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. and Commercial Engagements
- Previous DEFCON talks: WarRocketing & WarBallooning, (over Las Vegas ;-)
- Hobbies: R/C heli's, Deep Sea Fishing

Outline

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

What's this About?

- Aerial visual and wireless (802.11) surveillance
- Challenge: Personal previous attempts to capture and, more importantly to engage wireless targets from aerial platforms have been problematic:
- WarRocketing– limited air time, Warballooning– limited directional control, weak signals
- Others:
  - Blackhat 2011, Tassey & Perkins - WASP wireless spy drone
  - UAVForge, 2011 - Covert visual surveillance, No Winner

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

- Factors:
- Govt. required Heli operations be conducted beyond line of sight (LoS)
- Limited First Person View (FPV) R/C techniques
- Autonomous drone operation required, (including obstacle avoidance)
- Landings Problematic: Many Crashes – Teams needed better descent & flight attitude indicators

UAVForge – Flight Problems

Friday May 18, 2012

HALO, Extractor X, and Navy EOD attempt the baseline objectives. Rain prevents DHAKSHA from attempting baseline objectives.

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

Judges Scorecard

Evaluator	1	2	3	4	5	Average
Obj. 1	5	---	---	---	---	5.0
Obj. 2	5	---	---	---	---	5.0
Obj. 3	1	---	---	---	---	1.0
Obj. 4	0	---	---	---	---	0.0
Obj. 5	0	---	---	---	---	0.0
Obj. 6	0	---	---	---	---	0.0
Total	11	---	---	---	---	11.0

Notes: For this attempt the team employs a directional antenna suspended approximately 75 feet above the ground in a tree. UAV demonstrates erratic behavior during transition to forward flight, cause of failure is unknown.

UAVForge – Another Flight

Team Extractor X (Baseline)

07:27 - Start setup; team intends to conduct full baseline scenario
08:22 - Hover check; team suspends operations to replace failed servo
09:35 - Hover check
10:00 - Airborne; transition to forward flight
10:04 - Past the ROC at high altitude struggling under gusty winds
10:05 - UAV down in trees east of the road between the COW and MOUT
12:07 - UAV located in the trees about 75 feet above the ground; cease operations (UAV recovered by local tree service on May 20th)

Judges Scorecard

Evaluator	1	2	3	4	5	Average
Obj. 1	3	---	---	---	---	3.0
Obj. 2	3	---	---	---	---	3.0
Obj. 3	3	---	---	---	---	3.0
Obj. 4	0	---	---	---	---	0.0
Obj. 5	0	---	---	---	---	0.0
Obj. 6	0	---	---	---	---	0.0
Total	9	---	---	---	---	9.0

Notes: Operator recovers UAV from multiple departures from controlled flight where vehicle performs uncommanded 360 rolls about the longitudinal axis (aileron rolls). After the last departure the pilot is unable to recover the vehicle

What's New Since 2011?

- Technology has improved dramatically:
- Computers super tiny: Cotton Candy (30 grams)
- CC is Bluetooth, HDMI, and 802.11 capable
- Wifi Pineapple (Hak5): small + remotely assessable via 3G, 4G
- DJI Phantom = the first "consumer quality" drone that is easily flyable by the average person.

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-Pilot
  - Auto “Return to Home”
  - High payload capability: up to 400 grams
  - Relatively Inexpensive: $679. UAVForge Dones: $2K-9K

TechnoLust Overcomes Me: Let's build this!

- I envision 3 uses for Phantom Network Surveillance:

- Site Survey – large area / short time
- Observation and Communications Capture Platform for incidents such as the recent Boston Marathon Bombing
- Covert missions using the "Perch, Listen & Engage" technique from Rooftops or other normally inaccessible locations

