

WarBallooning – Kismet Wireless Eye in the Sky

Presented by:
Rick Hill
DEFCON 16
Sunday, Aug. 10



WarBallooning Concept

- Thanks for coming!
- WarDriving limited visibility in the city
- \$4.00 / Gallon gas means driving less
- Balloon – better platform than rocket
- Perfect for covering 5 - 10 mile Urban Areas
- Questions during talk welcome...

Project in a Nutshell

- Evolved from “WarRocketing” DC14
- Good, Bad comparison
- WarBalloon components
- Hardware Hacks involved
- Network Layout & Security
- Flying the WarBalloon

DEFCON 14

- Evolved from “WarRocketing” DC14



DEFCON 16

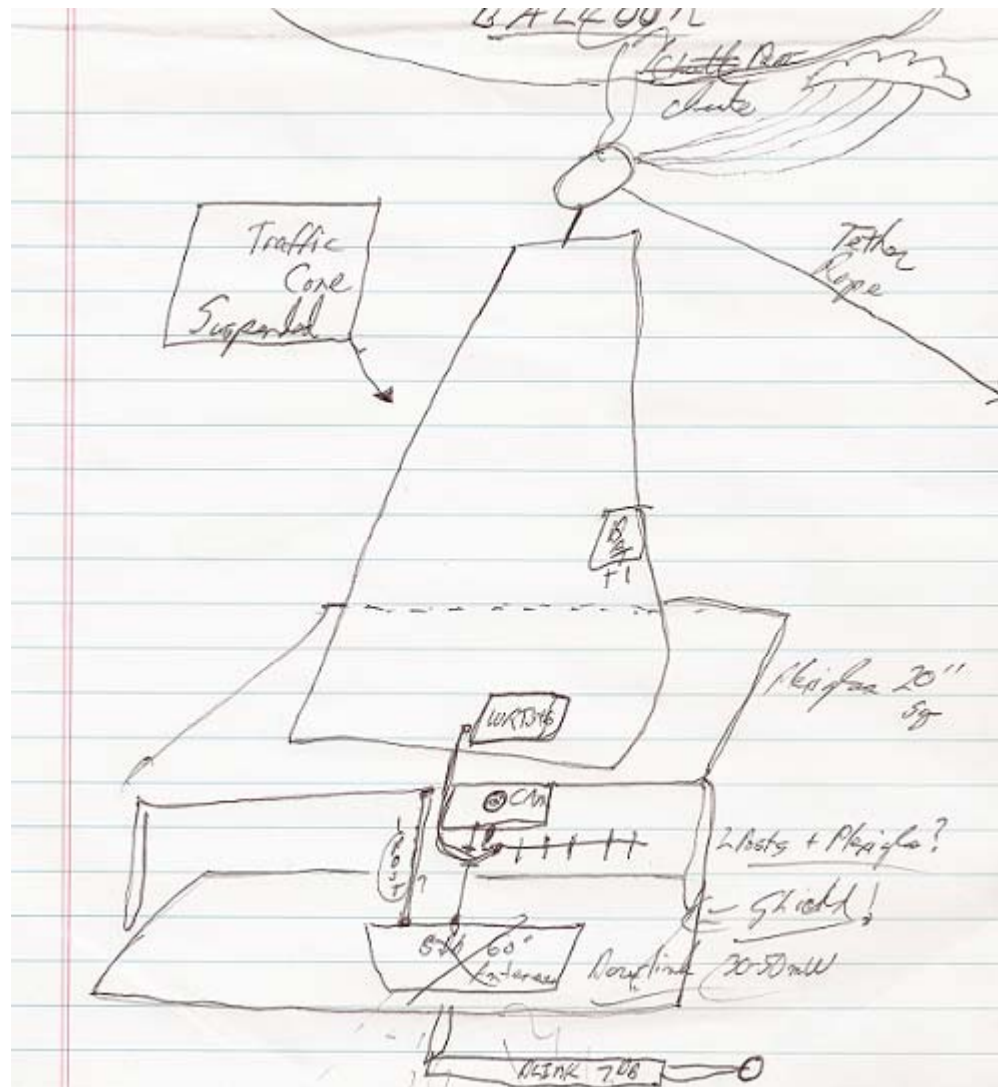
- New Platform:



