THREATS, ATTACKS, VULNERABILITIES, AND COUNTERMEASURES
Countermeasure: A safeguard that addresses a threat and mitigates risk.

Countermeasures are the controls and techniques to adopt in order to mitigate or prevent the exploitation of vulnerabilities of a specific software component.
Security Concepts

- The following key security concepts provide a frame for thinking about security when designing and architecting services:
  - **Auditing and Logging**: is used to monitor and record important activity, such as transactions or user management events, on both the client and the service.
  - Logged information should be recorded and stored to enable efficient auditing of events in the case of an attack or a suspected attack.
  - **Threats and attacks include**:
    - **Repudiation**: threat action aimed to perform illegal operations in a system that lacks the ability to trace the prohibited operations.
    - **Denial of service (DoS)**: An attacker overwhelms logs with excessive entries or very large log entries.
    - **Disclosure of confidential information**: An attacker gathers sensitive information from log files.
Security Concepts

- **Vulnerabilities include:**
  - Failing to audit failed logons.
  - Storing sensitive information in log files.

- **Countermeasures include:**
  - Identify malicious behavior.
  - Create secure audit trails.
Security Concepts

- **Authentication** is the mechanism by which your clients can establish their identity with your service, using a set of credentials that prove that identity. A username is an example of an identity, while a password is an example of a credential.

- **Threats and attacks include:**
  - **Network eavesdropping.** An attacker steals identity and/or credentials off the network by reading network traffic not intended for them.
  - **Brute force attacks.** An attacker guesses identity and/or credentials through the use of brute force.
  - **Dictionary attacks.** An attacker guesses identity and/or credentials through the use of common terms in a dictionary designed for that purpose.
Security Concepts

- **Vulnerabilities:**
  - Weak password policies
  - Passwords stored insecurely
  - Using weak authentication mechanisms

- **Countermeasures include:**
  - Use strong password policies.
  - Do not store credentials in an insecure manner.
  - Use authentication mechanisms that do not require clear text credentials to be passed over the network.
  - Encrypt communication channels to secure authentication tokens.
Security Concepts

• Authorization is a process by which a server determines if the client has permission to use a resource or access a file.
• Authorization is usually coupled with authentication so that the server has some concept of who the client is that is requesting access.

- Threats and attacks include:
  - Elevation of privilege. A user with limited privileges assumes the identity of a privileged user to gain privileged access to an application. For example, an attacker with limited privileges might elevate his or her privilege level to compromise and take control of a highly privileged and trusted process or account
  - Disclosure of confidential data.
  - Sensitive data is exposed in some unintended way to users who do not have the proper privileges to see it.
Security Concepts

- **Token stealing.** An attacker steals the credentials or token of another user in order to gain authorization to resources or operations they would not otherwise be able to access.

  - **Vulnerabilities:**
    - Relying on a single gatekeeper (e.g., relying on client-side validation only).
    - Using inadequate separation of privileges.

  - **Countermeasures:**
    - Use least-privileged accounts.
    - Enforce separation of privileges. Avoid building generic roles with privileges to perform a wide range of actions. Roles should be designed for specific tasks and provided the minimum privileges required for those tasks.
    - Use multiple gatekeepers. You should have one entry point that is secured. Within that channel, you might setup multiple gatekeepers, so that in the event there is a compromise, you can slow an attacker down, by creating more hurdles to jump through - or multiple choke-points for your application. However, you have to balance the complexity of multiple gatekeepers with keeping your design simple and easy to manage.
Security Concepts

- **Configuration Management**: Security settings, authentication, authorization, logging, and other parameters can usually be set in configuration files. Improper configuration can lead to security vulnerabilities.

- **Threats and attacks include:**
  - **Unauthorized access to configuration stores**: An attacker gains access to configuration files and is able to modify binding settings, etc.
  - **Retrieval of clear text configuration secrets**: An attacker gains access to configuration files and is able to retrieve sensitive information such as database connection strings.
Security Concepts

- **Vulnerabilities include:**
  - Using insecure configuration stores.
  - Storing clear text configuration data.
  - Using insecure administration interfaces. Unauthorized access to administration interfaces, ability to update configuration data, and unauthorized access to user accounts and account profiles.
  - Having too many administrators.

- **Countermeasures include:**
  - Encrypt sensitive sections of configuration files.
  - Use secure settings for various operations of Web services using configuration files.
**Security Concepts**

- **Message encryption** is used to protect sensitive data in-transport over the network. Encryption does not protect the integrity of the data, but only its confidentiality. Message encryption can be provided by either message security or transport security. Message security encrypts each message individually, while transport security encrypts the entire communication channel (e.g., with SSL).

- **Threats and attacks include:**
  - **Failure to encrypt messages.** An attacker is able to read message content off the network because it is not encrypted.
  - **Theft of encryption keys.** An attacker is able to decrypt sensitive data because he or she has the keys.
  - **Man-in-the-middle attack.** An attacker can read and then modify messages between the client and the service.
  - **The man-in-the-middle attack: in cryptography and computer security is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.**
Security Concepts

- **Vulnerabilities include:**
  - Not encrypting messages.
  - Using custom cryptography.
  - Distributing keys insecurely.
  - Managing or storing keys insecurely.
- **Countermeasures include:**
  - Use message security or transport security to encrypt your messages.
**Security Concepts**

- **Message signing** is used to protect the integrity of messages in transit over the network and to provide proof of the original sender. Signing does not protect the confidentiality of the data, but only its integrity and confidence in the original sender. Message signing can be provided by either message security or transport security. Message security signs each message individually, while transport security protects the entire communication channel (e.g., with SSL).

- **Threats and attacks include:**
  - **Data tampering.** An attacker modifies the data in a message in order to attack the client or the service.

- **Vulnerabilities include:**
  - Not using either message or transport security.

- **Countermeasures include:**
  - Turn on message or transport security.
A brute force attack is a trial-and-error method used to obtain information such as a user password or personal identification number (PIN). In a brute force attack, automated software is used to generate a large number of consecutive guesses as to the value of the desired data. Brute force attacks may be used by criminals to crack encrypted data, or by security analysts to test an organization's network security.
Sensitive Information in Log Files

- Every action you make on the Internet is logged somewhere.
- These records don't necessarily directly reveal who you are or where you live, but nonetheless they can contain a lot of sensitive information about you, your behavior and interests.