Drone Forensics
How the growing use of Unmanned Aerial Vehicles creates new forensic challenges for investigators

PLUS
- Inconsistent Tool Performance
- Faster Searching for Illegal Content
- Data Destruction on current hard disks
- From the Lab: Device Forensics in the IoT
The popularity of small Unmanned Aerial Vehicles (UAVs) (a.k.a. Drones) has been surging for several years now among both hobbyists and professionals in a range of industries, producing stunning videography, superb survey maps, and an increasing tempo of interference with manned aircraft operations.

But this growth has brought risks and threats as well. Malicious actors ranging from ISIS to drug cartels to local criminal organizations have also adopted these highly flexible and capable aircraft for their purposes. ISIS used off-the-shelf UAVs as early as 2014. A BBC article [1] suggests that Her Majesty's Prisons first saw drones overhead in 2013. A blog article[2] states that Mexican drug cartels were researching home built drones for drug deliveries in 2013 as well.

Her Majesty's Prisons reportedly investigated more than 160 drone-related incidents in the last eighteen months and a heavy lift consumer drone delivered 13kg of methamphetamine in California late last year. A weaponized DJI Mavic was captured from a Mexican drug cartel months later.

Drones are a component in a larger system, an unmanned aerial system (UAS). Information relating to UAS sourcing, construction, tactics, and operations are created, stored, and transmitted throughout the UAS environment. Information resides in sensors, “black box” log files, cell phones used as ground control stations (GCS), and in NVRAM on flight controllers, GPS chips and other difficult to access hardware. This data, when correctly extracted and accurately analyzed, provides valuable tactical and strategic intelligence about launch locations, flight profiles, and logistical and operational linkages.

It is important to remember that drones are not some strange new technology for which we require completely new tools and ways of thinking. Innovation is certainly required but it rests on existing forensic principles and techniques. Any drone can be broken down into component parts. Considered in this light, they are simply an instance of the Internet of Things (IoT) or a Cyber Physical Engineered System (CPES), a network of sensors, storage, CPUs, and actuators with network connections that enable them to share data and control information. All of these components are involved in a complex, often real time, flow of telemetry, sensor, and environmental data in clear text, binary, and encrypted formats.
The art and science of UAV forensics is at the point where mobile device forensics was 10 years ago.
So, a single drone is an IoT/CPES instance unto itself, several CPUs, a network and sensors all on board talking to external systems via network links. In most cases these external systems are a remote controller and the ground control station (GCS), often a standard mobile device. Extending outward, a swarm of drones is a collection of inter-operating IoT/CPES instances. To understand the entire environment we need to break all of these instances down into component parts, CPUs, networks, sensors etc., establishing a foundation, and building a complete picture from the component parts. Many of those component parts are familiar to us, particularly the mobile devices used to control the drones.

**Challenges**

There are a number of major challenges facing us:

- Learning what questions we can ask
- Learning where the data to answer those questions resides
- Learning how to extract and analyze that data
- Learning how to present the analysis in the most efficient form for the analyst
- Preparing for tomorrow, while answering today’s needs

For investigators and analysts working to mitigate threats from drones and utilize drone forensics in their operations, two challenges stand out:

1. We must prepare for tomorrow’s threats or we will be reacting to the threats rather than proactively addressing them.

   - There are many vendors other than DJI. ISIS are already using PixHawk flight controllers in their home built drones
   - Drones are part of unmanned systems. We must be able to analyze all of the components, not just the drone, or the mobile device, or the remote controller
   - Machine learning, artificial intelligence, and the use of swarms, are coming or are already in use, the classic dual use technology problem
   - 3D printing, a global supply bin, “maker spaces”, and hackers will all help enable one off, custom, or heavily modified drones that challenge our ability to extract and analyze data and other forensic evidence
   - Non-state, state, academic, and commercial organizations are all creating new capabilities and demonstrating possibilities for others to operationalize.