Balloon vs. Rocket

- The Rocket was a novel concept, but...
 - Explosives permits req'd
 - Launch only in rural areas
 - Stumbling limited to parachute drift time
- Balloon
 - Helium cost \$20/ lb. payload lift
 - More accepted by authorities
 - Still restricted near airports

1st Design Sketch – Traffic Cone



Design Considerations

- All components light weight
- Low Power consumption
- Safety (H2 = Hindenburg)
- Wireless SW must be passive - Kismet
- Secure Network

Hardware Components

- Balloon: Professional Aerial Photography
- WRT54G, v2
- Dlink 5220 Security Camera
- Fiber Optic Transceivers
- Yagi Antenna, Omni Antenna
- Container: thank you Igloo Cooler Co!

Software Components

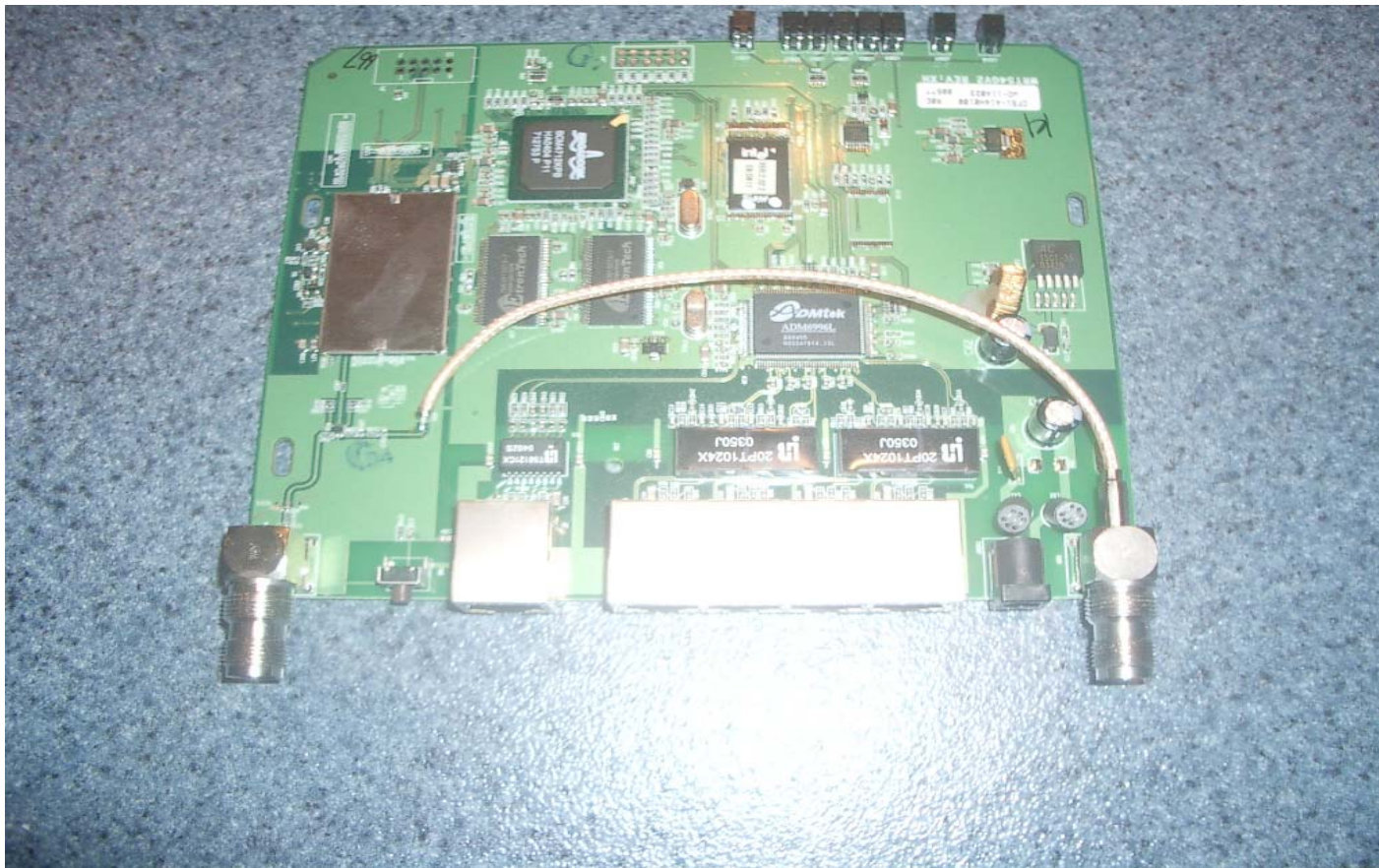
- Kismet Server, Drone
- Talisman 1.3.6
- Web Browser: Dlink 5220 view & control
- Suse Linux
- Flite Festival Speech Synthesis Software
- Kismac
- UNIX utilities: ssh v2, etc.

