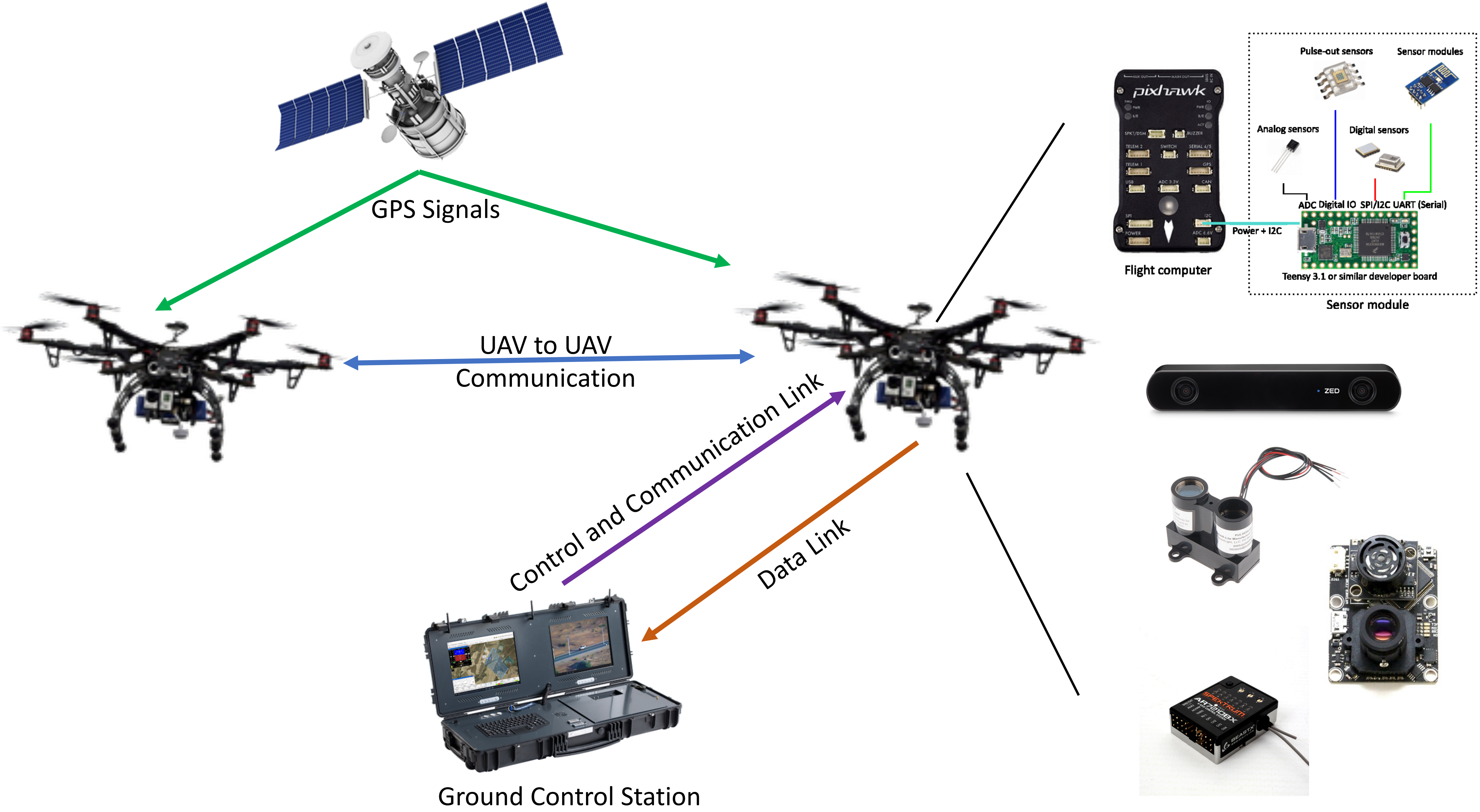
Introduction to Cybersecurity of UAV

Dr. Jiawei Yuan

Assistant Professor

University of University of Massachusetts Dartmouth

Supported by NSF DGE-1956193


GPS Signals
UAV to UAV
Communication
Control and Communication Link
Data Link
Ground Control Station
Flight computer
Pulse-out sensors
Sensor modules
Analog sensors
Digital sensors
ADC Digital IO SPI/I2C UART (Serial)
Power + I2C
Teensy 3.1 or similar developer board
Sensor module

