Assignment 2 - Threat Modeling and Security Control Selection
CSE 4380

Group Thorin

March 28th, 2025

Members:	Obadah Al-Smadi
	Betim Hodza
	Elliot Mai
	Benjamin Niccum
	Nicholas Pratt
Instructor:	Trevor Bakker

Contents

List of Figures

List of Tables

1 Threat Identification Report

1.1 Hardware

Asset	**Description**	**Threat(s)**
Antenna	Physical antenna that is used by telemetry module	• Physically break antenna to stop communication • Use EMP to disable communications
Camera	Physical camera for navigation and data acquisition	• Forcefully damage camera to hinder mission • Use EMP to disable transmission
Flight controller CPU	The brain of the drone. Controls motor speeds and processes sensor data.	• Connection Flood Request (Overload drone CPU with 1,000+ simultaneous control requests)
Navigation System	A complex system that guides and tracks drones location.	• Safe Landing Zone Hijack (Redirect drone to predefined zones via spoofed autopilot commands)
Flight Control Firmware	Onboard firmware that controls in-flight operations and flight characteristics.	• Firmware Exploitation (Flash malicious firmware via compromised updates)
IMU	Used to maintain stability and control of the drone during flight.	• Sensor Spoofing
RAM	Used by the CPU for data processing, performing calculations and running software.	• Buffer Overflow
Ground Control Station	A station used to manually monitor the drone's view and control it if needed. Has hardware and software and is placed on ground for access.	• Physical attacks (ambush, bombing, recon, jamming, espionage). • Network attacks (Zero-day vulnerability). • Software attacks (GCS configurer adversary).

Table 1: Threats to *Hardware* Assets

1.2 Software

Asset	Description	Threat(s)
Flight Control Algorithms	Stabilization Algorithms, Navigation Algorithms (GPS-based, autonomous), Real-Time Control Algorithms	• Planted Logic Bombs
Mission Planning and Execution Software	Mission Mapping Video Management System	• Maliciously Modified Firmware • System Vulnerability Exploited for Admin Access
Mobile App	Used for Remote Control and Monitoring	• Maliciously Modified Firmware • System Vulnerability Exploited for Admin Access • App Developers or Owners Accessing Confidential Data
Ground Control Station Software	Software Used at GCS to Communicate with X9	• Maliciously Modified Firmware • System Vulnerability Exploited for Admin Access
Flight Application Buffer	A temporary storage area in the drone's memory that holds data necessary for flight controls.	• Buffer Overflow Attack (Send data exceeding flight app buffer capacity)
Communication Link	The wireless communications between the drone and ground controls.	• Controller Spoofing (Forge drone identity packets to sever legitimate controller links)
RF Communications Protocol	The system of rules for RF communications between the drone and the controller.	• Protocol Reverse Engineering (Analyze drone RF signals to build protocol library)
Detection Algorithms	Software routines built into drone operations for sensor input, data analysis, and tracking.	• Autonomous Mitigation (Passive detection → ID rogue drones → execute cyber takeover)
Communication downlinks	Channels to transmit data to local controller like video feeds and assorted telemetry.	• Command Injection (Exploit unencrypted downlinks)
Authentication Systems	A security feature for authorization and authentication	• Clone Controller Attack (Replicate legitimate controller RF signatures)
GNSS Receiver	A communications device specifically for GPS that communicates with satellites.	• Time-of-Week Rollback Attack (Exploit GPS week number counter limitations)
Signal Processing Units	Hardware components that monitor sensor inputs and communications.	• CN0 Manipulation (Overpower legitimate satellite signals)

Table 2: Threats to *Software* Assets

1.3 Data

Asset	Description	Threat(s)
Camera Data	Photos Taken During Mission	• NEED
Mission Data	Coordinates/Location sent via Telemetry Module	• NEED
SSD	Stores sensitive data, i.e. flight plans and sensor data	• Theft or corruption

Table 3: Threats to *Data* Assets

1.4 Communication Lines

Asset	Description	Threat(s)
Telemetry Module	Write custom firmware to change Comm Lines to exfiltrate data	• Downgrade attack to intercept data
Communication Channels	GNSS/GPS, RF, 5G/LTE, Sat-Nav	• Jamming • Replay Attacks • Denial of Service • Downgrade Attack