TechnoLust …

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

Site Survey Payload

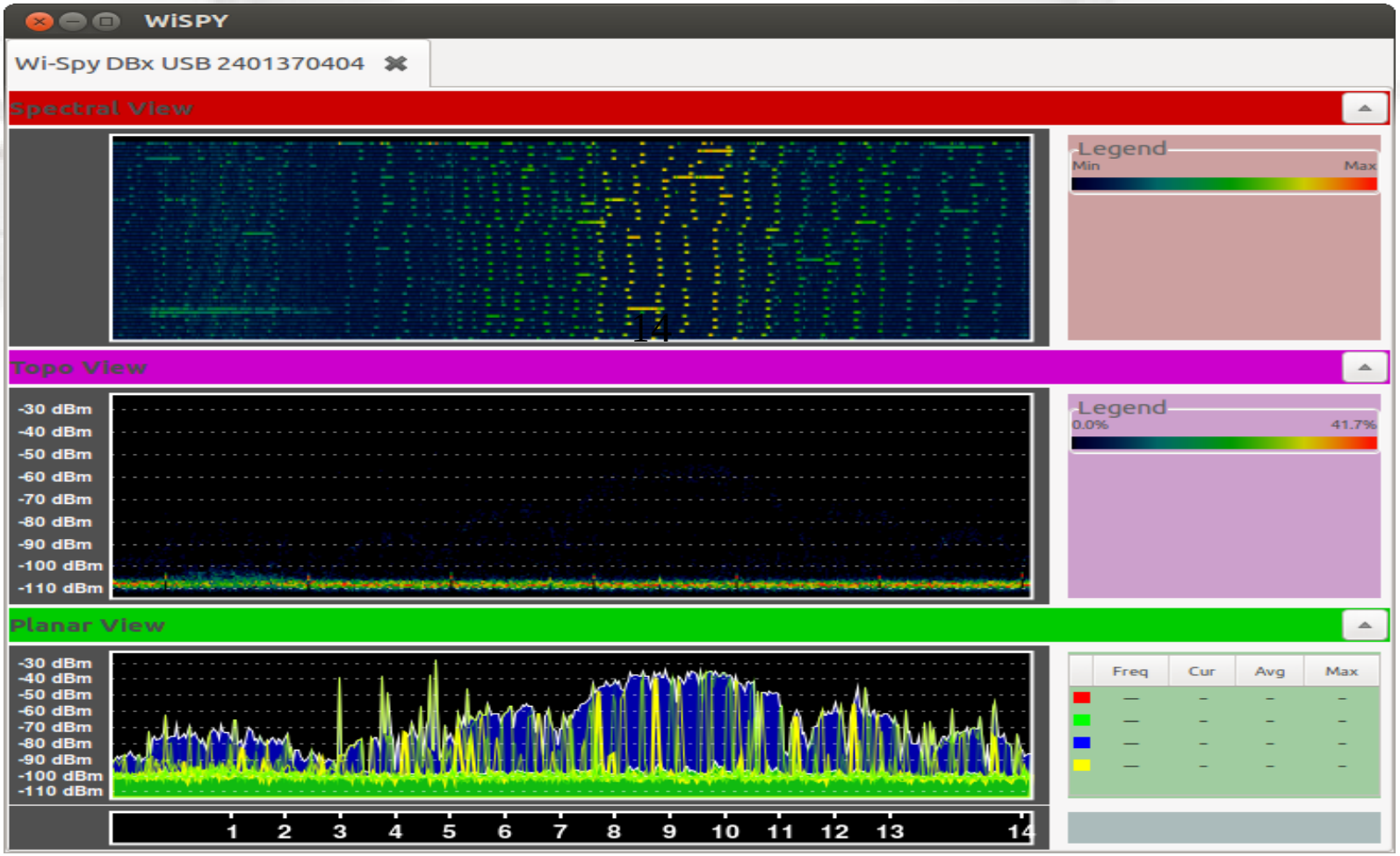
- Design Considerations:
- Cotton Candy makes a perfect headless computer
- Apple Bluetooth KB & Mouse “detach” instantly
- ARM processor runs Ubuntu or Android O/S
- 1.2 GHz ARM Cortex-A9 CPU, 1GB of RAM, image on microSD
- Wireless Tools: Kismet, Wispy (spectools) available, or pretty much any USB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

WiSpy Flight Results

- Lake Neighborhood: (more flights in Progress)

WiSpy Flight Results

- 2.4 Ghz:



We found 802.11 sources – What's next?

- The Flying Pineapple: Tools –> Airodump, sslstrip, site survey, etc.
- Payload Objectives:
  - [1] Land on a residential or commercial building, "Perch"
  - [2] Conduct Op's
  - [3] Return Phantom + payload safely to starting point

- "Perch, Listen, and Engage" predictably will become an important technique as in the words of DARPA:

  "The primary (perching) benefit is to increase (surveillance) persistence by reducing mission power demands while providing stable sensor emplacement."

