Ngee Ann Poly (CSF)

SECURE SOFTWARE DEVELOPMENT (SSD)

Mission 2.1:

Secure Software Concepts (CIA-AAAA-NP)

By:

Tan Jia Shun

CSF02

03/03/2020

Contents

[Attacker vs Defender in cybersecurity 3](#_Toc39401752)

[What is CIA Triad? 3](#_Toc39401753)

[Confidentiality 3](#_Toc39401754)

[Integrity 3](#_Toc39401755)

[Availability 3](#_Toc39401756)

[What is Authentication, Authorization, Auditing, Accountability? 3](#_Toc39401757)

[Authentication 3](#_Toc39401758)

[Authorization 3](#_Toc39401759)

[Auditing 3](#_Toc39401760)

[Accountability 3](#_Toc39401761)

[Explain Non-Repudiation, Data Privacy, Data Anonymization, Personal Data Protection Act. 4](#_Toc39401762)

[Non-Repudiation 4](#_Toc39401763)

[Data Privacy 4](#_Toc39401764)

[Data Anonymization 4](#_Toc39401765)

[Personal Data Protection Act (PDPA) 4](#_Toc39401766)

# Attacker vs Defender in cybersecurity

Attacker and defender in cybersecurity is like a 2-sided card, they may be doing the same thing but with opposite purpose. For attacker, what they do is access and get data from target that they may want to share but for defender, what they do is protect data you do not want to share. For explain, a attacker maybe working on compromise someone password reset process but on the other hand, the defender will be hardening the password reset process, but is working on password reset process but one is to protect and the other is to attack.

# What is CIA Triad?

CIA triad have three component which help to maintain a good security and they are:

## Confidentiality

It ensures that only authorised person can read or access the data. So that important data protected and will not be revealed to unwanted parties.

## Integrity

It prevents unauthorized alteration of data when sending from point to point as it the data may be sabotage or corrupted from software error, virus or hardware failures.

## Availability

Data should be available to all authorised user at all time. If the data is not reachable or taking too long to received, it can affect many organization workflows. For explain, you need to access a data file that your clients need but you cannot access it, it can affect your client wanting to work with your organization in the future.

# What is Authentication, Authorization, Auditing, Accountability?

## Authentication

A proof of user identity where the system can authenticate the user.

It can be done using:

1. Something you know: username and password
2. Something you are: fingerprint or face scan
3. Something you have: physical token
4. Something you do: signature

## Authorization

Checking of user permission or privilege given to the user to access or performing a certain action.

## Auditing

To control every access to the system so every authorised user have a restricted access to the system. This feature is mainly used to protect against unauthorized disclosure, corruption, modification, and destruction. This act as the first line of defence to avoid the unauthorized access and entry.

## Accountability

Tracking of data, resources and network usage. This allow system administrators to monitor all user activities and if user activities look suspicious, they are able to determine and traced back using the audit trails.

# Explain Non-Repudiation, Data Privacy, Data Anonymization, Personal Data Protection Act.

## Non-Repudiation

Non-Repudiation create evidence of event or action done on the system. Proving data integrity.

This is done using:

* Digital Signature
  + Proving of sender identity
* Timestamps
  + Prove the time and date when a certain event occurred explain the date and time when a document is composed.

## Data Privacy

Data privacy is how data is collected, shared, deleted and used by third parties. Every user has different privacy preferences and have the rights to know what data user lend to the third parties is used for. Therefore, there is also many data privacy laws to protect individuals right of their privacy.

## Data Anonymization

Data Anonymization is a process to protect private data by erasing or encrypting identifiers that connect an individual to stored data this help to keep the source anonymous, preventing attacker from attacking the data source. This also help to protect data as it have many data protection techniques too, for explain it has data masking which hide data with altered values using character shuffling, encryption, and word or character substitution techniques, making reverse engineering or detection impossible

## Personal Data Protection Act (PDPA)

PDPA protect individual personal data by setting various rule governing the collection, use, disclosure and care of personal data. It gives individual the rights to protect their personal data including rights of access and correction, and the needs of organisations to collect, use or disclose personal data for legitimate and reasonable purposes.

All organisation must comply to PDPA as well as the country common law specific industry law when handling personal data or else it may liable to a fine of up to $10000 per offence

Concepts of PDPA:

* Consent
  + Organisations may collect, use or disclose personal data only with the individual's knowledge and consent (with some exceptions).
* Purpose
  + Organisations may collect, use or disclose personal data in an appropriate manner for the circumstances, and only if they have informed the individual of purposes for the collection, use or disclosure.
* Reasonableness
  + Organisations may collect, use or disclose personal data only for purposes that would be considered appropriate to a reasonable person in the given circumstances.