Table 4: Threats to *Communication Lines* Assets

2 Attack Tree Diagrams

2.1 Disrupt Communication

Threatened Asset: Communication Lines

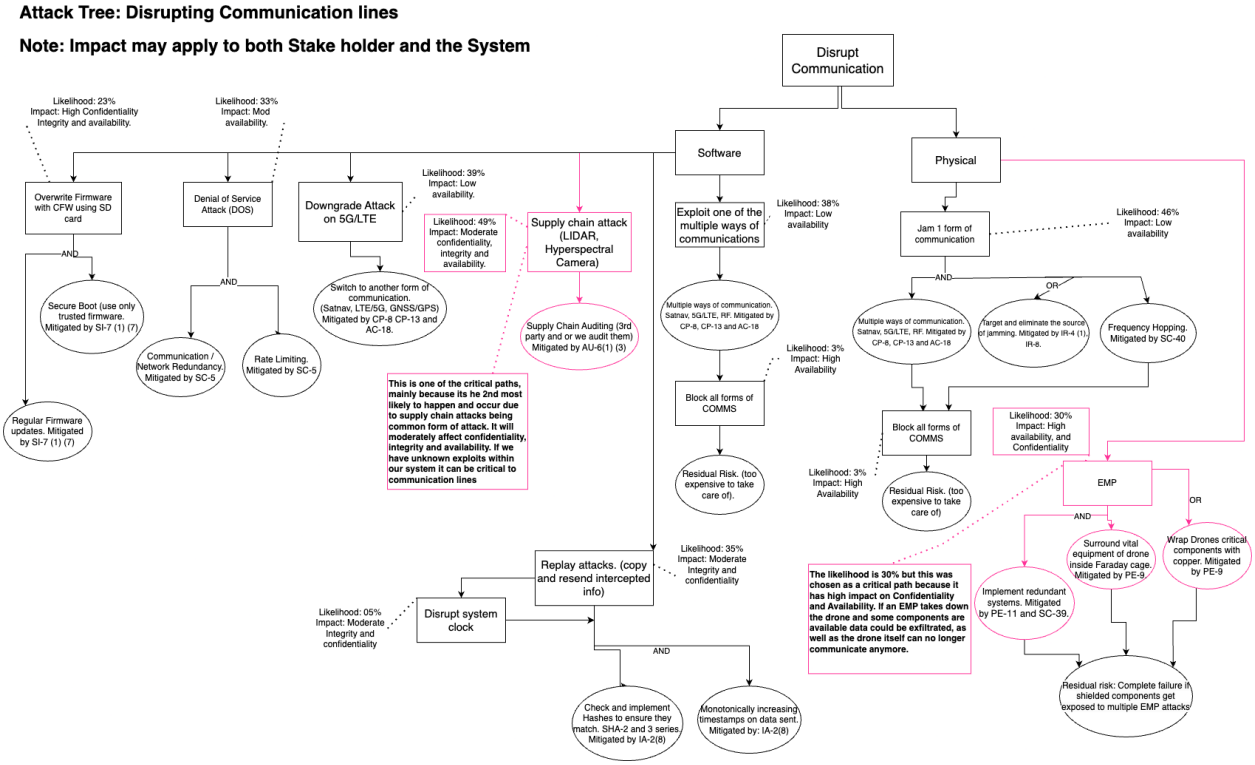

Figure 1: *Disrupt Communication* Attack Tree

2.2 Destruction of Ground Control Station

Threatened Asset: Data

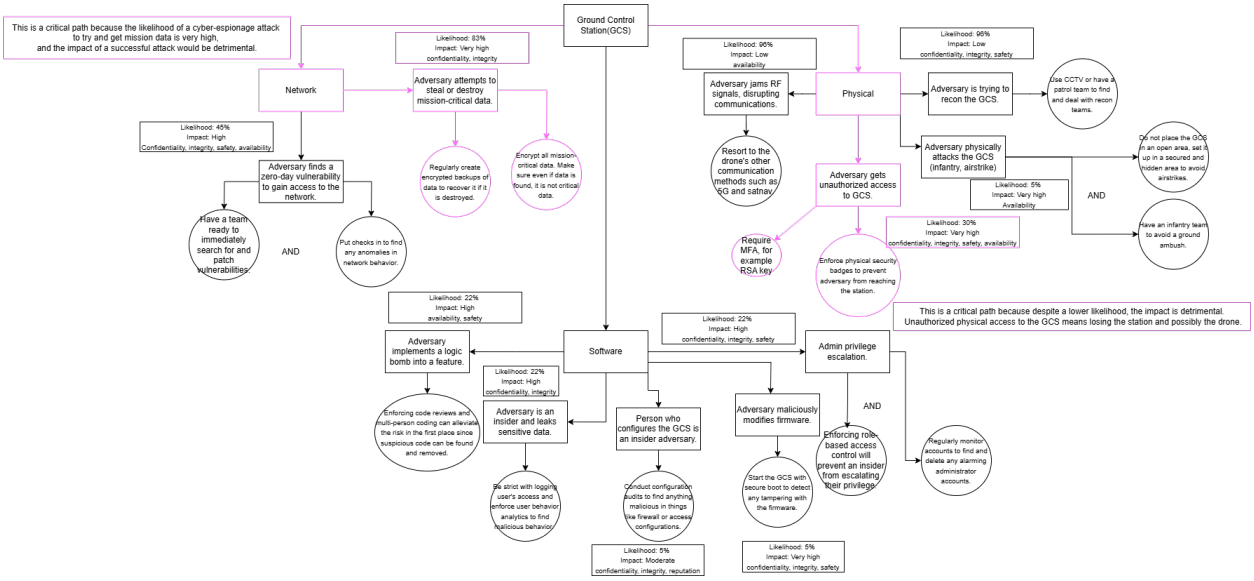

Figure 2: *Destruction of Ground Control Station* Attack Tree

2.3 Destruction via Direct Physical Force

Threatened Asset: Hardware

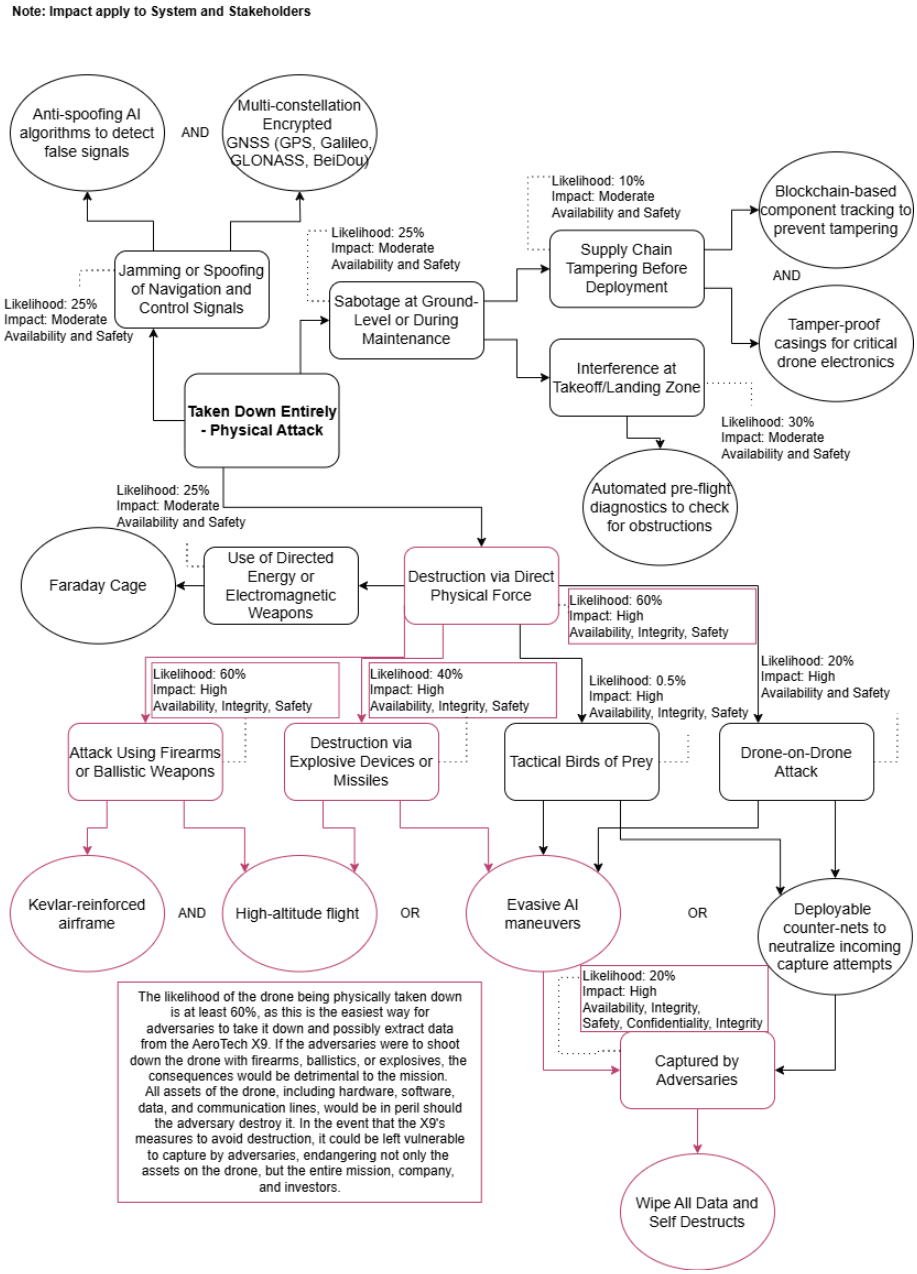

Figure 3: *Destruction via Direct Physical Force* Attack Tree

2.4 Interception via Electronic Force

Threatened Asset: Software

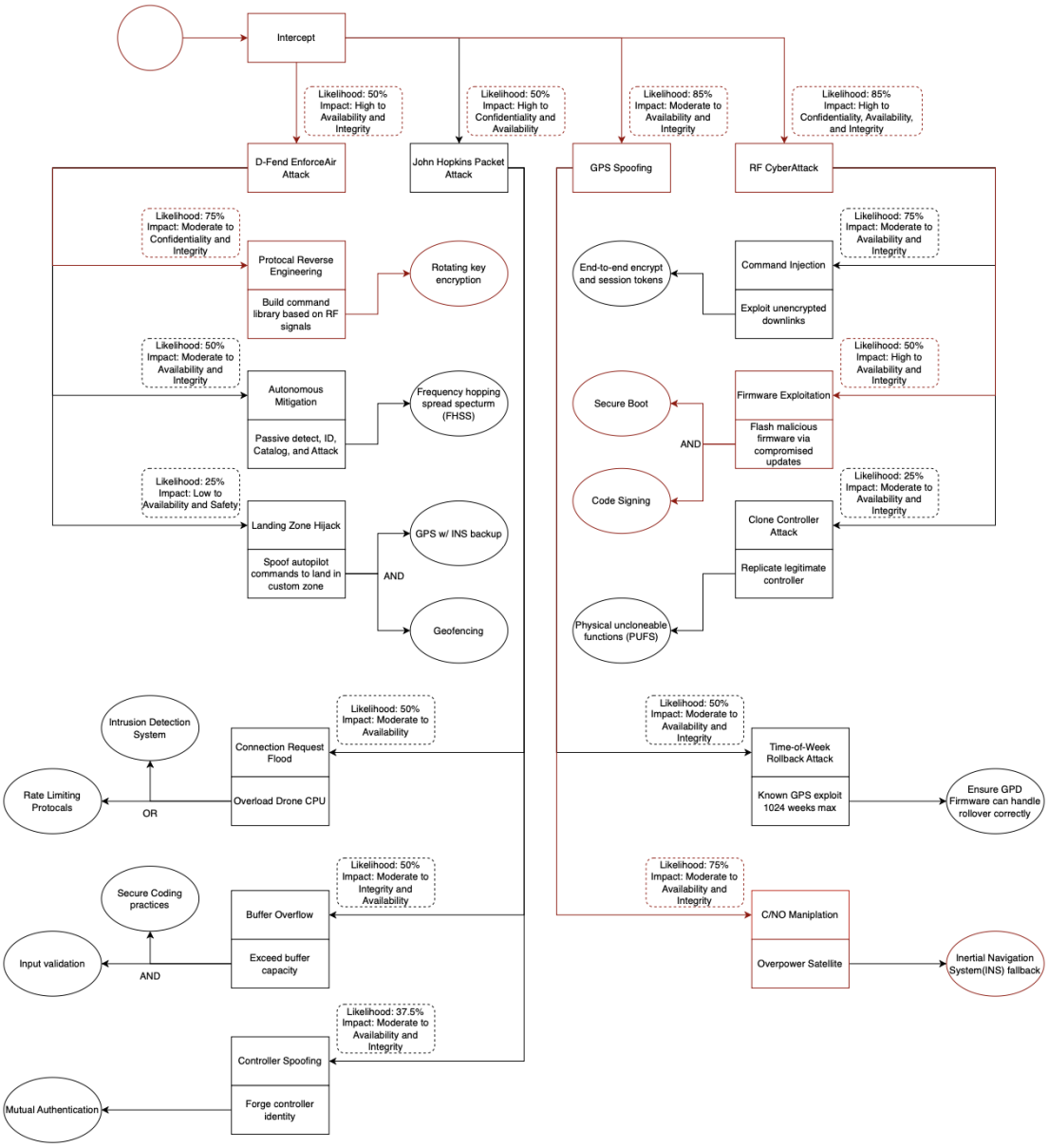

Figure 4: *Interception via Electronic Force* Attack Tree

3 Attack Tree Analysis Document

3.1 Disrupt Communication