Pineapple Remote Operation

- Remote admin. & monitoring via 3G or 4G (a sweet pen-testing drop box)
- Utilizes a relay server, ssh proxy (Hawaii)
- Autossh keeps the tunnel alive to the Pineapple (Hak5 episode 1112)
- Operations team shells into the Drone & utilizes command prompt or GUI. 1200 mAh LiPo life ~=2-3 hours with the T-Mobile Rocket ZTE-MF592 (GSM)
- CDMA devices consume 2x power! (not recommended)

Pineapple Offensive Ops

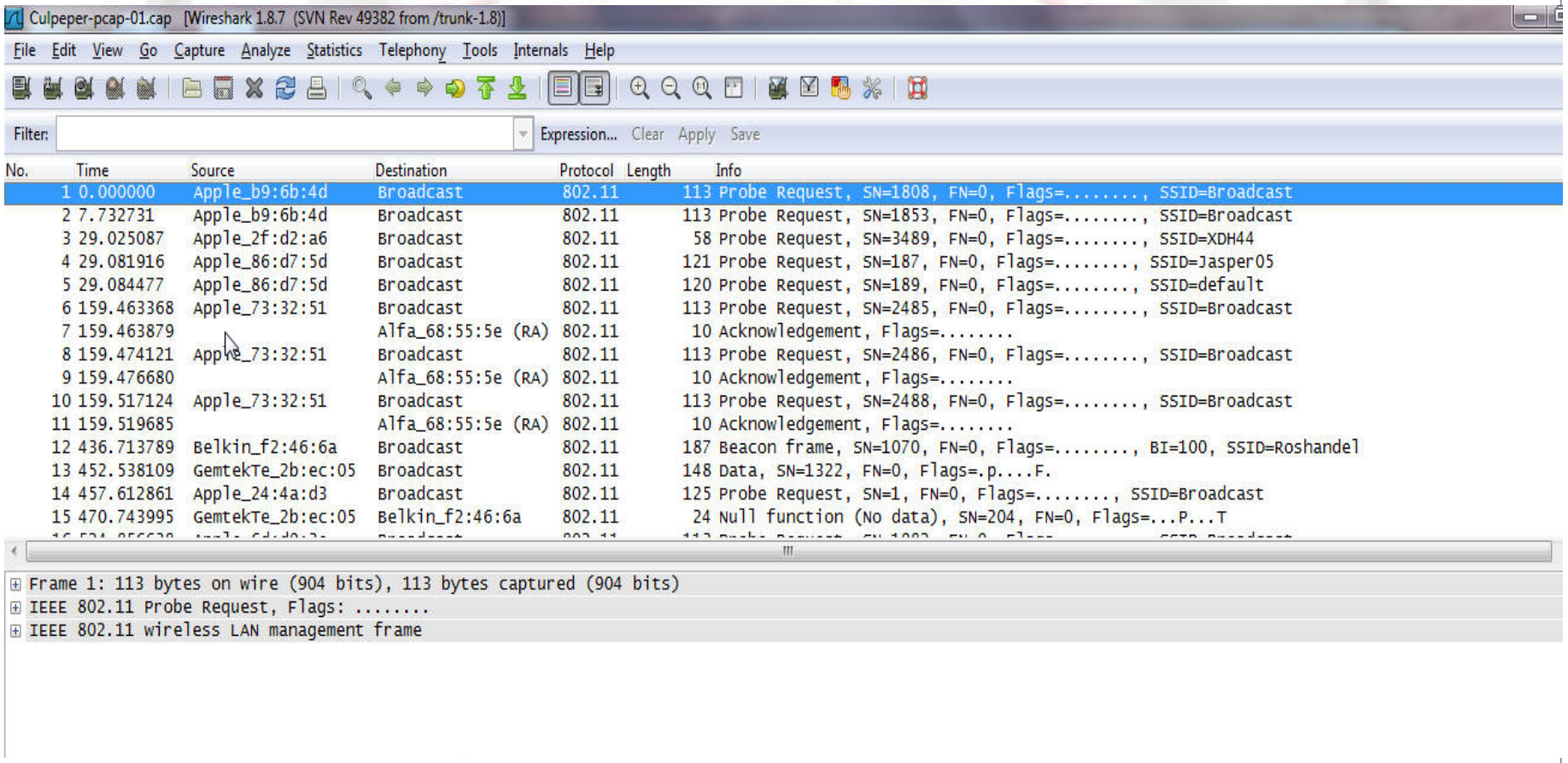
- Selected Pineapple Capabilities:
  - OpenWRT running Jasager – >“the yes man”
  - URL Snarf
  - DNS Spoofing
  - New http landing page for phishing, etc.
- **airodump-ng runs great in-flight!**
  - cd /usb/airodump-ng-logs
  - airomon-ng start wlan0 (monitor mode)
  - airodump-ng -w pcap mon0
- Demo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

Network Diagram

- Placeholder: Reverse ssh with Hawaii relay diagram shown here.
- **Update will be posted to DEFCON site.**

