Wireless communication, hacking programming

By Fabrizio Fernandez Soto
04/28/2025

Why UAV?

- An unmanned aerial vehicle is an aircraft with is aircrew removed and replaced by a computer system and a communication media.
- Widely used in in civil and military application.
- Civil applications: Photography, powerline inspection, agriculture, coastguard, fisheries, conservation, forestry, traffic agencies and police authorities, wildfire services, calamity monitoring and customs excise.
- Military applications: Target surveillance, demolish operations and border observations.

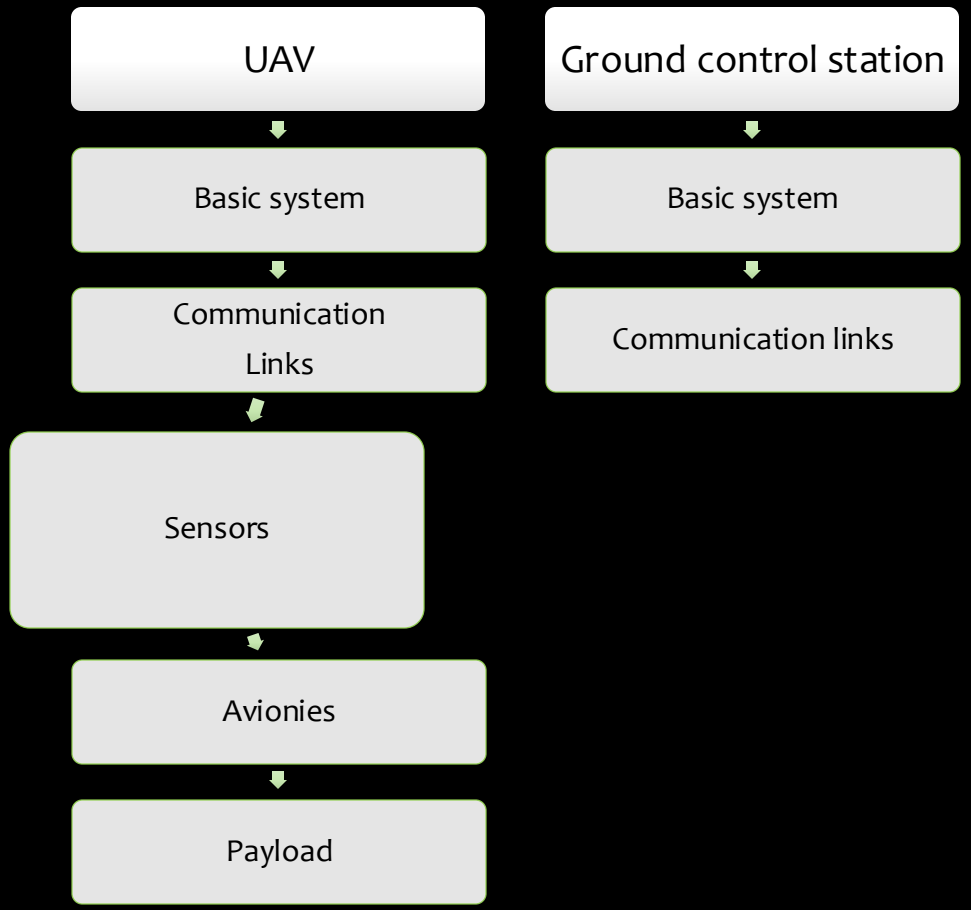
Information security activities

Physical security
Logical security
Application security
Operational security
Authentication
Telecommunication security
Confidentiality
Integrity
Availability
Non repudiation

Occurrences

- In Iraq 2009, and intruder broke in successfully, intercepted and distributed US military drone video and uploads at their own network
- In September 2011 at Creech Air force base in Nevada a "Keylogging" virus infected a US military UAV fleet.
- December 2011, Iranian forces capture an RQ-170 and after 3 years, with reverse engineering, same was built by Iran.

UAV communication



Weak areas

Data in transit is the most vulnerable part of communication devices
Highly sensor-driven assets are mission critical
GPS (Global position system) GNSS (Global navigation satellite system)
NBC sensors
Fluorescence detector
Air pressure sensor
Atmospheric composition monitoring
Thermal sensor
Laser range finder
Seismic
Speed and distance
Visual camera
RPM monitor sensor
Infrared detector
Acoustic sensor
Automatic dependent surveillance-broadcast (ADS-B) or IFF

Components of UAV system operation

A typical Unmanned Aerial Vehicle (UAV) system operation involves a coordinated interaction of hardware, software, personnel, and procedures to achieve mission objectives safely and efficiently.

