UAVs, IoT, and Cybersecurity

David Kovar, Kovar & Associates LLC

dkovar@gmail.com

usenix LISA16

December 4–9, 2016 | Boston, MA
www.usenix.org/lisa16 #lisa16

Terminology

- UAS – Unmanned Aerial System – Emphasis on system
- UAV – Unmanned Aerial Vehicle – The aircraft portion of the system
- Drone – Common term for any UAV but most often used to describe quads and other multirotor UAVs
- GCS – Ground Control Station – The flight control portion of the system. May include manual and automatic control features
- Data link – radio system to transmit data to and from the UAV. Often used for telemetry, sensor data, and FPV operation
- C2 link – radio system to transmit command and control instructions to the UAV
- FPV – First Person View – technology that enables the operator to fly the UAV from the perspective of the UAV

The Foundation – Security Engineering

Security engineering is about building systems to remain dependable in the face of malice, error, or mischance. As a discipline, it focuses on the tools, processes, and methods needed to design, implement, and test complete systems, and to adapt existing systems as their environment evolves. Security engineering requires cross-disciplinary expertise, ranging from cryptography and computer security through hardware tamper-resistance and formal methods to a knowledge of economics, applied psychology, organizations and the law. System engineering skills, from business process analysis through software engineering to evaluation and testing, are also important; but they are not sufficient, as they deal only with error and mischance rather than malice.

Ross Anderson "Security Engineering", 2nd Edition, Introduction


Putting UAVs in Context

UAVs are “Just” Vehicles

- The typical commercial UAV is a remote controlled aircraft with an off the shelf flight computer capable of autonomous operation that is carrying an optical sensor payload
- It is an inexpensive airframe running an inexpensive computer that is designed carry low cost, low power, high fidelity sensors to collect data for real time and post processing
- The data collection process is not innovative, the ability to do it in house for a low cost is new
- The value is in the raw and processed data and metadata
- The most important growth will not be in hardware, it will be in software and data analysis

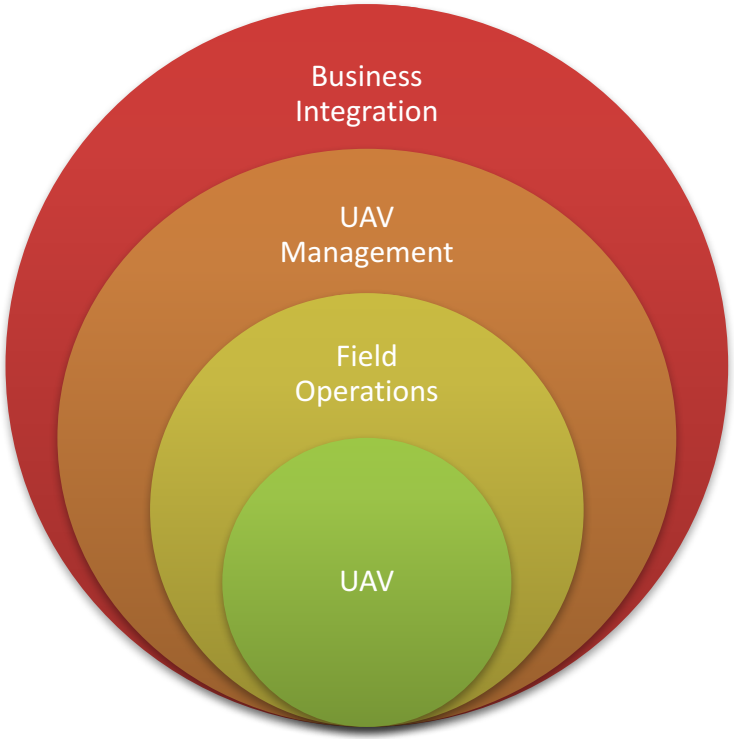
UAVs, Autonomous Vehicles, IoT

- The Internet of Things refers to the network of physical objects with embedded sensors, controllers, and electronics that enables those objects to exchange data with each other, vendors, operators, and other connected devices.
- A UAV has an onboard network of sensors, controllers, and network devices that share data related to operations and to the mission.
- The UAV “device” is a semi-autonomous “connected device”, one of many in the Internet of Things.
- UAV cyber security has much in common with IoT, SCADA, medical device, or connected vehicle cyber security.