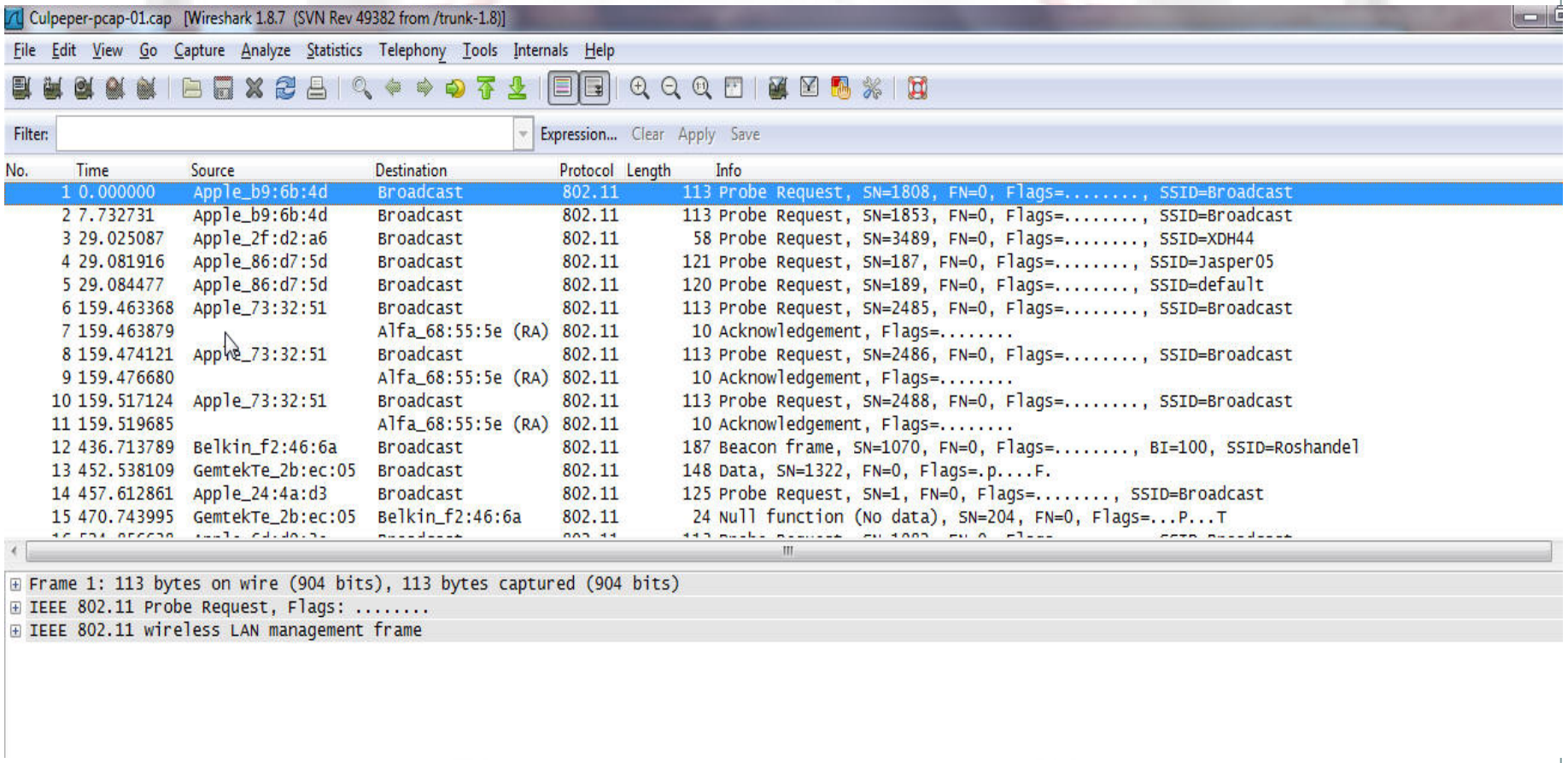
Pineapple Flight Results

- Airodump-NG:



Pineapple Flight Result2

- Airodump-NG:



Flight Video

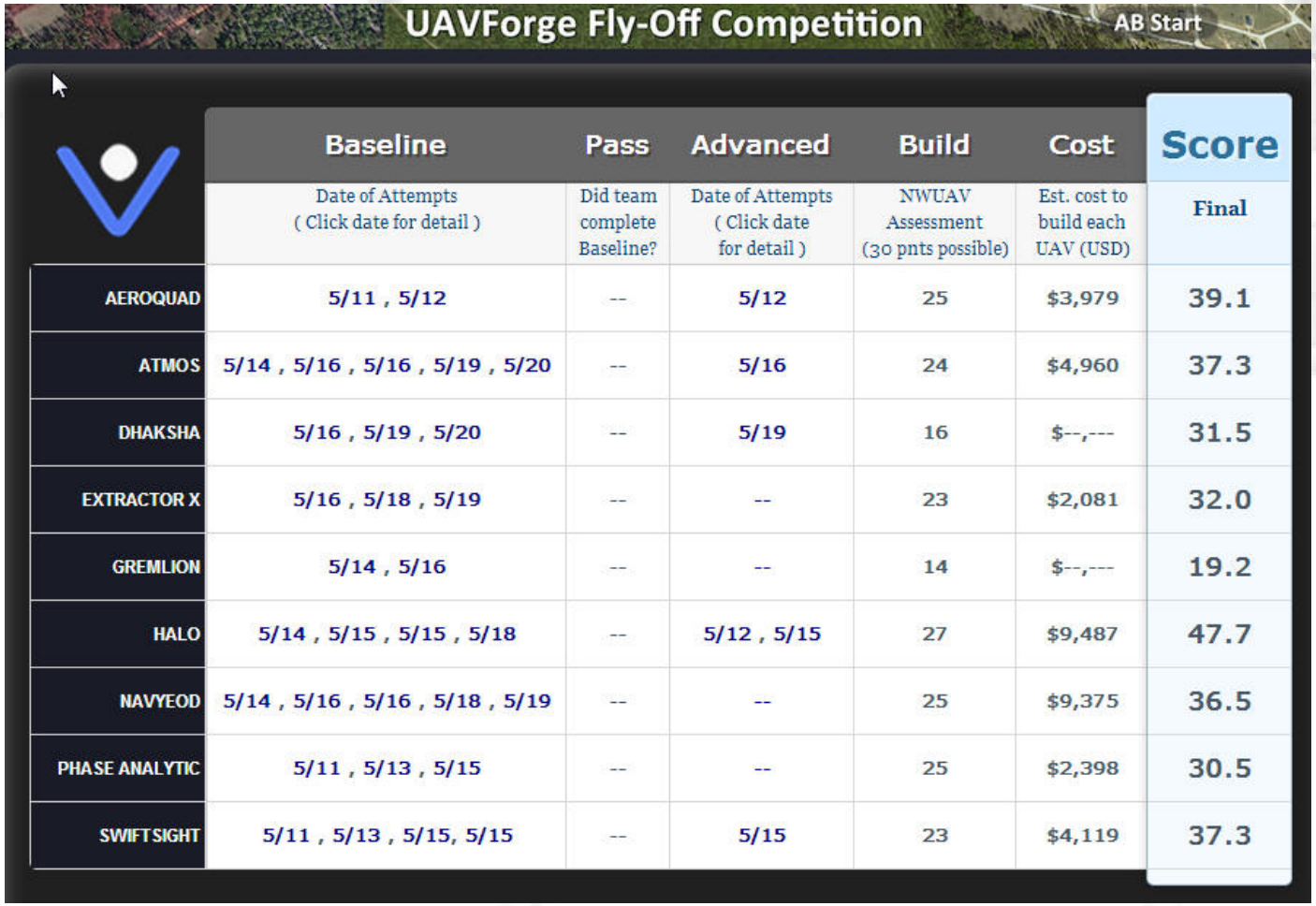
- This slide is a placeholder:
- **Show Phantom Mission Flight Videos here (5 min. MAX)**
- **No text: all live flights from July 2013**
- **Updates will be posted to DEFCON site.**

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

Conclusion / Future Work

- Phantom Network Surveillance Drone: successful proof of concept demonstration for “Perch, Listen, and Engage” wireless network surveillance.
- Next DARPA Challenge:
  - Full FPV for non-LoS operations
  - Autonomous operation with waypoints, (Naza-M available now.)
  - Descent rate instruments for precision landing
  - Extend 3 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 3 miles of any airport.**
- Do NOT violate people's privacy with cameras or other devices.

Legal & Safety Issues…

- Respect property rights: If your helicopter, drone, or other expensive equipment comes down on someone else's property (house, roof or land):
  - Probable Case – you may Never get it back,
  - Worst Case – you may be arrested for Trespassing
- In no way endanger people on the ground – this means flying away from other people and making sure everyone around you is aware of the aerial operation.
- For more info. on pending Legislation & Legal Issues, (see bibliography)

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

Questions?