IMT3501 - Threat Modeling and Privacy Assessment Lab

In this task, you are required to conduct an overall threat modeling process by characterizing threat information (assets, adversary and adversary action etc.) originating from various threat agents, to identify, analyze and discus all possible threats and better comprehend all types of threats to Out-patient Healthcare Monitoring System. Moreover, propose and suggest a list of countermeasures (security control) that are better for designing and implementing system protection solutions.

I. Threat Modeling Task

1. Understanding the concept of threat modeling.
2. Know when and why you should build a threat model and what it should document in it.
3. Build a basic but actionable threat model for your system.
4. Use a framework/tools that you feel more confident that would help you to threat model your system.

What the students are required to do:

1. Describe your system:
   - Revisit task 1 and identify and prioritize the system assets.
     - Sensitive and personal information.
     - What are the most critical assets for your system. Categorize based on CIA properties.
     - Does your system access/use/share assets with/ to other third party.
   - What are the trust levels of system users and threat agents?
     - Who are the eligible users (actors) in your system (revisit use cases)?
     - What is the role(s) will the eligible users (actors) play in your system?
     - Who are the ineligible users (threat agents) that may jeopardize your system?
     - How the eligible users' role(s) can be compromised by the ineligible users (threat agents) and jeopardize your system and the eligible users (actors)' data?
   - Revisit the general architecture you created and the functionalities you defined in the use cases, then design the system in terms of DFD (Data Flow Diagram)
     - Define the high-level way of disassembling the system and focusing on its functional components, and to analyze the flows of data through the system components.
2. Identify potential threat sources
   - What are the major threats? Focus on threat identification and classification based on:
     - Threat to system/ data confidentially
     - Threat to system/ data integrity
     - Threat to system/ data availability
     - Threat to the system eligible users (actors) authentication
     - Threat to the system eligible users (actors) authorization
     - Threat to the system eligible users (actors) non-repudiation

- Threat to the system eligible users (actors) privacy
- Which threats can happen to what use case (misuse case scenarios)?
  - Which threat would trigger what use case?
  - How would threat agents proceed/preform the attack?
  - What is the risk and the impact for your system according to the list of the identified threats (prioritize the threats)?

3. How should these threat/ attacks be prevents/mitigated?
   - Define the threat/risk security control
   - Threat mitigation plan
4. Document the threat modeling process
   - What has been done
   - Recommendation to the design team or/and to the policy makers at your organization (based on your findings of the threat modeling, what you think the policy makers/ designers, management board etc. should highly consider before they implement and deploy the system.). Focus on non-technical recommendation

Hints and tips:

i. Threat modeling methodologies:
   - Microsoft STRIDE model

ii. Recommended the use of figure and tables to map system components, assets, threat agents, threats to security control and mitigation plan.