

# A study on exploitation of UAVs: An increasing threat among cyber criminals

Cybercrime, IT Security and Risk

Sirajuddin Asjad

University of South-Eastern Norway  
Campus Kongsberg

May 2021

# Agenda

## 1. Introduction

### 1.1 Anatomy of a UAV

## 2. History of UAV security exploits and cyber attacks

## 3. Threats and vulnerabilities

### 3.1 Cyber-physical attack surfaces

## 4. Common attack methods

### 4.1 Sniffing attack

### 4.2 Spoofing and man-in-the-middle attack

### 4.3 Jamming and DoS attack

## 5. Conclusion

## 6. References

- Security of Unmanned Aerial Vehicles (UAVs)
- Increased popularity
- Military and non-military

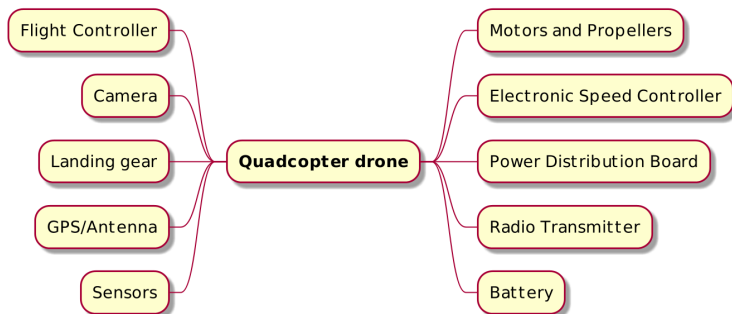
# Introduction

- Government, law enforcement, fire fighting, emergency rescue, and so on...



# Anatomy of a UAV

- Flight controller deployed at the center
- Electronic Speed Controllers (ESCs)
- Radio interface
- GNSS (GPS), radar antenna, multiband data-link antenna



# History of UAV security exploits and cyber attacks

- <https://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer>


## Exclusive: Iran hijacked US drone, says Iranian engineer

In an exclusive interview, an engineer working to unlock the secrets of the captured RQ-170 Sentinel says they exploited a known vulnerability and tricked the US drone into landing in Iran.



# History of UAV security exploits and cyber attacks

- <https://www.theguardian.com/world/2009/dec/17/skygrabber-american-drones-hacked>



PCI-E Internal TV Tuner Card MPEG Video DVR Capture Recorder PAL BG PAL I BOW4

Condition: **New**

Multi-buy:

Buy 1	Buy 2	Buy 3
£19.37 each	£19.18 each	£18.98 each

Quantity:  4 or more for £18.79 each

5 available

Price: **£19.37 each**

[Buy it now](#)

[Add to basket](#)






[Watch this item](#)

30-day returns

Postage: **£3.99 Economy Delivery** | [See details](#)  
International postage of items may be subject to customs processing and additional charges.

Item location: Shen Zhen, China  
Posts to: Europe | [See exclusions](#)

Delivery: **Estimated between Wed, 16 Jun. and Tue, 27 Jul.**  
Seller sends within 5 days after [receiving cleared payment](#).  
Please allow additional time if international delivery is subject to customs processing.

Payments:     

[Get more time to pay.](#) | [See payment information](#)

Returns: 30 days refund, buyer pays return postage | [See details](#)

[Have one to sell? Sell it yourself](#)

- Hardware attacks
- Software attacks
- Fault injection and exploitation
- Communication attacks



- Many attack surfaces exist in the cyber-physical domain
- Changes in the physical domain, and vice versa
- Massive consequences
- Manipulation of sensors and improper UAV navigation
  
- Navigation (GPS), fault handling, network layer
- Data-driven systems

- Sniffing attack
- Spoofing and man-in-the-middle attack
- Jamming and DoS attack

- Monitoring the communication channel
- Extract or "sniff" information through this channel
- Good key management and distribution

# Spoofing and man-in-the-middle attack

- Insert your own communication or messages
- Modify existing messages
- Compromise integrity of the UAV communication

- Denial of Service
- Flooding information with noise
- Compromises the availability of the UAV
- Hard to find solutions
- Add authentication to filter out malicious traffic

- Increasing popularity
- Still many issues in regard to security and cyber crime
- A new trend among cyber criminals, many different attack vectors
- Many unknown security challenges ahead
- Phishing attempts, social engineering

- <https://doi.org/10.1016/j.iot.2020.100218>
- <https://doi.org/10.1109/NTMS.2018.8328747>
- <https://doi.org/10.1109/ICPICS50287.2020.9201954>
- <https://publications.ffi.no/nb/item/asset/dspace:6791/20-01289.pdf>
- More in the portfolio report...