JOHNS HOPKINS
WHITING SCHOOL OF ENGINEERING

Engineering
for Professionals

EXPERTISE APPLIED.

Defending Against Consumer Drone Privacy Attacks: A Blueprint for a Counter Autonomous Drone Tool

Lanier Watkins, PhD

Chair of Computer Science and Cybersecurity Programs

Engineering for Professionals

Johns Hopkins University

Whiting School of Engineering

Objective

- To perform an initial security assessment on the sensors, wireless network, and GPS of autonomous drones looking for "Hard-to-Patch" Vulnerabilities

- To use these "Hard-to-Patch" Vulnerabilities to design a novel Counter Autonomous Drone Tool

Motivation

Drone Industry Faces Issues On All Fronts

- Privacy
  - ➢ Drones can be used to spy on you and your family
- National Security
  - ➢ Drones can be used to kill
- Consumer Safety
  - ➢ Vendors do not sufficiently warn consumers of security risks

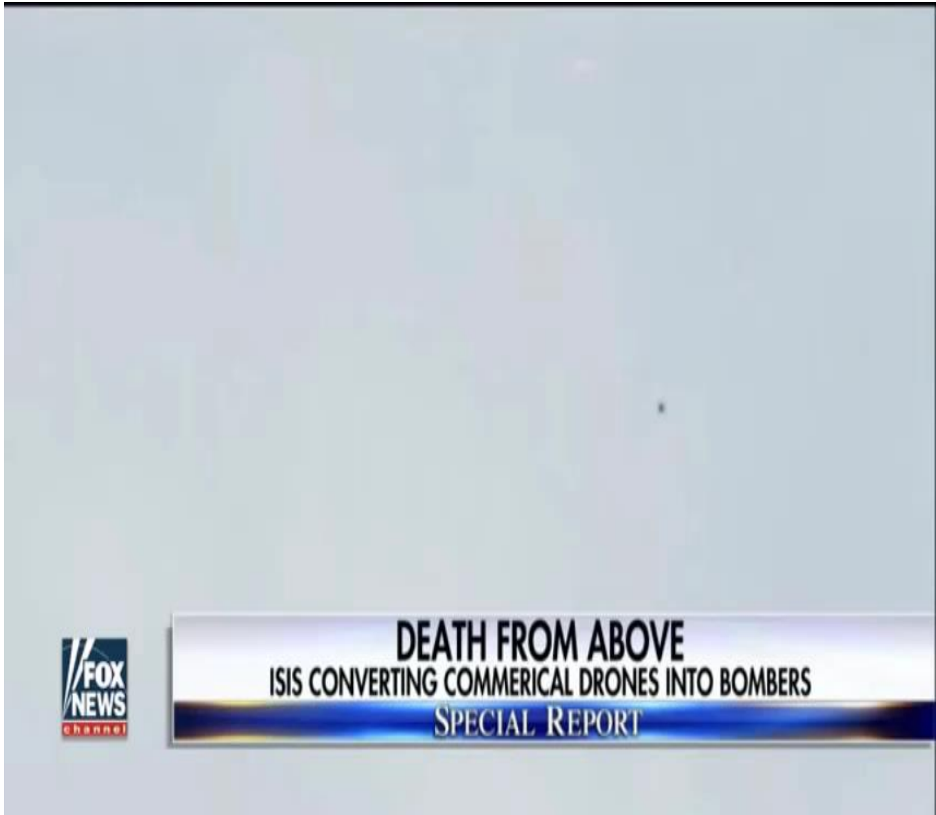
Agenda

- Introduction to the Rouge Drone Problem
- Notional Autonomous Drone
- Our Approach: Finding Hard-to-Patch Vulnerabilities
- Related Works
- Experimental Evaluation
- Results and Discussion
- Counter Autonomous Drone Tool Design
- Conclusion and Future Work

Introduction

Rouge Drone Problem (2015 – Present)

