Security and Privacy

Introduction

Security

Computer Systems: Everywhere and Interconnected

Critical Infrastructures

IOT

Financial Systems

Cloud computing

Business and Services

Health

Cyber Physical Systems

Vehicles

Industry

Social Networks

Entertainment

Education

Mobile devices

Government and Organizations

Computer Systems: Everywhere and Interconnected

Critical Infrastructures

IOT

Financial Systems

Cloud computing

Business and Services

Health

Cyber Physical Systems

Vehicles

This has raised security concerns tremendously, leading researchers and companies to create tools, techniques, standards and regulations

Education

Mobile devices

Government and Organizations

Security is the Biggest Concern

Successful Security Attack

Privacy Issues

- Violation of Confidential data

Security Issues

- Damages to the system
- Financial Loss
- Reputation Loss

Safety Issues

- Danger People's life
- Damaging the Nature

The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.

—***The Art of War,*** **Sun Tzu**

(4th century BC **)**

The combination of space, time, and strength that must be considered as the basic elements of this theory of defense makes this a fairly complicated matter. Consequently, it is not easy to find a fixed point of departure.

— ***On War, Carl Von Clausewitz***

(between 1816 and 1830***)***

*The combination of space, time, and strength that must be considered as the basic elements of this theory of defense makes this a **fairly complicated matter**. Consequently, it is not easy to find a fixed point of departure.*

— ***On War, Carl Von Clausewitz***

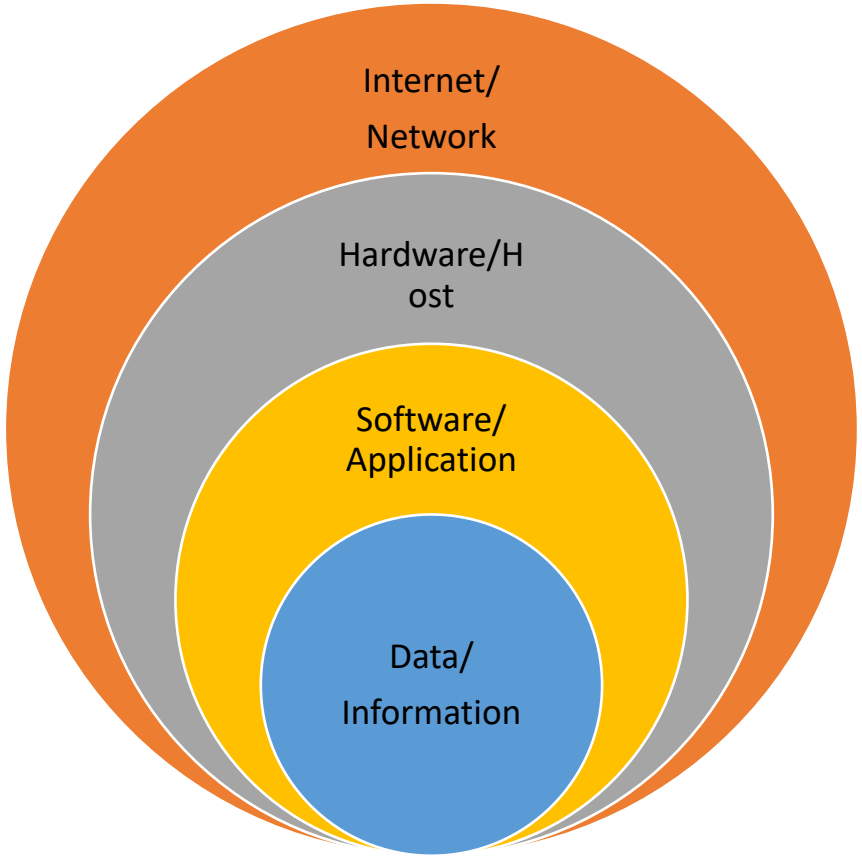
(between 1816 and 1830***)***

In computer system, to have an acceptable level of security in a system, we must consider many factors: the **complex architecture of systems**, the **type of system (security critical, business critical, safety critical**), **defense mechanisms implemented**, **fault tolerance mechanism** Implemented, **interests of attackers**