HW / SW Hacks

- WRT54G – install Talisman, ssh, Kismet drone
- Move antenna connector
- Remove case
- Mount in Igloo “Mini-Mate”

HW / SW Hacks

- WRT54G



HW / SW Hacks

- DLink 5220 Camera – install antenna
- Igloo Mount

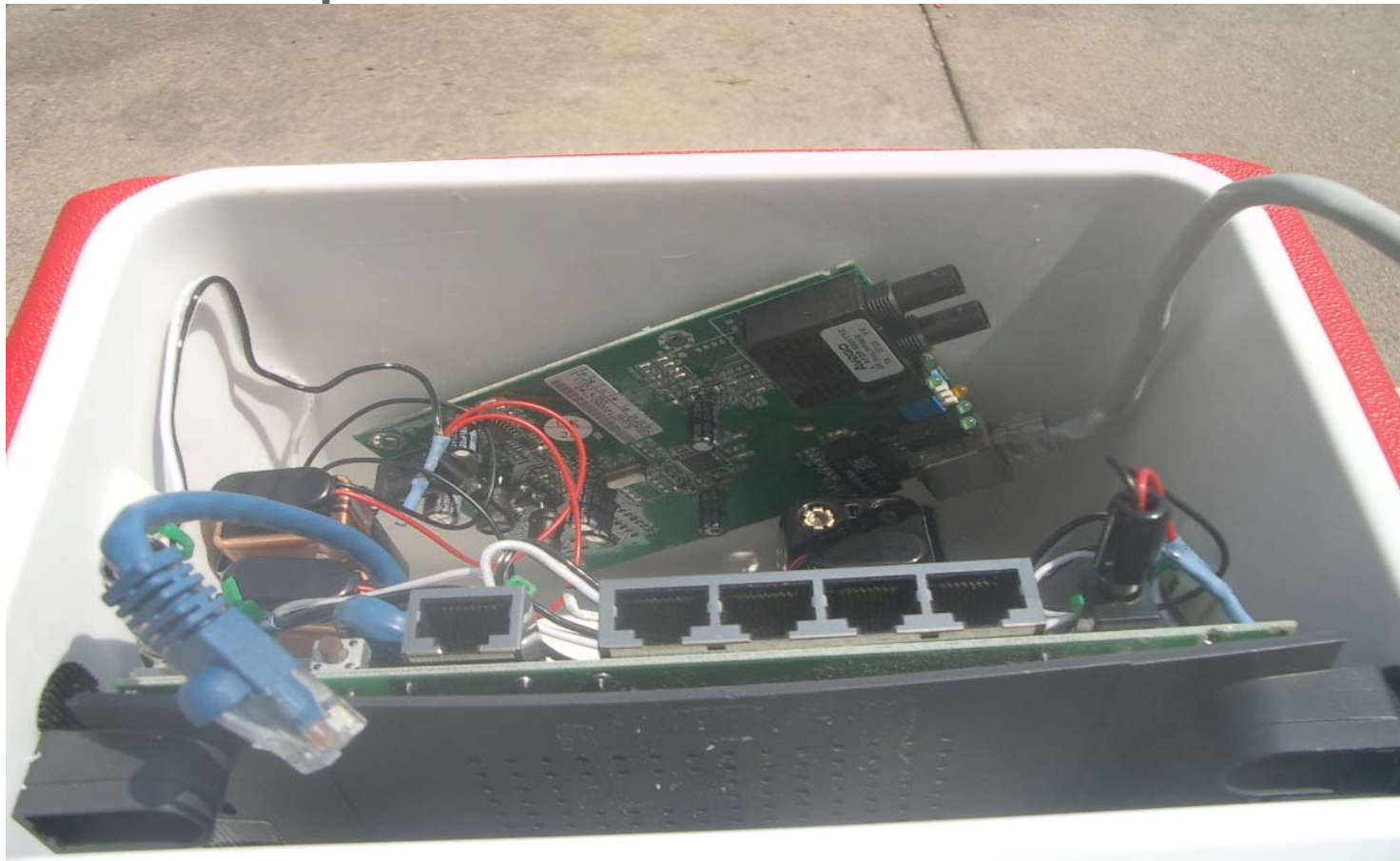


HW / SW Hacks

- Fiber Optic Link
- Inherently Secure
- High Bandwidth
- Low Weight – 50 meters / 1.5 lbs
- Use regular multimode fiber

