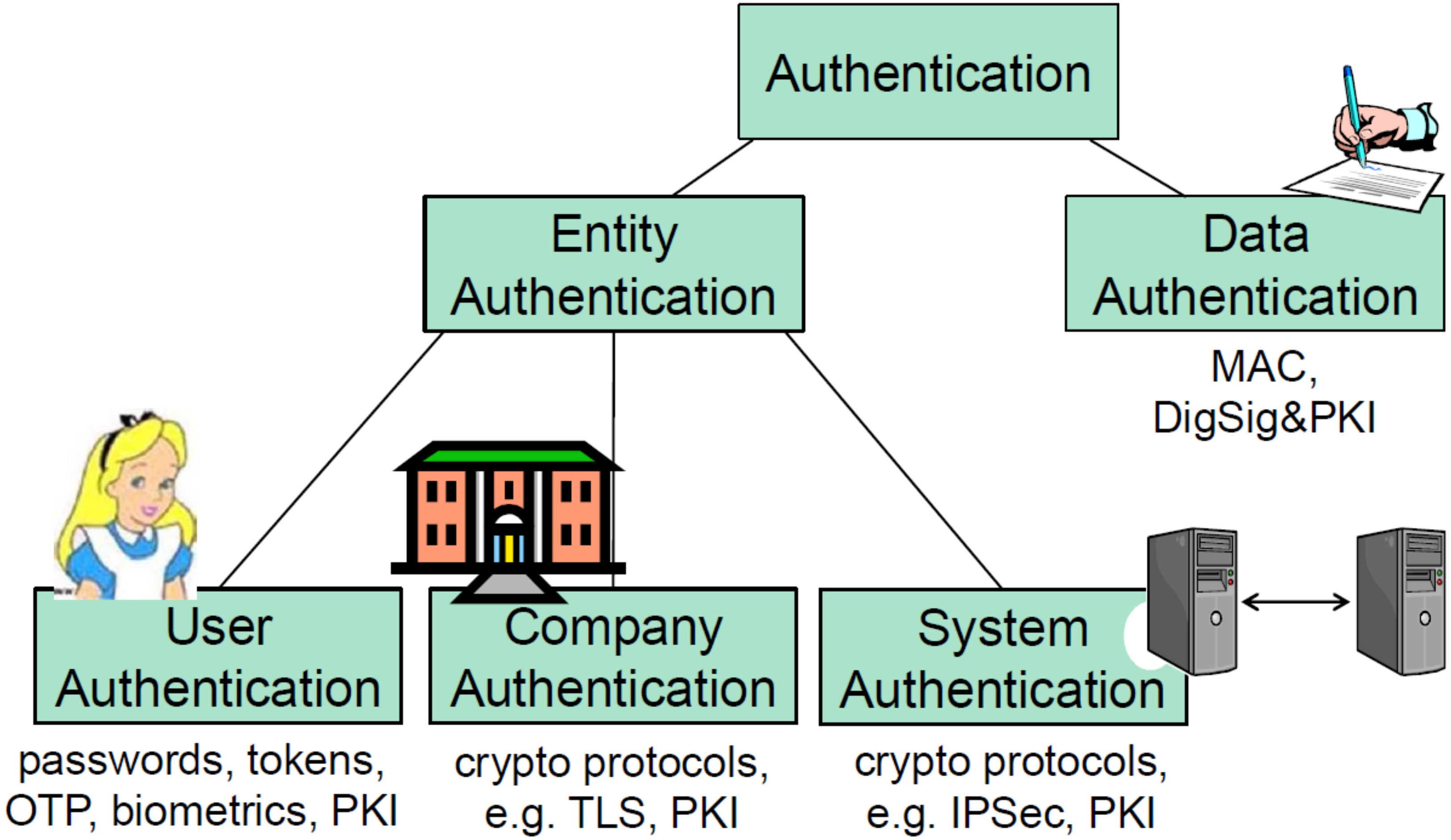


- System authentication (peer entity authentication):
  - a peer entity (system) in an association (connection, session) is the one claimed.



