Emerging Drone Cybersecurity Framework Integrating NIST CSF for Governmental and Commercial Use

Created by Roberto Hernandez, Md Razibur Rahman, Michael Travers

Introduction

- In recent times, the widespread adoption of unmanned aerial vehicles (UAVs), or drones, has brought about notable security concerns in addition to their broad range of uses. As these devices become more powerful and readily available, they present threats that span from breaches of privacy to potential use in terrorism. This study examines and analyzes the latest developments in drone security, drone vulnerabilities, focusing on bringing forth a layered framework in counter-drone systems, changes in regulatory policies, and the rise of cybersecurity vulnerabilities affecting UAVs, the latest developments in drone security, focusing on the vulnerabilities of drones, including counter-drone systems, regulatory changes, and emerging standards such as those underlined in the **Detect Act**.

DETECT Act, NIST CSF

- The Detecting Emerging Threats to Critical Infrastructure Through Drones Act of 2023—known as the **Detect Act**—was introduced by Senators Mark Warner and John Thune to address growing concerns about the cybersecurity of commercial and governmental drone operations, however this proposal towards NIST was never put into place.
- This study examines and analyzes the latest developments in drone security, drone vulnerabilities, focusing on bringing forth a layered framework in counter-drone systems, changes in regulatory policies, the rise of cybersecurity vulnerabilities affecting UAVs, and emerging standards such as those outlined under the **Detect Act**. This Act, introduced by Senators Warner and Thune, called for the establishment of a national standard by NIST for detecting and managing vulnerabilities in critical drone components. By aligning this framework with NIST's work, we aim to create a practical, commercial solution that addresses these vulnerabilities through layered security measures.

DETECT Act, NIST CSF cont.

- Cybersecurity Framework 2.0. Initially release in 2014 and in February 2024 NIST released the first major update known as the CSF 2.0. Initially created to help secure United State critical infrastructure but was quickly adopted by companies across all industries. This was helpful to know what to do without having it prescribed to them of exactly how they needed to implement cyber security. The cyber security framework has 3 primary components. The **core**, **implementation tiers** and the **profiles**. The core is a set of cyber security outcomes that can be used to understand what is it that I need to do or a series of desired outcomes and is understood by all. This core is made up of 5 functions: **Identify, protect, detect, respond, and recover**. This set a road map to better manage risks.

Current Threats

ATTACK TYPE	CIA COMPROMISE	CURRENT MITIGATIONS
Man-in-the-Middle (MitM) Attacks	Confidentiality, Integrity	Use encrypted communication protocols (e.g., MAVLink 2.0 with encryption), VPNs, TLS
GPS Spoofing	Integrity, Availability	GPS authentication systems, anti-spoofing algorithms, redundant navigation systems
Denial of Service (DoS)	Availability	Rate-limiting, traffic analysis, DDoS protection services
GPS Jamming	Availability	GPS jamming detection, alternative navigation systems (e.g., visual odometry, IMUs)
De-Authentication Attacks	Availability, Integrity	802.11w (Protected Management Frames), strong encryption, and authentication protocols

Current Security Controls

Security Control	Function	Use Case	Advantages	Disadvantages / Limitations
MAVLink 2.0	Message Signing	Communication between UAV and GCS	Prevents message spoofing, Integrity of messages	Limited implementation in some drones, Requires additional processing power
WPA3	Encryption	Securing Wi-Fi networks	Strong encryption (AES), Protection against brute force attacks	Power-intensive, Limited compatibility with older devices
DroneCAN	Bus Protocol	Communication between UAV components (e.g., flight controller, sensors)	Robust, scalable, and fault-tolerant	Limited security features (No encryption by default)
ZigBee	Wireless Communication	Low-power communication for IoT components	Low power consumption, Secure communication via AES	Short range, Vulnerable to jamming attacks
Bluetooth	Wireless Communication	Short-range communication for UAVs and peripherals	Low power, Easily available	Vulnerable to man-in-the-middle attacks, Limited range
802.11w (Protected Management Frames)	Encryption	Enhances WPA2/WPA3 security for management frames	Protects against spoofing and DoS attacks	Can impact performance, Requires compatible hardware

Layered, Modular Approach

Identify Critical Assets

- Flight Control Firmware
- Controller Interface (GCS
- UAV Sensors
- Telemetry Data

Secure Communication Setup

- Data Links should implement TLS/DTLS: Telemetry, video, control before transmission.
- Use **MAVLink** 2.0, or other secure **CAN** protocols
- Enable **message signing and encryption**.