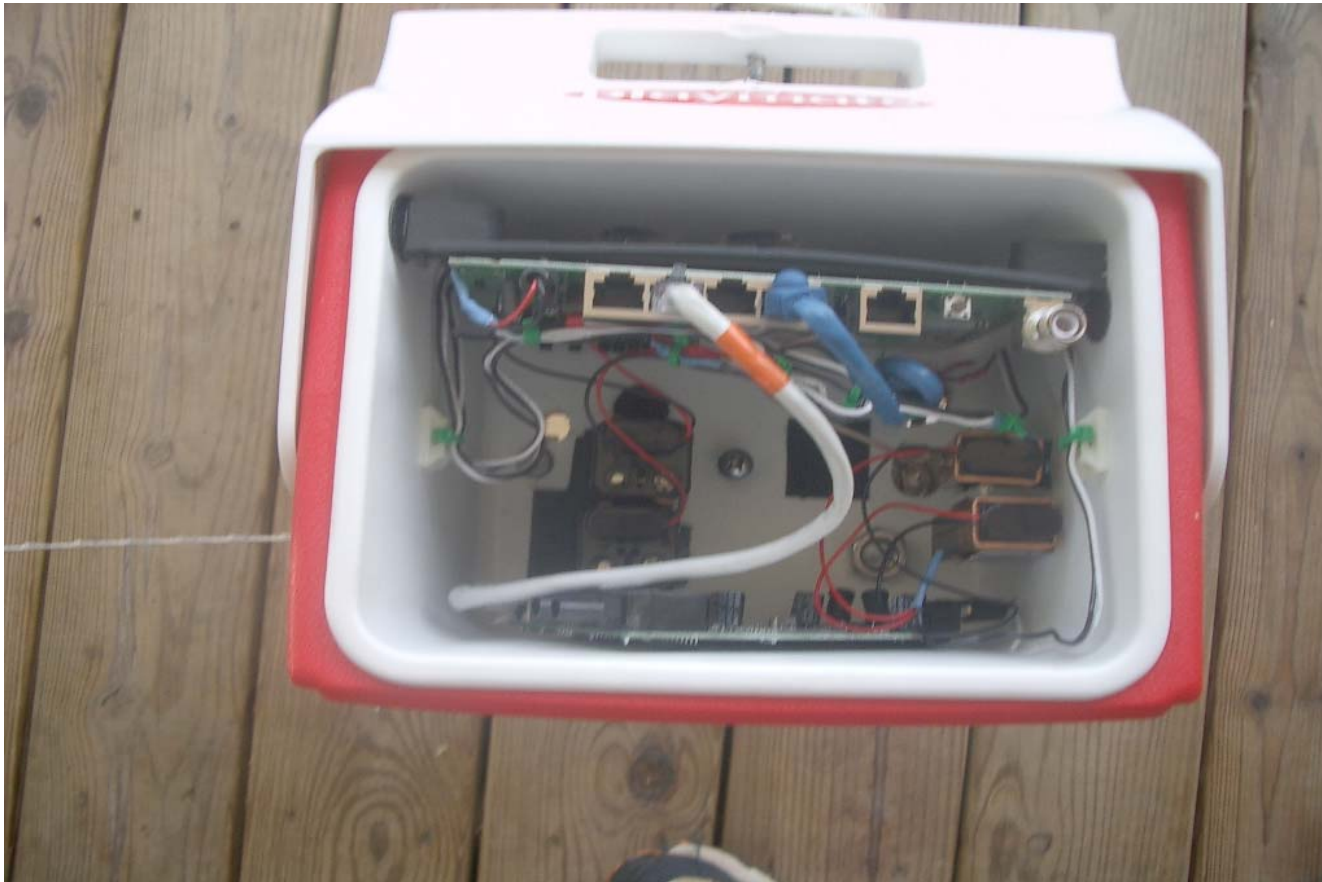
HW / SW Hacks

- Fiber Optic Transceiver – Case removal



HW / SW Hacks

- Completed Payload



IP Based Robotics

- DLINK 5220 consists of a CCD camera, web server, and pan & tilt controller
- As the Pan motor is quite strong, we're using it to aim the high gain antenna @ stumbling targets
- Speed, camera focus, snapshots, MPEG video's all controllable via the web-interface

