Wireless Aerial Surveillance Platform

W.A.S.P.
DEFCON 19
Introduction
Who we are.
• “Dude, I have an idea…”
  • Build a UAV
    • Provide remote penetration testing capabilities
    • Useable flight time (~1 hour)
    • Man portable
• Design Philosophy
  • Low cost
  • Utilize open source and off-the-shelf components
  • Focus on system integration not component design
  • Easily repeatable by anyone
Specifications
So what is it?
• FMQ-117B U.S. Army surplus target drone
  • Foam construction
  • ~14 pound take-off weight
• E-Flite 90 brushless out runner motor
  • Castle Creations Phoenix 85HV ESC
  • 17”x10”electric propeller
• 2x 6 cell 22.2v 5000mAh LiPo batteries
Avionics
• JR Spektrum Dx6i Transmitter and Receiver
  • 2.4GHz
• DIY Drones ArduPilot
  • ArduShield
  • XY&Z Infrared sensors
• Various servos
• XBee Pro with AdaFruit adapter
  • 900MHz
  • Telemetry downlink
Payload
- Via Epi PX5000eg Pico-ITX motherboard
  - 1 GHz Via C7 CPU
  - 1GB ram
  - 8GB Voyager GTR Flash drive
  - Backtrack 5
- USB 4G dongle
  - Internet connection
  - OpenVPN connection to Backend
  - Session Initiation Protocol (SIP) back haul
- XBee Pro module
  - 900MHz
  - PPP tunnel to Base Station
- Universal Serial Radio Peripheral (USRP)
Base Station
• Gumstix Overo Earth
  • ARM Cortex-A8 600Mhz
  • Chestnut43 add-on module
  • 4.3” touchscreen display
  • XBee Pro
    • 900MHz
    • PPP tunnel to the payload
• DIY Drones ArduStation
  • XBee Pro
    • 900MHz
    • Telemetry down-link from Ardupilot
• Asus WL-330gE Wi-Fi Access Point
  • Allows easy and direct access to payload
• Intel P4 3.06GHz HT Processor
• 4GB Memory
• 500GB Hard Drive
• NVIDIA GTX 470
  • CUDA Processor
• Software
  • Pyrit
    • ~19,300 Pairwise Master Keys (PMKs) / second
  • Asterisk
  • WPA Brute Force Dictionary
    • 4 GB
    • 354,638,643 Entries
    • 4.5 hours to process entire dictionary against WPA handshake
  • OpenVPN Server
Capabilities

Yes, but what does it do?
System Topology
Capabilities

Movie goes here
• Base station
  • Telemetry
  • Wi-Fi Accessibility
    • “WASP – Base Station” access point
• Backtrack 5 based payload
  • Kismet
  • Aircrack, Airbase-ng, all the BT5 tools
• Universal Software Radio Peripheral (USRP)
  • GNU Radio, OpenBTS
  • IMSI Catcher
Project Costs
How much is this going to cost me?
- Airframe Free
- Payload ~ $640
- USRP ~ $1600
- Avionics & R/C ~ $800
- Power-plant ~ $800
- Gumstix Overo Earth ~ $350
- ArduStation ~ $100
- Wi-Fi AP ~ $50
- 7 port USB Hub $40
- Project Box ~ $10
Backend Station

- Generic x86 PC ~ $600
- NVIDIA Video Card ~ $300
Total Cost

Cost So Far: ~$5960.00
+ Misc. Costs: ~$500.00
Total Cost: ~$6190.00

Not counting mistakes
Lessons Learned

Mistakes cost money.
Save some by using ours.
• Looking ahead 3 steps or more
  • Poor choices today can limit tomorrow’s potential
• You will crash, learn from your failures
• Good / Bad decisions
  • MIG vs. EasyStar
  • VIA Epiia vs. ARM payload
  • Propeller size
  • Attitude sensor location

System Design
VS.
Knee Jerk Problem Solving
• This has no custom parts. Everything is easily available online
• The average enthusiast can build and operate this
• This is what we came up with, not the limit of possibilities
• People automatically assume you are an evil bastard trying to destroy their hobby / job / life
• Online communities can see you as a potential threat, so don’t expect a lot of hugs and kisses
• We received threats that we were going to be reported to the FAA, FCC, FBI, NSA, NAACP, AARP, GI-Joe, the Air Force, Air Traffic Control and our moms if we didn’t stop ruining it for everybody

This might not make you popular
• It’s never as hard as it seems, or as easy as it looks
• Unforeseen issues take up time & money
• You will crash
  • Do not expect perfection the first time
• Cheap is a relative term

The Reality Of It All
• Chris Paget’s Defcon 18 “Practical Cellphone Spying” talk
• DIY Drones – ArduPilot / ArduStation
  • http://www.diydrones.com
• Backtrack – Penetration Testing Tools Distribution
  • http://www.backtrack-linux.org/
• Basic Micro – Power Supplies
  • http://www.basicmicro.com/
• Gateway Electronics St Louis – Electronics & Components
  • http://www.gatewaycatalog.com/
• Gumstix – Ultra-small ARM based Computers & Accessories
  • http://www.gumstix.com/
• Horizon Hobby – R/C Supplies
  • http://www.horizonhobby.com/
• Sparkfun – Xbees, antennas and more
  • http://www.sparkfun.com/commerce/categories.php
• VIA – PICO-ITX motherboards
• Dave Farquhar
  • Editor Extraordinaire

• Our significant others
  • For being very understanding and putting up with countless hours spent not paying attention to them.
Questions?
https://www.rabbit-hole.org