Assignment 1:
System Characterization and Risk Categorization

February 6, 2025

Objective

To thoroughly understand the AeroTech X9 drone system's architecture, data flows, and operational context, and to accurately categorize its information system based on potential impact levels according to federal guidelines.

Background

The **AeroTech X9** is an advanced UAV designed by AeroTech Industries for multi-sector applications. Key features include:

- **Autonomous Navigation**: AI-driven obstacle avoidance and dynamic route optimization.
- **High-Resolution Imaging**: 4K camera and thermal sensors for detailed data capture.
- **Secure Communication**: Encrypted data transmission using AES-256 and RSA algorithms.
- **Modular Payloads**: Customizable payload bays for various mission-specific equipment.
- **Extended Range and Endurance**: Capable of 4-hour flights covering up to 200 km.
- **Real-Time Data Processing**: Onboard edge computing for immediate analysis.

Instructions

1. System Description

Provide a comprehensive overview of the AeroTech X9 drone system, covering the following aspects:

1. **Purpose and Capabilities**:
    - Explain the intended use cases of the X9 across different sectors.
    - Detail the drone's capabilities, including flight performance, sensor suites, and communication mechanisms.
2. **System Components**:
    - List all hardware components (e.g., airframe, propulsion system, sensors, communication modules).
    - Describe the software components, including the operating system, navigation algorithms, and data processing applications.
    - Identify any third-party components or services integrated into the system.
3. **Stakeholders**:
    - Identify all stakeholders, including operators, maintenance personnel, end-users, clients, and regulatory bodies.
    - Discuss the roles and responsibilities of each stakeholder group.
4. **Operational Environment**:
    - Describe the various environments where the X9 operates (urban, rural, maritime, etc.).
    - Discuss environmental factors that may impact operations (weather conditions, terrain, electromagnetic interference).

2. Data Flow Analysis

Analyze how data moves within and outside the AeroTech X9 system:

1. **Data Identification**:
    - Enumerate all types of data the drone processes, stores, or transmits (e.g., flight telemetry, sensor data, control commands, logs).
    - Classify data based on sensitivity and criticality.
2. **Data Flow Diagrams (DFDs)**:
    - Create Level 0 (Context Diagram) showing the system's boundary and interactions with external entities.
    - Develop Level 1 DFDs to illustrate major data flows between system components.
    - Include annotations explaining each data flow, its purpose, and data types involved.
3. **Interfaces**:

- Identify all interfaces (wired, wireless, APIs) the drone uses to communicate with ground control stations, satellites, other drones, or IoT devices.
- Discuss the protocols used (e.g., Wi-Fi, LTE, satellite communication) and their security features or vulnerabilities.

3. Security Categorization

Determine the proposed security categorization of the AeroTech X9 system:

1. **Reference Standards**:
   - *FIPS 199* Standards for Security Categorization of Federal Information and Information Systems. https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf
   - *NIST SP 800-60 r2* Guide for Mapping Types of Information and Systems to Security Categories. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-60r2.iwd.pdf
2. **Impact Levels**:
   - Use *FIPS 199* and *NIST SP 800-60* Volume II to assign Low, Moderate, or High impact levels for confidentiality, integrity, and availability for each identified information type.
   - Consider the potential impact on operations, assets, individuals, and other organizations in case of a security breach.
3. **Overall Categorization**:
   - Aggregate the impact levels to determine the system's overall security category.
   - Explain how you applied the highest impact principle in your determination.
4. **Justification**:
   - Provide a detailed rationale for each assigned impact level.
   - Discuss potential consequences of unauthorized disclosure, modification, or destruction of information.
   - Include references to specific sections of *FIPS 199* and *NIST SP 800-60* that support your decisions.

Deliverables

- **System Description Document**: A comprehensive report covering all aspects outlined in Section 1.
- **Data Flow Diagrams**: Level 0 and Level 1 DFDs with annotations.
- **Security Categorization Whitepaper**: Detailed analysis and justification of the security categorization.

Evaluation Criteria

- **Comprehensiveness**: Depth and breadth of system understanding demonstrated.
- **Accuracy**: Correct application of *FIPS 199* and *NIST SP 800-60* guidelines.
- **Clarity**: Clear, logical, and well-organized presentation of information.
- **Justification**: Strong, evidence-based reasoning for categorization decisions.