الهيئة الوطنية للأمن السيبراني
National Cybersecurity Authority

Cybersecurity aspects of Unmanned Aerial Systems

Classification: Public

Date: November 16th , 2022

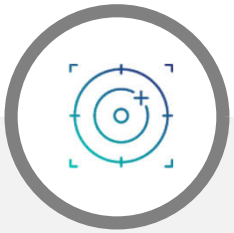
Cybersecurity aspects of Unmanned Aerial System - UAS

Types and components of UAS

1

Important Cybersecurity facts of UAS

2



Cyber attacks of UAS

3

Leveraging vulnerabilities and attacks vectors to protect from UAS

4

1 Types and components of UAS

Two types of UAS

Remotely piloted.

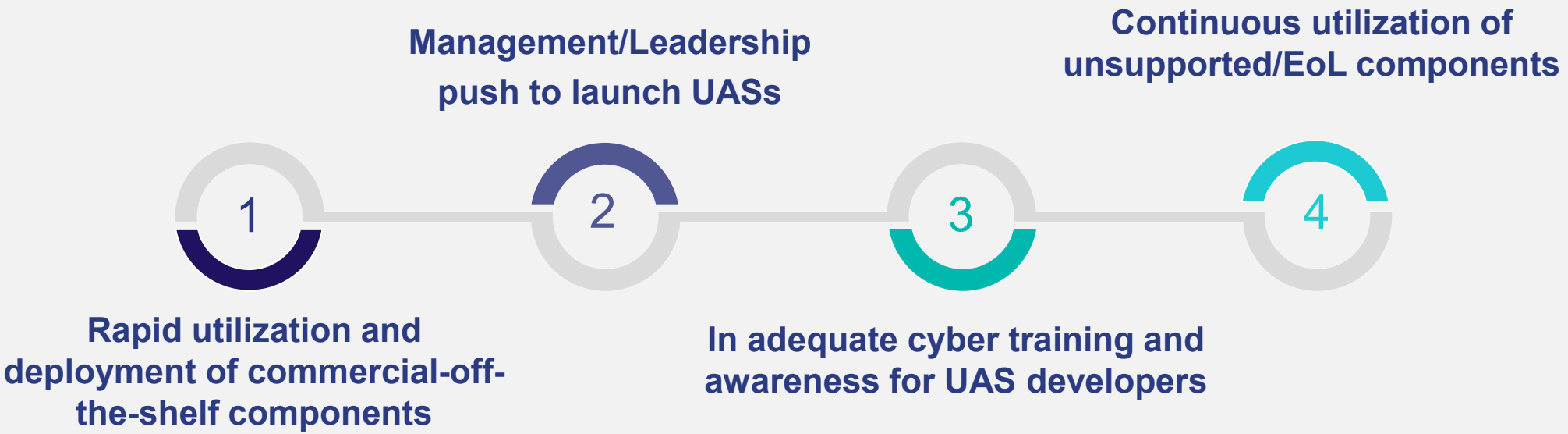
Autonomous.

Most of UASs have:

1. CPU/RAM
2. Wi-Fi/RW/Satellite communication
3. Sensors (GPS & Accelerometer, Radiation sensors, etc.)
4. Storage
5. Battery
6. Camera
7. Payload
8. Aeronautical Hardware
9. A controller for manual flight operations