- Last past 5 years this problem has been exacerbating
  - ➢ Current issue, user controlled drones
  - ➢ Autonomous drones, future issue
  - ➢ Endangering critical infrastructure and private citizens
- Don’t take my word for it, let’s hear from government officials, journalist, and experts [1][2][3][4]



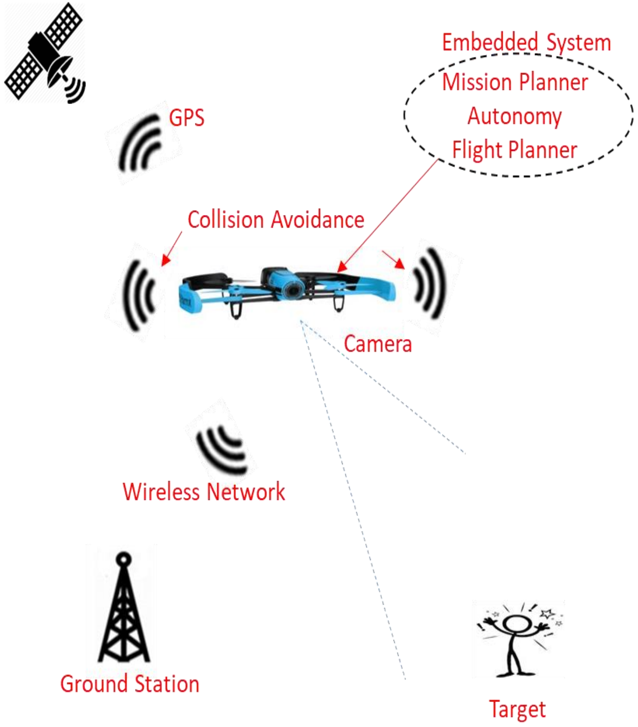
Notional Autonomous Drone

4 Levels of Autonomy [5]:

- Level 0: fully user controlled – manual
- Level 1: semi-autonomous (low) - user makes the rules, drone follows them
- Level 2: semi-autonomous (high) - drone makes its own rules, user approves them
- Level 3: fully autonomous - drone makes its own rules and executes them at will

Autonomous drones have embedded systems that can:

- Communicates with the drone's:
  - Wireless network
  - Rotors
  - Sensors (camera, collision avoidance, inertial unit)
- Execute code for:
  - Autonomy – manages systems in drone to achieve goals
  - Mission Planner - provides an overall goal for drone
  - Flight Planner – interfaces with GPS to produce coordinates



DJI Autonomous Drones

DJI Active Track [6]

- Level 1: semi-autonomous (low) - user makes the rules, drone follows them
  - Allows user to select a target to track and record
  - Using the camera and sensors, drone autonomously follows and records target while avoiding obstacles

DJI Spark Highlights [7]

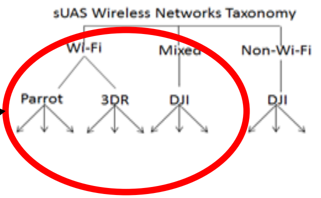
- User can connect using smartphone and DJI Go app over Wi-Fi
- Active Track
- Infrared collision avoidance
- Camera vision tracking
- GPS

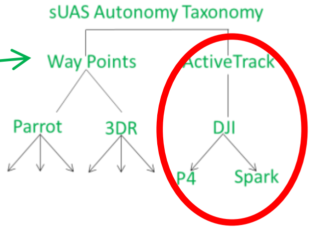
DJI Phantom 4 Highlights [8]

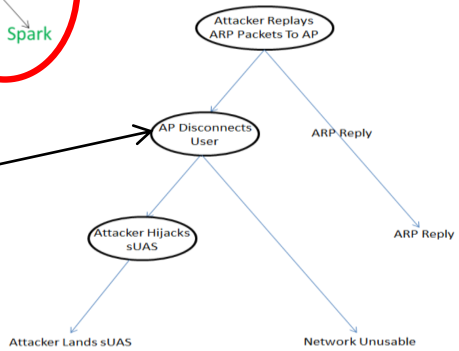
- User can connect using smartphone and DJI Go app over RF
- Active Track
- GPS
- Camera vision tracking and collision avoidance