- Data origin authentication (message authentication):
  - the source of data received is as claimed

Taxonomy of Authentication



Authentication

Entity Authentication

Data Authentication

MAC, DigSig&PKI

User Authentication

passwords, tokens, OTP, biometrics, PKI

Company Authentication

crypto protocols, e.g. TLS, PKI

System Authentication

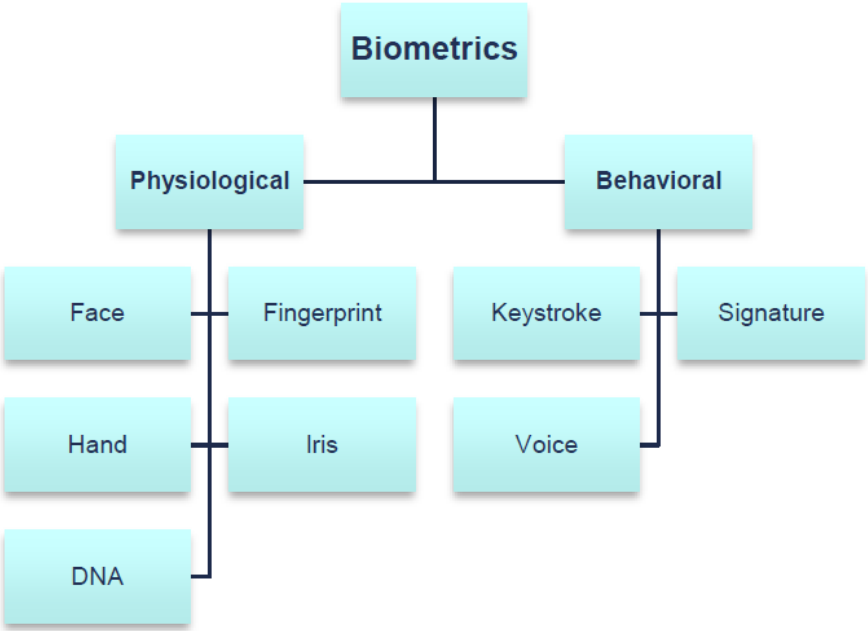
crypto protocols, e.g. IPSec, PKI

Three Factors of Authentication

- **Something You Know**
  - Password
  - PIN

- **Something You Have**
  - Smart Card
  - RSA Token
  - Hardware authentication device(Yubikey)

- **Something You Are**
  - Biometrics



Biometrics

Physiological

Behavioral

Face

Fingerprint

Hand

Iris

DNA

Keystroke

Signature

Voice

General Password Rules

- Passwords should be strong
  - 8 Characters Minimum
  - Combination of Upper Case & Lower Case Letters, Numbers, and Special Characters
- Passwords should not be written down
- Passwords should not be shared
- Passwords should be regularly changed (Every 60 to 90 days)
- Passwords should not be reused
  - Don’t allow reuse of last 4 passwords
- Account lockout policies should be used
  - Lockout user after 3 failed login attempts
- Default passwords should be changed
  - New user default password expires after 1st use

Two-Factor Authentication

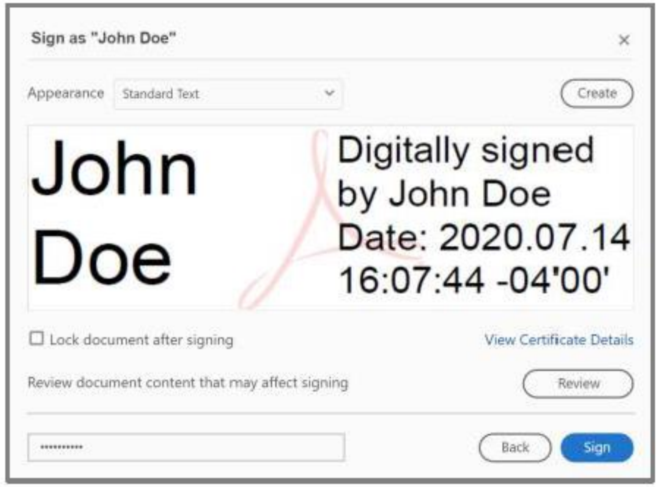
- Common Practice to Increase Security that uses a combination of two of the three factors of authentication
  - Something You Have
  - Something You Know
  - Something You Are
- Using a code generator is the most popular method of two-factor authentication. This method is where you have an app on your phone that generates a code you need to enter and your password. This code changes every 30 seconds, so it's impossible to guess.
- An authenticator app is similar to a code generator, but instead of generating a code, it gives you a push notification on your phone that you need to approve to log in. A physical token is a small device you carry that generates a code. Biometrics is a newer method of two-factor authentication that uses something unique about you, like your fingerprint, to log you in.