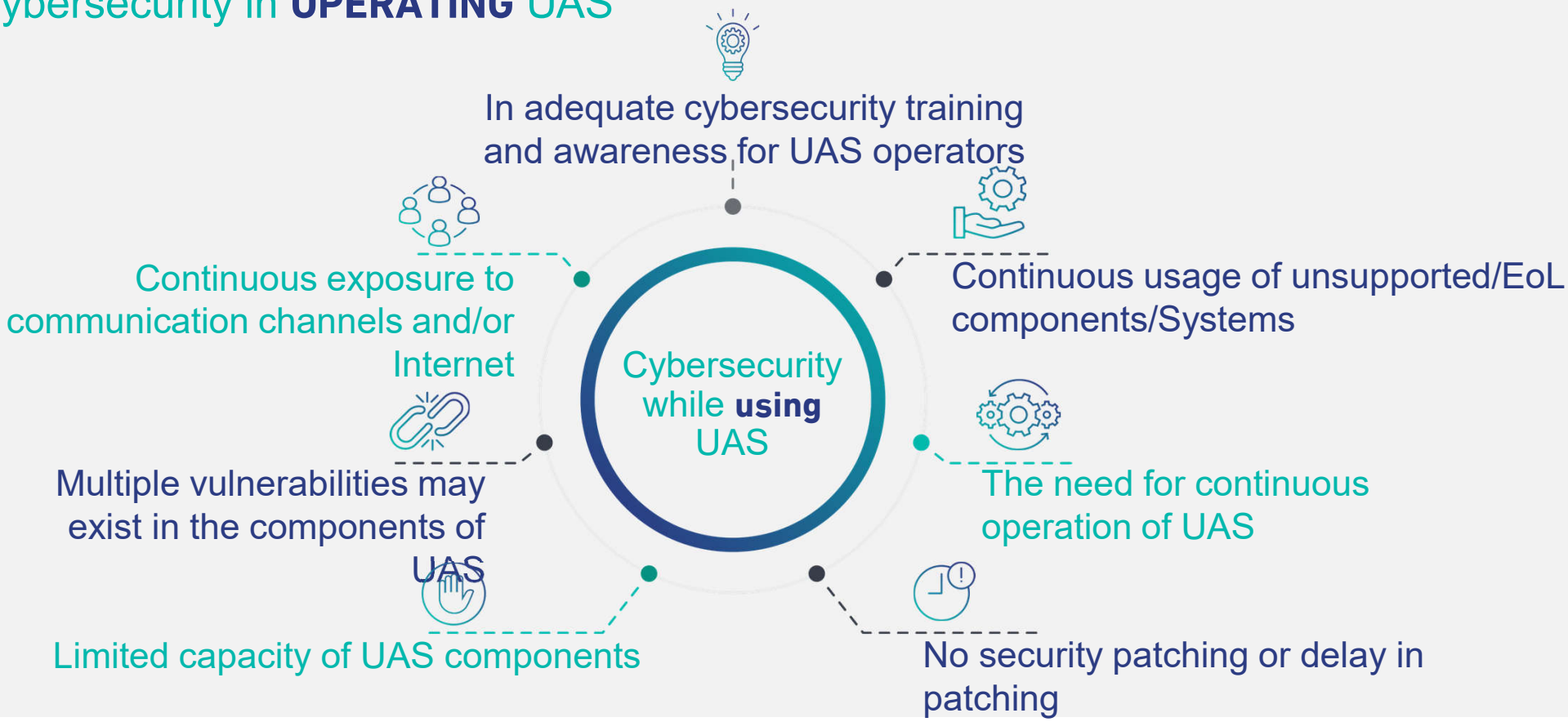
2 Important Cybersecurity facts of UAS

Cybersecurity in **DEVELOPING** UAS



2 Important Cybersecurity facts of UAS

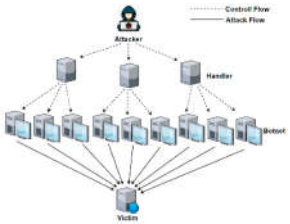
Cybersecurity in **OPERATING** UAS



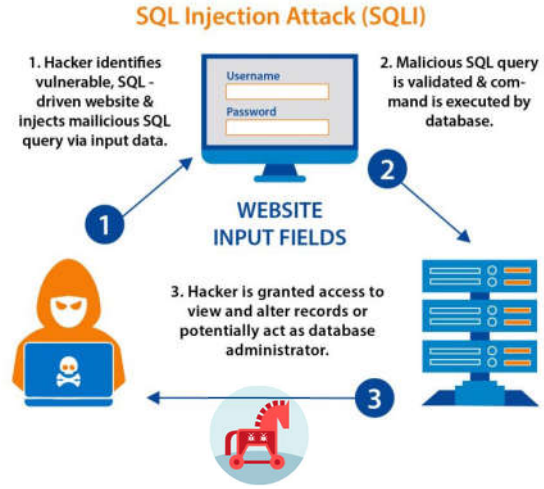
3 Cyber attacks of UAS

Cyber attacks of UAS could compromise system/data's :

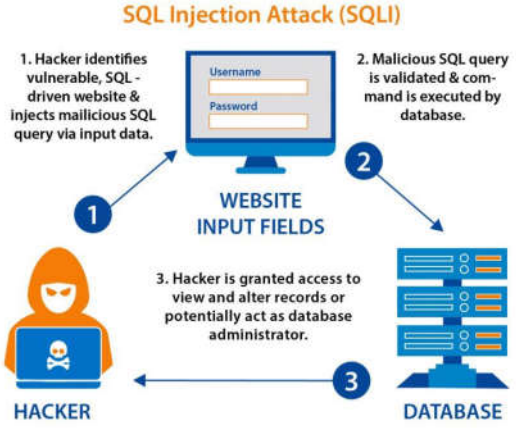
Availability by DoS/DDoS, malware (ransomware).