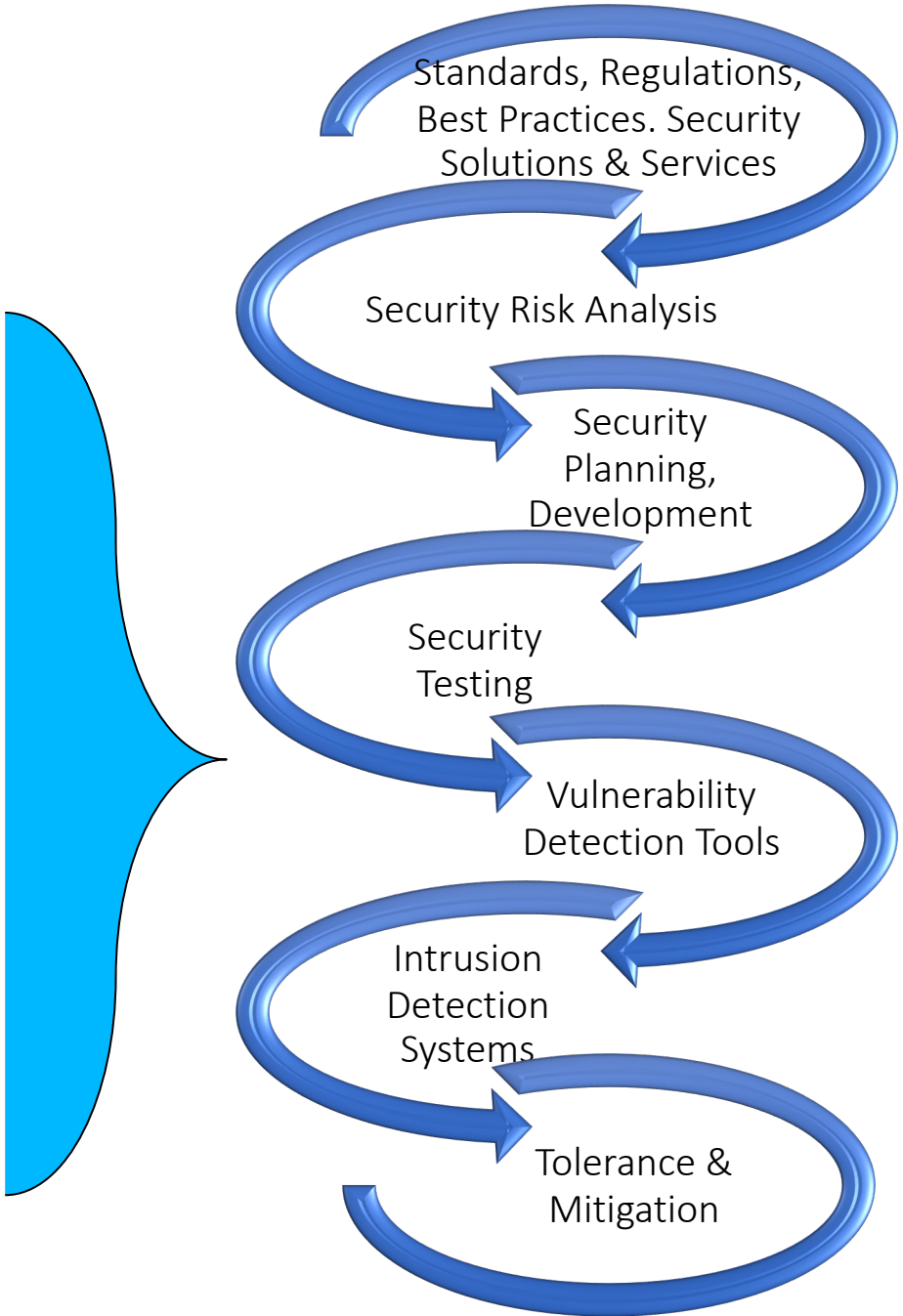
Defense in Depth

- Defined by the National Security Agency (NSA)

Idea: defend a system against any specific attack using **several independent methods**.



The Onion Model of Defense in Depth



Three Important Questions…

Is it possible to Identify all Threats in all layers?

If so, Is it possible to find a defensive solution for each identified threat?

If so, how much resources (money, time and human resources) are required to implement or apply such a solution?