UAV Integration With The Enterprise

Integrating UAVs into the Business

Increasing Detail - Requirements



Increasing Refinement - Product

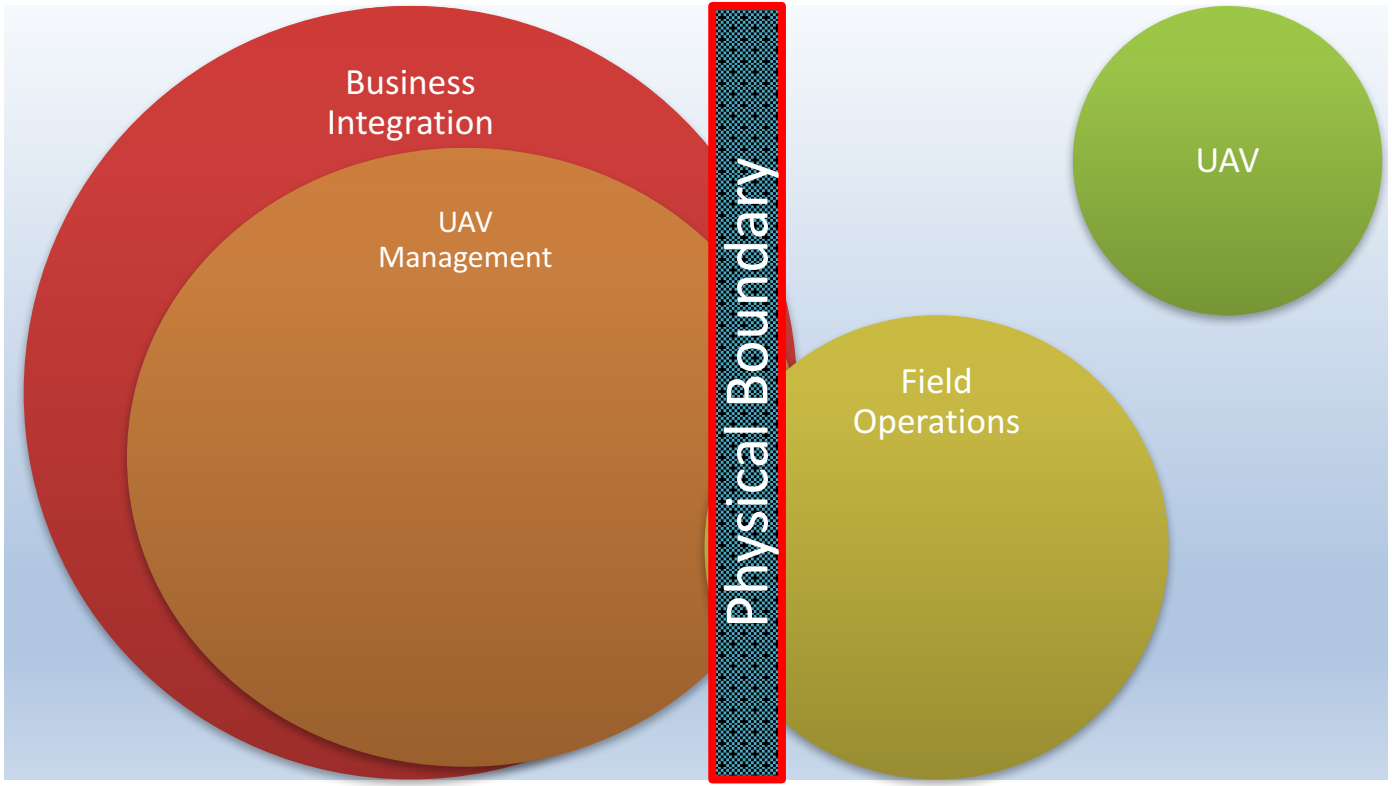
Mission requirements, data analysis, integration
[Data analysis, business systems]

Mission planning & tasking, purchasing, staffing, maintenance
[Business, inventory, maintenance systems]

Field team, logistics, flight operations
[*Ground control station, data link, remote controller]*