Confidentiality by MiTM, SQL Injections, or Malware (Spyware, Trojan).



Integrity by MiTM, SQL Injections, or Reply



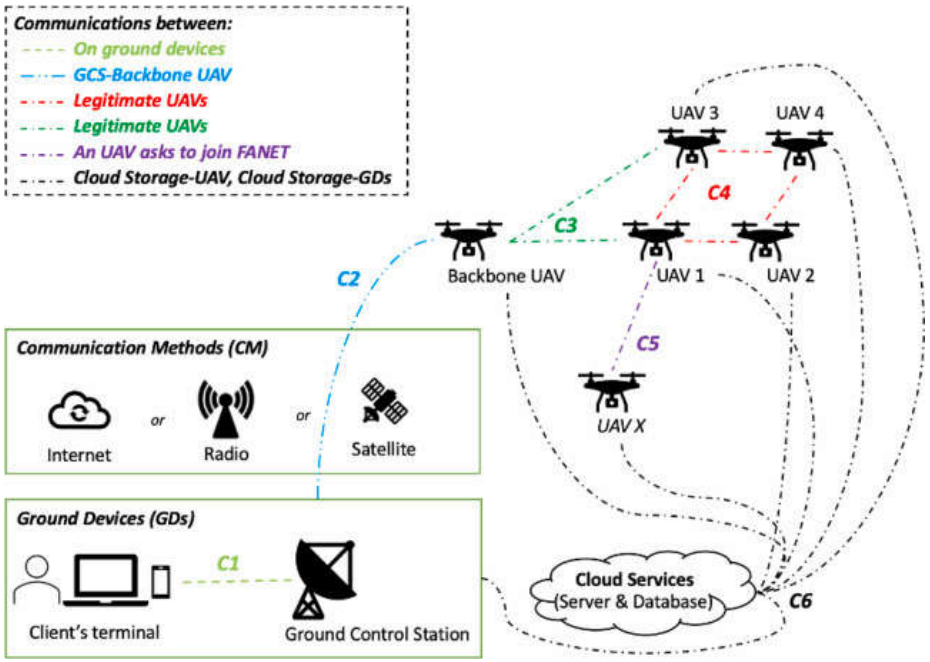
3 Cyber attacks of UAS/UAV

Types of communications

1. **Drone-To-Drone**
   (Internet of drones (IoD), Flying Ad-hoc NETwork (FANET))
2. **Drone-To-Ground station**
   Radio, 3GPP compatible network
3. **Drone-To-Network**
   Wi-FI, 3GPP compatible network
4. **Drone-To-Satellite**
   GPS

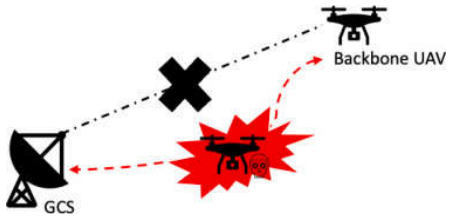
Defense targets:

- Hardware-level,
- Software-level,
- Communication-level, and
- Sensor-level.