Attack: Overwrite Firmware with CFW using SD card

- **Likelihood:** 5%
- **Impact:** High to Confidentiality, Integrity and Availability

Attack: Denial of Service Attack (DOS)

- **Likelihood:** 38%
- **Impact:** Low to Availability

Attack: Downgrade Attack on 5G/LTE

- **Likelihood:** 30%
- **Impact:** Low to Availability

Attack: Supply chain attack (LIDAR, Hyperspectral Camera)

- **Likelihood:** 40%
- **Impact:** Moderate to Confidentiality and Integrity and Availability

Attack: Replay attacks. (copy and resend intercepted info)

- **Likelihood:** 36%
- **Impact:** Moderate to Integrity and Availability

Attack: Disrupt system clock

- **Likelihood:** 5%
- **Impact:** High to Availability

Attack: Supply chain attack (LIDAR, Hyperspectral Camera)

- **Likelihood:** 40%
- **Impact:** Moderate to Confidentiality and Integrity and Availability

Attack: Modifying data in Telemetry Module

- **Likelihood:** 25%
- **Impact:** Moderate to Confidentiality and Integrity

Attack: Exploit one of the multiple ways of communications

- **Likelihood:** 27%
- **Impact:** Moderate to Confidentiality and Integrity

Attack: Block all forms of COMMS

- **Likelihood:** 9%
- **Impact:** High to Availability

Attack: Jam 1 form of communication

- **Likelihood:** 75%
- **Impact:** Low to Availability

Attack: EMP

- **Likelihood:** 30%
- **Impact:** High availability, and Confidentiality

3.1.1 Critical Path 1: EMP

The likelihood is 30% but this was chosen as a critical path because it has high impact on Confidentiality and Availability. If an EMP takes down the drone and some components are available data could be exfiltrated, as well as the drone itself can no longer communicate anymore.

3.1.2 Critical Path 2: Supply chain attack (LIDAR, Hyperspectral Camera)

This is one of the critical paths, mainly because its he 2nd most likely to happen and occur due to supply chain attacks being common form of attack. It will moderately affect confidentiality, integrity and availability. If we have unknown exploits within our system it can be critical to communication lines

3.2 Destruction of Ground Control Station

Attack: Steal/Destroy critical mission data

- **Likelihood:** 83%, cyber-espionage has become a regular in warfare, and with data being a top target, it should be expected.
- **Impact:** Very high to Confidentiality and Integrity, mission success could be compromised.