User Identification and Authentication

- Identification: Not the same as authentication.
  - Before you give out credentials, you “Identity Proof” somebody.
  - Validates someone’s identity before credentials are issued
  - Method: Passport, name, biometrics
- User authentication
  - Prove that you are the one you claim to be
- Main threat: Spoofed identity and false login
- Controls:
  - Passwords
  - Personal cryptographic tokens
    - OTP generators, etc.
  - Biometrics
    - Id cards

Non-Repudiation
(Strong form of Data Authentication)

- Used to prevent an entity from denying an action took place.
  - Non-repudiation of origin: proof that data was sent.
  - Non-repudiation of delivery: proof that data was received.
- Control: digital signature
  - Cryptographic evidence that can be confirmed by a third party


Sign as "John Doe"

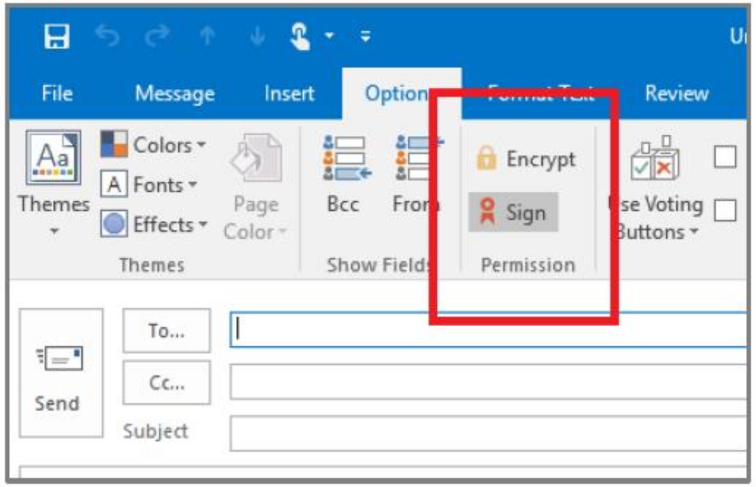
Appearance: Standard Text

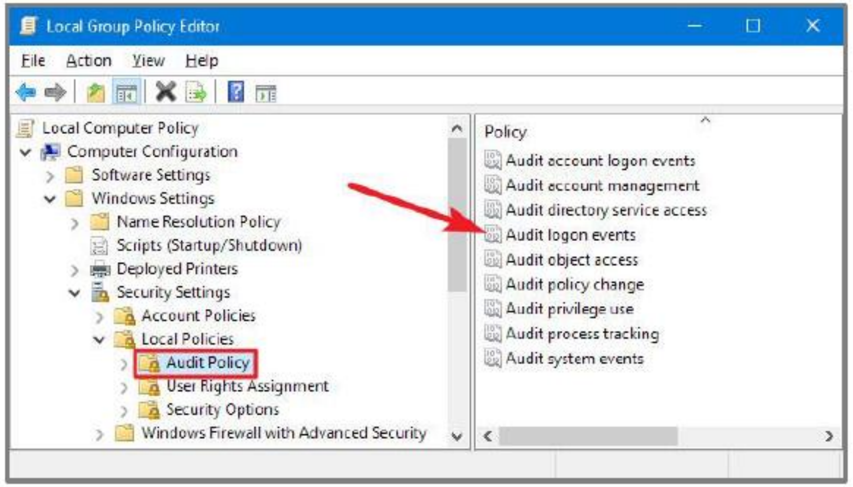
John Doe

Digitally signed by John Doe
Date: 2020.07.14
16:07:44 -04'00'

