Phantom Network Surveillance UAV / Drone

RICKY HILL

DEFCON 21

8/3/2013

About Me

- Security Consultant, D.C. Area
- Specialties: Wireless & SCADA Security
- US Govt. & Commercial
- Previous DEFCON Talks:

  WarRocketing & WarBallooning, (over Las Vegas ;-)
- Hobbies: R/C heli's, Deep Sea Fishing

What Talk is NOT About

- Having UR Dry Cleaning Delivered ->

NBC10.com

A Philadelphia dry cleaner is taking freshly laundered clothes to new heights by using a drone to deliver the cleaning to customers.

Outline

- Intro - Aerial Wireless Surveillance
- Past attempts: Balloons, Rockets, UAVForge
- New Technology: The Phantom Drone
- Building the Network Surveillance Drone
- Flights & Results
- Conclusion

What this is Really About

- Aerial, wireless (802.11) network surveillance

<u>Past Attempts:</u>

- DARPA - UAVForge, 2011
- Blackhat 2011: WASP spy drone

UAVForge “Perch and Stare”

- OK, so this hawk doesn’t have a Pineapple, but he’s definitely perfected the technique! ->

But I luv Heli's & Drones: Why did UAVForge fail?

- 143 teams from 153 countries competed -> **No One Won.**
- Factors:
  - Govt. required op's beyond LoS
  - Limited FPV capabilities
  - Ambitious, autonomous operations
  - Some highlights (uavforge.net)

UAVForge Crashes

Team GremLion (Baseline)

Team HALO (Baseline)

08:21 - Start setup; team intends to conduct full baseline scenario

08:25 - Airborne

08:27 - UAV departs controlled flight; UAV down east of the road in the trees

08:36 - Vehicle recovered with extensive damage

09:02 - Cease operations

Meet “THE” DJI Phantom

- DJI Innovations introduced the Phantom JAN 2013
- It quickly gained a reputation for being the most stable drone platform in the air today
- Features:
  - GPS
  - Auto “Return to Home”
  - Payload: up to 400 grams
  - $679. UAVForge Dones: $2K-9K

What's New since 2011?

- Technology has improved dramatically:
- Tiny computers: Cotton Candy (30 gr.)
- CC: Bluetooth, HDMI, 802.11 capable
- Wifi Pineapple: remote 3G, 4G
- DJI Phantom = the first "consumer quality" drone that is easily flyable by the average person.

TechnoLust Overcomes Me: Let's build this!

- Designed & Built 2 payloads:
- Cotton Candy + WiSpy or KillerBee
- Flying Pineapple = Hak5 Pineapple + GSM 3G/4G

