Concept of 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).

Main Security objectives - CIA triad

- **Confidentiality -** The requirement that private (privacy) or secret information not be disclosed too unauthorized individuals. Confidentiality protection applies to data in storage, during processing, and while in transit.
- **Integrity**
  - **Data integrity:** The property that data has not been altered in an unauthorized manner while in storage, during processing, or while in transit.
  - **System integrity:** The quality that a system has when performing the intended function in an unimpaired manner, free from unauthorized manipulation.
- **Availability -** Availability is a requirement intended to assure that systems work promptly and service is not denied to authorized users.
- There are three other security objectives – Accountability, Assurance, and Authentication.
- Confidentiality is dependent on Integrity, if the integrity of the system is lost, then there is no longer a reasonable expectation that the confidentiality mechanisms are still valid.
- Integrity is dependent on Confidentiality, If the confidentiality of certain information is lost (e.g., the superuser password), then the integrity mechanisms are likely to be by-passed.
- **Authentication -** Encompasses identity verification, message origin integrity, and message content integrity.
- There are three levels of impact on organizations or individuals. Low – limited adverse, Moderate – serious adverse, High – catastrophic adverse.
- **Confidentiality**
  - **Low –** information on subject requirements
  - **Moderate –** student enrollment information
  - **High –** student grade information
- **Integrity**
  - **Low –** Many Web sites offer anonymous online polls to their users with very few safeguards. However, the inaccuracy and unscientific nature of such polls is well understood.
  - **Moderate –** A Website offers a forum to registered users to discuss some specific topic. Either a registered user or a hacker could falsify some entries. If the forum exists only for the enjoyment of the users, brings in little or no advertising revenue. The Web master may experience some data, financial, and time loss.
  - **High -** A hospital patients' allergy information stored in a database. An employee (e.g., a nurse) who is authorized to view and update this information

deliberately falsifies the data. Inaccurate information could result in serious harm or death to a patient and expose the hospital to massive liability.

- **Availability**
  - **Low** - An online telephone directory lookup application. Although the temporary loss of the application may be an annoyance, there are other ways to access the information.
  - **Moderate** - The public Website for a university provides information for current and prospective students and donors.
  - **High** - Consider a system that provides authentication services for medical databases. An interruption of service results in the inability for doctors to access the patients' medical records.

Physical Threats

- **Tornado** generates winds causing structural damage, roof damage, loss of outside equipment, damage from wind and flying debris, temporary loss of local utility and communications.
- **Tropical cyclones** hurricanes, tropical storms, and typhoons causing significant structural damage and damage to outside equipment, damage to public infrastructure, utilities, and communications. **Countermeasure** - emergency supplies for personnel as well as a backup generator are needed.
- **Earthquake** causing complete, destruction, with significant and long-lasting damage to data centers and other facilities, computer hardware and infrastructure equipment, including the collapse of raised floors, personnel are at risk from broken glass and other flying debris.
- **Ice storm or blizzard** causing some disruption of or damage to facilities.
- **Lighting** causing disruption of utilities and communications, can range from no impact to disaster, disruption of electrical power and there is the potential for fires
- **Flood** causing long-lasting effects and the need for a major cleanup especially facilities that are in flood areas at low elevation.
- **Inappropriate temperature and humidity**
  - Most computer systems should be kept between 10 and 32
  - degrees Celsius. Outside this range, resources might continue to operate but produce undesirable results.
  - If temperature around a computer gets too high, the computer cannot adequately cool itself, and internal components can be damaged.
  - If the temperature gets too cold, the system can undergo thermal shock when it is turned on, causing circuit boards or integrated circuits to crack.
  - High humidity can result in corrosion. Condensation can threaten magnetic and optical storage media. Condensation can also cause a short circuit, which in turn can damage circuit boards.
  - **Countermeasure:** Having environmental-control equipment of appropriate capacity and appropriate sensors to warn of thresholds being exceeded.
- **Static electricity**
  - A person or object that becomes statically charged can damage electronic equipment by an electric discharge.

