Phantom Network Surveillance
UAV / Drone
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 ->

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

Past Attempts:
- DARPA - UAVForge, 2011
- Blackhat 2011: WASP spy drone
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)
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 Drones: $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
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->

  guid=&userId=rickhill&password=sciocco&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=RSS$01$$CDB5FF1AVMOIHQSPOTLRSINVP
  UMGHRSOSIQOKUPHKHONPIMKSVQTVOHVKHGLQINTPVPSVMGTVKVNNUQPKQPPTPMRHONMSUKUH
  NSRTGKJMSILPOHMUIPGGHKUTOMMVJRPGLHCLRKLKHGUTQRPUNJQMRVHPVNHJMKUHTTJHU
  LNOTVUSPPVNLTVJVGKUNKHLJVOGJOPURLKUVDOPKUUHLIURPJTMQRUGKMORMIHGONKQGLKN

- 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.1an -- [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.1an -- [22/Jul/2013:21:03:14 -0400] "GET
http://dr9idja2ykfn5.cloudfront.net/assets/scriptaculous/effects-
bebf7d8d39630e13f4298a680b9dcd6b0.js HTTP/1.1" --
How did we compare to UAVForge Team Scores?

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

<table>
<thead>
<tr>
<th>Advanced Behaviors</th>
<th>Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Demonstrate safety in flight during a “communications out” condition.</td>
<td>(5 pts)</td>
</tr>
<tr>
<td>2. Demonstrate an autonomous transition from flight mode to observation mode for surveillance and then transition back from observation mode to forward flight</td>
<td>(25 pts)</td>
</tr>
<tr>
<td>3. Demonstrate a simple user interface and vehicle controls which exhibits ease of vehicle operations with minimal pilot workload</td>
<td>(25 pts)</td>
</tr>
<tr>
<td>4. Mitigate the vehicle’s acoustics signature level in flight and transition to observation mode</td>
<td>(25 pts)</td>
</tr>
<tr>
<td>5. Demonstrate an integrated obstacle avoidance capability</td>
<td>(15 pts)</td>
</tr>
</tbody>
</table>
How did we compare to UAVForge Team Scores?

### UAVForge Fly-Off Competition

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

Phantom = 35
5th 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 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?

[Image of Altimeter One]

- 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/
- Cotton Candy Computer: http://www.fxitech.com/cotton-candy/what-is-it/
Site Survey Payload
Site Survey Payload - Hardware

- Cotton Candy: [www.store.cstick.com](http://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](http://www.metageek.net)
- Eflite 1S, 3.7v Battery [redrockethobbies.com](http://redrockethobbies.com)
- Protek 2A USB Adapter: [http://www.bigsquidrc.com](http://www.bigsquidrc.com)
Site Survey Payload - Software

- **WiSpy**: install spectools->
  - [http://www.kismetwireless.net/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](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](http://hakshop.myshopify.com)
- Protek 2A USB Adapter:
  [http://www.bigsquidrc.com](http://www.bigsquidrc.com)
- Eflite 2S, 1300 mAh, 7.4 v battery
  [redrockethobbies.com](http://redrockethobbies.com)
- T-Mobile ZTE MF591 Rocket 3G 4G
  [http://t-mobile.com](http://t-mobile.com)
Enabling T-Mobile USB Mass Storage & Swap Space:

Note: You must mount storage and swap via UUID’s!
- `sudo BLKID`
- `Enter uuid in fstab`
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:**
  - Foxtech RC-305 Receiver [foxtechfpv.com](http://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]