Site Survey Payload

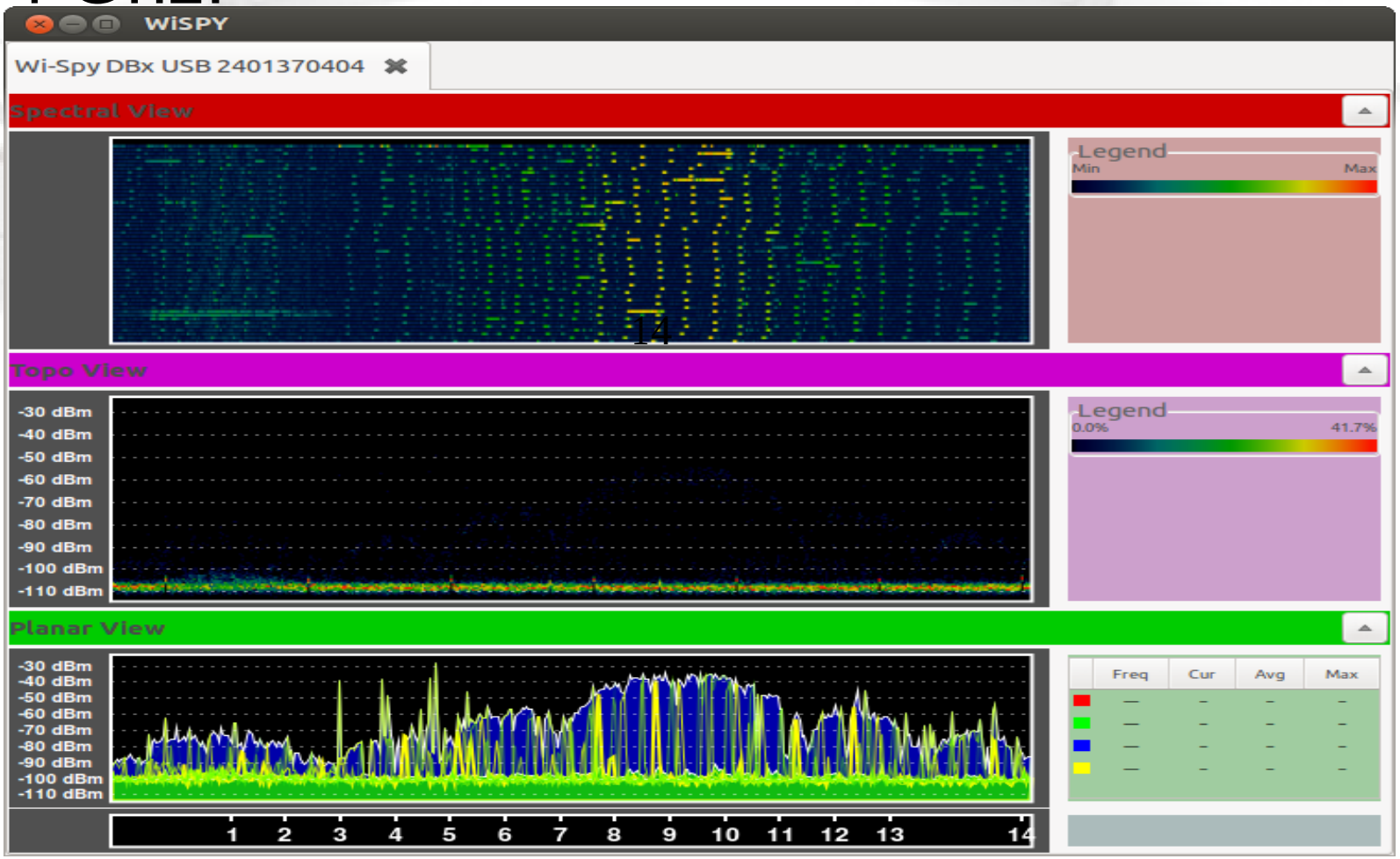
- Cotton Candy makes a perfect headless computer
- Apple Bluetooth KB & Mouse “detach” instantly
- ARM processor runs Ubuntu or Android O/S
- 1.2 GHz ARM Cortex-A9 CPU, 1GB of RAM, image on microSD
- Wireless Tools: Kismet, Wispy (spectools) available, or pretty much any USB device, even Killerbee for ZIGBEE

WiSpy Flight Results

- VA Waterfront Neighborhood:

WiSpy Flight Results

- 2.4 Ghz:

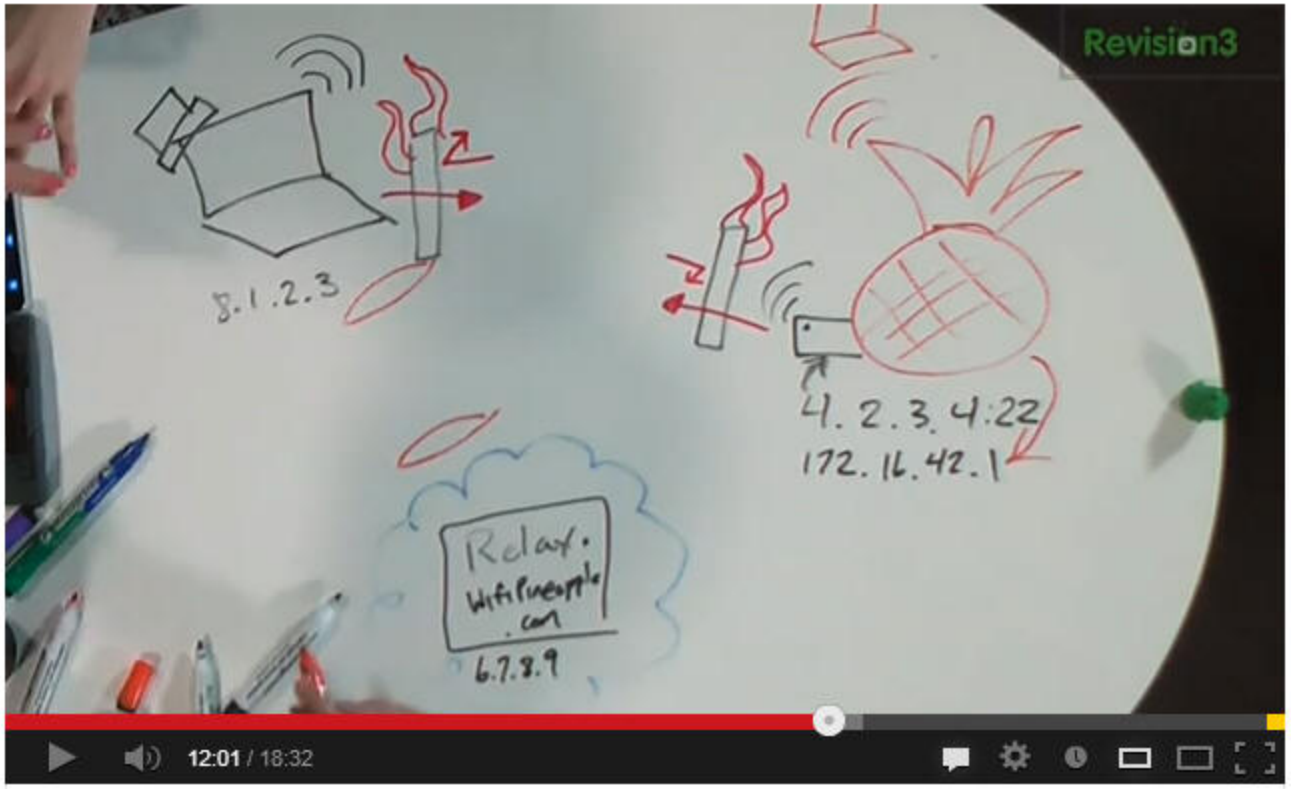


We found 802.11 sources – What's next?

- The "Flying Pineapple":
- Tools: Airodump, sslstrip, site survey, et. al.
- Payload Objectives:
  - [1] Land on any unique Vantage Point: Buildings, Towers, Balconies, etc. "Perch"…
  - [2] Conduct Op's
  - [3] Return Phantom safely to Starting Point

Network Diagram

- Reverse ssh tunnel -> Hawaii Relay Server



Hak5 Video
Episode 1112

Pineapple Offensive Ops

- Selected Pineapple Capabilities:
  - OpenWRT running Jasager – >“the yes man”
  - URL Snarf
  - DNS Spoofing
  - New http landing page for phishing, etc.
- airodump-ng runs great in-flight!
  - cd /usb/airodump-ng-logs
  - airomon-ng start wlan0 (monitor mode)
  - airodump-ng -w pcap mon0

Flight2: Airmon-NG

- Public Beach Flyover:
- AIRMON-NG
- In-Flight Monitor Mode
- NO! We are not looking for Bikini's…
- How many people using wireless here?
- Flight video & pcap

“Oh NO!!!” Moments

- All was not perfect with our Phantom Adventures…
- A couple Incidents you may find amusing->
- Video

Crash: Phantom v2

Flight3: Rooftop Landing

- Large Party Platform overlooking recreation area @ the Lake:
- AIRMON-NG
- Site Survey
- UrlSnarf
- Great Vantage Point! (Video)

Flight3: Results

- sslstrip->

```
2013-07-22 22:05:52,363 SECURE POST Data (login.medscape.com):
guid=&userId=rickhill&password=scirocco&Log+In=Log+In
2013-07-22 22:05:55,509 POST Data (g63.p4.webrootcloudav.com):
TV=1&TT=UBC&SV=134218395&InstanceMID=2b365aba9a35a73a62d764b067e90bd957fa
68fd78ca2e109ff186fe46158f0d&HEADERS=$$$01$$$CDB5FF1AVMOIHNQSPOTLRJSINVPU
UMGHRSOSIQOOKUPHKHONPIMKSQVTVOHVKHGLQINTPVVPSVMGTKVNNUQPKQPPPTMRHONMSUKUH
NSRTGKJMSILOPOHMUIPGGHKUTOMMVJRPHGLGHRLKPHGUTQRPUNJUQMRVHPVNPHJMKUHMTTJHU
LNOTVUSPPVNKLVJVGKUNKHSLJVOGJOPURLKUVSORPKUUHLIURPJTMQRUGKMORMIHGONKQGLKN
```