    - Static electricity discharges as low as 10 volts can damage sensitive electronic circuits.
    - Discharges in the hundreds of volts can create significant
    - damage.
    - Discharges from humans can reach into the thousands of volts, so this is a nontrivial threat.
- **Fire, smoke**
    - a threat to human life and property
    - release of toxic fumes
    - water damage for fire suppression
    - smoke damage
    - **Countermeasure –** Involves a combination of alarms, preventive measures, and fire mitigation
        - Common walls have at least a one-hour Fire-protection rating.
        - Air conditioning designed so as not to spread fire.
        - Positioning of equipment to minimize damage
        - Flammables must not be stored in this area.
        - Hand-operated fire extinguishers readily available, clearly marked, and regularly tested.
        - Automatic fire extinguishers installed.
        - Important records, documents stored in fireproof cabinets.
- **Water**
    - a threat to computer equipment, paper, electronic storage media.
    - danger is an electrical short
    - moving water: plumbing, water from rain, snow, and ice
    - water from as far as two floors above will not create a hazard
    - floodwater leaves a muddy residue that is extraordinarily difficult to clean up.
    - **Countermeasure -** Water sensors should be located on the floor of computer rooms or under raised floors. Should cut off power automatically in the event of a food.
- **Dust**
    - This threat is often overlooked even fibers from fabric and paper are abrasive and mildly conductive, although generally equipment is resistant to such contaminants.
    - Larger influxes of dust can result from a controlled explosion of a nearby building and a windstorm.
    - Equipment with moving parts, such as rotating storage media and computer fans, are the most vulnerable to damage from dust.
    - **Countermeasure -** Proper filter maintenance and regular room maintenance
- **Infestation**
    - broad range of living organisms, including mold, insects, and rodents
    - mold can be harmful to both personnel and equipment
    - insects, particularly those that attack wood and paper, are also a common threat.

Technical Threats

- **Undervoltage**
  - Undervoltage condition occurs when the equipment receives less voltage than is required for normal operation
  - Most computers withstand voltage reductions of about 20% without shutting down and without operational error.
  - Deeper dips or blackouts lasting more than a few milliseconds trigger a system shutdown.
  - No damage is done, but service is interrupted.
- **Overvoltage**
  - because of utility company supply anomaly or lightning
  - can destroy silicon-based components, including processors and memories
- **Electromagnetic Interference**
  - Noise along a power supply line
  - Fans, heavy equipment, and even other computers generate electrical noise that can cause problems with the computer you are using.
  - This noise can be transmitted through space as well as through nearby power lines.
  - Other source is high-intensity emissions from nearby commercial radio stations and microwave relay antennas.
  - Even low-intensity devices, such as cellular telephones, can interfere with sensitive electronic equipment.
  - **Countermeasure –**
    - Uninterruptible power supply (UPS) should be employed for each piece of critical equipment.
    - UPS is a battery backup unit that can maintain power to processors, monitors, and other equipment for a period of minutes.
    - UPS units can also function as surge protectors, power noise, filters, and automatic shutdown devices when the battery runs low.
    - For longer blackouts a generator is needed.

Human Based Threats

Human-caused threats are less predictable than other types of physical threats. Humans seek the most vulnerable points.

- **Unauthorized physical access** – Servers, mainframe computers, network equipment, and storage networks are generally located in a restricted area, with access limited to a small number of employees.
- **Unauthorized physical access** can lead to other threats, such as theft, vandalism, or misuse.
- **Theft** of equipment and theft of data by copying or Eavesdropping and wiretapping
- **Vandalism** – destruction of equipment and data
- **Misuse –** improper use of resources by those who are authorized to use them, or not authorized at all

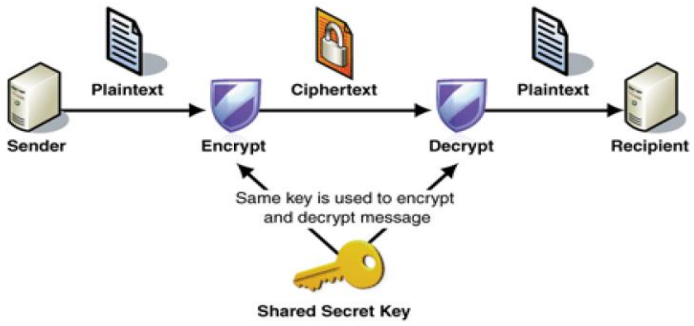
Countermeasure: One general prevention measure: is the use of ***cloud computing***.

- Restricting access to the building in which the resource is housed. Does not address the issue of unauthorized insiders or employees.
- Putting the resource in a locked cabinet, safe, or room.
- A machine may be accessed, but it is secured to an object that is difficult to move.
- A movable resource is equipped with a tracking device so that a sensing portal can alert security personnel.
- A portable object is equipped with a tracking device so that its current position can be monitored continually.
- Surveillance systems are part of building security. Such systems should provide real-time remote viewing as well as recording.