Leverage Approach From Watkins et al.[9]

1. Develop UAS Security Focused Taxonomies
   - Our approach is to classify sUAS in terms of its main components (i.e., potential attack surfaces):
     1. wireless network
     2. embedded system
     3. GPS
     4. navigational system
     5. autonomy
   - Taxonomies facilitates penetration testing
2. Consider existing autonomous sUAS vulnerabilities
3. Perform zero-day penetration testing on multiple autonomous sUAS
4. Document successful exploit attack trees
5. Look across attack trees for multiple autonomous products
6. Build counter sUAS tool using *Hard-to-Patch* vulnerabilities
   - *Hard-to-Patch* vulnerabilities are likely cross vendor and based on financial infeasibilities (i.e., doesn't make financial sense to fix)







Related Work: User-Controlled Drone Security Assessments

- Watkins et al. [9]
  - ➢ Assessed the security of user-controlled drones by focusing on the major components
    - They broke COTS drones into 4 components:
      - wireless network
      - GPS
      - navigational system
      - embedded system.
    - They performed a security assessment of multi-vendor drones, found vulnerabilities, verified "Hard-to-Patch" with vendor, and weaponizied vulnerabilities to produce a counter drone tool.
  - ➢ Counter drone tool was based on Wi-Fi de-authentication and fingerprinting

Our approach is similar, but the distinction is that we:

- Look solely at autonomous drones
- Propose a design for a counter autonomous drone tool

	DJI Phantom 3 Response	Parrot Bebop II Response	3DR Solo Response
ARP Replay Attack*	Mobile Device Disconnect	Mobile Device Disconnect	Wi-Fi Controller Disconnect
MDNS Replay Attack	Not Vulnerable	Mobile Device Disconnect	Not Vulnerable
MAVLink Command Injection Attack	Not Vulnerable	Subverts Primary Controller	Subverts Wi-Fi Controller
Aircrack-ng Deauthentication Attack*	Mobile Device Disconnect	Mobile Device Disconnect	Wi-Fi Controller Disconnect
Bebop I Denial of Service Attack	Not Vulnerable	Not Vulnerable	Not Vulnerable
Bebop I Buffer Overflow Attack	Not Vulnerable	Not Vulnerable	Not Vulnerable
802.11 Protocol Stack Fingerprinting*	Uniquely identifies sUAS	Uniquely identifies sUAS	Uniquely identifies sUAS

***Hard-to-patch vulnerabilities (affect all top vendors) are highlighted in red**

Related Work: User-Controlled Drone Security Assessments

- Birnbach et al. [10]
  - ➢ Focused on privacy violation use cases
    - "Peeping Tom" drones
  - ➢ Counter drone solution born from analysis of commonality of popular drones
    - Counter drone tool was based on Wi-Fi detection and tracking

Our approach is similar, but the distinction is that we:

- Look solely at autonomous drones
- Propose a design for a counter autonomous drone tool

(a) Outside view (b) Inside view

Brand	Model	Video Downlink	Speed (m/s)
DJI[8]	Phantom 3 Standard	Wi-Fi (2.4 GHz)	16
	Phantom 3 Advanced/Pro	Lightbridge	16
	Phantom 4	Lightbridge	20
Parrot[9]	AR.Drone 2.0	Wi-Fi (2.4 GHz)	11.11
	Bebop	Wi-Fi (2.4, 5.8 GHz)	13
	Bebop 2	Wi-Fi (2.4, 5.8 GHz)	18
Protocol[10]	Dronium One WiFi Ed.	Wi-Fi (2.4 GHz)	N/A
Yuneec[11]	Typhoon H	Wi-Fi (5.8 GHz)	13.5
	Tornado H920	Wi-Fi (5.8 GHz)	11.11
3D Robotics[12]	Solo	Wi-Fi (2.4 GHz)	24.6
	IRIS+	Wi-Fi optional	22.7
	X8+	Wi-Fi optional	30

TABLE II: Features of popular drones with live-view video.

