# Drone Vulnerabilities: A Comprehensive Security Analysis

Based on OWASP Drone Security Cheat Sheet and Research

With over 7 million drones expected to be operational by 2025, understanding and addressing drone security vulnerabilities has become critical. This infographic examines the key security risks facing drone systems and provides insights into mitigation strategies.

## Drone System Components

All three components present unique security vulnerabilities that can be exploited by attackers.

### Unmanned Aircraft (UmA)

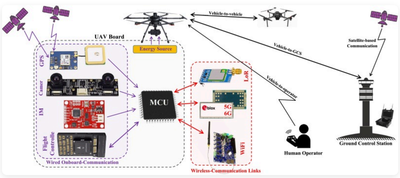
The physical drone including sensors and onboard systems

### Ground Control Station (GCS)

Interface used to control and monitor drone operations

### Communication Data-Link (CDL)

Network connection between drone and GCS




*Drone Communication System Architecture including sensors and communication modules*

## OWASP Top 10 Drone Security Risks

1. **Insecure Communication Risk** — Unencrypted data transmission
2. **Weak Authentication/Authorization Risk** — Inadequate access controls
3. **Insecure Firmware/Software Risk** — Vulnerabilities in drone software
4. **Inadequate Personal Data Protection Risk** — Mishandling of sensitive data
5. **Lack of Secure Update Mechanism Risk** — Insecure update processes
6. **Insecure Third-party Components Risk** — Vulnerable libraries/modules
7. **Insufficient Network Security Risk** — Vulnerabilities in network services
8. **Physical Security Weaknesses Risk** — Tampering with drone components
9. **Insecure Data Storage Risk** — Unprotected data on drone
10. **Lack of Logging and Monitoring Risk** — Undetected security breaches

## Key Vulnerability Categories

### Communication Vulnerabilities

Unencrypted transmission, spoofing attacks, Wi-Fi weaknesses, and insecure protocols like MAVLink, CAN Bus, ZigBee, Bluetooth, and Wi-Fi.

### Authentication & Access Control

Open ports on companion computers, user misconfiguration, weak WiFi authentication with low entropy, and inadequate access controls.

### Data Protection

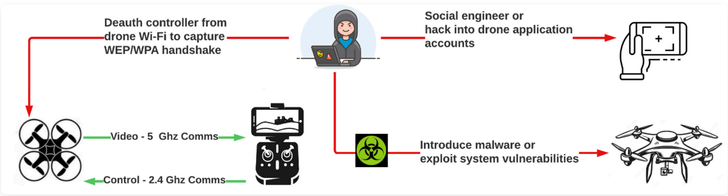
Unencrypted storage, sensitive data in RAM, cleartext transmission of sensitive information, and plaintext storage of credentials.

### Physical Security

Unsecured USB ports, exposed hardware, insecure supply chain, and improper decommissioning of retired drones.

### Sensor Security

GPS spoofing, manipulation of camera feeds, altimeter tampering, and other sensor data manipulation attacks.




*Drone Attack Process showing how vulnerabilities can be exploited*

## Real-World Drone Security Breaches

### DJI Mavic Pro Vulnerabilities

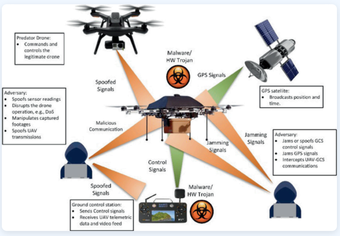
Over 130 security flaws identified including path traversal, unsigned firmware, race conditions, GPS spoofing vulnerability, and low entropy WiFi authentication.

### Emotion Drone/Eachine E58

Unprotected WiFi network, cleartext transmission of control commands, reverse-engineerable mobile app, and hardcoded FTP credentials.

### Military Drone Incidents

Russian Electronic Warfare equipment deployed to counter Ukrainian drones, demonstrating real-world exploitation of drone vulnerabilities in conflict zones.




*Various methods for attacking drone systems*

## Mitigation Strategies & Best Practices

- Implement end-to-end encryption for all communications
- Regularly update firmware and software with verified signatures
- Implement physical security measures including tamper detection
- Enable network security features (WPA3, 802.11w MFP)
- Conduct regular security assessments and penetration testing
- Use strong authentication mechanisms and role-based access control
- Encrypt sensitive data both in transit and at rest
- Use secure communication protocols (MAVLink 2.0 with message signing)
- Implement comprehensive logging and monitoring
- Stay informed about latest vulnerabilities and threats


*Various drone application scenarios requiring different security approaches*

**Sources:** OWASP Drone Security Cheat Sheet, OWASP Top 10 Drone Security Risks, Security Analysis of Drones Systems (Yaacoub et al.), SecQuest White Paper, Alias Robotics DJI Case Study

This infographic provides a comprehensive overview of drone vulnerabilities. For detailed technical information, please refer to the source documents.