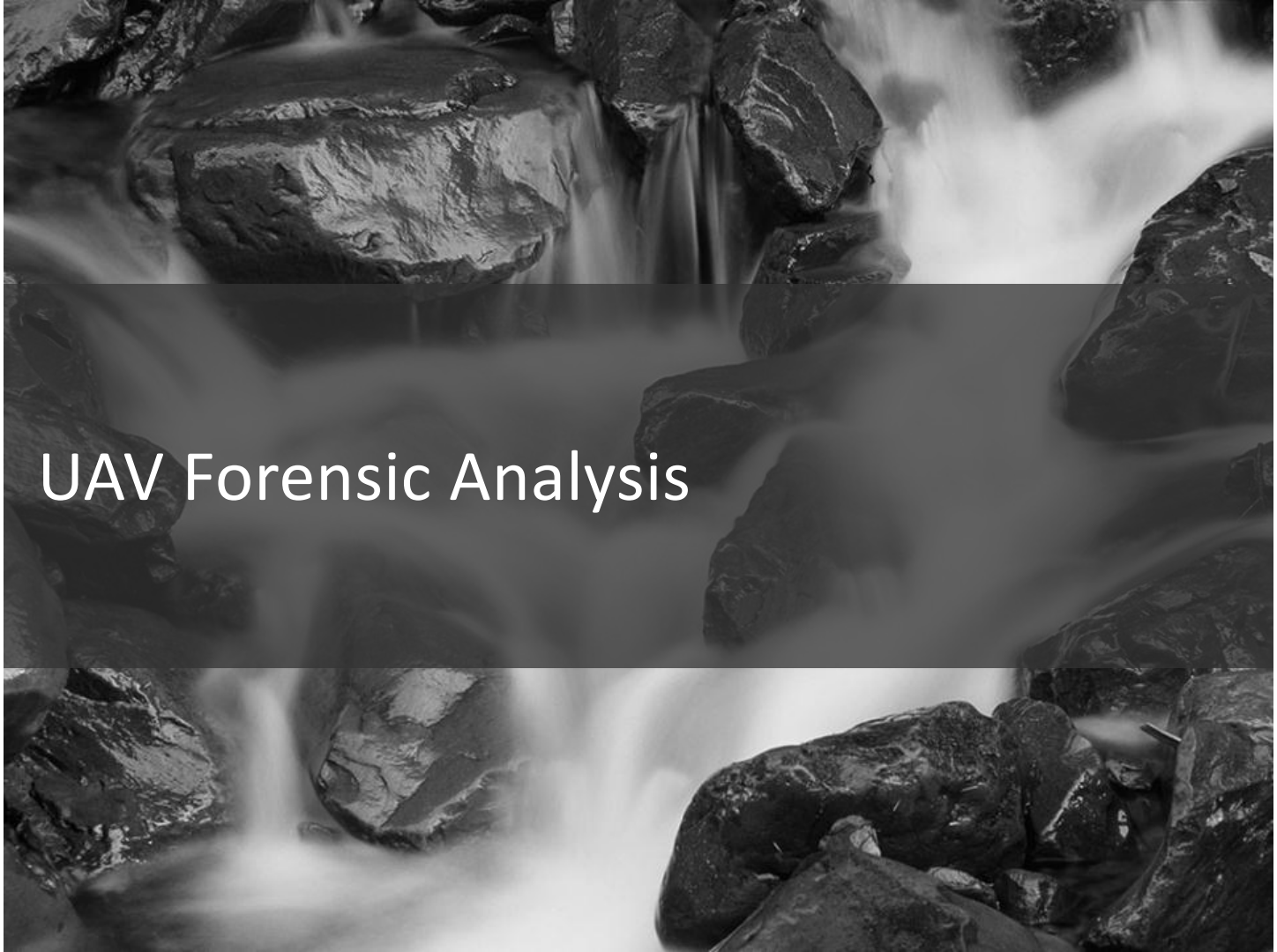
UAV *[Flight controller, payload, flight sensors]*

Integrating UAVs into the Business – Reality



UAV Operational Workflow

Mission Planning	Approval	Execution	Analysis	Delivery
▸ Criteria	▸ Business	▸ Logistics	▸ Data validation	▸ Product delivery
▸ Airframe	▸ Site logistics	▸ Flight crew	▸ Product generation	▸ Product support
▸ Payload	▸ Safety	▸ Weather	▸ Quality assurance	▸ Lessons learned
▸ Operator	▸ Legal	▸ Flight operations		▸ Reporting
▸ Location	▸ Risk			▸ Billing
▸ Time frame	▸ Flight operations			


UAV Forensic Analysis

Where Is Your Data

What data is in your system?

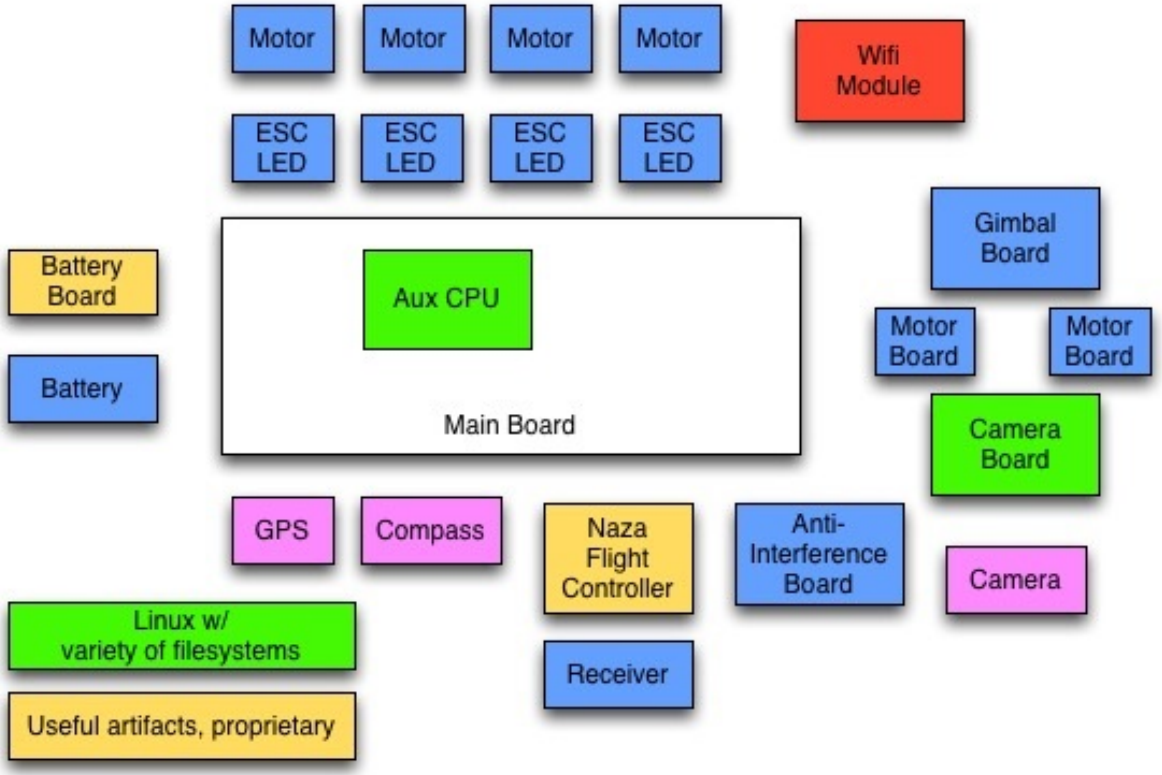
Where is it at rest?