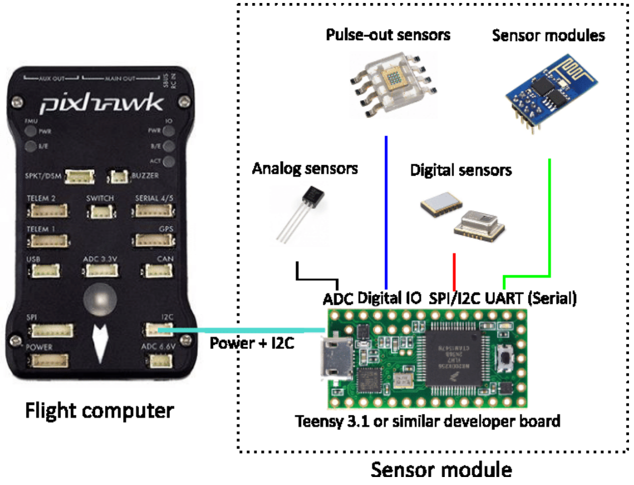
Threats to UAV

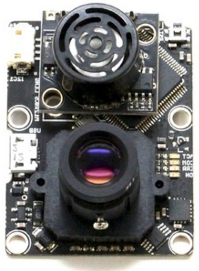
- Hardware-oriented Security Threats.
- Threats to the communication and network of UAVs.
- Data security and privacy.

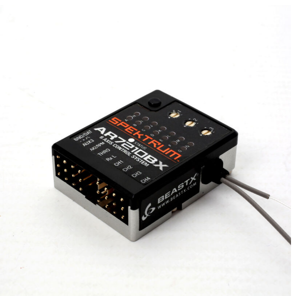
Supported by NSF DGE-1956193

Hardware-oriented Security Threats

- UAV is not only vulnerable to the threats that target the specific UAV hardware components, but also to common vulnerabilities that compromise the reliability and dependency of electronics.







Supported by NSF DGE-1956193

Malicious Hardware

- UAV adopts various commercially available chips or embedded system IPs.

- These black-box components may include backdoor, malicious firmware, and hardware Trojans from untrusted IP vendors or hostile agents.

- Once the malicious hardware components are installed and connected to the network, they can be used by the adversary for different attacks.

Supported by NSF DGE-1956193

In-field Hardware Tampering

- The adversary who gets physical access to the hardware of UAVs and tamper with the embedded computing and sensing components.

- For example, hardware devices like camera, accelerometer, microphone, GPS, or even battery of UVAs can be manipulated by attackers through a physical connection.

- Other attacks can also be implemented via physical access, e.g., malware can be stored on USB and injected to UAVs through firmware upgrade.

Supported by NSF DGE-1956193

Counterfeit Electronics

- Counterfeit electronic has been a dominant concern for hardware security, which directly impacts the reliability and dependency of numerous electronic products and systems.

- More and more used or discarded UAV parts might be recycled from electronic trash and reused in building new UAVs.

- If recycled sensors or micro-controllers are utilized, the reliability and security of UAVs will be significantly compromised.

Supported by NSF DGE-1956193

Threats to the communication and network

- Communication and network of UAVs have been identified as critical components that raise cybersecurity risks.
    - UAV – GCS
    - UAV – UAV
    - UAV – Air traffic control
    - GPS
    - UAV – External computing platform (e.g., cloud computing, edge computing)

Supported by NSF DGE-1956193

Purposes of the Adversary

1. Obtain and make use of sensitive information sent from/to UAVs
2. Modify data sent from/to UAVs
3. Take control of the UAV
4. Confuse the UAV and other valid entities that communicate the UAV
5. Deny of service, i.e., disable the communication between UAV and other valid entities (e.g., ground control station, GPS, ATC)

Supported by NSF DGE-1956193

Potential Threat Consequence

1. The disclosure about the partial or all sensitive information betting transmitted, the identity of the communicating entities, the frequency and volume of communication, and the communication protocol being used;
2. Confusing or misleading UAVs and other valid entities in the UAS;
3. Taking control of the UAVs;
4. The crash of UAVs or aerial traffic accidents;
5. Threats to civilian and military safety.

Supported by NSF DGE-1956193

GPS Jamming and Spoofing

- Jamming is the presence of a competing signal that prevents the GNSS receiver from decoding the true satellite signal.
  - The GNSS signals are so weak at the earth’s surface that they are below the surrounding background noise level.
  - Consequently, it does not take much of an interfering signal to jam the receiver.