Related Work: Autonomous Drone Security Assessments

- Apvrille et al. [11]
  - ➢ Short paper proposes to use SysML-Sec environment via TTool:
    - to preserve security and privacy in autonomous drone embedded system design
    - for formal verification of design
- Demonstrates feasibility using autonomous Parrot drone

Our approach is similar, but the distinction is that we:

- Perform actual penetration testing on actual autonomous drones
  - ➢ Authors likely did not penetration test prototype

From: Ivan Djelic <ivan.djelic@parrot.com> Sent: Tue 3/28/2017 7:52 AM
To: Watkins, Lanier A.
Cc: jerome.bouvard@parrot.com
Subject: Re: Parrot Bebop 1 and Bebop 2

Dear M. Lanier,

Our drones have always been "open" products by default, lacking any security protection.
It is very easy to connect to a Bebop drone, open a telnet session with root permissions.
Our drones allow easy hacking and modification.
Regardless of the fact that this policy is questionable, it made a lot of vulnerability disclosures somewhat spurious, as we already knew that we offered no protection against unsophisticated, basic attacks.

Last year we introduced optional Wi-Fi WPA2 authentication, which helped cover of lot of vulnerabilities.
After this new feature was introduced, your students identified a vulnerability (october 24, 2016, deauthentication) which we were completely unaware of; it was indeed helpful, and helped us understand existing Wi-Fi vulnerabilities.
Thanks for your work, and responsible disclosure policies.

Best regards,
--
Ivan Djelic
Drone Software Manager
Parrot Drones

Experimental Setup

- **Autonomous Drones**
  - DJI Phantom 4
  - DJI Spark
- **Hardware**
  - Attack laptop
  - HackRF One
  - 1.5-foot Yagi 1.58GHz antenna
  - Smartphone
  - 1,220 Lux Multi-color LED Floodlight
  - 850 nm infrared spotlight
  - Indoor test facility
- **Software**
  - Kali Linux
  - Custom Python scripts








Experimental Procedure

- In our experimental procedure we:
  1. Performed remote security assessment on the sensors, wireless network, and GPS of each drone, looking for *Hard-to-Patch* vulnerabilities
  2. Developed exploits for each vulnerability found
  3. Communicated vulnerabilities to vendor and verified they would not patch vulnerabilities
  4. Designed a counter autonomous drone tool by using only *Hard-to-Patch* vulnerabilities

Normal DJI Active Track Behavior Experiment

TABLE I. NORMAL ATRAK FLIGHT PLAN DATA

OSD.ctrl Device	OSD.flight Action	OSD.fly cState	APP WARN
Onboard Device	None	NaviSubMode_Tracking	

- OSD.ctrl Device: Device Controlling Drone
- OSD.flight Action: Pre-programmed Flight Action
- OSD.fly cState: Current Flight Mode
- APP WARN: Current Warnings