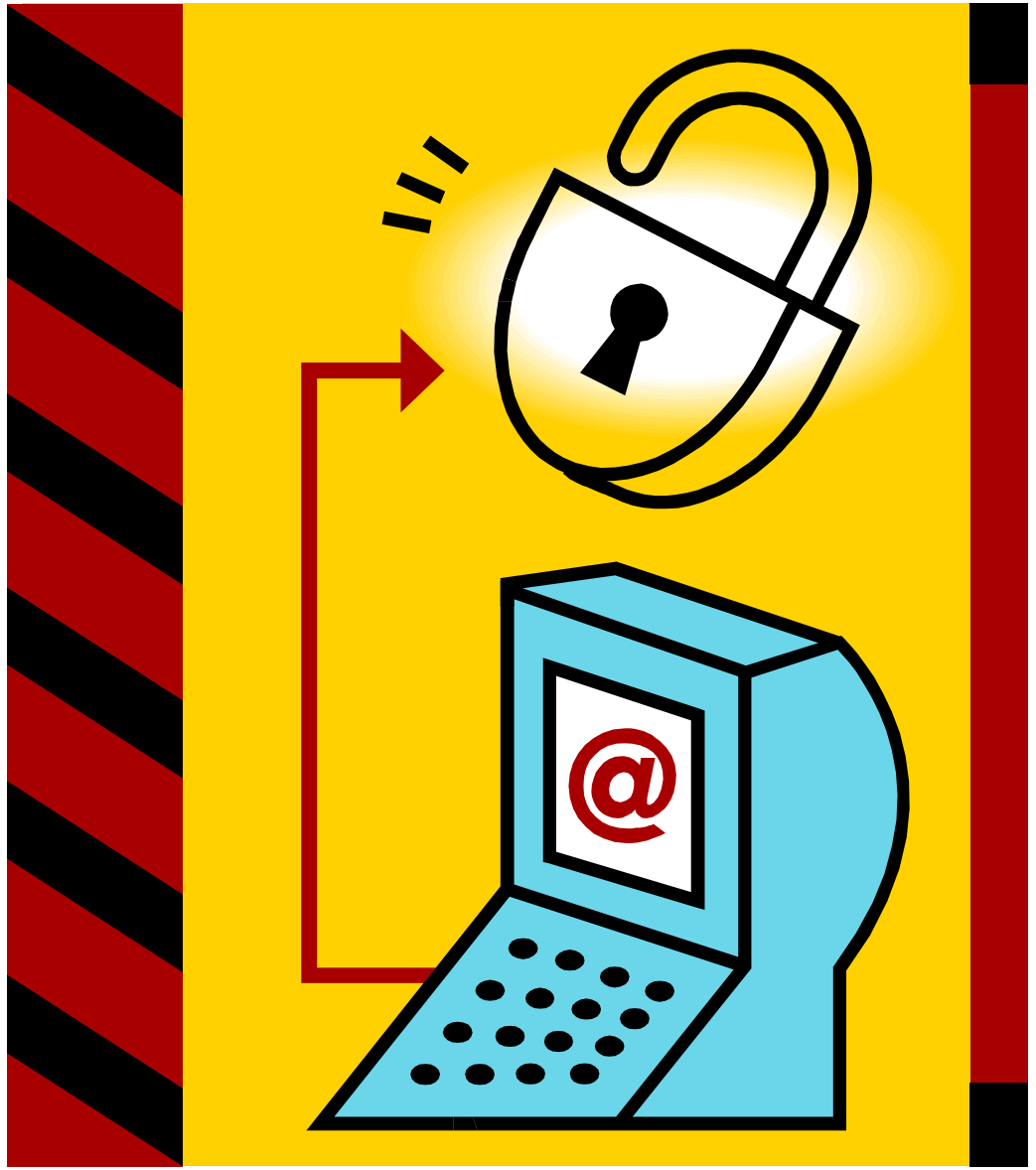
Security Risk Analysis

- Essential factors, after identifying the threats:
  - Frequency of possible threats
  - Impact level (severity)

- *Not easy to be done effectively*

Definition: Network and Internet Security

"measures to **deter**, **prevent**, **detect**, and **correct** security violations that involve the **transmission of information**"



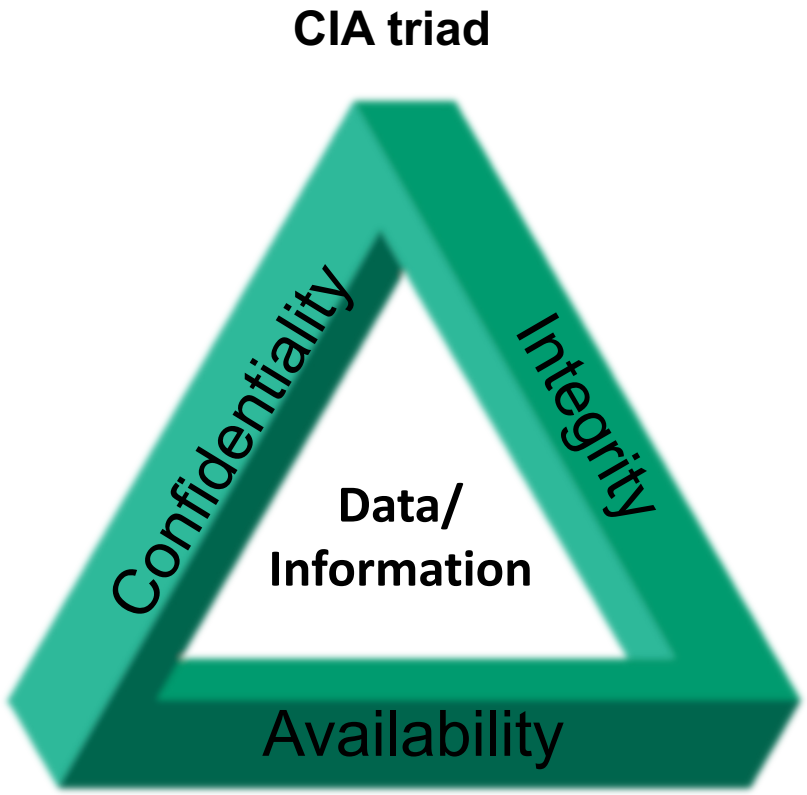
Definition: Network and Internet Security

- **Deterrence**
  - Deterrence strategies seek to influence an adversary's behaviour, discouraging them from engaging in unwanted activities.
  - Can be achieved by influencing the costs versus gains assessment of potential perpetrators (e.g., heavy penalties)
- **Prevention**
  - Using techniques, tools and controls to prevent an attack (e.g., firewalls, encryption)
- **Detection**
  - Using tools or techniques to monitor and detect an attack or intrusion (e.g., intrusion detection systems)
- **Correction**
  - Use strategies to mitigate an attack and make corrections (vulnerability removal) in the system to become more secure

Definition: Computer Security

"the protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources. **(includes hardware, software, firmware, information/data, and telecommunications)** ***"***

The (National Institute of Standards and Technology) NIST Computer Security Handbook



Computer Security Objectives

Confidentiality

This term covers two related concepts:

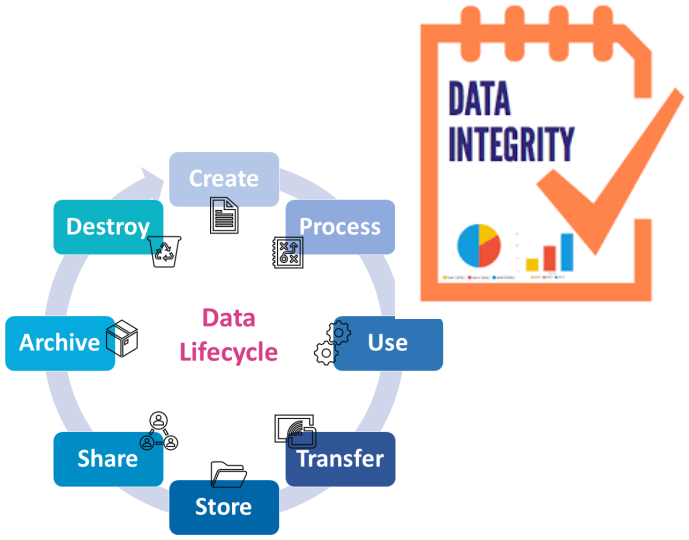
- Data confidentiality
  - Assures that **information is not made available** or disclosed to **unauthorized individuals**
- Privacy
  - Assures that **individuals control** or influence what information related to them may be collected and stored, and by whom and to whom that information may be disclosed

A loss of confidentiality means unauthorized disclosure of information.

Computer Security Objectives

Integrity

- Data integrity
  - Assures that **data is changed** only in a specified and **authorized manner**
- System integrity
  - Assures that a **system performs its intended function** in an unimpaired manner, free from deliberate **unauthorized manipulation of the system**



A loss of integrity means unauthorized modification or destruction of data or system.

Computer Security Objectives

Availability

- Assures **that systems work promptly** and **service is not denied** to authorized users

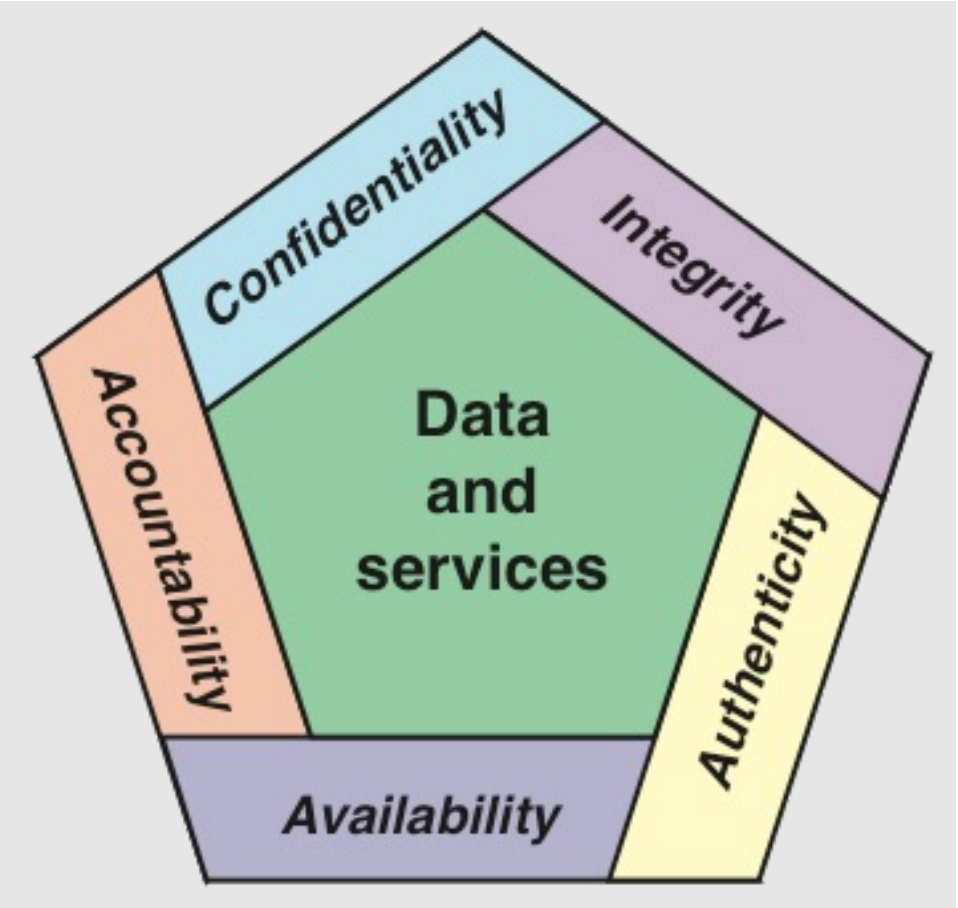
The loss of the service translates into a large financial loss and customer loss.

Computer Security Objectives

Accountability (non-repudiation):

- Trace a security breach to a responsible party.

- Systems must keep records of their activities to be able to trace security breaches.