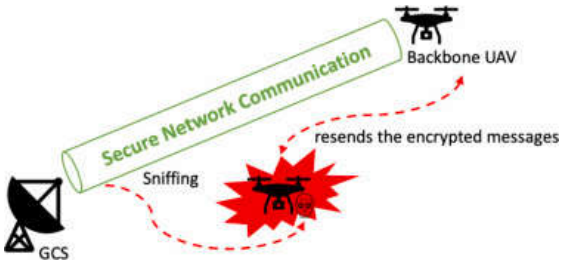


Source: https://www.sciencedirect.com

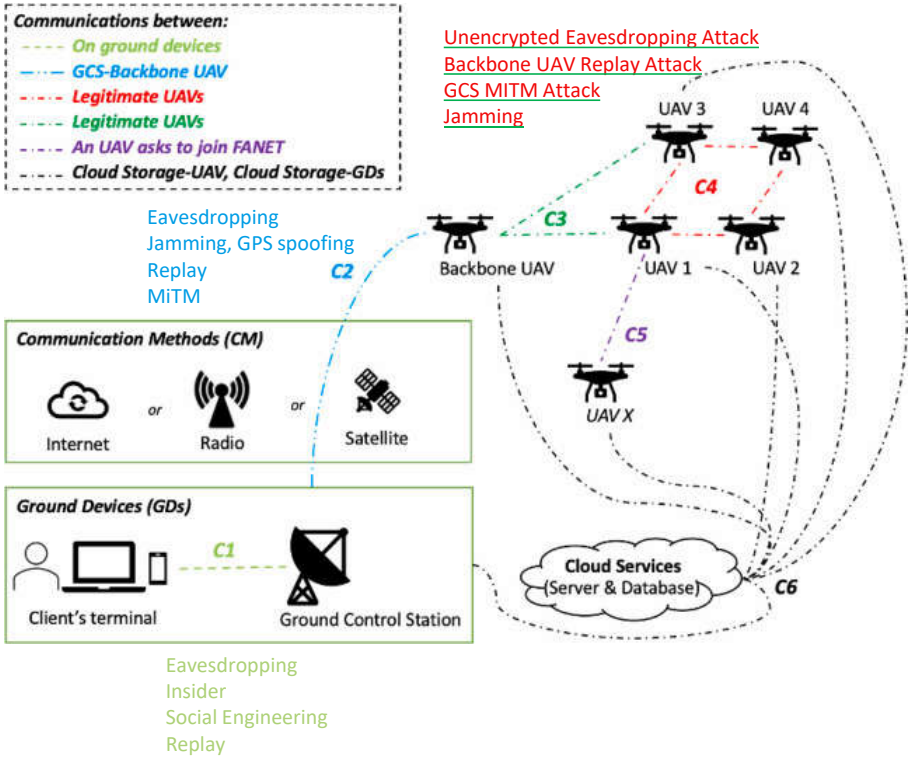
4 Leveraging vulnerabilities and attacks vectors to protect from UAS

