

# Wrap-up; Terms and definitions from Course 5, Week 2

Our focus in this section was on a major theme of security: protecting assets.

A large part of this relates to privacy.

We should all enjoy the right to decide who can access our information.

As we learned, there are several controls in place that help secure assets.

We began the section by exploring effective data handling processes that are founded on the principle of least privilege.

We then explored the role of encryption and hashing and safeguarding information.

We explored how symmetric and asymmetric encryption works and how hashes further safeguard data from harm.

We then turned our attention to standard access controls. Properly authenticating and authorizing users is what maintaining the CIA triad of information is all about!

We used the AAA framework of security to take a detailed tour of identity and access management systems and the access controls that validate whether or not someone is who they claim to be.

Well done making it through the first half of the course!

You're making great progress so far, and I hope you keep it up.

Remember, your background and experiences are valuable in this field.

This combined with the concepts we're covering will make you a valuable contributor to any security team.

Up until this point, we've been exploring the defensive side of security, but security isn't all about planning ahead and waiting for something to happen.

In the next part of our journey,

we're going to continue developing a security mindset by taking a more proactive look at security from the perspective of attackers.

I'll meet you there!

---

# Glossary terms from week 2

**Access controls:** Security controls that manage access, authorization, and accountability of information

**Algorithm:** A set of rules used to solve a problem

**Application programming interface (API) token:** A small block of encrypted code that contains information about a user

**Asymmetric encryption:** The use of a public and private key pair for encryption and decryption of data

**Basic auth:** The technology used to establish a user's request to access a server

**Bit:** The smallest unit of data measurement on a computer

**Brute force attack:** The trial and error process of discovering private information

**Cipher:** An algorithm that encrypts information

**Cryptographic key:** A mechanism that decrypts ciphertext

**Cryptography:** The process of transforming information into a form that unintended readers can't understand

**Data custodian:** Anyone or anything that's responsible for the safe handling, transport, and storage of information

**Data owner:** The person that decides who can access, edit, use, or destroy their information

**Digital certificate:** A file that verifies the identity of a public key holder

**Encryption:** The process of converting data from a readable format to an encoded format

**Hash collision:** An instance when different inputs produce the same hash value

**Hash function:** An algorithm that produces a code that can't be decrypted

**Hash table:** A data structure that's used to store and reference hash values

**Identity and access management (IAM):** A collection of processes and technologies that helps organizations manage digital identities in their environment

**Information privacy:** The protection of unauthorized access and distribution of data

**Multi-factor authentication (MFA):** A security measure that requires a user to verify their identity in two or more ways to access a system or network

**Non-repudiation:** The concept that the authenticity of information can't be denied

**OAuth:** An open-standard authorization protocol that shares designated access between applications

**Payment Card Industry Data Security Standards (PCI DSS):** A set of security standards formed by major organizations in the financial industry

**Personally identifiable information (PII):** Any information used to infer an individual's identity

**Principle of least privilege:** The concept of granting only the minimal access and authorization required to complete a task or function

**Protected health information (PHI):** Information that relates to the past, present, or future physical or mental health or condition of an individual

**Public key infrastructure (PKI):** An encryption framework that secures the exchange of online information

**Rainbow table:** A file of pre-generated hash values and their associated plaintext

**Salting:** An additional safeguard that's used to strengthen hash functions

**Security assessment:** A check to determine how resilient current security implementations are against threats

**Security audit:** A review of an organization's security controls, policies, and procedures against a set of expectations

**Security controls:** Safeguards designed to reduce specific security risks

**Separation of duties:** The principle that users should not be given levels of authorization that would allow them to misuse a system

**Session:** A sequence of network HTTP basic auth requests and responses associated with the same user

**Session cookie:** A token that websites use to validate a session and determine how long that session should last

**Session hijacking:** An event when attackers obtain a legitimate user's session ID

**Session ID:** A unique token that identifies a user and their device while accessing a system

**Single Sign-On (SSO):** A technology that combines several different logins into one

**Symmetric encryption:** The use of a single secret key to exchange information

**User provisioning:** The process of creating and maintaining a user's digital identity

---

Revision #5

Created 3 August 2023 08:59:46 by naruzkurai

Updated 15 August 2023 18:44:12 by naruzkurai