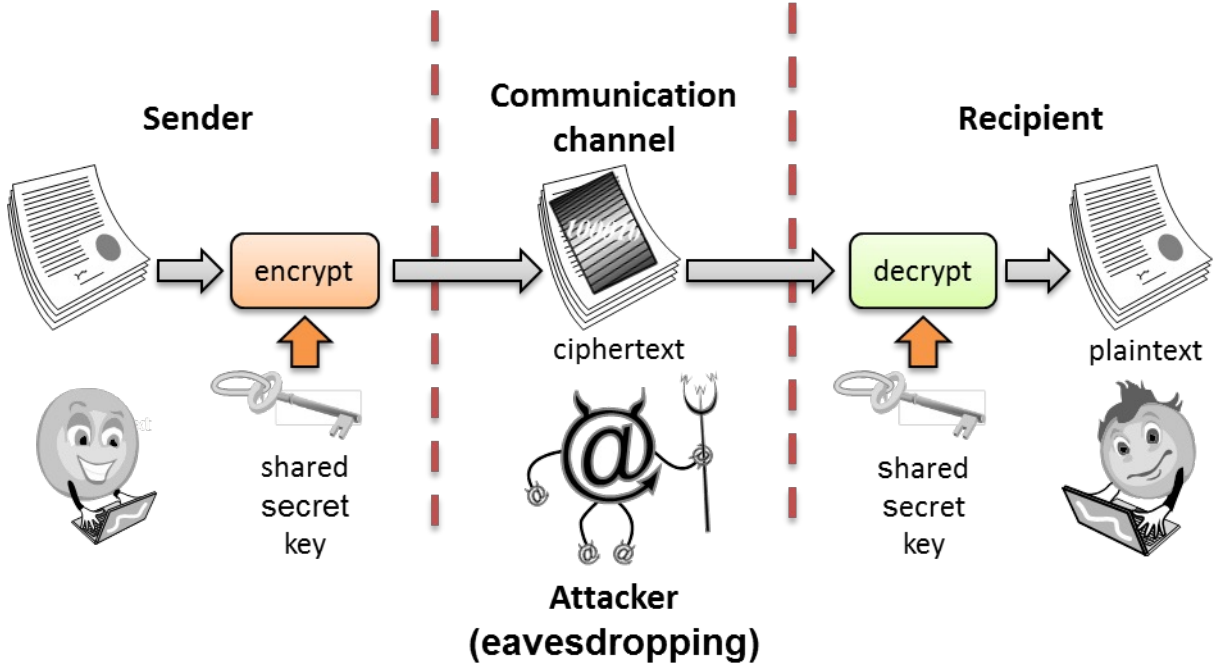


Authenticity:

verifying that users are who they say they are

Tools for Confidentiality

- **Encryption:** the **transformation** of information using a secret key, called an **encryption key**, so that the transformed information can only be read using another secret key, called the **decryption key** (which may, in some cases, be the same as the encryption key).

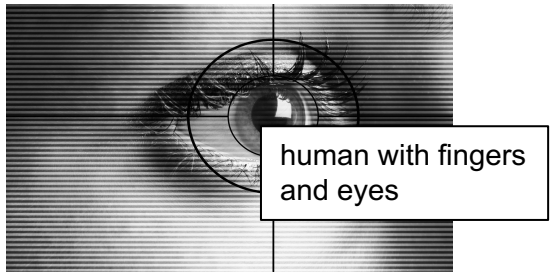


Tools for Confidentiality

- **Access Control:** rules and policies that limit access to confidential information to those people and/or systems with a "**need to know**."
    - This ***need to know*** can be determined by **identity**, such as a person's name or a computer's serial number, or by a **role** that a person has, such as being a manager or a computer security specialist.

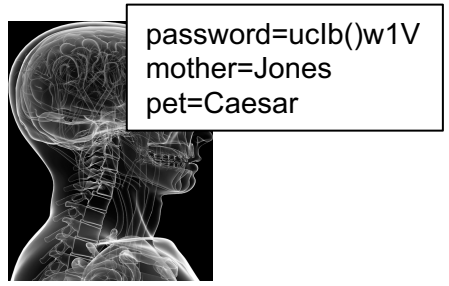
Tools for Confidentiality

- **Authentication:** the **determination** of the **identity** or **role** that someone has.
- This determination can be done in a number of different ways, but it is usually based on a combination of
  - something the person has (like a smart card or a radio key for storing secret keys),
  - something the person knows (like a password),
  - something the person is (like a human with a fingerprint).



Something you are

Something you have



Something you know

Tools for Confidentiality

- **Authorization:** the **determination** if a person or system **is allowed access to resources**, based on an access control policy.
  - While, authentication verifies the identity of a user (person or system), authorization determines their access rights
  - Such authorizations should prevent an attacker from tricking the system into letting him have access to protected resources.
- **Physical security:** the establishment of **physical barriers** to limit access to protected computational resources.
  - locks on cabinets and doors, the placement of computers in windowless rooms, the use of sound dampening/absorbing materials, and even the construction of buildings or rooms with walls incorporating copper meshes (called Faraday cages) so that electromagnetic signals cannot enter.

Tools for Confidentiality

- **Anonymity:** the property that certain records or transactions **not to be attributable to any individual.**

- Methods:
  - **Aggregation**: the combining of data from many individuals so that disclosed sums or averages cannot be tied to any individual.
  - **Mixing**: the intertwining of transactions, information, or communications in a way that cannot be traced to any individual.
  - **Proxies**: trusted agents that are willing to engage in actions for an individual in a way that cannot be traced back to that person.
  - **Pseudonyms**: fictional identities that can fill in for real identities in communications and transactions, but they are known only to a trusted entity.

