CSCE 5565 Quiz 2- Fall 2023

Question 1 (10 points)

What is the difference between attack tree and fault tree?

Attack tree	**Fault tree**
Analyzes security threats and vulnerabilities	Analyzes errors and system failure scenarios
Security risks and breaches	System reliability, safety, and failures
Eg: Used to access the security of network, software application, or system, etc., (partial)	Eg: Used in analyzing the reliability of a manufacturing process, or aircraft, etc., (partial)
Attack tree represents attacks against a system in a tree structure, with the goal as the root node and different ways of achieving that goal as leaf nodes.	Fault-tree analysis is a top-down approach to identify the component level failures (basic event) that cause the system level failure (top event) to occur.

One proper and exact difference gets 10 marks.

Problem (30 points)

You have been tasked with providing security expertise for the development of a fleet management system. The figure below illustrates the architecture of the system.

Question 2.1. Utilize the SRIDE method to identify and enumerate the threats relevant to the server sub-system located on the right side of the figure below.

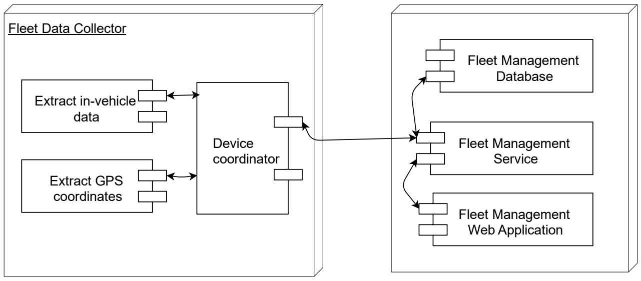
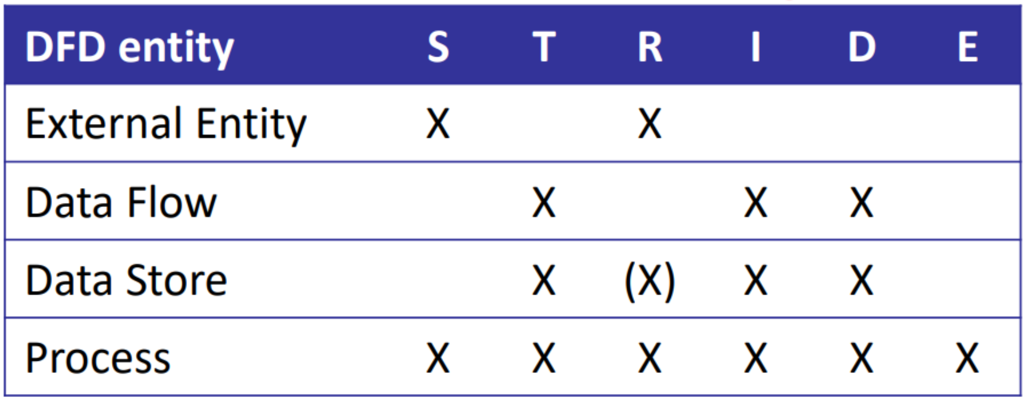


Figure 1: Architecture of the fleet management system.

STRIDE for Fleet Management Database is like Data Store in below table.

STRIDE for Web Application is like Process in below table.

STRIDE for Fleet Management Service is like Data Flow in the table below.



DFD entity	S	T	R	I	D	E
External Entity	X		X			
Data Flow		X		X	X	
Data Store		X	(X)	X	X	
Process	X	X	X	X	X	X

STRIDE for process – 5 Marks and STRIDE for other (either one) – 5 Marks.

Question 2.2. List three threats to the system depicted in Figure 1. For each threat, detail at least one attacker capability necessary to exploit it.

Threat	**Attacker capability**
Spoofing the position	Physical access to the device GPS system
Deleting records of the drivers	Remote access to the web application
Deleting the records of a driver	Physical access to the database server

Above are a few examples of threats and attacker capabilities. Providing at least 3 would give full marks. Each one with attacker capability carries 3-4 Marks.

Question 2.3. Determine the risk exposure associated with the threat of 'Falsifying the position of a vehicle managed by the fleet management system.' Show your process for estimating this risk exposure.

Likelihood:

- Elapsed time – few days

- Required expertise – Moderate expertise

- Required knowledge of the system – expert knowledge

- Window of opportunity – few hours

- Required equipment and tool – GPS Spoofing hardware

Bonus to all.