The mission planner uses specialized software (e.g., Mission Planner, DJI Pilot) to define the flight path, waypoints, and altitude based on the mission's requirements—whether it's aerial mapping, surveillance, or inspection. Meanwhile, the ground crew conducts a thorough inspection of the UAV, checking the airframe for damage, ensuring the battery is charged, and verifying that sensors (such as cameras or LiDAR) are functioning correctly. The remote pilot checks communication links between the Ground Control Station (GCS) and the UAV, confirming that telemetry data (altitude, GPS signal, battery status) is being transmitted in real time. Additionally, the team reviews weather conditions and airspace restrictions to ensure compliance with aviation regulations (e.g., FAA Part 107, EASA rules)

MAV Function

You're standing in a sunflower field, holding a radio controller while your quadcopter hovers 50 meters above. Unseen by the naked eye, thousands of digital messages are racing between your controller and the drone every second - this is **MAVLink at work**.

Pre-Flight Handshake (The Digital Greeting)
As you power on your drone, the flight controller (a Pixhawk 4) boots up and immediately starts broadcasting MAVLink packets over the radio telemetry:
"Hello ground station, I'm Drone #1, running ArduCopter v4.3, GPS locked, battery at 100%".

Your tablet running Mission Planner receives this packet, decodes it, and displays the information. Meanwhile, it responds with its own MAVLink message:
"Acknowledged Drone #1. Standby for mission parameters."

Mission Upload (The Flight Plan Transfer)
You tap "Upload Mission" on your tablet. MAVLink packages your 12-waypoint survey pattern into a series of **MISSION_ITEM** messages. Each contains:

- Latitude/longitude
- Altitude (30m AGL)
- Camera trigger commands

Packet analysis by wireshark

Is the process of capturing, inspecting, and interpreting network traffic using Wireshark, a popular open-source network protocol analyzer.

Key aspects of packet analysis with Wireshark:

Packet capture

Protocol decoding

Filtering & searching

Traffic analysis

Security & forensics

Troubleshooting

Critical messages identification in network traffic (using wireshark)

Identifying critical messages in network traffic involves detecting security threats, errors, or performance impacting events. Wireshark helps analyze packets to find anomalies, attacks, or critical system communications.

Types of critical messages:

Security threats & attacks

Network errors & failures

Critical system & application messages

How to identify critical messages in wireshark:

Capture traffic: start wireshark and select the correct interface (wifi/ethernet)

Apply display filters: Use these wireshark filters to detect critical messages.

Use wireshark's built-in tools: Expert info, IO graph, flow graph, follow TCP stream.

Export & report findings: export suspicious packets, generate statistics.

Real-world example: Detecting a brute force attack.

Filter, check frequency, identify attacker's IP, block the IP.

Skills required to hacking

Networking fundamentals: Understanding of TCP/IP, UDP, DNS, DHCP, ARP,HTTP/HTTPS, FTP, SSH, etc.

Ability to analyze traffic using Wireshark, Tshark, or Tcpdump.

Operating systems: Linux/Unix, Windows & Active directory, command line

Programming & scripting: Python; for exploit development automation, and hacking tools.

Bash/PowerShell: for scripting attacks and post-exploitation.

C/C++: for reverse engineering and malware analysis.

JavaScript/PHP: for web exploitation like XSS, SQLi.

Cybersecurity concepts: OWASP Top 10 (SQLi, XSS, CSRF, etc.

Cryptography: (SSL/TLS,AES, RSA, hashing).

Vulnerability assessment & penetration testing (VAPT).

Hacking-specific skills:

Reconnaissance & footprinting: Passive/active OSINT (Google, dorking, shodan, maltego).

WHOIS, DNS Enumeration, subdomain brute-forcing.

Exploitation: Metasploit framework.

Buffer overflows, ROP, and Shellcode Development.

How to keep our devices safe from hackers?

For computers:

Install antivirus & anti-malware

Keep OS & Software updated

Use strong passwords

Bitwarden, KeePass

Enable Two-factor authentication

For smartphones: Lock screen protection, use pin 6+ digits, disable Bluetooth and wifi when not in use, encrypt your phone.

Advanced protection (For tech-savvy users)

Use a VPN

Enable disk encryption

Disable unused services

Regularly backup data

What to do if hacked?

Disconnect from the internet, scan for malware, change all passwords, factory reset if necessary, report to authorities.