Where is it in motion?

Where is it vulnerable?

What threats target what parts of the system?

What Is In A Quad Rotor UAV



UAV CPUs and “Operating Systems”

The flight controller is the core system in a UAS and amounts to the aircraft’s CPU & operating system.

Open Source

- Openpilot
- Ardupilot (APM, Pixihawk)
- Multiwii
- KKmultipcopter

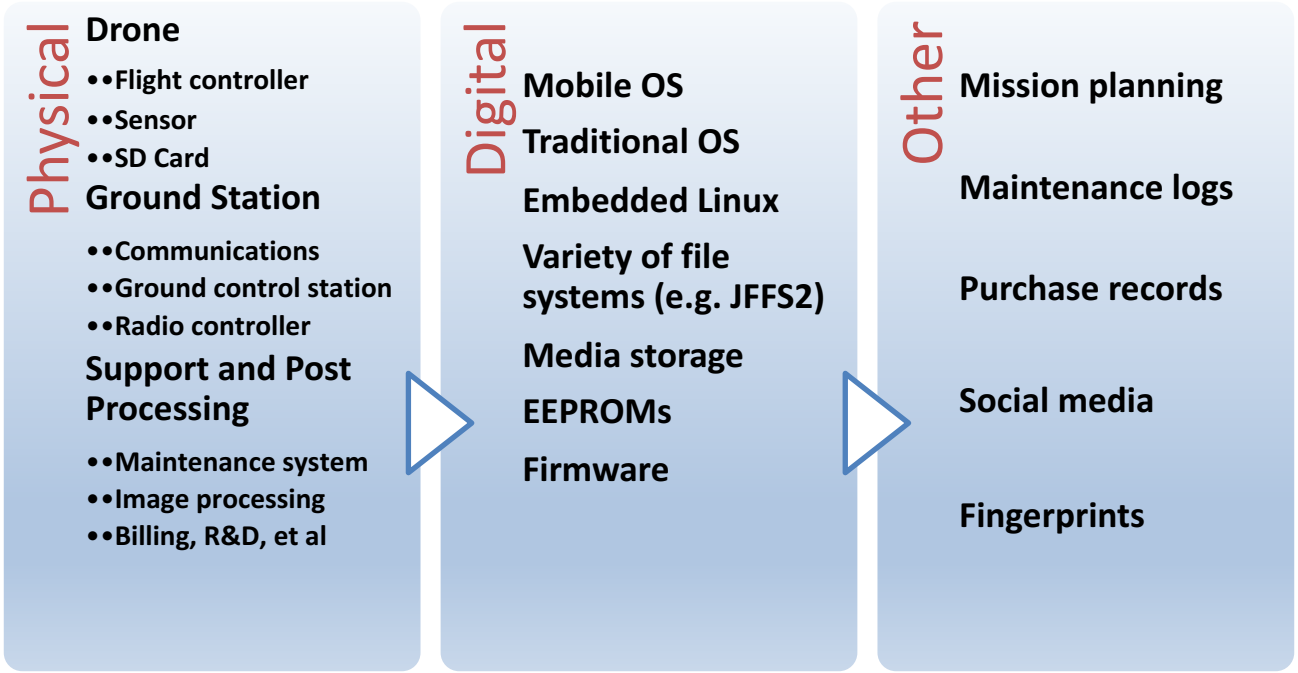
Commercial

- Parrot AR Drone FC
- Naza (DJI)
- Wookong (DJI)
- Dualsky (FC450, etc)