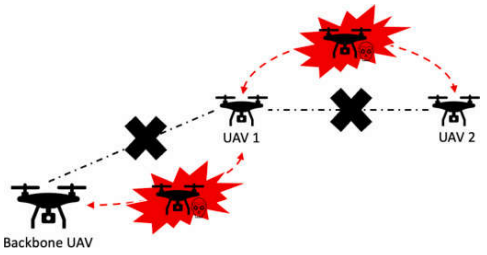


GCS MITM Attack



Backbone UAS Replay Attack



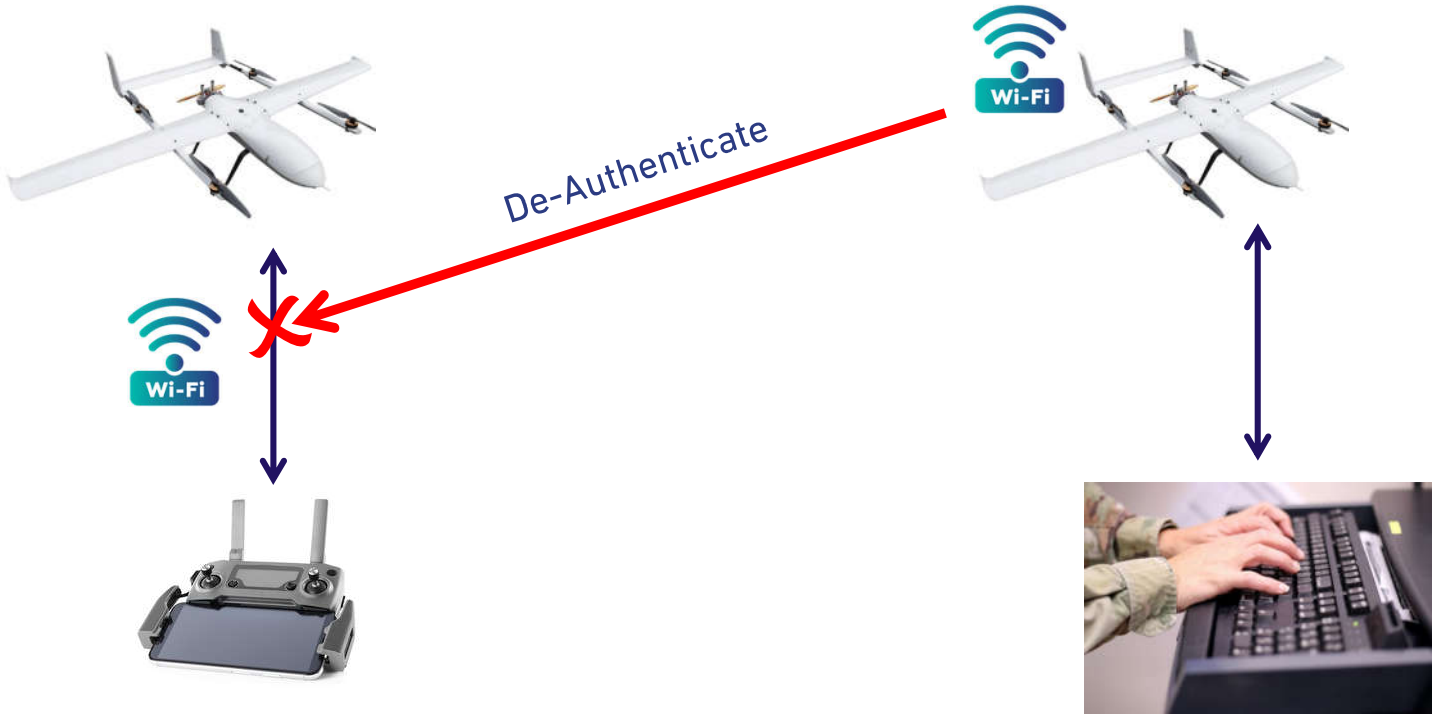


UAS MITM Attack

Source: https://www.sciencedirect.com/

4 Leveraging vulnerabilities and attacks vectors to protect from UAS

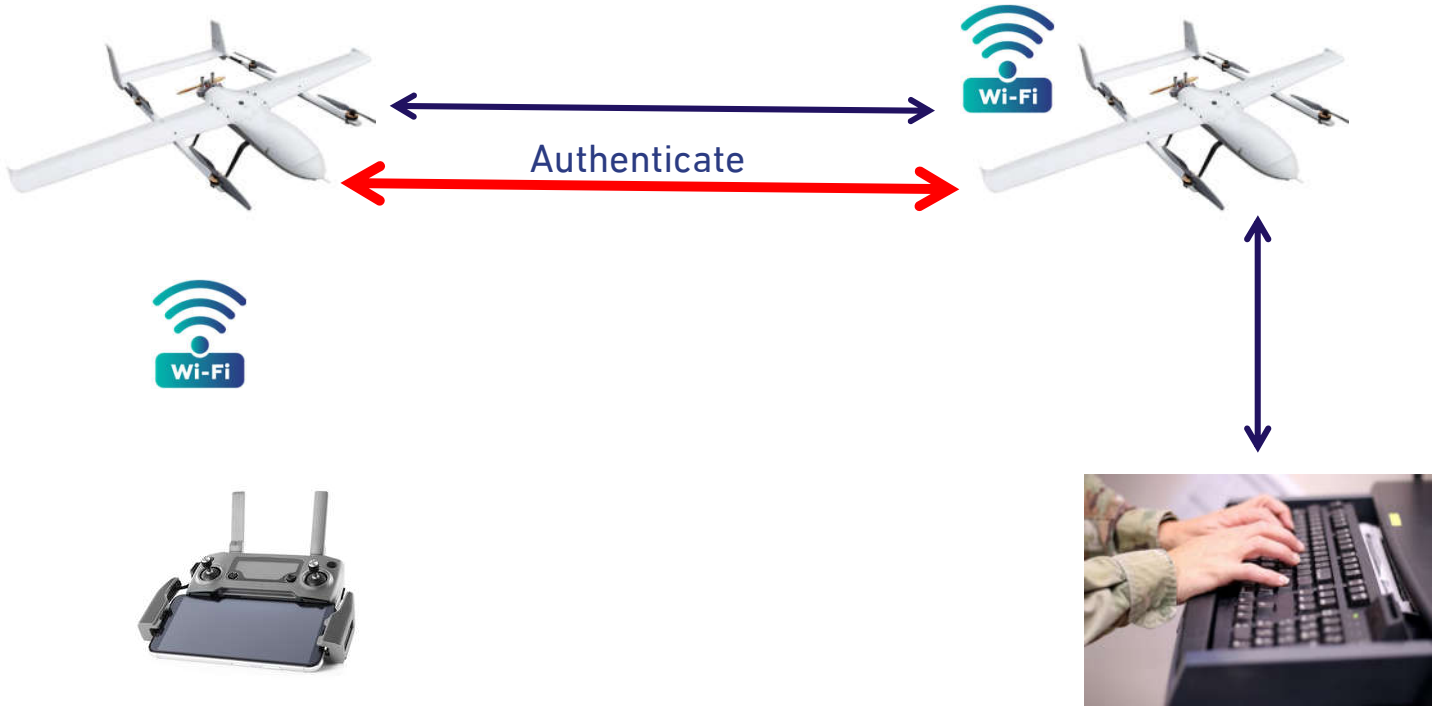
SkyJack Attack (Drone takeover)