- urlsnarf->

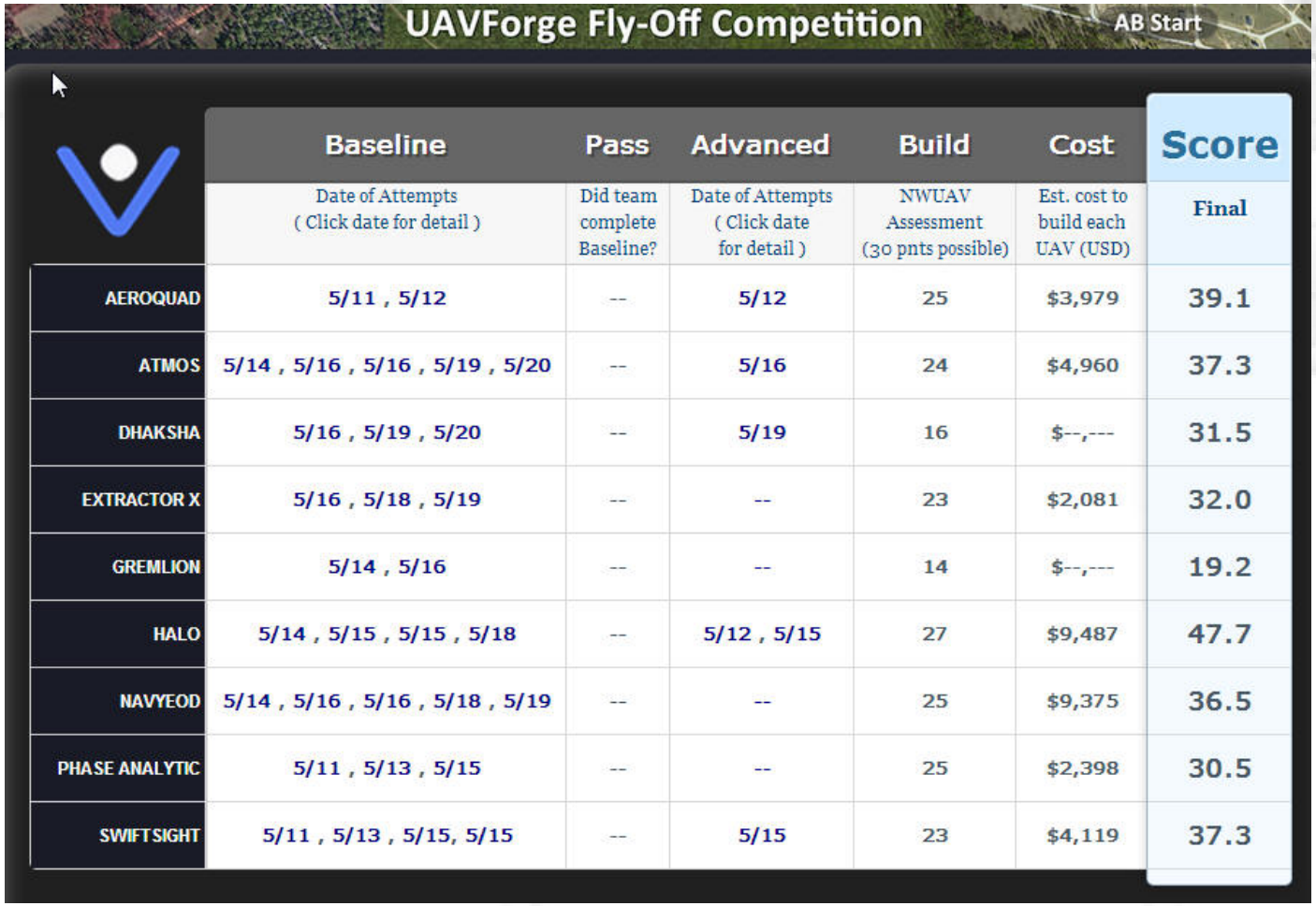
```
"http://www.spokeo.com/" "Mozilla/5.0 (Windows NT 6.1; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.72 Safari/537.36"
Owner-VAIO.lan - - [22/Jul/2013:21:03:14 -0400] "GET
http://dr9idja2ykfn5.cloudfront.net/assets/application-
0008011ffee2eb38a784aec9392414d7.js HTTP/1.1" - -
"http://www.spokeo.com/" "Mozilla/5.0 (Windows NT 6.1; WOW64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/28.0.1500.72 Safari/537.36"
Owner-VAIO.lan - - [22/Jul/2013:21:03:14 -0400] "GET
http://dr9idja2ykfn5.cloudfront.net/assets/scriptaculous/effects-
bef7d8d39630e13f4298a680b9dcd6b0.js HTTP/1.1" - -
```