Attacking Optical Sensor Experiment

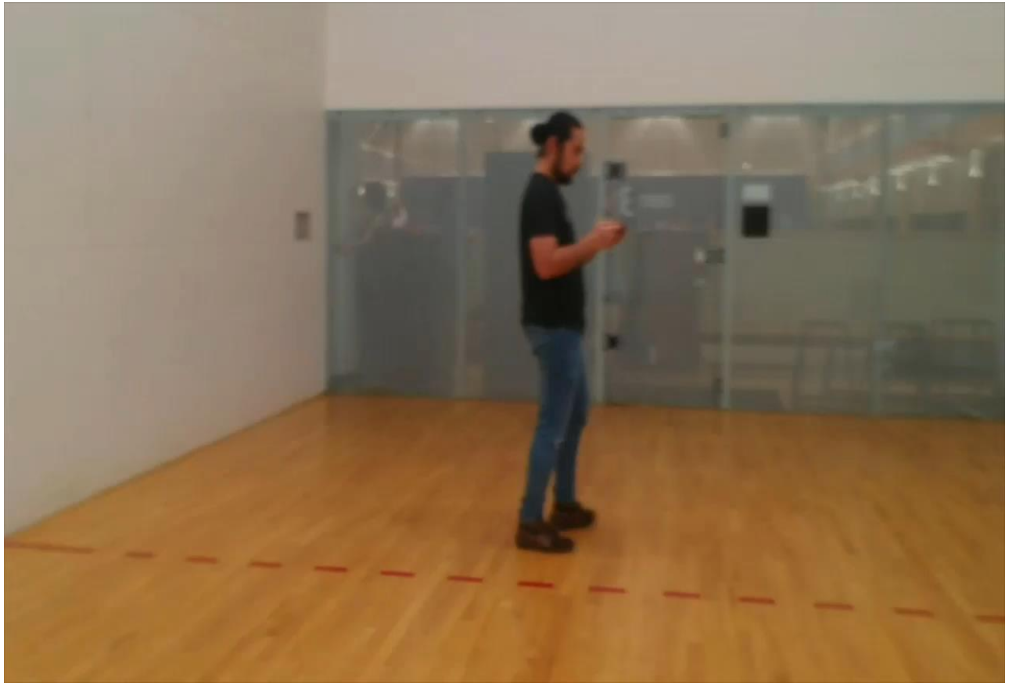


TABLE II. ATRAK BRIGHT LIGHT ATTACK FLIGHT PLAN DATA

OSD.ctrl Device	OSD.flight Action	OSD.fly cState	APP WARN
Onboard Device	None	NaviSubMode_Tracking	
RC	None	GPS_Atti	Subject Lost

Denotes abrupt change in control device

Attacking Collision Avoidance Sensor Experiment

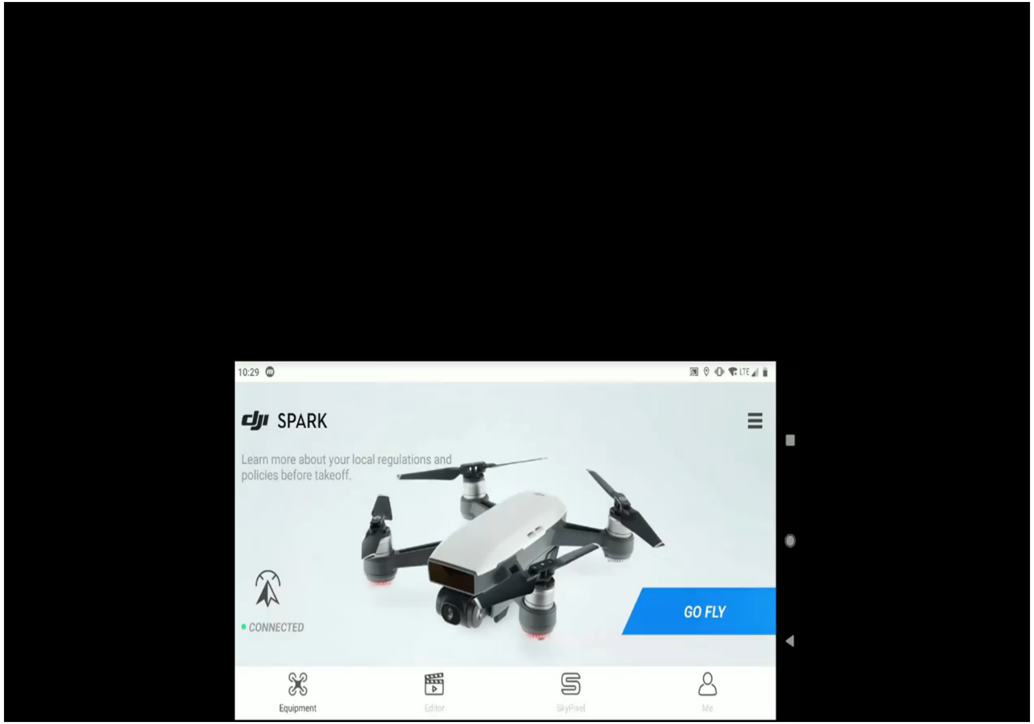


TABLE III. ATRAK INFRARED ATTACK FLIGHT PLAN DATA

OSD.ctrl Device	OSD.flight Action	OSD.fly cState	APP WARN
Onboard Device	None	NaviSubMode_Tracking	
RC	None	GPS_Atti	