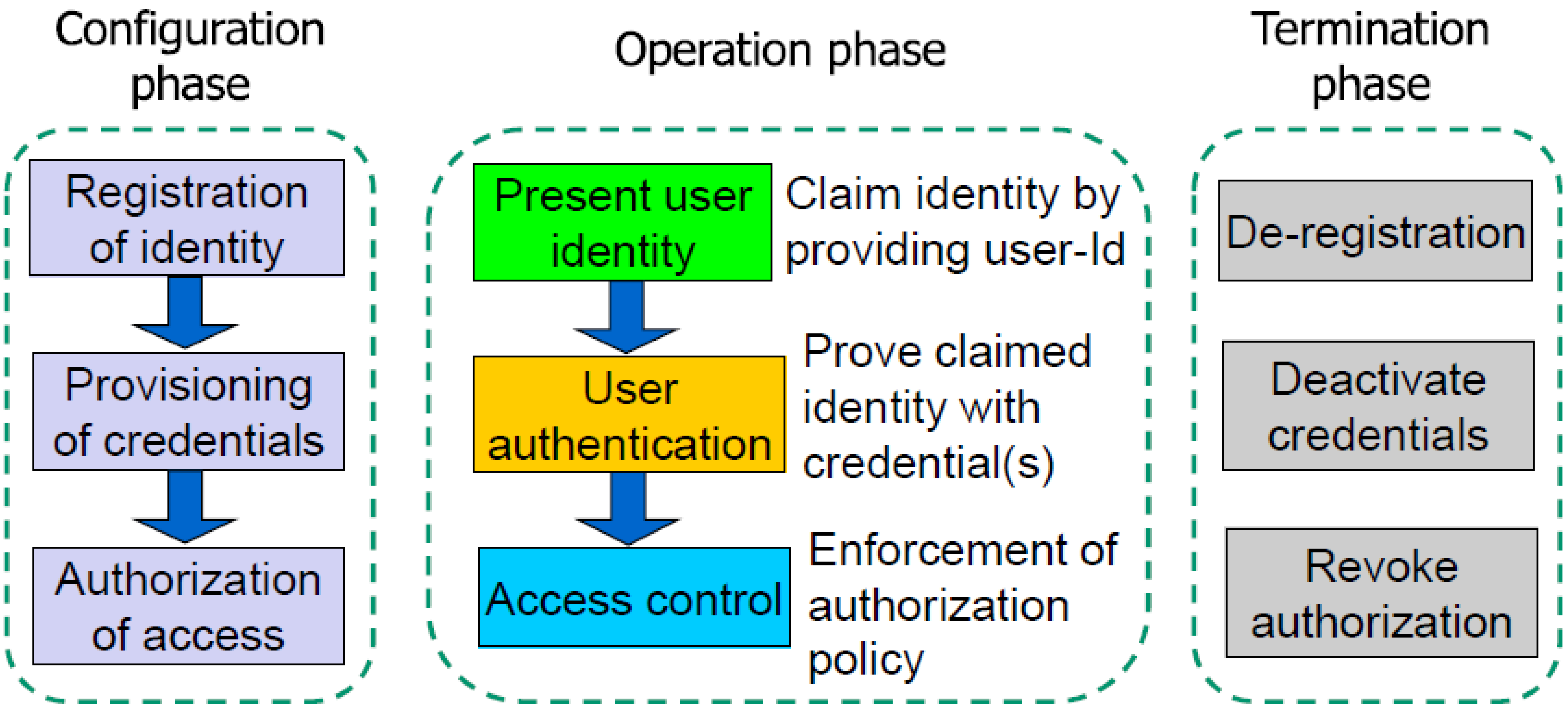
□ Lock document after signing

Review document content that may affect signing





Identity and Access Management (IAM) Phases



Configuration phase

Registration of identity

Provisioning of credentials

Authorization of access

Operation phase

Present user identity

Claim identity by providing user-Id

User authentication

Prove claimed identity with credential(s)

Access control

Enforcement of authorization policy

Termination phase

De-registration

Deactivate credentials

Revoke authorization