**Group Exercise: Threat Modelling a Space System**

**Dr Basel Halak, University of Southampton (basel.halak@soton.ac.uk)**

**Objective**: Develop a threat model for a fictional satellite system using concepts covered in the lecture. Your goal is to identify potential security risks and propose appropriate mitigation strategies.

1. **Scenario Overview**

You are performing a security analysis for a fictional Earth observation satellite system operated by "OrbitSafe Corp." Below is a high-level description of the system, which you will use to conduct the threat model.

1. **System Description**

The satellite system is composed of four primary segments: User Segment, Ground Segment, Link Segment (Communication), and Space Segment (Satellite). In the **User Segment**, mission operators and data analysts access satellite data and control the satellite through a software application called **OrbitView**. They authenticate via usernames, passwords, and multi-factor authentication (MFA) and have remote access to the platform. The **Ground Segment** includes ground stations responsible for sending commands and receiving data, consisting of a Mission Control Centre and a Data Processing Centre. These stations use private networks, VPNs, and firewalls to secure data transfer and system integrity. The **Link Segment** handles uplink and downlink communications, transmitting commands to the satellite and receiving data. This communication relies on radio frequencies and satellite-specific protocols, with encryption ensuring the security of data transfer. In the **Space Segment**, the satellite captures high-resolution images, transmits data to the ground segment, and manages on-board operations through an autonomous computing system. Security measures include encrypted data storage, anti-jamming capabilities, and tamper-resistant hardware.

1. **Student Tasks**

Each group will work through the following steps to develop a threat model for the system. The aim is to analyse the description collaboratively, identify risks, and propose solutions.

**Step 1: Identify Key Assets & Segments**  
Discuss and identify the critical assets in the system that need protection, considering all segments: user, ground, link, and space. Think about what data, controls, and interfaces are crucial to the system's functioning and security. For example, you might ask what data most valuable, which communications are most sensitive, and where the main risks lie. As a deliverable, create a list of key assets and draw a high-level diagram of the satellite system, illustrating how segments connect and interact.

**Step 2: Brainstorm Potential Threats**  
Using the STRIDE framework, identify threats for each segment. Consider spoofing attacks, where an adversary could impersonate legitimate users; tampering scenarios, where data or communications might be altered; and other concerns such as information disclosure risks, denial-of-service attacks, and privilege escalation attempts. For each identified threat, discuss its potential impact on system security and operations. The goal is to compile a list of threats for each segment and assess their implications.

**Step 3: Analyse Risks & Prioritize**  
With a clear list of threats, analyse their likelihood and impact on the system. Discuss which threats are most probable and what consequences they might have if realized. Prioritize the risks based on severity and potential damage to the mission. As an outcome, produce a prioritized list of threats, emphasizing those that are both likely and have high potential impact.

**Step 4: Propose Mitigations & Countermeasures**  
For the high-priority threats, brainstorm and propose mitigation strategies. Discuss how you might apply security controls, such as encryption, access control mechanisms, or tamper-resistant hardware. Consider the use of HSM to protect against specific threats. For example, you could debate how encryption might protect the data stream or whether tamper-resistant features could safeguard on-board systems. Your deliverable is a set of countermeasures for each high-priority threat, along with explanations of how these security measures address the identified risks.

**Step 5: Report back your main findings**