4 Leveraging vulnerabilities and attacks vectors to protect from UAS

https://www.youtube.com/watch?v=EHKV01YQX_w
https://github.com/samyk/skyjack/blob/master/skyjack.pl

SkyJack Attack



More examples

bbc.com/news/technology-35709676

Police drone can be hacked with $40 kit, says researcher

2 March 2016

The researcher did not disclose the make or model of the drone he successfully hacked

A security researcher has reported finding a way to hijack a high-end drone, using parts costing as little as $40 (£29).

WIRED

Most U.S. Drones Openly Broadcast Secret Video Feeds

Four years after discovering that militants were tapping into drone video feeds, the U.S. military still hasn't secured the transmissions of more than half of its fleet of Predator and Reaper drones, Danger Room has learned. The majority of the aircraft still broadcast their classified video streams "in the clear" -- without encryption. With a minimal amount of equipment and know-how, militants can see what America's drones see.

FOUR YEARS AFTER discovering that militants were tapping into drone video feeds, the

threatpost Podcasts Malware Vulnerabilities InfoSec Insiders Webinars

Hack Allows Drone Takeover Via 'ExpressLRS' Protocol

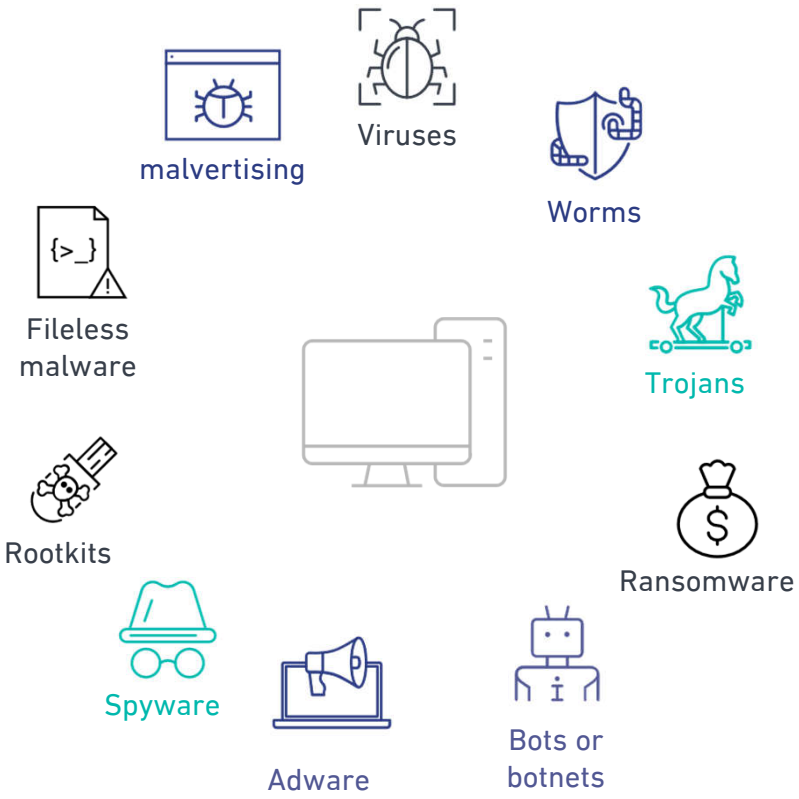
A radio control system for drones is vulnerable to remote takeover, thanks to a weakness in the mechanism that binds transmitter and receiver.

ExpressLRS is an open-source long range radio link for RC applications, such as first-person view (FPV) drones. “Designed to be the best FPV Racing link,” wrote its authors on Github. According to the report the hack utilizes “a highly optimized over-the-air packet structure, giving simultaneous range and latency advantages.”
The vulnerability in the protocol is tied to the fact some of the information sent over via over-the-air packets is link data that a third-party can use to hijack the connection between drone operator and drone.

3

Attack vectors of UAS

Types of Malware



THANK YOU