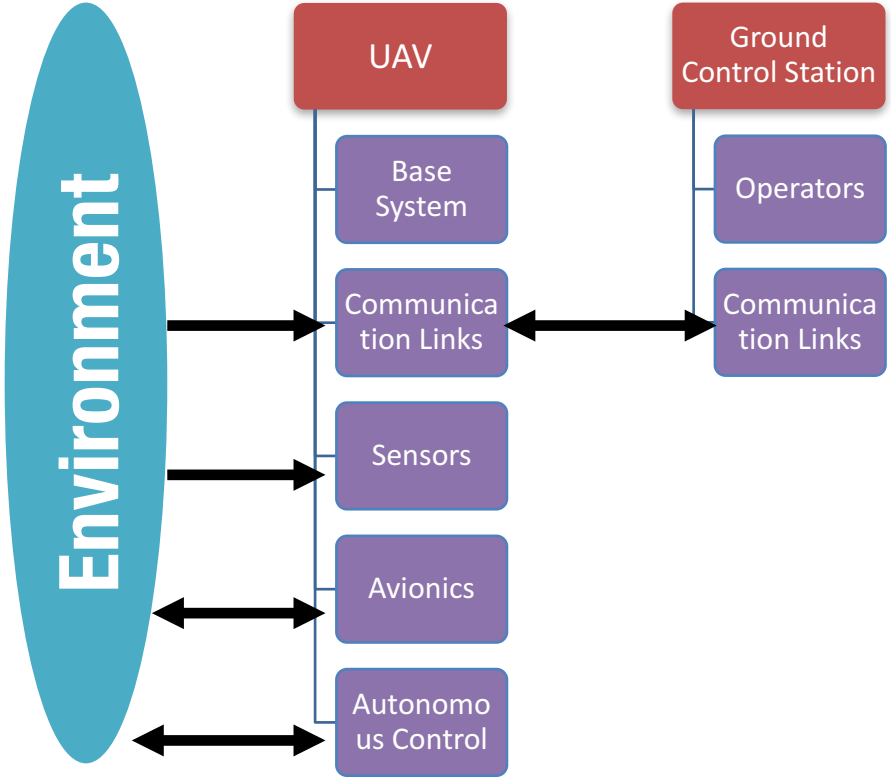
Airware is trying to be the Microsoft/IBM of the UAV world, selling hardware and software for all phases of UAV operations

Linux is the predominant OS for onboard UAV systems

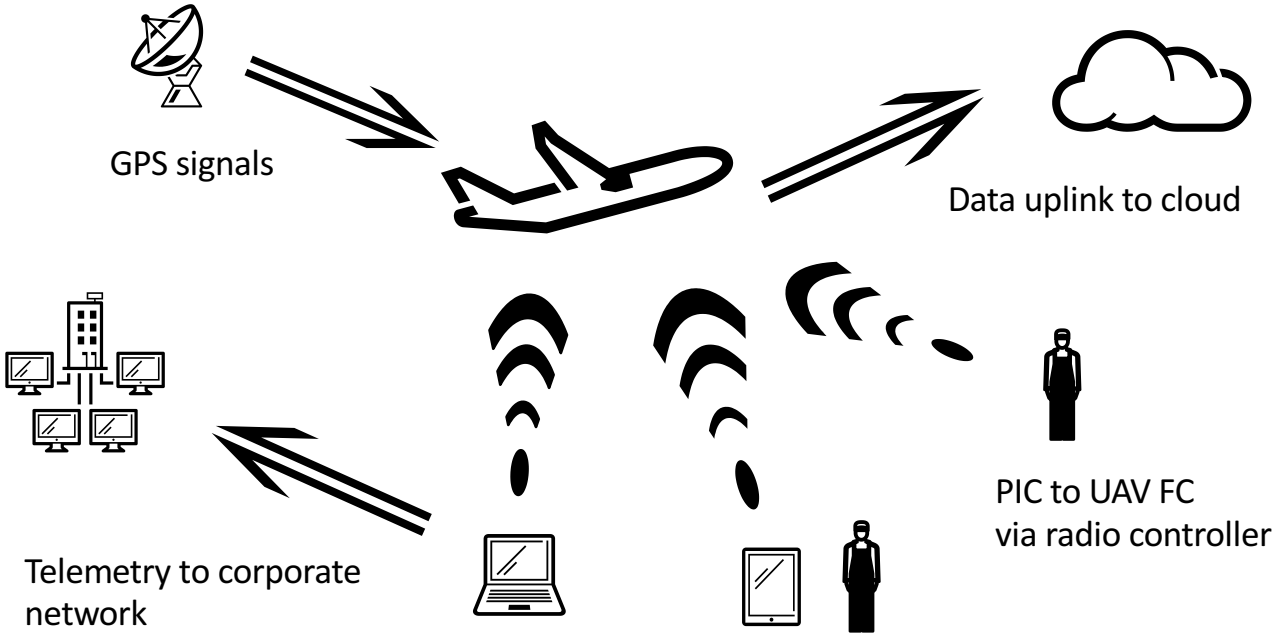
UAV Forensic Artifacts



UAV Data Flows



UAV Data Flows




Example Risks

Ground Control Station

Application configuration files contain interesting information

```
Path:       /mobile/Applications/com.dji-
innovations.DJEye/Library/Preferences/com.dji-
innovations.DJEye.plist
```

