SECURE SOFTWARE DEVELOPMENT (SSD)

Diploma in ISF

Academic Year (AY) 20/21 – Semester 3 (April `20)

WEEK 1: FEEDBACK

SECURE SOFTWARE CONCEPTS

Source: Official (ISC)^2 Guide To The CSSLP CBK - Second Edition – by Mano Paul

Last Updated: 01/04/2020

Attacker Vs. Defender

- The defender
  - Play vigilante 24x7,
  - Guarding against all attacks
  - Constrained to play by the rules of engagement
- The attacker has the upper hand
  - Can strike anytime
  - Needs to be able to exploit just one weakness
  - Need not have to play by the rules

Secure Software Concepts

- Acronym: CIA – AAAA – N – P
  - Confidentiality
  - Integrity
  - Availability
  - Authentication
  - Authorization
  - Accountability
  - Auditing
  - Non-repudiation
  - Data Privacy
    - Data Anonymization
    - Personal Data Protection Act

Confidentiality

- Confidentiality is the security concept that has to do with protection against unauthorized information disclosure. It has to do with the viewing of data. Not only does confidentiality assure the secrecy of data but it also can help in maintaining data privacy.

Integrity

- Integrity is a security concept that assures protection against unauthorized alterations or modifications of data.
- Integrity of software has two aspects to it. First, it must ensure that the data that is transmitted, processed and stored is as accurate as the originator intended and secondly, the software performs reliably as it was intended to.

Availability

- Availability is the security concept that is related to the access of the software or the data or information it handles.
- It assures protection against denial of service.
- It also ensures business continuity program (BCP) where the system downtime is minimized and that the impact upon business disruption is minimal.

Authentication

- A security concept that verifies and validates identity information that is supplied.
- It answers the question “Are you who you claim to be?”
- Factors of authentication
  - What you know? – Password, PIN (memory)
  - What you have? – Security Token, Smartcard (physical)
  - Who you are? – Fingerprint, Iris scanner (Biometrics)

Authorization

- A security concept that has to do with the checking of an subject's rights and privileges before granting access to the objects that the subject requests.
- The requestor is referred to as the subject and the requested resource is referred to as the object. The subject may be human or non-human such as a process or another object. The subject may also be categorized by privilege level such as an administrative user, manager, or anonymous user.
- Examples of an object include a table in the database, a file or a view.

Authorization

- An example of authorization based on the privilege level of the subject is an administrative user may be able to create, read, update and delete (CRUD) data but an anonymous user may be allowed to only read (R) the data, while a manager may be allowed to create, read and update (CRU) data.

Accountability

- A security concept that protects against repudiation threats.
- Non-repudiation addresses the deniability of actions taken by either a user or the software on behalf of the user. Accountability to ensure non-repudiation can be accomplished by auditing when used in conjunction with identification.

Auditing

- A security concept that addresses the logging of transactions so that at a later time a history of transactions can be built, if needed.
- It answers the question, “Who (subject) did what (action) when (timestamp) and where (object)?”
- Auditing is a *detective* control and it can be a *deterrent* control as well.

Non-Repudiation

- A security concept that addresses the deniability of actions taken by the software or the user.
- It ensures that the actions taken by the software on behalf of the user (intentionally or unintentionally) cannot be refuted or denied.

Data Privacy

- Data privacy is suitably defined as the appropriate use of data. When companies and merchants use data or information that is provided or entrusted to them, the data should be used according to the agreed purposes.
- In some cases, companies have sold, disclosed, or rented volumes of the consumer information that was entrusted to them to other parties without getting prior approval.

Source: https://blog.eiqnetworks.com/blog/bid/313892/the-difference-between-data-privacy-and-data-security

Data Anonymization

- The act of permanently and completely removing personal identifiers from data, such as converting personally identifiable information (PII) into aggregated data.
- Anonymized data cannot be linked to any one individual account.
- Anonymization techniques are useful to assure data privacy.
- These techniques include:
  - Replacement.
  - Suppression.
  - Generalization
  - Pertubation

Personal Data Protection Act

- Refer the link below:
  - https://www.pdpc.gov.sg/legislation-and-guidelines/overview