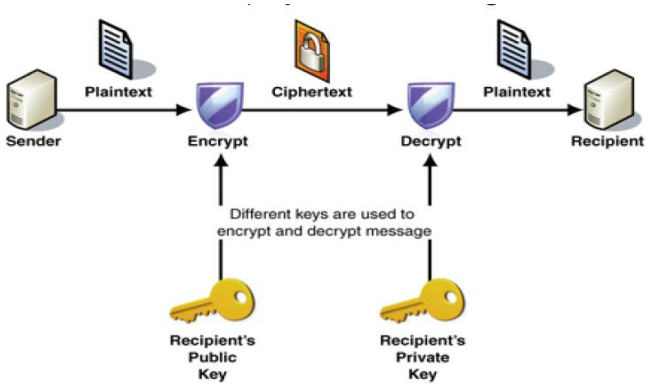
Algorithmic control

Encryption Schemes

1. **Symmetric encryption schemes -** The encryption key is the same as (bit by bit) the decryption key, or the decryption key can be calculated from the encryption key in polynomial time.



2. **Asymmetric encryption schemes -** The encryption key and the decryption key are different. Calculating the decryption key from the encryption key is infeasible (intractable). Infeasible: we do not know polynomial time algorithm for it.



	Symmetric	**Asymmetric**
Secrecy of the keys	keys are kept secret (K)	(PK; SK) public and secret key

Handling the keys	key exchange algorithms are needed	Public Key Infrastructure
Computational time	fast algorithms	slow algorithms
Size of messages	large size	small size
Examples	TDES, AES	RSA, ElGamal, elliptic curve encryption

Attacks

- The goal of the adversary:
  - to get the secret decryption key
  - to get the plaintext for a given ciphertext
- Attack scenarios:
  - Ciphertext Only Attack (passive attack)
  - Known Plaintext Attack (passive attack)
  - Chosen Plaintext Attack
    - Non-adaptive (passive attack)
    - Adaptive (active attack)
  - Chosen Ciphertext Attack
    - Non-adaptive (passive attack)
    - Adaptive (active attack)

Hash Functions

Definíció

By a hash function, we mean a map $H : \{0,1\}^* \to \{0,1\}^n$, $n \in \mathbb{N}$.

Thus, hash functions map arbitrarily long strings to strings of fixed length.

- e.g.: MD5, SHA-1, SHA-256, SHA-512, SHA-3(Keccak, 2015)
- verifying data integrity: Cryptographic hash functions can be used to check whether a file has been changed. The hash value of the file is stored separately. The integrity of the file is checked by computing the hash value of the actual file and comparing it with the stored hash value. If the two hash values are the same, then the file is unchanged.
- hash value is called message digest
- avalanche effect: If an input is changed slightly (for example, flipping a single bit), the output changes significantly (e.g., half the output bits flip)
- Typically, a cryptographic hash function H : X -> Y has three properties:

- **Preimage resistance**: Given $y \in Y$, it's computationally infeasible to find $x \in X$ such that $H(x) = y$.
- **Second preimage resistance**(weak collision resistant): Given x, it's computationally infeasible to find another x' such that $x \neq x'$ and $H(x) = H(x')$.
- **Collision resistance**(strong collision resistant): It's computationally infeasible to find any two distinct values $x, x' \in X$ such that $H(x) = H(x')$.

Digital Signatures

- **Properties:**
  - data integrity and
  - authenticity of the message
  - non-repudiation

Definíció

A signature scheme is a-tuple of three algorithms $DS = (Key, Sign, Ver)$ satisfying the following:

- *Key: The key-generation algorithm Key takes as input a security parameter k and outputs a pair of keys (PK, SK). These are called the public key and the secret key, respectively.*
- *Sign: The signing algorithm Sign takes as input a secret key SK and a message $m \in \{0,1\}^*$. It outputs signature $s = Sign_{SK}(m)$.*
- *Ver: The deterministic verification algorithm Ver takes as input a public key PK, a message m, and a signature s. It outputs TRUE meaning valid or FALSE meaning invalid.*

$\mathcal{M}$: message space
$\mathcal{S}$: signature space

Goals of the adversary

- **Total break:** The adversary can compute the signer's secret key and therefore forge any possible signature on any message.
- **Universal forgery:** The adversary can create a valid signature for any given message.
- **Selective forgery:** The adversary succeeds in forging the signature of some message of his choice.
- **Existential forgery:** The adversary succeeds in forging the signature of one message, not necessarily of his choice.

