Assignment 1 - System Categorization
Security Categorization
CSE 4380

Group Thorin

February 28th, 2025

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

Contents

1 Executive Summary

This whitepaper evaluates the security classification of the AeroTech X9 drone system using established federal guidelines. Originally designed for commercial applications, the X9 is now being upgraded to meet military-grade specifications for defense use. This transition introduces heightened security requirements due to its enhanced surveillance, intelligence-gathering, and operational capabilities. By analyzing the confidentiality, integrity, and availability of its data, this document assigns a security classification to guide risk management and compliance measures.

2 Introduction

The upgrade of the AeroTech X9 drone from commercial to military use introduces new and enhanced information systems that require proper categorization and vulnerability analysis. Furthermore, existing systems from the commercial iteration must be reevaluated, as they could interact with new features in unexpected ways, potentially creating security risks.

3 Purpose

The purpose of this whitepaper is to evaluate and assign a security classification to the AeroTech X9 drone system based on its transition from commercial to military-grade use. This classification will guide risk management strategies and compliance with relevant security frameworks, ensuring secure operations in defense environments.

4 Security Categorization

4.1 Information Types

- GNSS / GPS: Our GNSS device communicates using Chips-Message Robust Authentication (Chimera) and provides secure communication between the drone and the operator. It will switch to one of the 3 other modules if it fails or gets jammed.
- LTE / 4G: Our LTE/4G communications uses TLS 1.2 and provides secure communication between the drone and the operator. It will independently switch when jamming occurs or when loss of function occurs in one of the 3 modules of communication.
- SatNav: Our SatNav allows for Beyond-Line-of-Sight (BLOS) Operations, and will be encrypted with AES-256-GCM. it will also switch if one of the 3 modules fail.
- (IMU) Inertial Measurement Unit: The IMU is used to measure the drones position, it contains critical data to keep the drone flying correctly. If tampered it could result in lost control of the system and potential loss of life.
- Telemetry Module: Used for real-time monitoring and secure data transmission between the drone and ground station. It utilizes AES-256 encryption with secure key exchange (Diffie-Hellman or ECC) to prevent interception and maintain integrity.
- Flight Control board: Our Flight Control Board has Automatic actions on waypoints: suitable for cargo drop or camera shots, Transponder ADS-B IN for UTM (Unmanned Traffic Management), and Flare and parachute activation for target drones. This module helps ensure availability of the drone and protects it from worst case scenarios. The confidentiality is important to consider for this device as it has data flowing into it that could be confidential and vital to its integrity (drone drop points and return points).

- High-Res Camera: Our High-Resolution camera is equipped with advanced security features to ensure the integrity and confidentiality of captured data. The camera stores data using AES-256-CBC on an full encrypted drive.
- Thermal Imaging Camera: Thermal imaging sensor for night operations and heat detection. If sensor data intercepted it could reveal mission critical information.
- AeroTech Flight Software: AeroTech's in-house flight software is designed with security implementation first, making sure that the integrity of flight software is the upmost importance. As well as keeping confidential information secure and encrypted in memory.
- Encrypted Data (flight, image, comms data): The Drone process image data and flight data, as well as has secure encrypted communication standards in place when in transit TLS 1.2 (telemetry module). It also keeps data encrypted at rest as well when storing image data (AES-256-CBC).
- LIDAR sensor: Used for topographical mapping and obstacle detection. If sensor data intercepted it could reveal mission critical information.
- CPU: Used for executing all programs and commands on the drone.
- RAM: Used for hold all process currently being executed.
- SSD: Used as a non-volatile alternative to RAM for storing Operating System data as well as encryption key and authentication certificates..