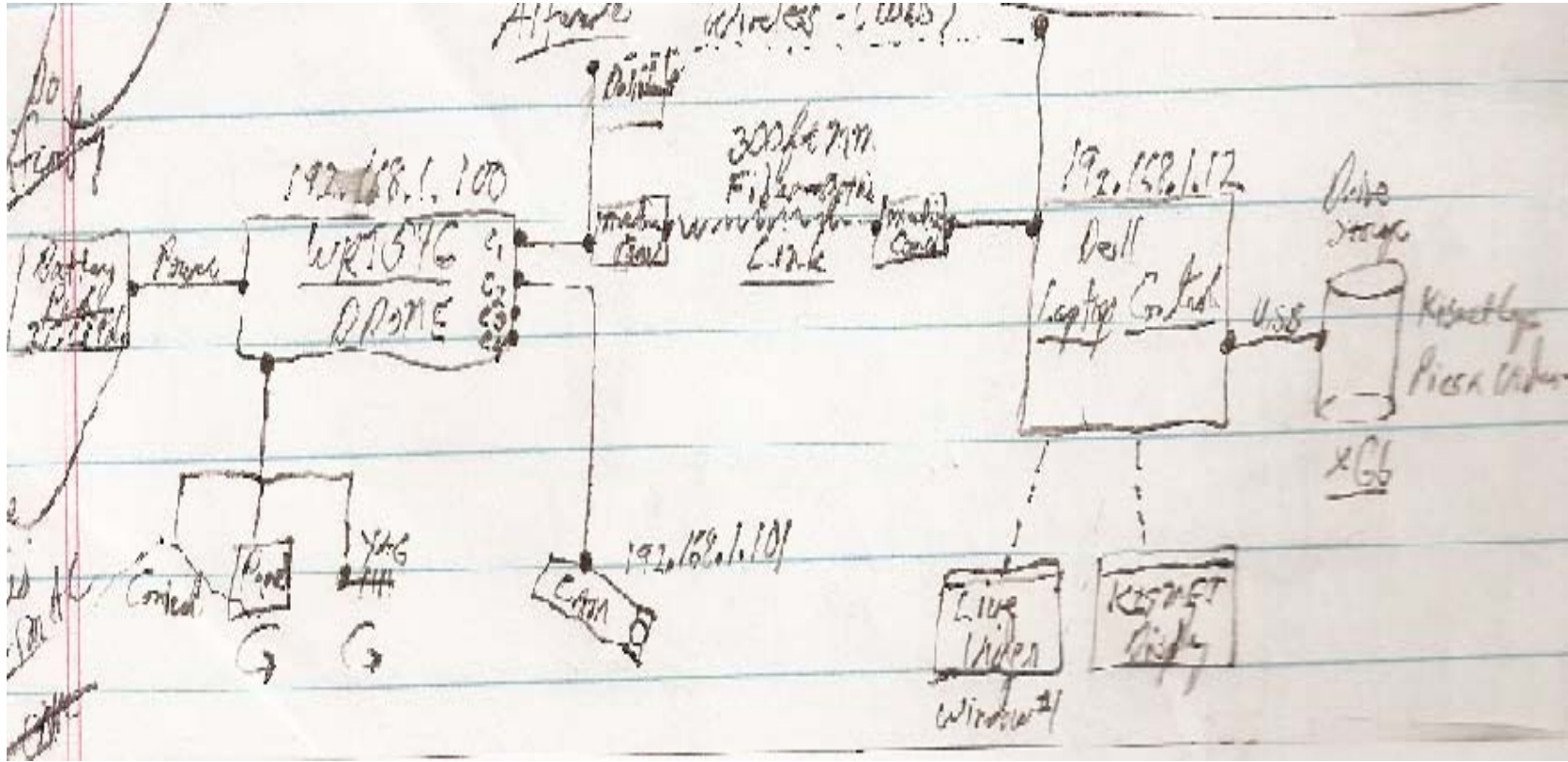
IP Based Robotics

- Other IP Robotics
- Phy2Phy Project->
<http://phy2phy.wikidot.com/start>
- SCADA – IP control of Industrial Systems
 - MODICON PLC's
 - Siemens PLC's
 - <http://www.controlbyweb.com/products.html>

IP Based Robotics

- Security is the Achilles Heel
- Digital Bond has done pioneering work in SCADA Security
 - Nessus Plugin's for SCADA systems
 - Homeland Security
 - Department of Energy
 - <http://www.digitalbond.com/>

Network Sketch



Balloon Network

- WRT54G – Passive Monitoring Only, Data streamed to Kismet Server on ground Hard Drive (HD)
- DLINK 5220 Camera & AP:
 - Web Server used to Control Camera & Antenna Movement
 - Camera AP -> Disabled
 - Video Streamed -> Ground HD
 - Verizon Aircard -> Possible EVDO link to Internet
 - Cell phone Browsing of Aerial Pics

Balloon Network - Security

- Security Considerations:
 - Closed Network - Fiber Optic Transmission
 - SSH & Certificates – Command Line Access to WRT54G
 - AP Not Possible in Drone Mode (IDS)
 - DDNS Use

Flying the WarBalloon

- Biggest Challenge:
 - Not building the WarBalloon
 - FAA Approval
- Letter to Las Vegas Terminal Radar Approach Control (TRACON)

Flying the WarBalloon

- Subject: Proposed Balloon Display over the Riviera Hotel.
- Sent By: ricklhill@adelphia.net On: May 12, 2008
- To: manager@faa.gov (FAA Las Vegas ATC)

Sir: Thanks for taking time to talk to me (FRI) concerning FAA regulations for Moored Balloons. As we discussed, my group would like to fly a Balloon during the annual DEFCON convention to be held at the Riviera Convention Center, AUG 8-10, 2008. We understand that safety is of paramount importance as the Riviera is located < 5 miles from Las Vegas Airport (LAS).

As you requested, following is the Balloon Description & Tentative Operating Plan: Balloon to be flown is a maximum 6 ft. diameter unit with a 113 cu. ft. Helium capacity, (to be purchased from Southern Balloon Works. Note this is a commercial advertising Balloon similar to the ones flown by Car Dealerships...