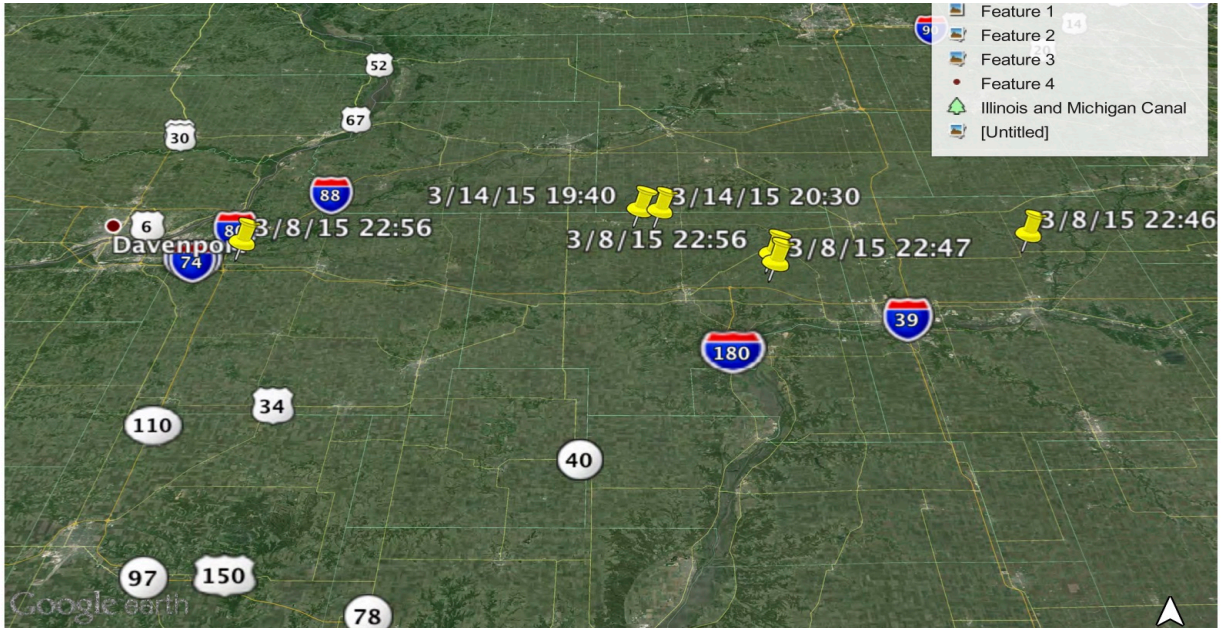
Excerpts

```
email = XXXXXXX@gmail.com; (DJI account information)
password = XXXXXX;

ground_station = 1; (User is flying with waypoints)
fpv_mode = 0;       (User is not flying FPV)
```

Ground Control Station

Using the data from the GCS, you can plot operation locations.



Real Time Data Interception

Connect via WiFi and send commands to the flight controller using ser2net.

```
** Rcv from port 0x08, seq     0, cmd 0x04, subcmd 0x00, error 0, payload
len  0
0x0400: server says hello!
** Sent to  port 0x0a, seq     3, cmd 0x53, subcmd 0x00, error 0, payload
len  0
** Rcv from port 0x0a, seq     2, cmd 0x49, subcmd 0x00, error 0, payload
len  52
[0x49]: Seq     2, GPS sats 4, home [+40.431455, -89.311694] loc
[+40.431496, -89.311653], accel xyz [+00, +00, +00], ag +1.2 meter,
compass roll/pitch/heading [180, 180, 093], batt 12065mV (74%), unknown 6
[0x53]: Seq     3, battery <5200mA, 5440mA>, current level <12090mV,
4619mA>, unknown 6e fc 63 54 1e 03 00
```

Question: If you are uploading data to the cloud in real time, where are your credentials?

Hijack of a UAV

- Several commercial UAVs use WiFi for command & control and data.
- A user can identify the SSID, deauthenticate the UAV, and then capture the UAVs attempt to reestablish the link. Once the link is established, they can control the UAV, download telemetry, or download sensor data.
- Other commercial solutions use 915Mhz links using the MavLink protocol which can also be hijacked.
- An deauth/assume control attack has been demonstrated on the majority of the consumer/commercial remote controllers independent of the data link

If you have access to the C2 or data link, you can also change waypoints and other mission parameters.

Sensor Metadata

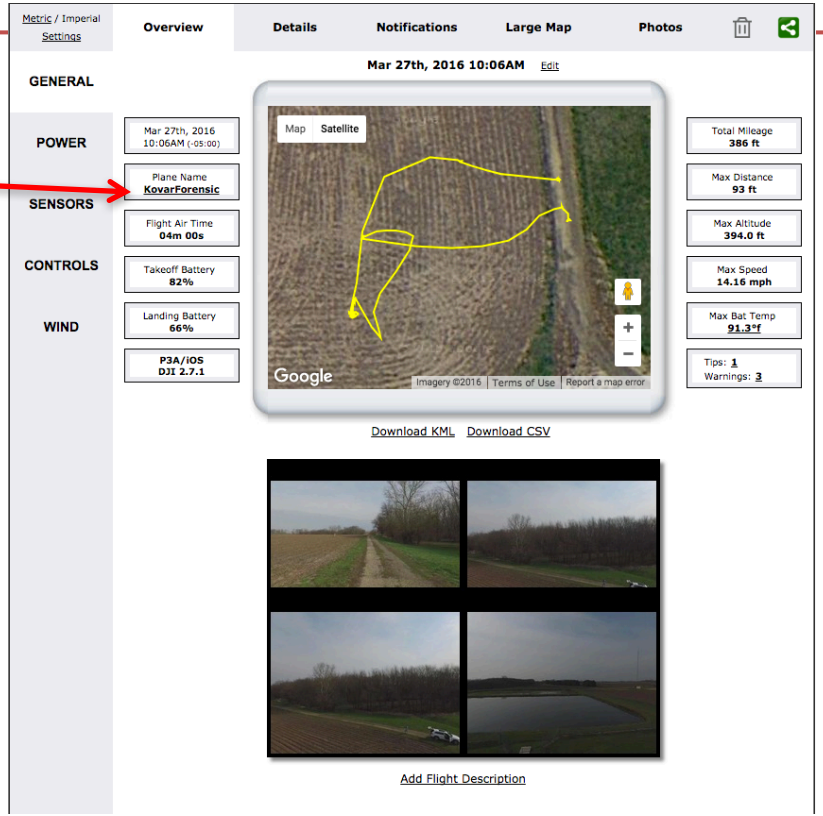
The purpose of a camera is to take a picture, and EXIF data tells a story about the camera and where it was taking pictures.