4.2 Impact Levels (Confidentiality, Integrity, Availability)

Information Types	Confidentiality	Integrity	Availability
GNSS/GPS Module	L Disclosure to the information module will lead to minimal impact in the system. Most of the data sent between the module is GNSS coordinates they aren't highly sensitive. ([2] 3.2)	L Manipulation of the module could lead to minimal impact in integrity, as we can switch to another module instead of using GNSS. ([2] 4.2.2.2)	L Due to loss of availability there will be minimal impact to the systems capability, since we can switch to other methods of communication. ([2] 4.2.2.3)
LTE/4G	M Disclosure to the information sent between the LTE/4G module and the controller could lead to Serious loss of human life, as an adversary can contain extra sensitive data as it's not only being used for control of the drone, but in link with the telementry module too. ([2] 4.2.2.1)	L Manipulation of the module could lead to minimal impact in integrity, as we can switch to another module instead of LTE / 4G if there's interference. ([2] 4.2.2.2)	L Due to loss of availability there will be minimal impact to the systems capability, since we can switch to other methods of communication. ([2] 4.2.2.3)
SATNAV	L TD is closure to the information sent between the SatNav module will lead to minimal impact in the system, as most of the data is satellite related navigation. ([2] 3.2)	L Manipulation of the module could lead to minimal impact in integrity, it does limit the range of the drone as there's no over the horizon communication that could be done proficiently. ([2] 4.2.2.2)	L Due to loss of availability there will be minimal impact to the systems capability, since we can switch to other methods of communication ([2] 4.2.2.3)
IMU	L If IMU data is disclosed there's minimal impact of confidentiality, the data is mostly used for the drones orientation for autoflight, or normal flight procedures. ([2] 4.2.2.1)	H Severe impact may occur that could include a loss of life if the IMU is manipulated. It's critical that we ensure accurate measurements of motion and orientation or the drone will be inoperable. ([2] 4.2.2.2)	H Without the IMU the drone can't autocorrect itself, which can cause it to crash and not fly correctly even with autopilot. ([2] 4.4.2.4)
Telemetry Module	M Disclosure of the information transmitted between the Module could lead to significant unauthorized access to sensitive data of the operations being taken in place. This could compromise the security of comms and allow adversaries to intercept transmissions and know the purpose of a mission. ([2] 4.2.2.1)	L Changing the data transmitted in the module could lead to errors and inconsistencies between communication. This isn't our only option to communicate so it'll minimally impact the mission. ([2] 4.2.1 Table 7.)	L Loss of availability would have minimal impact of overall system capabilities. Alternative Communication methods can be employed to maintain operation. ([2] 4.2.1 Table 7, 4.2.2.3)

Information Types	Confidentiality	Integrity	Availability
Flight Control Board	L Disclosure of information processed on the board could lead to minor operational disruptions. This could compromise the security of the drones system allowing for potential exploits to be done. ([2] 3.2)	H Severe impact will occur if the integrity of the FCB is compromised, as it's used for not only autopilot but helps assist in manual flight for an operator. ([2] 4.2.2.2 Table 7)	H Severe impact will occur if the Availability of the FCB is lost, similarly to Integrity it will loose autopilot but normal controls for flying the drone manually. ([2] 4.4.2.4)
High-Res Camera	L The images themselves can contain confidential information, leading to potential mission operations disruptions. But in terms of compromises to operations this will be minimal. ([3]4.2.2.1.)	L Minimal impact of the system will occur for tampering image data for the camera. We have other camera's to switch to and from, and it won't disrupt operations much. ([2] 4.2.2.2)	L Minimal impact could occur for the loss of availability of the camera, it will impact mission capability as if we switch to thermal imaging camera, it won't be the best way to operate the drone ([2]4.4.2.3)
Thermal Camera	L The images themselves can contain confidential information, but the image cla themeral cameras won't lead t distruptions. But in terms of to operations, this will be min ([2] 3.2)	L Minimal impact of the system will occur for tampering image data for the thermal camera. It can be an inconvenience but as long as we have redundant systems it won't disrupt operations much. ([2] 4.2.2.2)	L Minimal impact could occur for the loss of availability of the thermal camera, it will impact mission capabilities as we could get crucial information from thermal cameras, but it won't be huge disruptions. ([2] 4.4.2.4)
CPU	H With unauthorized access an attacker could extract cryptographic keys from the CPU allowing them to decrypt messages on all other parts of the system or perform a memory dump to extract flight plans and other mission critical data. ([2] 4.2.2.1)	H With unauthorized access an attacker could cause catastrophic damage to the system. They could overload the CPU and causing delays in the processing of sensor data or cause a kernel panic, cutting off connection to ground control, and causing the drone to crash. ([2] 4.4.2.4)	H if the CPU becomes unavailable, severe consequences in mission capabilities will occur, causing our drone to be inoperable. ([2] 4.4.2.4 and 4.2.2.3)
RAM	M Volatile memory could disclose severe mission critical data, although the difficulty to exploiting this is harder then some of the others, it's a possibility. ([2] 4.2.2.1)	M Serious impact could lead to interruptions to the drone's operation, but this is also unlikely to occur. Changing the RAM data would require a lot of work but could mean that the system is already compromised from some other reason. ([2] 4.4.2.2)	H If volatile memory is unavailable critical mission capabilities will not be available and will lead to catastrophic damage. ([2] 4.4.2.4, 4.2.2.3.)

