Assignment 2:
Threat Modeling, Attack Tree Analysis, and Security Control Selection

February 28, 2025

Objective

To identify potential threats to the AeroTech X9 system by constructing detailed attack trees, understanding how these threats could exploit system vulnerabilities, and proposing mitigation strategies. And select and tailor appropriate security controls for the AeroTech X9 drone system based on its security categorization, ensuring that all security requirements are adequately addressed.

Background

The program office has looked at our input on the proposed system categorization level and determined the categorization of our proposed drone is **Moderate-Moderate-Moderate**.

Instructions

1. Threat Identification

1. **Asset Inventory**:
    - List all critical assets within the X9 system that require protection, such as the control system, communication channels, onboard data storage, and physical components.
    - Categorize assets based on their importance and role in system functionality.
2. **Potential Threats**:
    - For each asset, identify potential threats using sources like threat catalogs, industry reports, and brainstorming sessions.
    - Consider both external threats (e.g., hackers, environmental hazards) and internal threats (e.g., insider threats, system failures).

2. Attack Tree Construction

Develop at least four attack trees to model how identified threats could materialize:

1. **Methodology**:
    - Understand the principles of attack tree analysis and how it applies to cybersecurity.
    - Ensure consistency in notation and structure across all attack trees.
2. **Root Node**:
    - Define the ultimate goal of an attacker for each asset (e.g., "Gain Unauthorized Control of Drone", "Intercept Sensitive Data").
3. **Branches and Leaves**:
    - Break down the root goal into sub-goals and actions required to achieve them.
    - Include both logical (AND/OR) relationships to represent different attack strategies.
4. **Visualization**:
    - Create clear and legible diagrams using software tools like Microsoft Visio, draw.io, or any other suitable application.
    - Ensure that all nodes are labeled and relationships are clearly indicated.

3. Analysis of Attack Trees

Analyze the attack trees to assess risks:

1. **Likelihood Assessment**:
    - Estimate the probability of each attack path based on factors such as required resources, skill level, and existing vulnerabilities.
    - Use a qualitative scale (e.g., Low, Medium, High) or assign numerical probabilities.
2. **Impact Assessment**:
    - Determine the potential impact on the system and stakeholders if an attack path is successfully exploited.
    - Consider confidentiality, integrity, availability, safety, and reputational aspects.
3. **Critical Paths**:
    - Identify the attack paths with the highest combined likelihood and impact.
    - Explain why these paths are considered critical.

4. Mitigation Strategies

Propose strategies to mitigate the risks identified in the attack trees:

1. **Control Mapping**:
    - For each critical attack path, map existing or proposed security controls that could prevent or detect the attack.
    - Reference specific controls from *NIST SP 800-53 Rev. 4* where applicable.
2. **Feasibility Discussion**:
    - Discuss the practicality of implementing the suggested controls in terms of cost, technical complexity, and potential impact on system performance.
    - Consider any trade-offs or residual risks.

5. Baseline Control Selection

1. **Reference Standards**:
    - Consult *NIST SP 800-53 Rev. 4* to identify the baseline security controls corresponding to the system's impact level of Moderate-Moderate-Moderate.
    - Consult *CNSSI No. 1253* to identify the control correlation identifier(CCI) corresponding to the security controls in the previous item.
    - Ensure that you consider controls across all control families (e.g., Access Control, Audit and Accountability, System and Communications Protection).
2. **Control Listing**:
    - Compile a comprehensive list of selected baseline controls in a spreadsheet or table format.
    - Organize controls by family and include control identifiers, names, and a brief description.

6. Control Tailoring

Customize the baseline controls to fit the specific needs of the AeroTech X9 system:

1. **Customization**:
    - Review each control to determine its applicability and adjust parameters as necessary (e.g., password complexity requirements, audit log retention periods).
    - Document any organization-defined parameters and settings.
2. **Supplemental Controls**:

- Identify additional controls or control enhancements required due to unique system characteristics, high-priority risks identified in Assignment 1, or specific regulatory requirements.
- Justify the inclusion of each supplemental control.

3. **Control Removal**:
   - Evaluate whether any baseline controls are not applicable to the X9 system.
   - Provide a strong justification for omitting any control, ensuring that risk acceptance is appropriately documented.

7. Documentation

For each control, provide detailed information:

- **Control Identifier and Name**: As per *NIST SP 800-53 Rev. 4*.
- **Control Enhancement(s)**: List any applicable enhancements and their details.
- **Implementation Approach**:
  - Describe how the control will be implemented in the context of the X9 system.
  - Include technical, administrative, and physical aspects where applicable.
- **Justification for Tailoring Decisions**:
  - Explain why certain parameters were set or adjusted.
  - Discuss how the tailoring aligns with organizational policies and risk tolerance.

Deliverables

- **Threat Identification Report**: A document detailing the assets, threats, and rationale.
- **Attack Tree Diagrams**: Visual representations of attack paths for critical assets.
- **Attack Tree Analysis Document**: An analysis of likelihood, impact, and critical paths.
- **Mitigation Strategies Proposal**: Recommended controls and implementation considerations.
- **Security Control Traceability Spreadsheet**: A detailed list of selected and tailored controls.
- **Tailored Security Control Baseline Document**: A narrative document explaining the tailoring process and decisions. Each security control in the baseline must be discussed. Rationale for inclusion or exclusion must be included . This information is determined in Section 7

Evaluation Criteria

- **Alignment**: Correct mapping of controls to the system's security categorization and risk profile.
- **Tailoring Justification**: Logical and well-supported reasoning for control additions, modifications, or removals.
- **Completeness**: Inclusion of all necessary controls and relevant enhancements.
- **Documentation Quality**: Clarity, thoroughness, and professionalism in control descriptions and justifications.