How did we compare to UAVForge Team Scores?

	Baseline Objectives	Points
1.	Conduct operations, preflight, and safety checks	(5 pts)
2.	Perform vertical take-off and flight within specified altitude	(5 pts)
3.	Orient heading and fly to observation area	(5 pts)
4.	Transition from flight mode to surveillance mode and conduct observations for the time specified	(5 pts)
5.	Complete observations and transition from surveillance mode to flight mode while maneuvering around obstacles	(5 pts)
6.	Exit observation area, transition to specified altitude and land back at home base at the Flight Preparations area	(5 pts)

	Advanced Behaviors	Points
1.	Demonstrate safety in flight during a "communications out" condition.	(5 pts)
2.	Demonstrate an autonomous transition from flight mode to observation mode for surveillance and then transition back from observation mode to forward flight	(25 pts)
3.	Demonstrate a simple user interface and vehicle controls which exhibits ease of vehicle operations with minimal pilot workload	(25 pts)
4.	Mitigate the vehicle's acoustics signature level in flight and transition to observation mode	(25 pts)
5.	Demonstrate an integrated obstacle avoidance capability	(15 pts)

How did we compare to UAVForge Team Scores?



UAVForge Fly-Off Competition

AB Start

	Baseline	Pass	Advanced	Build	Cost	Score
	Date of Attempts (Click date for detail)	Did team complete Baseline?	Date of Attempts (Click date for detail)	NWUAV Assessment (30 pnts possible)	Est. cost to build each UAV (USD)	Final
AEROQUAD	5/11 , 5/12	--	5/12	25	$3,979	39.1
ATMOS	5/14 , 5/16 , 5/16 , 5/19 , 5/20	--	5/16	24	$4,960	37.3
DHAKSHA	5/16 , 5/19 , 5/20	--	5/19	16	$--,---	31.5
EXTRACTOR X	5/16 , 5/18 , 5/19	--	--	23	$2,081	32.0
GREMLION	5/14 , 5/16	--	--	14	$--,---	19.2
HALO	5/14 , 5/15 , 5/15 , 5/18	--	5/12 , 5/15	27	$9,487	47.7
NAVYEOD	5/14 , 5/16 , 5/16 , 5/18 , 5/19	--	--	25	$9,375	36.5
PHASE ANALYTIC	5/11 , 5/13 , 5/15	--	--	25	$2,398	30.5
SWIFTSIGHT	5/11 , 5/13 , 5/15, 5/15	--	5/15	23	$4,119	37.3

Phantom = 35
5 th place

Conclusion / Future Work

- Phantom Network Surveillance Drone:
- Successful proof of concept of “Perch, Listen, and Engage” wireless network surveillance
- Highly effective site survey tool

Next Time

- Next DARPA Challenge:
  - Full FPV for non-LoS operations
  - Autonomous operation with waypoints, (Naza-M available now.)
  - Descent rate instruments for precision landing
  - Extend 4 Hr. surveillance capability with better power design... Multiple building operations become possible.