- Image Description : DCIM\100MEDIA\DJI_0030.JPG
- Make : DJI
- Camera Model Name : FC300S
- Date/Time Original : 2016:03:27 10:15:57
- Create Date : 2016:03:27 10:15:57
- GPS Version ID : 3.2.0.0
- GPS Latitude Ref : North
- GPS Longitude Ref : West
- GPS Altitude Ref : Above Sea Level
- Aperture : 2.8
- GPS Altitude : **74.6 m Above Sea Level**
- GPS Latitude : 40 deg 32' 15.84" N
- GPS Longitude : 89 deg 30' 50.63" W
- GPS Position : 40 deg 32' 15.84" N, 89 deg 30' 50.63" W

DJI Phantoms ~~do not~~ did not record altitude in the EXIF data ~~unfortunately~~.

Log Files

- Healthy Drones view
- Shows the location and flight path
- Shows the UAV's name
- Shows other data in the other categories
- The address may even be in the Details section



Legal Third Party Collection of Data

“By using the Service, you grant DroneDeploy a non-exclusive, irrevocable, fully paid and royalty-free, transferable, sublicensable, worldwide license to use, copy, reproduce, process, adapt, modify, publish, transmit, display, and distribute your User Content.”

DroneDeploy Terms of Service

Legal Third Party Collection of Data

"The Recipient further understands and agrees that his data including, but not limited to, *flight telemetry data and operation records* could be uploaded to and maintained on a DJI-designated server under certain circumstances."

DJI legal document

"When you choose to self-authorize or "unlock" flight operations on DJI hardware control applications (including DJI Go (the "DJI Go App")) in locations that are categorized by DJI's Geospatial Environment Online system as raising safety or security issues, we collect and retain geolocation information relating to your decision."

DJI web site, Privacy page

Legal Third Party Collection of Data

"OAM (Office of Aviation Management) highly recommends that, before choosing any particular aircraft, from any manufacturer, especially those that might be used for sensitive purposes, that your technical people fully understand what information may be transmitted, to whom it might be transmitted to, and whether it matters to your program."

Source – Dept. of Interior internal communication obtained through FOIA request

Complete report:

https://wordpress.com/post/integriography.wordpress.com/838


Exposing Self Selected Valuable IP

We Are Not Collecting Useless Imagery

- We are imaging:
  - Critical infrastructure
  - Test crops
  - New construction
  - Infrastructure impacted by disaster
  - Test tracks with prototype equipment
- We are not imaging things of little value

We Are Self Identifying Valuable IP

- We are documenting assets of particular value, documenting change, growth/value add, decay/value decrease
- Mission plans, even before imagery is collected, reveal intention and interest
- Flight logs and UAV management data contain sensitive information
- We are identifying IP as valuable by our planning and activity, documenting that interest, and sharing and storing it in the cloud


UAV Risk Management

IoT Security Challenges

Potential issues contributing to the lack of security and privacy best practices include:

- lack of IoT supply chain experience with security and privacy
- lack of incentives to develop and deploy updates after the initial sale
- difficulty of secure over-the-network software updates
- devices with constrained or limited hardware resources (precluding certain basic or “common-sense” security measures)
- devices with constrained or limited user-interfaces (which if present, may have only minimal functionality)
- devices with malware inserted during the manufacturing process.

BITAG – Internet of Things Security and Privacy Recommendations

Unique Challenges - Fleet Management

- Build cybersecurity into your fleet management program
  - Data and asset classification is critical
  - Discovery. Control. Visibility
- Data collection - Pervasive. Effective. Forever. (Jordi Sanchez)
- There are existing models for fleet management to learn from

Unique Challenges - Airspace Management

- Can you manage the airspace over your site?
- Can you detect your own UAVs and those UAVs which are not yours? Can you differentiate between the two?
- Can you monitor your UAV and detect changes during flight?
- Do you have a response plan that covers the detection of a foreign UAV or compromised UAV?