Denotes abrupt change in control device

Attacking GPS Experiment

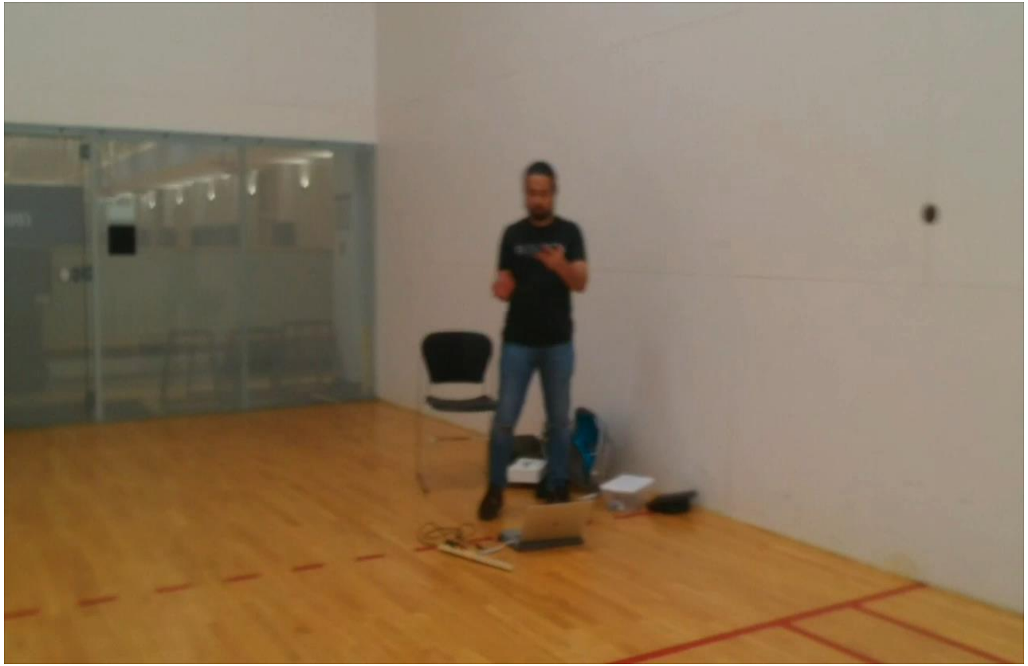


TABLE IV. ATRAK GPS ATTACK FIGHT PLAN DATA

OSD.ctrl Device	OSD.flight Action	OSD.fly cState	APP WARN
Onboard Device	None	NaviSubMode_Tracking	
RC	Airpt	AutoLanding	NoFly Zone

Drone forced out of autonomous mode

Attacking Wireless Network Experiment

TABLE V. ATRAK WIRELESS DEAUTH. ATTACK FLIGHT PLAN DATA

OSD.ctrl Device	OSD.flight Action	OSD.fly cState	APP WARN
Onboard Device	None	NaviSubMode_Tracking	
RC	GoHme	AutoLanding	

Drone forced out of autonomous mode

De-authenticating drone's controller breaks Active Track

Summary of Results

TABLE II. SUMMARY OF AUTONOMOUS DRONE VULNERABILITIES

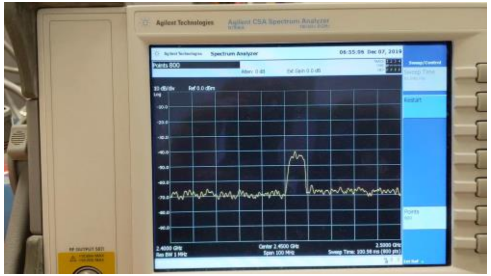
Drone	Component	Vulnerability	Range	Behavior
P4/Spark	Optical Sensor	1,220 Lux White Light	$\leq 3m*$	Breaks Autonomy Code and Hovers
P4/Spark	GPS	GPS Spoofing	$\leq 3m$@	Breaks Autonomy Code and Lands
Spark	Wireless Network	Wi-Fi Deauth.	$\leq 20m$	Break Autonomy Code and Lands
Spark	IR Sensor	850nm IR Light	$\leq 3m*$	Breaks Autonomy Code and Hovers