Legal & Safety Issues

- Do NOT attempt to fly a quadcopter as large and expensive as the Phantom without experience! (I highly recommend joining an R/C club or getting a mentor). Start small: the Blade MQX quadcopter is ideal…
- Under current FAA rules flying beyond LOS or above 400 ft. AGL is Illegal
- **Under no circumstances fly within 5 miles of any airport.**
- Do NOT violate people's privacy with cameras or other devices.

How High is 400 ft?

- www.apogeerockets.com $49

Shout Outs

Thanks To->

- Tenacity Alpha Ops Team - Flight Support
- Nick Hopler: Heli' Op's & Video Production
- Hobby Hangar, Chantilly, VA

Checked your Roof Lately?

Questions?

Bibliography

- DARPA UAVForge project site: http://www.uavforge.net/
- DJI Innovations, Inc. Phantom: http://www.dji-innovations.com/product/phantom/
- Cotton Candy Computer: http://www.fxitech.com/cotton-candy/what-is-it/
- WiFi Pineapple (Hak5): “The Hot-Spot Honeypot Pen-Testing Platform”: http://wifipineapple.com/
- Congressional Research Service, “Integration of Drones into Domestic Airspace: Selected Legal Issues”, Dolan and Thompson, April 4, 2013

Site Survey Payload

Site Survey Payload - Hardware

- Cotton Candy: www.store.cstick.com
- Apple Bluetooth Wireless Keyboard, A1314
- HP Bluetooth Touch to Pair Mouse, #H4R81AA#ABA
- Wi-Spy Spectrum Analysers, 900 Mhz, 2.4, 5 Ghz www.metageek.net
- Eflite 1S, 3.7v Battery redrockethobbies.com
- Protek 2A USB Adapter: http://www.bigsquidrc.com

Site Survey Payload - Software

- WiSpy: install spectools->
  - http://www.kismetwireless.net/spectools/
- Cotton Candy – attach bluetooth KB & mouse:
  - hcitool scan (finds bluetooth addresses)
  - sudo apt-get install bluez-compat
  - sudo hidd-connect <address>

Killerbee Zigbee Payload

- Hardware: Amtel ATA-RZusbstick with firmware flash for Killerbee, (Joshua Wright)
- Cotton Candy HW Config, (same as Wi-Spy)
- Software:
  - https://code.google.com/p/killerbee
  - apt-get install python-gtk2 python-cairo python-usb python-crypto
  - cd /killerbee
  - python setup.py install
  - zbstumbler, zbfind, etc.

Pineapple Payload

Pineapple Payload - Hardware

- WiFi Pineapple Mark IV
  http://hakshop.myshopify.com
- Protek 2A USB Adapter:
  http://www.bigsquidrc.com
- Eflite 2S, 1300 mAh, 7.4 v battery
  redrockethobbies.com
- T-Mobile ZTE MF591 Rocket 3G 4G
  http://t-mobile.com

Pineapple Payload - Software

- Enabling T-Mobile USB Mass Storage & Swap Space:
  - https://forums.hak5.org/index.php?/topic/25882-how-to-enable-usb-mass-storage-with-swap-partition/
- Note: U must mount storage and swap via UUID's!
  - sudo BLKID
  - Enter uuid in fstab

Pineapple – Internet Relay

- Persistent ssh, Hak5 episode 1112-> http://hak5.org/episodes/hak5-1112
- Relay Server Provider: digitalocean.com
- Software:
  - cd /etc/ssh (on relay)
  - nano sshd_config
  - AllowTcpForwarding “yes”
  - GatewayPorts “yes”

FPV Parts List

- First Person View (FPV) Hardware:
  - Mini FPV Camera with 5.8Ghz TX Combo, http://www.unmannedtechshop.co.uk/fpv-gear/5-8ghz-tx-rx/mini-fpv-camera-with-5-8ghz-tx-combo.html
  - Foxtech RC-305 Receiver foxtechfpv.com

Phantom Drone Adds / Improvements

- High Performance Props
  - Graupner E-Prop 9x5 (2x CW, 2x CCW) team-blacksheep.com
- Extended Landing Gear
  - PhantoMounts Carbon Fiber Landing Gear rcdude.com
- Battery Tray
  - PhantoMounts Wide CF Battery Tray rc-drones.com