Integrity

- **Integrity:** the property that information has not be altered in an unauthorized way.
- Tools:
  - **Backups**: the periodic archiving of data.
  - **Checksums**: the computation of a function that maps the contents of a file to a numerical value. A checksum function depends on the entire contents of a file and is designed in a way that even a small change to the input file (such as flipping a single bit) is highly likely to result in a different output value.
  - **Data correcting codes**: methods for storing data in such a way that small changes can be easily detected and automatically corrected.

Availability

- **Availability:** the property that information is accessible and modifiable in a timely fashion by those authorized to do so.

- Tools:
  - **Physical protections**: infrastructure meant to keep information available even in the event of physical challenges.
  - **Computational redundancies**: computers and storage devices that serve as fallbacks in the case of failures.

Authenticity

- **Authenticity:** is the ability to determine that statements, policies, and permissions issued by persons or systems are genuine (verifying that users are who they say they are)

- Tools:
  - **Two-factor authentication (2FA) or Multi-factor authentication (MFA)**, asking for several identity related information

Accountability

- Accountability (Non-repudiation): is the ability to trace a security breach to a responsible party (that cannot deny it)

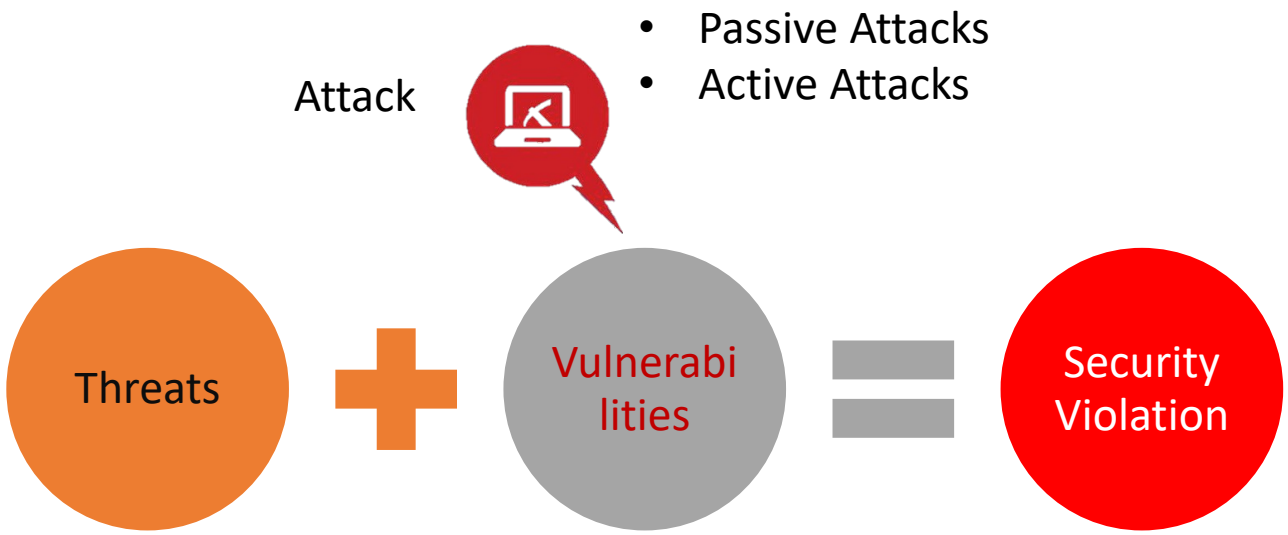
- Tools:
  - **Logging:** log all activities and transactions in the system
  - **Digital signatures**. These are cryptographic computations that allow a person or system to commit to the authenticity of their documents in a unique way that achieves non-repudiation, which is the property that authentic statements issued by some person or system cannot be denied.

Threats and Attacks

- **Threat -** A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

- **Attack -** An assault on system security. An **intelligent act** to **evade security services** and **violate the security policy** of a system.

