Assignment 01 – Notebook

Task 1: Read the Paper (0 points)

Paper: ARANZAZU-SUESCUN, Catalina et al. Securing IoT Surveillance Airport Infrastructure. In: **2024 International Conference on Smart Applications, Communications and Networking (SmartNets)**. IEEE, 2024. p. 1-7.

The paper discusses implementing an airport surveillance system using the Internet of Things (IoT), focusing on the MQTT protocol and its associated security threats. This document addresses the following key questions:

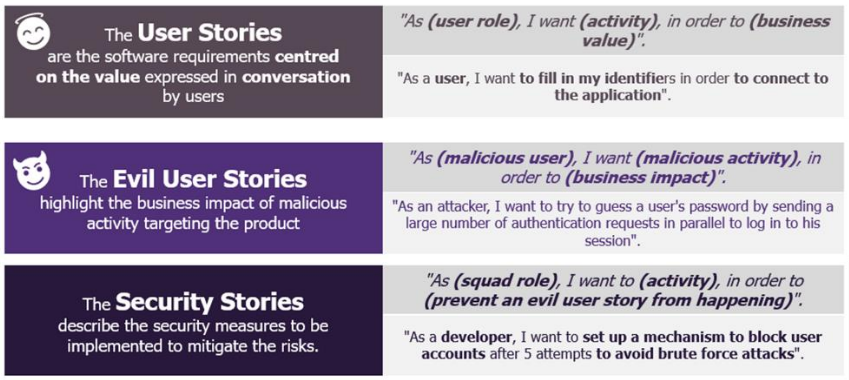
- What is the publisher/subscriber pattern, and how is it implemented within the MQTT protocol?
- What are the primary security threats to an airport surveillance system utilizing MQTT?

Task Submission: You do not need to submit anything in this task.

Task 2: Requirement Elicitations (10 points)

Based on the previous paper and using the problem presented in the CYSE Final Project, create a set of evil and security stories that describe how the MQTT will be used in the study case environment.

- **Tip 1:** Define the evil and security stories using the following STANDARD.



The **User Stories** are the software requirements **centred on the value** expressed in **conversation** by users	*"As **(user role)**, I want **(activity)**, in order to **(business value)**".* "As a **user**, I want **to fill in my identifiers** in order **to connect to the application**".
The **Evil User Stories** highlight the business impact of malicious activity targeting the product	*"As **(malicious user)**, I want **(malicious activity)**, in order to **(business impact)**".* "As an attacker, I want to try to guess a user's password by sending a large number of authentication requests in parallel to log in to his session".
The **Security Stories** describe the security measures to be implemented to mitigate the risks.	*"As **(squad role)**, I want to **(activity)**, in order to **(prevent an evil user story from happening)**".* "As a **developer**, I want to **set up a mechanism to block user accounts** after 5 attempts **to avoid brute force attacks**".

- **Tip 2:** Remember, the focus is on business language. You must map the security issues of the MQTT in a specific domain problem, in other words, how its issues could impact the goal of the rescue system proposed in the project problem definition.

Task Submission: You must submit a Word file with the evil and security cases using the directions provided.

Task 3: Architecture of the Problem Description using DFD (20 points)

Using the methodology proposed in the classroom, develop a DFD that represents the system, given that it will be designed to support the following evil and security user cases. Use the OWASP Threat Dragon[1] To document the system's architecture. Your work has identified which components the reference evil and user stories affect and enumerates the threats using the standard proposed in the following table.

Tip 1: Remember to represent the study case architecture in your DFD.

Tip 2: Use the method explained in the classroom and the study case provided to avoid conceptual mistakes.

Tip 3: Remember that your model must be used to answer the spinoff questions based on the proposed requirements (documentation, evil, and security stories). Also, the model could provide enough details of threat enumeration (task 4).

Tip 4: Poor model (DFD) impacts the other tasks.

Tip 5: For each DFD component, you must fill in the description in the OWASP Threat Dragon.

Task Submission: You must submit the JSON file created using the OWASP Threat Dragon and the PDF.

Task 4: Threat Enumeration using STRIDE (40 points)

Based on the previous information, enumerate the threats related to the evil and security stories using the STRIDE. Use the OWASP Threat Dragon to document the threat enumeration using STRIDE. Your work has identified which components of reference evil and user stories affect and enumerate the threats, utilizing the standard proposed in the following table.

It is crucial to avoid generic threat enumeration and contextualize it with the scenario, as research on the Internet shows how this threat happens in real scenarios. It does not mean that you must be a prolix.

[1] https://www.threatdragon.com

Threat Enumeration Standard	
*[**threat source**] [**prerequisites**] can [**threat action**], which leads to [**threat impact**], negatively impacting [**impacted assets**].*	
Spoofing Example	**Denial of Service Example**
*[**A sniffer tool**] [**with access to the channel**] can [**monitor it**], which leads to [**could insert fake messages**], negatively impacting [**the reliability of the system**].*	*[**A hacker**] [**with access to the channel and a packages generator**] can [**flood the channel**], which leads to [**the system not handling legitimate messages**], negatively impacting [**its availability**].*

- **Tip 1:** The treat enumeration must be contextualized with the problem.
- **Tip 2:** The treat enumeration could not be generic and must consider that it is already defined the MQTT solution (Eclipse Mosquitto[2]).
- **Tip 3:** Use external libraries to support your enumeration (CAPEC, CWE, CVE).
- **Tip 4:** For each enumeration, you must submit a short description (a page maximum) explaining in detail (technical the enumeration), including citing the CAPEC or CWE/CVE used to support your explanation.
- **Tip 5**: You must submit the JSON file created using the OWASP Threat Dragon with the **following fields must be filled.**

Field	Description
Title	A concise description of the threat.
Type	STRIDE category
Description	The threat enumeration must follow the above standard. To complement the information, **add a new line with the Likelihood.**

Task Submission:

[2] https://mosquitto.org/

- You must submit the JSON file created using the OWASP Threat Dragon and the PDF.
- You must submit a Word file with a technical explanation about the enumerated threats.

Task 5: Attack Flow (30 points)

After an initial investigation, your group discovers that a group of hackers used a derivation of the **Golden Cup**[3,4] Spyware will implement a command-and-control channel using the MQTT protocol. Based on its insight, design an attack flow that enumerates this attack.

You must use the MITRE Attack Flow tools to design the attack flow.[5]. Attack flow is a data model with supporting tooling and examples for describing sequences of adversary behaviors. Attack flows help defenders understand, share, and make threat-informed decisions based on the sequence of actions in a cyber-attack. Flows can be analyzed to identify common patterns in adversary behavior, overlayed on ATT&CK Navigator layers to understand defensive coverage, and create a foundation for intel-driven adversary emulation plans.

Tip 1: Understand the original use of the Golden Cup and understand each change are required to be effective in the new scenario (observation: maybe it is not required nothing…).

Task Submission:

- You must submit the "afb" file created inside the MITRE Attack Flow.
- You must submit a Word file with a technical explanation (1 page long) about the specific attack flow, showing the difference from the original exploitation case.

[3] https://attack.mitre.org/software/S0535/

[4] https://www.itpro.com/spyware/31458/attackers-targeting-world-cup-fans-with-golden-cup-android-app-loaded-with-spyware

[5] https://mitre-engenuity.org/cybersecurity/center-for-threat-informed-defense/our-work/attack-flow/