Attack: Zero-day vulnerability is exploited

- **Likelihood:** 45%, zero-day vulnerabilities are possible, but hard to find since they are not known exploits.
- **Impact:** High to Confidentiality, integrity, safety, and availability. A zero-day vulnerability can give the adversary persistent access to data, or the ability to disrupt the drone.

Attack: Logic bomb implemented into a feature

- **Likelihood:** 22%, this would require a long-term insider with high levels of privilege.
- **Impact:** High to safety and availability. A logic bomb could disrupt the GCS/drone operations unpredictably.

Attack: Insider leaks critical data to adversary

- **Likelihood:** 22%, this would require a long-term insider with a high level of privilege.
- **Impact:** High to Confidentiality and Integrity. If mission-critical data is leaked, it will most likely compromise the operation.

Attack: GCS configurer is an insider adversary

- **Likelihood:** 5%, this would require the person who configures the GCS to be an insider who has a high-trust role and admin permissions.
- **Impact:** Moderate to Confidentiality, integrity, and reputation. If the configurer is an adversary, then the configurer can introduce/hide long-term compromises like backdoors or an exploitable firewall.

Attack: Firmware gets modified by adversary

- **Likelihood:** 5%, Getting access to modify firmware is difficult and requires a high level of privilege.
- **Impact:** Very high to Confidentiality, integrity, and safety. Adversary attacks to firmware are very hard to detect and can be detrimental.

Attack: Admin privilege escalation

- **Likelihood:** 22%, Usually most vulnerabilities that cause this are known exploits that get patched. However, it is still possible with zero-day vulnerabilities.

- **Impact:** High to Confidentiality, integrity, and safety. If the adversary is able to create an admin account, they can gain control over the system.

Attack: RF jamming

- **Likelihood:** 96%, Jamming tools are widespread and can be expected to be used.
- **Impact:** Low to availability. A disruption won't cause permanent damage to the GCS/drone, but important data flow can be stopped.

Attack: Unauthorized physical access to GCS

- **Likelihood:** 30%, the GCS can be physically accessed through a brute force physical attack or ambush or through an insider.
- **Impact:** Very high to Confidentiality, integrity, safety, and availability. If adversary gets physical access to the GCS, then the drone can be taken control of much more easily, or having compromising modifications done to the drone.

Attack: Physical attack (infantry, Airstrike)

- **Likelihood:** 5%, Considering the GCS will be hidden, it is unlikely that it would be found for a physical attack.
- **Impact:** Very high to availability. If the drone is attacked and destroyed, then the GCS is lost, and in turn the drone loses all control and can also be lost.

Attack: Reconnaissance on GCS

- **Likelihood:** 96%, Generally, adversaries will conduct consistent recon before planning a physical/cyber attack.
- **Impact:** Low to Confidentiality, integrity, and safety. Recon on the GCS alone cannot hurt the GCS/drone, but it can give the adversary data for a future attack which can.

3.2.1 Critical Path 1: Unauthorized physical access to GCS

The likelihood is only moderate at 30%, but the impact is devastating. If the adversary manages to get unauthorized physical access to the GCS via any means, then the adversary gets access to data, control of the drone, communication, and now has free reign over the drone.

3.2.2 Critical Path 2: Steal/Destroy critical mission data

This attack path is critical because cyber-espionage has become so regular in cyber-attacks that it can be highly expected to be attempted against a GCS with several forms of communication and data transfer that can be intercepted. And if that attack is successful, then critical data can be stolen or destroyed, like enemy target locations or ally hiding spots.