Information Types	Confidentiality	Integrity	Availability
SSD	H With unauthorized access, an attacker could steal data from the SSD, leading to the exposure of classified mission system information and mission-critical data. ([2] 4.2.2.1)	H With unauthorized access, an attacker could modify any data stored on the SSD such flight plans or insert new data such as malware. ([2] 4.4.2.4)	M With unauthorized access, an attacker could corrupt or wipe the data stored on the SSD, rendering it inaccessible. ([2] 4.4.2.3)
AeroTech Flight Software	M The flight software includes proprietary and sensitive information within, this can lead to serious breaches in confidentiality if our adversaries copy or use our techniques. ([2] 4.2.2.1)	H Severe damage and loss of human life could occur if the integrity is compromised, as the flight controller is important to keep the drone operating properly, if it's manipulated in some sort of way it could severely disrupt operations.([2] 4.4.2.2)	H Loss of availability will mean that the drone can no longer operate properly. Severe damage could happen if availability is lost during flight with the drone, as it's a mission critical device. ([2] 4.4.2.4)
Encrypted Data	M if the encryption keys for any of the data get exposed then serious mission data gets exposed and can cause damage. ([2] 4.2.2.1)	M Tampering of encrypted data can lead to significant disruptions to operations, as it could be mission critical to keep it secure. ([2] 4.2.2.2)	L Loss of availability of this data doesn't affect mission critical resources or affects the drone much. ([2] 4.2.2.3)

4.3 Overall Categorization

Overall Categorization	Confidentiality	Integrity	Availability
High impact system: NIST-800-60: 4.4.3	H	H	H

4.4 Reference Standards

- [1] FIPS 199: Standards for Security Categorization of Federal Information and Information Systems
- [2] NIST SP 800-60: Guide for Mapping Types of Information and Information Systems to Security Categories

5 Conclusion

The transition of the AeroTech X9 from commercial to military use necessitates a thorough reassessment of its security classification. With its enhanced capabilities, the system faces new threats that require stringent risk management measures. As the AeroTech X9 continues to evolve, continuous evaluation and improvement of security protocols will be necessary to address emerging threats and maintain operational readiness.

References

[1] National Institute of Standards and Technology. Security requirements for cryptographic modules. Technical Report Federal Information Processing Standards Publications (FIPS PUBS) 199, U.S. Department of Commerce, Gaithersburg, MD, 2004.

[2] National Institute of Standards and Technology. Guide for mapping types of information and information systems to security categories. Technical Report NIST Special Publication (SP) 800-60, Vol. I Rev. 1, U.S. Department of Commerce, Gaithersburg, MD, 2008.

[3] National Institute of Standards and Technology. Guide for conducting risk assessments. Technical Report NIST Special Publication (SP) 800-30, Rev. 1, U.S. Department of Commerce, Gaithersburg, MD, 2012.