Subject :

Nathan House - Volume 1: The Threat & Vulnerability Landscape

know yourself

* We can create files such that when someone opens that file, or click on a link, you are notified about it on email.
  - → go to stationX canary tokens
  - → generate canary token
  - → get notified when someone opens it

* Protect what you value the most. Identifying the security assets is the most important. Eg: Personal Identifiable Information or your credit card details.
* Privacy is nobody seeing what you do, but potentially knowing, who you are. Eg. an encrypted email to a friend.
* Anonymity is nobody knowing who you are, but potentially seeing what you do. Tor is an anonymizing service.
* Pseudonymity is when you wish to gain a reputation against an identity. Eg. If someone is on the social media with a different fictional name, then you may not know who they are but you can attribute posts & activities to them. (A false identity)

* All of the above are assets that we want security from threats posed by adversaries.
* A threat will try to exploit vulnerabilities in your security to access your assets.

$$\text{Risk} = (\text{Vulnerabilities}) \times (\text{Threats}) \times (\text{Consequences})$$

* Risk Assessment: Identifying assets that you want to protect from exploitation.

Subject :

PAGE NO.:
DATE:

★ 100% risk & 100% anonymity are not guaranteed. You are never 100% protected.

★ Threat modelling:

① Select the security system you want to integrate

↓

② Implement the chosen system

↓

③ Assess the effectiveness of the system

↓

④ Monitor the system to check if a weakness is discovered.

★ Privacy & Anonymity ∝ Security you need

★ To select the appropriate security control, we do risk assessment.

→ The security controls need to enable security attributes.

→ For every asset, think about:

- Confidentiality: Do you want the asset to be disclosed?
- Integrity: Do you want the asset to be unintentionally altered? (No modifications)
- Availability: Do you want it to be destroyed? (Available when needed)

∴ CIA → Confidentiality, Integrity, Availability

∴ A person requesting security over an entity must inform what they need? They need C? I? A?

- The CIA doesn't cover all security needs. Hence, we need a more comprehensive attribute system.

Subject :

PAGE NO.:
DATE:

★ Parkerian Hexad: Six Security Attributes

→ Confidentiality
→ Possession (Loss of Control)
→ Integrity
→ Authenticity (Authorship)
→ Availability
→ Utility (Usefulness)

★ There are three other security attributes, not a part of Hexad:

→ Non-repudiation (Sender cannot deny sending a message)
→ Authorization (what permissions you have)
→ Authentication (verifies the identity of the user)

★ Defence-in-Depth: If one fails, other can defend.

Prevention (eg. encryption) → Detect (eg. canary token) → Recover

★ Zero Trust Model: The lesser you trust, the lower your risk.
→ Mitigate the risk by distributing the trust

∝ ∝ ∝