2. We must know what is possible to ask of the data and we must challenge vendors to enable us to answer those difficult questions.

Different cases will lead investigators in different directions obviously, but some common questions that investigators should be prepared to answer are:

- What happened during this flight? Where did it start, how high did it fly, what route did it take?
- What other flights did this aircraft perform?
- What other sites might have seen this aircraft?
- What are the history, flight, maintenance, software, and firmware, of this aircraft?
- Did an expert maintain it capable of
- What components of the aircraft are uniquely identifiable and traceable?
- What identifiable components, such as batteries, are shared with other aircraft?
- Can we link this aircraft to a larger operation?
- What questions should we be prepared to ask operators, service providers, and vendors to enhance our investigations? What can we expect them to know, and to share?
- How do we frame the questions to encourage an efficient and accurate response?

**Where is the Data?**

There are three ways of thinking about UAVs that help an investigator identify all of the potential sources of forensic artefacts. Evidence from one source will lead you to evidence from other sources. Combined, they produce a compelling picture of the immediate flight, but also of operations, logistics, and supply chain. The three approaches are: Physical, Process, and Flow.

**Evidence**

- Mission planning
- Approval
- Execution
- Analysis
- Delivery

Each phase involves documentation, communication, or activity that can be collected and analyzed. Some artefacts reside on drone specific hardware or in drone specific databases but a lot of useful information is available to normal tools once the investigator knows where to look.
Flow evidence derives from the communication between the drone, the environment, its supporting systems, and systems on the Internet. Wi-Fi traffic can be collected and analyzed, cell tower logs will support evidence of the operator's location extracted from the drone, DNS tables will show that the operator was using a specific third party drone data analysis service.

**What Data is Available?**

Most investigators will work with one of two primary log sources, the drone and the mobile device used as a ground control station. The drone's logs are generally very detailed, containing frequent entries from every system on the drone. The mobile device usually has a less robust version of the data on the drone but adds more information about the user's actions, such as setting waypoints and changing views in the application.

Both sources generally contain the following fundamental information:

- Serial number of the aircraft and some components
- Version numbers for critical firmware
- State change information such as launch/land, manual/waypoint operation, GPS available or unavailable
- Geo-location information for critical locations - launch, land, and home point
- Flight track information

The onboard logs for most DJI products contain information from the following systems:

**Drones are not some strange new technology for which we require completely new tools and ways of thinking.**

**Attribution**

Accessibility, availability, and lack of registration enforcement pose one of the greatest challenges to investigators. Anyone with a credit card and shipping address can order highly capable and flexible drones online with few restrictions. This is true for the common consumer drones but also for drones such as the DJI Agras MG-1 that can be purchased from Walmart or Amazon. The MG-1 has a powerful propulsion system that enables the MG-1 to carry up to 10kg of liquid payloads, including pesticide and fertilizer. The combination of speed and power means that an area of 4,000-6,000m² can be covered in just 10 minutes. A significant threat in the wrong hands.

**Cyber Physical Engineered Systems**

Cyber-physical systems (CPS) are engineered systems that are built from, and depend upon, the seamless integration of computational algorithms and physical components.
Vision Positioning
Telemetry
Barometric
GPS
Flight Controls
Gimbal
Motors
Batteries
Message Console

Different models and different versions of firmware will add or remove systems. For example, the agricultural model adds a sprayer system to the drone. References to it exist in some versions of the firmware even if it is not equipped.

Collecting Evidence

Many vendors provide ready access to the onboard logs and often to the application logs as well. Access to the onboard logs is generally through a USB port on the flight controller and the logs appear in a mountable filesystem.

Older DJI models stored the onboard logs on a SD card epoxied onto the main board of the drone. For forensically sound extraction the card could be physically removed and imaged. Alternatively, the drone could be put in "flight data mode" and the files would be available via a mountable filesystem.