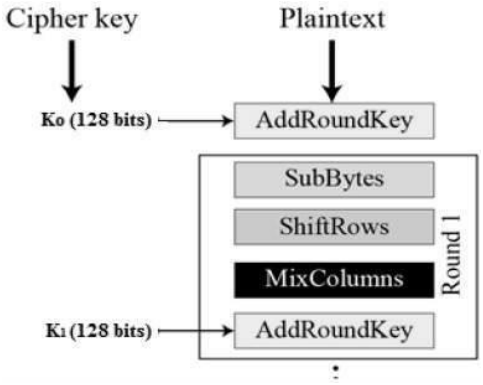
AES (Advanced Encryption Standard)

The features of AES are as follows −

- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details

Interestingly, AES performs all its computations on bytes rather than bits. Hence, AES treats the 128 bits of a plaintext block as 16 bytes. These 16 bytes are arranged in four columns and four rows for processing as a matrix. AES uses 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Each of these rounds uses a different 128-bit round key, which is calculated from the original AES key.

Each round comprises of four sub-processes



Byte Substitution (SubBytes) – The 16 input bytes are substituted by looking up a fixed table (S-box) given in design. The result is in a matrix of four rows and four columns.

Shiftrows – Each of the four rows of the matrix is shifted to the left. Any entries that 'fall off' are re-inserted on the right side of row. Shift is carried out as follows −

- First row is not shifted.
- Second row is shifted one (byte) position to the left.
- Third row is shifted two positions to the left.
- Fourth row is shifted three positions to the left.
- The result is a new matrix consisting of the same 16 bytes but shifted with respect to each other.

MixColumns – Each column of four bytes is now transformed using a special mathematical function. This function takes as input the four bytes of one column and outputs four completely new bytes, which replace the original column. The result is another new matrix consisting of 16 new bytes. It should be noted that this step is not performed in the last round.

Addroundkey – The 16 bytes of the matrix are now considered as 128 bits and are XORed to the 128 bits of the round key. If this is the last round then the output is the ciphertext. Otherwise, the resulting 128 bits are interpreted as 16 bytes and we begin another similar round.

The process of **decryption** of an AES ciphertext is similar to the encryption process in the reverse order. Each round consists of the four processes conducted in the reverse order.

RSA

Asymmetric encryption scheme: AE = (Key; Enc; Dec)

- Key:
  1. Randomly choose two large primes: p, q.
  2. Calculate RSA modulus: $n = p \cdot q$.
  3. Calculate Euler totient: $\phi(n) = (p-1)(q-1)$.
  4. *Randomly choose* an integer e: $1 < e < \phi(n)$ and $(e, \phi(n)) = 1$. (e is the encryption exponent)
  5. Calculate d: $1 < d < \phi(n)$ and $ed \equiv 1 \pmod{\phi(n)}$. ($d$ is the decryption exponent)

  $PK = (n, e)$, $SK = d$ and $\phi(n), p, q$ are secret parameters
  $\mathcal{P} = \mathcal{C} = \mathbb{Z}_n$
- $Enc_{PK}(m) = m^e \pmod{n}$ $\forall m \in \mathcal{P}$ and for a $PK = (n, e)$.
- $Dec_{SK}(c) = c^d \pmod{n}$ $\forall c \in \mathcal{C}$ and for a $SK = d$.

Example:

Asymmetric encryption scheme: $AE = (Key, Enc, Dec)$

- Key:
  1. Randomly choose two large primes: $p = 5, q = 11$.
  2. Calculate RSA modulus: $n = p \cdot q = 55$.
  3. Calculate Euler totient: $\phi(n) = (p-1)(q-1) = 40$.
  4. *Randomly choose* an integer e: $1 < e < \phi(n)$ and $(e, \phi(n)) = 1$, $e = 3$.
  5. Calculate d: $1 < d < \phi(n)$ and $ed \equiv 1 \pmod{\phi(n)}$, $d = 27$.

  $PK = (n = 55, e = 3)$, $SK = d = 27$ and
  $\phi(n) = 40, p = 5, q = 11$ are secret parameters
  $\mathcal{P} = \mathcal{C} = \mathbb{Z}_{55}$
- $m = 8$ and $PK = (55, 3)$: $Enc_{PK}(m) = 8^3 \pmod{55}$
  $8^3 \equiv 17 \pmod{55}$
- $c = 17$ and $SK = 27$: $Dec_{SK}(c) = 17^{27} \pmod{55}$
  $17^{27} \equiv 8 \pmod{55}$

Attacks against textbook RSA

- **Special Message Spaces** - Try each possible plaintext from the special message space. (Brute Force)
- Relationship between Encrypted Messages.