3.3 Destruction via Direct Physical Force

Attack: Jamming or Spoofing of Navigation and Control Signals

- **Likelihood:** 25%
- **Impact:** Moderate to Availability and Safety

Attack: Sabotage at Ground-Level or During Maintenance

- **Likelihood:** 25%

- **Impact:** Moderate to Availability and Safety

Attack: Supply Chain Tampering Before Deployment

- **Likelihood:** 10%
- **Impact:** Moderate to Availability and Safety

Attack: Interface at Takeoff/Landing Zone

- **Likelihood:** 30%
- **Impact:** Moderate to Availability and Safety

Attack: Destruction via Direct Physical Force

- **Likelihood:** 60%
- **Impact:** High to Availability, Integrity, and Safety

Attack: Use of Directed Energy or Electromagnetic Weapons

- **Likelihood:** 25%
- **Impact:** Moderate to Availability and Safety

Attack: Attack Using Firearms or Ballistic Weapons

- **Likelihood:** 60%
- **Impact:** High to Availability, Integrity, and Safety

Attack: Destruction via Explosive Devices or Missiles

- **Likelihood:** 40%
- **Impact:** High to Availability, Integrity, and Safety

Attack: Tactical Birds of Prey

- **Likelihood:** 0.5%
- **Impact:** High to Availability, Integrity, and Safety

Attack: Drone-on-Drone Attack

- **Likelihood:** 20%
- **Impact:** High to Availability, Integrity, and Safety

Attack: Captured by Adversaries

- **Likelihood:** 20%
- **Impact:** High to Availability, Confidentiality, Integrity, and Safety

3.3.1 Critical Path 1: Destruction via Physical Force

The likelihood of the drone being physically taken down is at least 60%, as this is the easiest way for adversaries to take it down and possibly extract data from the AeroTech X9. If the adversaries were to shoot down the drone with firearms, ballistics, or explosives, the consequences would be detrimental to the mission. All assets of the drone, including hardware, software, data, and communication lines, would be in peril should the adversary destroy it. In the event that the X9's measures to avoid destruction, it could be left vulnerable to capture by adversaries, endangering not only the assets on the drone, but the entire mission, company, and investors.

3.4 Interception via Electronic Force

Attack: Connection Request Flood

- **Likelihood:** 50%
- **Impact:** Moderate to Availability

Attack: Safe Landing Zone Hijacking

- **Likelihood:** 25%
- **Impact:** Low to Availability and Safety

Attack: Firmware Exploitation

- **Likelihood:** 50%
- **Impact:** High to Integrity and Availability

Attack: Buffer Overflow Attack

- **Likelihood:** 50%
- **Impact:** Moderate to Integrity and Availability

Attack: Controller Spoofing

- **Likelihood:** 37.5%
- **Impact:** Moderate to Availability and Integrity

Attack: Protocol Reverse Engineering

- **Likelihood:** 75%
- **Impact:** Moderate to Confidentiality and Integrity

Attack: Autonomous Mitigation

- **Likelihood:** 50%
- **Impact:** Moderate to Availability and Integrity

Attack: Command Injection

- **Likelihood:** 75%
- **Impact:** Moderate to Integrity and Availability

Attack: Clone Controller Attack

- **Likelihood:** 25%
- **Impact:** Moderate to Availability and Integrity

Attack: Time-of-week Rollback Attack

- **Likelihood:** 50%
- **Impact:** Moderate to Availability and Integrity

Attack: CN0 Manipulation

- **Likelihood:** 75%
- **Impact:** Moderate to Availability and Integrity

3.4.1 Protocol Reverse Engineering

This attack is classified as a critical path due to its moderate likelihood and potential to compromise Confidentiality and Integrity. Attackers analyze communication protocols to exploit weaknesses, enabling unauthorized decryption or spoofing of commands. Mitigation via AES-256 rotating key encryption ensures continuous cryptographic freshness, rendering reverse-engineered protocols obsolete before attackers can exploit them.

3.4.2 Firmware Exploitation

Identified as a critical path with high likelihood, this attack targets vulnerabilities in drone firmware to manipulate flight logic or disable security controls. Impacts include loss of Integrity and Availability. Implementation of secure boot and code signing prevents execution of unauthorized firmware, as validated by Galois' secure UAV software demonstrating resistance to buffer overflow exploits.

3.4.3 CN0 Manipulation

This high-likelihood attack manipulates GPS carrier-to-noise density ratios (C/N0), degrading navigation accuracy to disrupt Availability and Integrity. Attackers use low-cost tools to spoof signals, causing drift or crashes. Mitigation through INS (Inertial Navigation System) backup ensures continuous operation during GPS outages, maintaining positional awareness via gyroscopes and accelerometers.