- Spoofing is the intentional transmission of fake GNSS signals to divert users from their true position.
  - Spoofing requires sophisticated equipment to recreate the satellite signals, so it is more difficult to do, but it is also more difficult to detect than jamming

Supported by NSF DGE-1956193

GCS Control Signals Spoofing

- Injecting false wireless control commands using the data link can be accomplished by a man-in-the-middle attack.

- The adversary blocks the legitimate communication between the UAV and the ground control station and begins commanding the drone herself.

- A covert wireless injection is also possible if the adversary acts in both directions to trick both the drone and the ground control into believing they are communicating with each other

- Software such as SkyJack can be installed on a malicious drone that takes a predator role to take control of civilian WiFi operated drones

Example: https://www.youtube.com/watch?v=aPtElNXoY6k&feature=emb_logo

Supported by NSF DGE-1956193

GCS Control Signals Jamming

- The fail-safe protocol of UAVs assumes that the lost link state is the result of a malfunction in the data link and that the UAV is able to navigate itself autonomously using GPS signals to return to its base.

- This is not the case if the UAV is under attack, because the adversary is also likely to jam the GPS signals as well, which leads the UAV to fly aimlessly with no control.

Supported by NSF DGE-1956193

Jamming or Spoofing the UAV Communication

- Spoofing telemetric data and video feeds from UAV to GCS can directly influence the operator commands, which can possibly result in a drone crash

- Spoofing ADS-B signals by continuously feeding the UAV with malicious ADS-B signals to trick it into diverting its course in order to avoid collisions and ultimately directing it to the desired territory

Supported by NSF DGE-1956193

Intercept UAV-GCS communication

- Autonomous low-altitude UAVs rely on the video captured by their cameras for navigation and collision avoidance

- An attacker who has knowledge of the system parameters and is able to gain access to the flight controller can intercept the system calls issued to the kernel and replace the genuine footage with a fabricated one.

- A direct consequence of this attack is the hijacking of the drone by intentionally landing it at a location other than the originally intended one.

Supported by NSF DGE-1956193

Insufficient Authentication

- The lack of authentication or weak authentication that can be somewhat bypassed.

- Examples:
    - the communication of ADS-B data for air traffic control does not have secure authentication by default.
    - The authentication Micro Air Vehicle Link (MAVLink) is based on a pre-shared key.

Supported by NSF DGE-1956193

Denial of Service

- A denial-of-service attack can be launched on such small drones given that the adversary can access the flight controller parameters and therefore is able to disrupt the UAV system.

- Some models of this category of drones are relatively small, they encompass moderately powered processors.

- Accordingly, flooding their network cards with random commands via the data link can force such drones to go into an unexpected state and possibly halt their operation.

Supported by NSF DGE-1956193

Injecting Falsified Sensor Data

- Directed energy can be used to control the electromagnetic spectrum, which is not limited to radio and radar frequencies but also includes infrared, visible, and ultraviolet signals

- Example: an external source of audio energy was used to alter the output of a UAV Microelectromechanical gyroscope by interfering with its resonance frequency, which led the drone to lose control and crash.

Supported by NSF DGE-1956193

Lack of Encryption

- The communication of ADS-B data does not have any encryption to protect the confidentiality of the data.

- MAVLink does not provide message encryption to guarantee low latency of communication

Supported by NSF DGE-1956193

Security Requires of UAV

- Authorized access: The UAV system must provide means to ensure that only authorized operators are granted access to its resources including both the ground control station and the aircraft.

- Availability: All the elements of the UAV system should be guaranteed to perform their required functions under defined spatial and temporal circumstances such that the system sustains its availability without disruption during its operational period.

Supported by NSF DGE-1956193

Security Requires of UAV

- Data Confidentiality: The UAV system should employ mechanisms to mitigate unauthorized disclosure of the telemetric and control information.

- System integrity: The UAV system should be able to guarantee the authenticity of its software and hardware components

Supported by NSF DGE-1956193

Security Requires of UAV

- Accountability of Actions: The UAV system should employ mechanisms that enforce non-repudiation to ensure that operators are held responsible for their actions.

Supported by NSF DGE-1956193

Reference

- *Riham Altawy and Amr M. Youssef. 2016. Security, Privacy, and Safety Aspects of Civilian Drones: A Survey. ACM Trans. Cyber-Phys. Syst. 1, 2, Article 7 (February 2017), 25 pages.*

Supported by NSF DGE-1956193