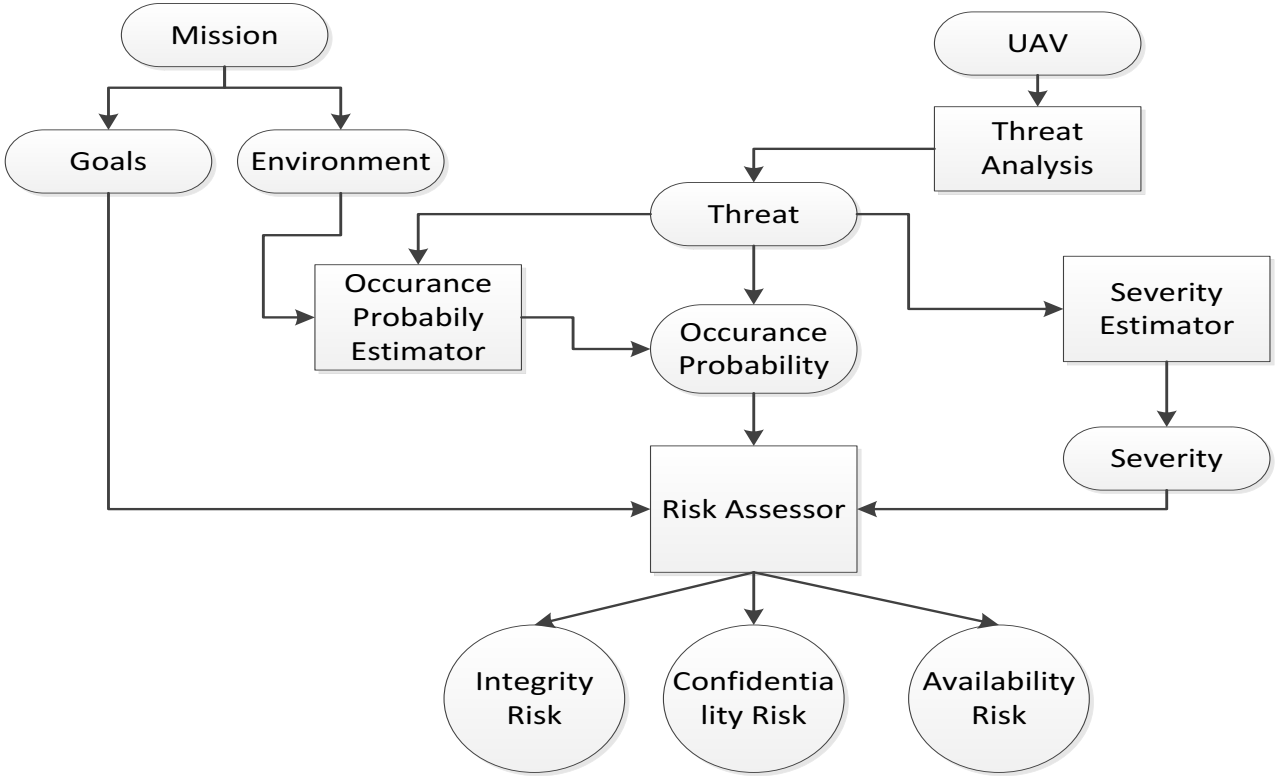
UAV Risk Management Factors

- Physical exposure
- Communication systems
- Storage media
- Sensor systems
- Fault handling mechanisms
- Mission planning systems
- Maintenance systems

UAV Risk Assessment Environment

- UAVs do not operate within the confines of a facility
- Risk assessment must take into account operating environment
  - Geographic
  - Weather
  - Local, state, and national law, regulation, and policy
  - Mission requirements
  - Mission plan

UAV Risk Assessment Model




What Should Be Done

People, Process, Technology

- Hire people who are security focused
  - People will circumvent the best security processes and technology
- Implement sound, reasonable security processes around your intellectual property
  - Learn, apply, and live security engineering
  - Push security out to all departments that touch IP, such as purchasing
  - Secure the entire supply chain
- Invest in useful, well supported (internally and externally) technology

Regulation

“That (bypassing regulations and standards) might accelerate innovation today, but it means there will be few regulatory tools in place to cope with the many ethical, logistical, and safety challenges that lie further down the self-driving road. And if industry experts can decide to simply skirt the requests of state regulators, the prospects for future regulation look dim.”

Mark Harris, “How Otto Defied Nevada and Scored a $680 Million Payout from Uber”

Securing Unmanned ~~Aerial~~ Systems

- Design security into all components rather than adding it in later
- Collect and retain least amount of information, know where information resides, know where it moves, encrypt everything
- Select vendors who share your vision
- Conduct a complete security audit of the environment as designed. Include privacy, risk, fraud
- Conduct a complete security audit of the environment as implemented and perform regular audits going forward
- Include the UAV environment in threat intelligence, security monitoring, incident response, vulnerability management, and audit programs
- Train staff on all risk elements associated with the UAV infrastructure and associated data

Resources

- NTIA UAV best practices on privacy, transparency, and accountability issues- https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-unmanned-aircraft-systems
- BITAG – Internet of Things Security and Privacy Recommendations - http://www.bitag.org/report-internet-of-things-security-privacy-recommendations.php
- My blog on many things UAV - https://integriography.wordpress.com/