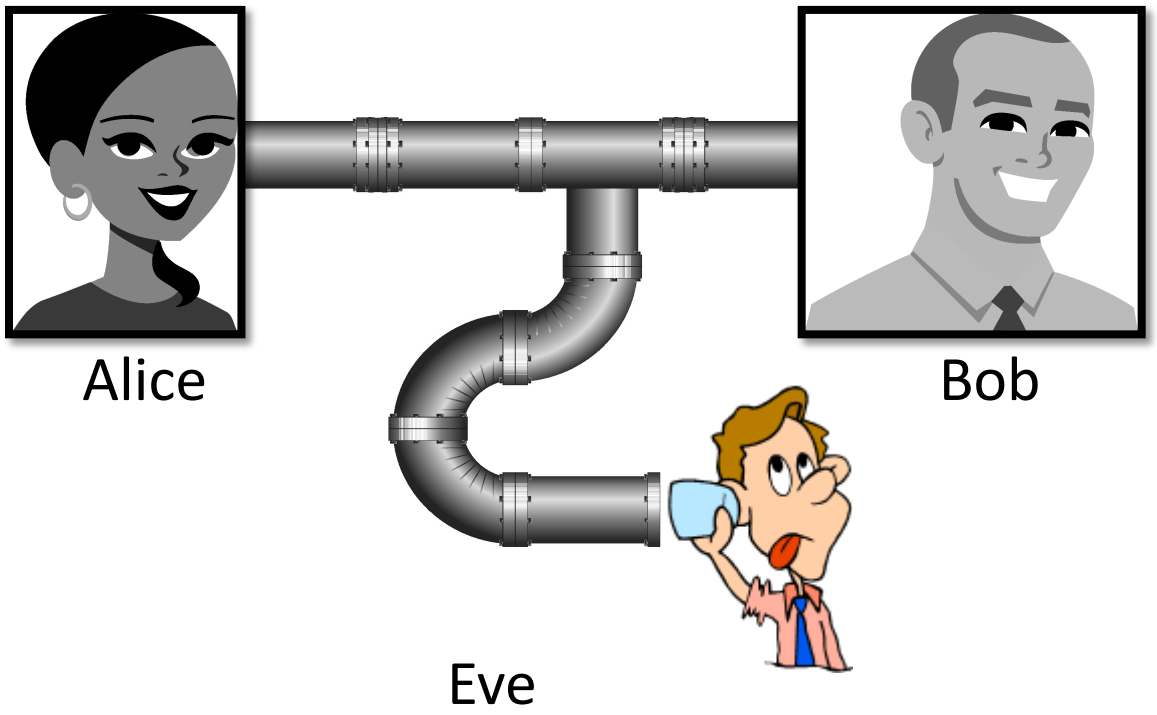
Threats and Attacks



- **Natural Threats** (e.g., floods)
- **Unintentional Threats** (e.g., an employee mistakenly gains access to private information)
- **Intentional Threats** (e.g., spyware, malware, unsatisfied employee, malicious users)

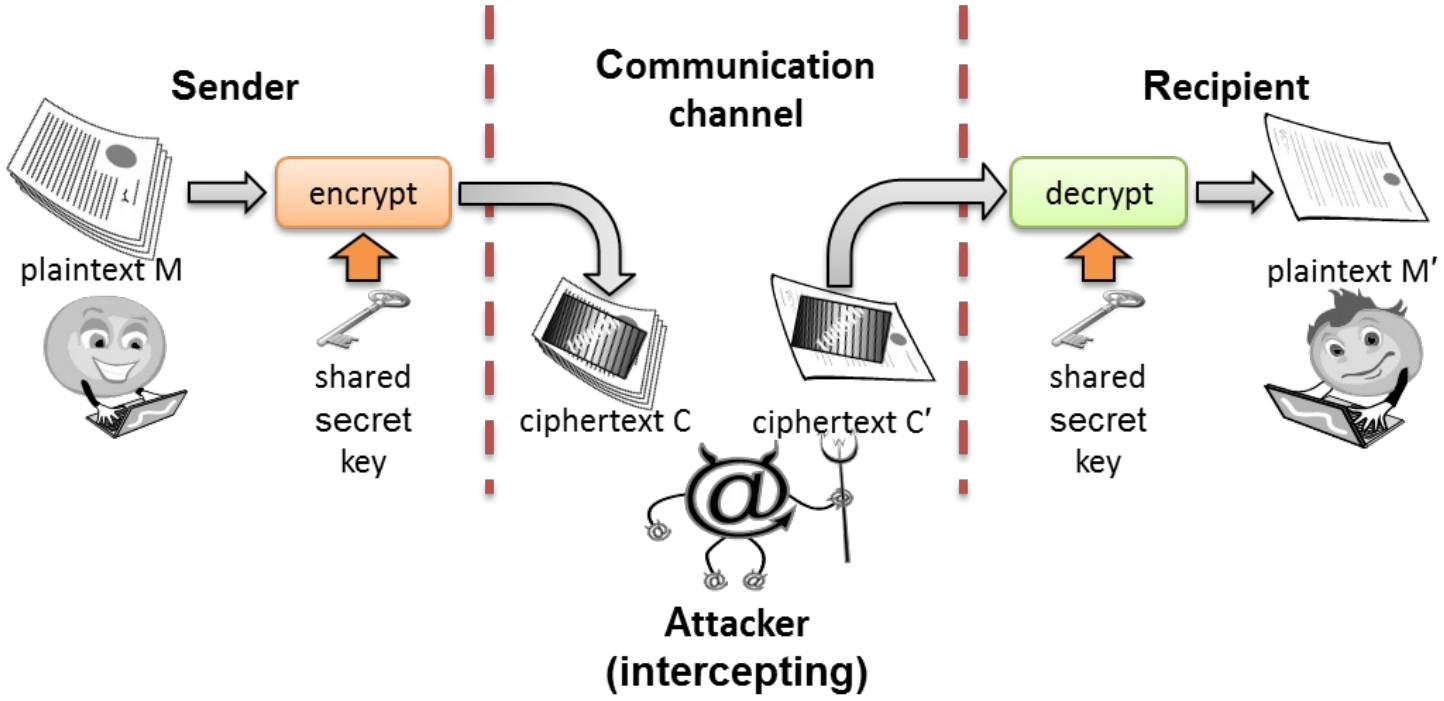
Attacks

- **Eavesdropping**: the **interception of information** intended for someone else during its transmission **over a communication channel**.