Access Control and Authentication Hardening

- Use WPA3 + 802.11w in Wi-Fi connected UAVs.
- Enforce key-based SSH, disable default passwords.
- Apply MAC filtering and hide SSIDs.
- Use Bluetooth LE Secure Connections if applicable.

Sensor and Signal Authenticity

- Implement GPS spoofing detection (entropy checking, cross-analysis of data sources,
- Apply checksums to sensor input.
- Fail-safe behavior on signal of anomalies (ex., hover or return home)

Access Control Mechanisms

- Enforce strict SSH key-based access, Bluetooth LE Secure Connections, and Wi-Fi WPA3 security with MAC filtering and SSID suppression.

Physical and Supply Chain Security

- Secure boot processes, hardware encryption chips, and trusted component sourcing.

Logging and Monitoring Integration

- Real-time telemetry logging, intrusion detection on communication links, and health monitoring of onboard systems.

Modular Relation to NIST CSF

Drone Security Module	Mapped CSF Function	Justification
Identify Critical Assets	**Identify**	Determines what needs protection by identifying UAV components and data flows.
Secure Communication Setup	**Protect**	Implements encryption and secure protocols (e.g., MAVLink 2.0, TLS) to protect communications.
Access Control and Authentication Hardening	**Protect**	Enforces strong access restrictions (e.g., SSH, WPA3, MAC filtering) to prevent unauthorized use.
Sensor and Signal Authenticity	**Detect**	Detects spoofed or tampered signals via cross-checks and fail-safes (e.g., GPS spoofing detection).
Access Control Mechanisms	**Protect**	Reinforces earlier protections with stricter controls (key-based SSH, Bluetooth LE).
Physical and Supply Chain Security	**Protect**	Safeguards integrity of firmware/hardware at the physical and supply chain level (e.g., secure boot, chip-level encryption).
Logging and Monitoring Integration	**Detect** & **Respond**	Enables continuous telemetry monitoring and intrusion detection, supporting both early warning and response.

Future Work

Real-World Implementation and Field Testing

Testing in live scenarios—such as emergency response, urban air mobility, or agricultural surveillance—will validate the scalability, latency, and resilience of the framework under actual operational stress.

Integration with AI-Driven Autonomous Decision-Making

Incorporating real-time machine learning and AI-driven anomaly detection into drone navigation and threat response systems with adaptive security systems (IDS/IPS) that evolve with threat patterns that will hopefully enhance UAV self-defense capabilities without constant human oversight.

Internet of Drones (IoD) Architecture and Swarm Security

As drone swarms and interconnected UAV networks gain popularity, future research must address the cybersecurity implications of multi-drone coordination. Specific focus should be given to defending against distributed denial-of-service (DDoS) attacks, spoofing within a swarm, and maintaining secure inter-drone communication channels.

References

- https://www.sciencedirect.com/science/article/pii/S1874548219300034?casa_token=nql0KHHa_McAAAAA:ytCOLzpQyuS6H1KdKFsXu41VvXxaVx29ud32rYrZIflzbfCihvD4ndQMcL98u592MgrslisBpJQ
- https://www.sciencedirect.com/science/article/abs/pii/S2214209622000997
- https://ieeexplore.ieee.org/document/8903295
- https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=10750190
- https://jpt.spe.org/iso-approves-first-standard-commercial-drone-operation
- https://research-ebsco-com.udc.idm.oclc.org/c/3qtkhf/viewer/pdf/qqxysmeus5?route=details
- https://cheatsheetseries.owasp.org/cheatsheets/Drone_Security_Cheat_Sheet.html
- https://github.com/microsoft/AirSim/releases