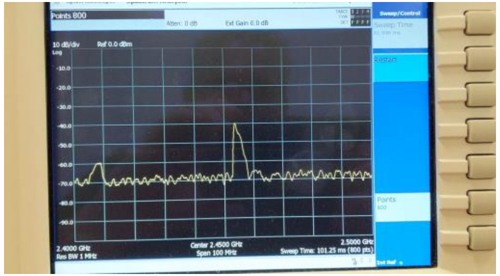
*Extended by increasing intensity
@Extended by using better antenna

Risks Associated With These Vulnerabilities

- The Bad
  - Consumer Safety
    - While in Active Track Mode, thieves could steal drone
- The Good
  - National Security & Citizen Privacy
    - Weaponized vulnerabilities could be used to neutralize threats

Counter Autonomous Drone Tool Design





Autonomous Drone Tool Design:

1. Detect autonomous drones using HackRF One
   - ➢ Major challenge
     - ➢ Discern between DJI drone and local networks Wi-Fi
       - ➢ Non-Wi-Fi DJI drones operate in 2.4GHz frequency band just like Wi-Fi drones

2. Mitigate autonomous drones using weaponized vulnerabilities

Future Work

- In future work, we plan to:
  1. Collaborate with RF Engineers to build Counter Autonomous Drone Tool
  2. Test and refine Counter Autonomous Drone Tool
  3. Work with DJI to reduce security risks for consumers

References

1. https://www.youtube.com/watch?v=SCJDlzayPMk
2. https://www.youtube.com/watch?v=BwjRY5oQtaA
3. https://www.youtube.com/watch?v=uh3jHa33kQY
4. https://www.youtube.com/watch?v=boPzM0YW53A
5. M. Ball, V. Callaghan, "Perceptions of Autonomy: A Survey of User Opinions towards Autonomy in Intelligent Environments", In IEEE International Conference on Intelligent Environments, 2011.
6. Developer.dji.com. (2018). Advanced Sensing - Object Detection Sample - DJI Onboard SDK Documentation. [online] Available at: https://developer.dji.com/onboard-sdk/documentation/sample-doc/advanced-sensing-object-detection.html.
7. Spark User Manual, Available: https://dl.djicdn.com/downloads/Spark/Spark%20User%20Manual%20V1.6-.pdf
8. Phantom 4 User Manual, Available: https://dl.djicdn.com/downloads/phantom_4/20170706/Phantom_4_User_Manual_v1.6.pdf
9. L. Watkins, J. Ramos, G. Snow, J. Vallejo, Wi.H. Robinson, A.D. Rubin, J. Ciocco, F. Jedrzejewski, J. Liu, and C. Li, "Exploiting Multi-Vendor Vulnerabilities as Back-Doors to Counter the Threat of Rogue Small Unmanned Aerial Systems," In ACM Proceedings of the MobiHoc Workshop on Mobile IoT Sensing, Security, and Privacy, June 26, 2018.
10. S. Birnbach, R. Baker, and I. Martinovic, "Wi-Fly?: Detecting Privacy Invasion Attacks by Consumer Drones," Network and Distributed System Security Symposium (NDSS), February, 2017.
11. L. Apvrille, Y. Roudier, T. Tanzi, "Autonomous drones for disasters management: Safety and security verifications", In URSI Atlantic Radio Science Conference, 2015.

Questions?

Lanier Watkins, PhD
JHU EP Program Chair, Computer Science and Cybersecurity
The Johns Hopkins University
Lanier.Watkins@jhuapl.edu
404-406-5426