In October of 2017, the log files on DJI Mavic's running the latest firmware vanished, users could no longer instruct the drone to expose the SD card via the USB port. Investigations revealed that in newer Mavic models the SD card slots were present but empty. It seemed unlikely that DJI completely disabled such a valuable source of maintenance and failure data. Further investigation determined that the log files had been moved to storage on the flight controller and that they were no longer accessible via flight data mode.

DJI's Assistant 2 application provides some ability to export the flight logs however:

- the resulting files are sometimes corrupted,
- the process is unreliable, and
- the application reports some user activity to DJI's servers.

DJI certainly has access to these files using in-house tools. Researchers located an exploit that provides limited access to the files.

It is expected that this change in the user's ability to access flight logs on their own aircraft will extend to some or all future models. If this trend continues, exploits may be the best option for extracting flight logs. For drones with failed electronics JTAG or chip off data extraction maybe the only option.

Log Structure

Some vendors provide flight log data on the drone in the form of CSV files. This is certainly the simplest source to work with but doesn't necessarily reflect the way that the systems actually record the data.

Two common flight controllers, PixHawk and DJI's family, write log messages from each subsystem as individual records as they come in so the structure is more similar to a network packet capture than an event log. Viewing this data as a table rather than as a series of distinct but related messages obscures valuable nuances in the data.

DJI complicates flight log analysis by encoding each record and by not publishing the file format. Vendors developing analytical tools are further challenged by the fact that the file, record, and field formats and names change depending on the model, firmware version, and other factors. A tool that supports a DJI Phantom 3 will not automatically support a Phantom 4. Support for a Mavic Pro running today's firmware will not necessarily fully support the next release of the firmware.

Onboard v Mobile Devices

As noted earlier, flight log data resides both on the drone and on the mobile device. The log files from vendor and third party applications are generally less of a moving target and are subject only to the access controls provided by the operating system.

Conclusion

The art and science of UAV forensics is at the point where mobile device forensics was ten years ago and will likely follow a similar trajectory with surges in understanding and capabilities offset by development of security controls that inhibit our ability to access and comprehend the data. Drones will never be as ubiquitous as mobile devices but they will certainly play crucial roles in our society. As drones continue to advance in capabilities and come into wider and wider use by both legitimate users and by malicious actors, it is essential that law enforcement, corrections, security and military professionals increase their levels of knowledge and preparedness regarding drone threats, including the art and science of drone forensics.
Missing Valuable Data

Many law enforcement agencies are currently failing to find and recover valuable evidence from drones.

Kovar & Associates purchased a DJI Mavic drone from a police auction site in the U.S. It arrived intact but with signs that someone had started to disassemble it but stopped. Continuing the process, we extracted an intact micro SD card and found over 30 flight logs on the card, valuable evidence of where and how it had been operated.

Many law enforcement agencies are not aware of the volume and value of data present on drones and on the supporting devices, so greater awareness is needed.

Widely used mobile forensic tools like XRY and Cellebrite now support drone forensics for many of the most popular models.

Internet of Things (IoT)

The Internet of Things (IoT) is the network of physical devices, vehicles, home appliances and other items embedded with electronics, software, sensors, actuators, and network connectivity which enables these objects to connect and exchange data. Each thing is uniquely identifiable through its embedded computing system but is able to inter-operate within the existing Internet infrastructure.

(Source: Wikipedia)

REFERENCES

2. http://missouridronelaw.blogspot.com/2013/05/if-drones-are-illegal-then-only.html

David Kovar is the CEO and founder of URSA, Inc. (Unmanned & Robotics Systems Analysis), which focuses on the collection, integration, analysis, and presentation of UAV-related data for fleet management, criminal investigations, failure analysis, and predictive analysis. He has worked in digital forensics and cyber security since the mid 1990’s and formerly led EY’s U.S. incident response program.

Joel Bollo is CEO of MSAB, a mobile forensic technology company. MSAB products are used by law enforcement, military, security and other government agencies in over 100 countries worldwide to investigate crime, gather intelligence, fight terrorism and support other missions.