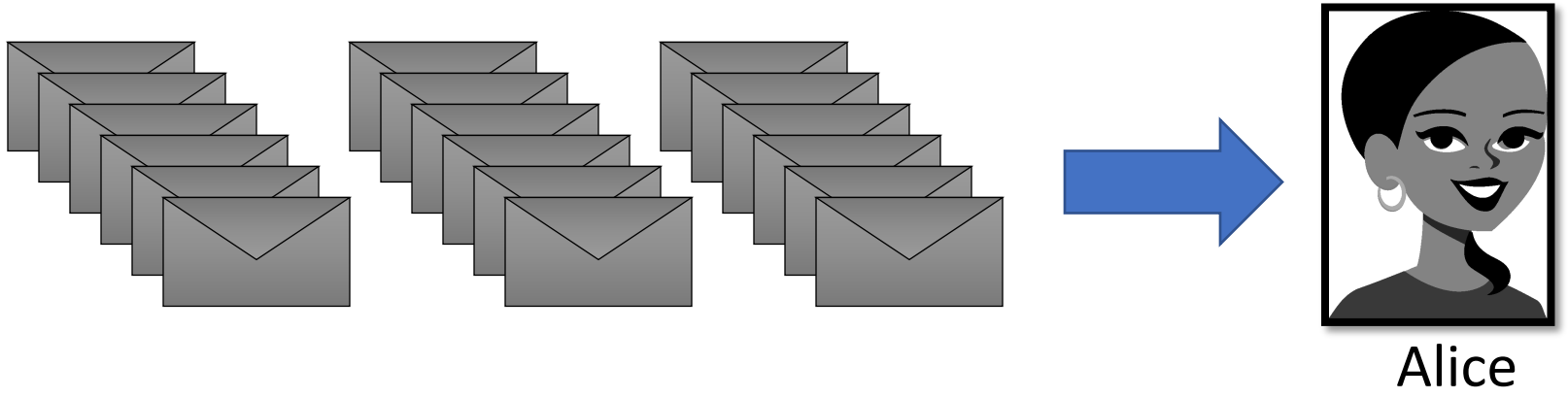
Threats and Attacks

- **Alteration**: unauthorized modification of information.
  - Example: the man-in-the-middle attack, where a network stream is intercepted, modified, and retransmitted.



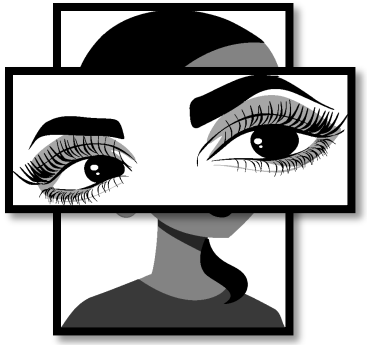
Threats and Attacks

- **Denial-of-service**: the interruption or degradation of a service or data access.
  - Example: email spam, to the degree that it is meant to simply fill up a mail queue and slow down an email server.



Threats and Attacks

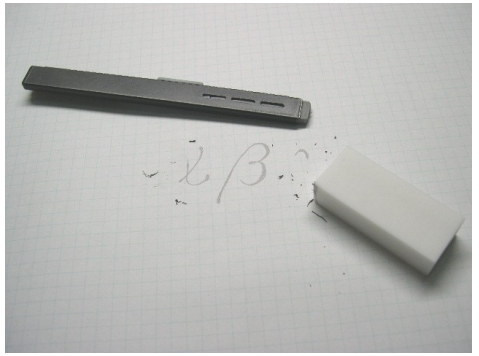
- **Masquerading**: the fabrication of information that is purported to be from someone who is not actually the author.



“From: Alice”
(really is from Eve)

Threats and Attacks

- **Repudiation**: the denial of a commitment or data receipt
  - This involves an attempt to back out of a **contract or a protocol that requires the different parties to provide receipts acknowledging that data has been received.**
  - It usually happens when **a system does not adopt adequate controls to properly track and log users' actions**, thus making repudiation possible.
  - **When repudiation is possible, users can manipulate data without being known**



Threats and Attacks

- **Correlation and traceback**: the integration of multiple data sources and information flows to determine the source of a particular data stream or piece of information.

Privacy

Privacy

- There are things that other people should not see or know (Elgesem, 1996)
- It is a human right, but it is not absolute **when** or **to what extent** privacy is preserved

"Computers did not invent or even cause privacy issues"

Computers systems' **processing**, **storage** and **transmission** capabilities cause major challenges to privacy

What is New with Computers?

- Data Collection
  - Massive and cheap storage potentiates collecting and saving data
- Data Sharing
  - Massive data sharing
- Control the Ownership of Data
  - How to get back disseminated data?

Definition: Information Privacy

“the right to control who knows certain things about you.”

[Pfleeger]

“the right of an entity to be secure from unauthorized disclosure of sensitive information that is contained in an electronic repository”

[Bertino]

- Challenges:
  - Controlled Disclosure
    - We do not have complete control …
  - What each person considers private is subjective
    - No standard of what is private …

Data Confidentiality and Privacy

- Data confidentiality
  - Assures that **information** is not made available or disclosed to unauthorized individuals

- Privacy
  - Assures that **individuals** control or influence what information related to them may be collected and stored, and by whom and to whom that information may be disclosed

Focus of this Course

- Anonymity in Data Publishing:
  - The simple idea: remove personally identifiable information (PII)
- Differential Privacy:
  - Released DB reveals “little” about any individual
- Processing and Searching of Encrypted Data
  - Homomorphic Encryption
- Secure Computation and Privacy
  - How to compute a function in the safest way possible (guarantee minimal information leakage)
- Federated Learning Privacy
  - How to learn from distributed data in a distributed manner but preserve privacy

Bibliography