Flying the WarBalloon

- Operation: the Balloon (unmanned) is to be moored via the supplied tether line from the edge of the Riviera convention center, monitored at all times, and flown at less than 150 ft. AGL, daylight operation only. Balloon will have a 3.5 lb. payload. For safety it is equipped with a self-deploying parachute capable of lowering the payload gently to the ground in case of Balloon failure (bursting.) You also mentioned that nearby building heights could be important: I did some research & found that Turnberry Towers - (adjacent to our flight location) comes in at 477 ft., while Wynn down the street in the other direction is 614 ft. in height.

If you would, please review our plan and let us know if you think the proposed operation is feasible, (& legal per FAA 101 regulations.) Appreciate your time and any advice you can offer.

Regards,
Rick Hill

Crazy Man

- OK, so a Laptop & Lawn Chair did come to mind. (I do NOT recommend)



Flying the WarBalloon

- Virginia Test Flight – 29 JUN



Flying the WarBalloon

- VA Test Flight



Flying the WarBalloon

- VA Test Flight – No AP's here- Tornados



Flying the WarBalloon

- Kismet Output

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	Network	NetType	ESSID	BSSID	Info	Channel	Cloaked	Encryption	Decrypted	MaxRate	MaxSeenRate	Beacon	LLC	Data	Crypt
2	1	infrastructure	makiko	00:1C:10:4A:C0:4E		6	No	None	No	54	0	25600	29973	112775	0
3	2	infrastructure	UJPH1	00:18:01:E8:97:CF		4	No	WEP	No	11	0	25600	27281	3121	3120
4	3	infrastructure	VeroLAN151CWFB	00:02:2D:B4:54:EE		8	Yes	WEP	No	11	0	25600	14652	13585	13500
5	4	infrastructure	428KB	00:18:01:E1:7D:E3		4	No	WEP	No	11	0	25600	21953	2520	2520
6	5	infrastructure	VeroLAN151LCA	00:02:2D:9D:E9:DD		1	Yes	WEP	No	0	0	100	0	9	0
7	6	infrastructure	VeroLAN151CLB	00:20:A6:51:42:CF		1	Yes	WEP	No	0	0	100	0	10	0
8	7	infrastructure	VeroLAN151AXA	00:30:F1:62:80:1B		64	Yes	WEP	No	0	0	100	0	3	0
9	8	infrastructure	XRLA2	00:18:01:ED:1A:47		8	No	WEP	No	18	0	25600	5199	382	382
10	9	infrastructure	O76U1	00:18:01:EB:63:E3		8	No	WEP	No	18	0	25600	249	18	18
11	10	ad-hoc	\334VL151LC	02:37:80:31:99:F2		6	No	WEP	No	11	0	25600	3	0	0
12	11	infrastructure	VeroLAN151FAAa	00:30:F1:64:F7:B9		64	Yes	WEP	No	0	0	100	0	10	0
13	12	infrastructure	VeroLAN151FAB	00:02:2D:A8:D8:5D		6	Yes	WEP	No	0	0	100	0	9	0
14	13	infrastructure	VeroLAN151AXB	00:02:2D:2D:4B:3E		1	Yes	WEP	No	0	0	100	0	10	0
15	14	infrastructure	VeroLAN151CLAa	00:30:F1:5B:10:47		64	Yes	WEP	No	0	0	100	0	9	0
16	15	infrastructure	<no ssid>	00:14:BF:79:F6:A2		0	No	WEP	No	0	0	0	23	136	0
17															
18															
19															
20															

Summary

- **Aerial platforms do provide superior LOS to WIFI targets.**
- **Wind is not your friend:**
 - **No Wind: perfect for directional antenna**
 - **5 MPH: OK**
 - **10 MPH: Use the OMNI**
 - **15 MPH: Forget It!**
- **DEFCON Results: TBD**

QUESTIONS?



Now
or drop by
The Wireless Village
Breakout Area
Thanks!