TRACKING SPIES IN THE SKIES

ABOUT THE TALK

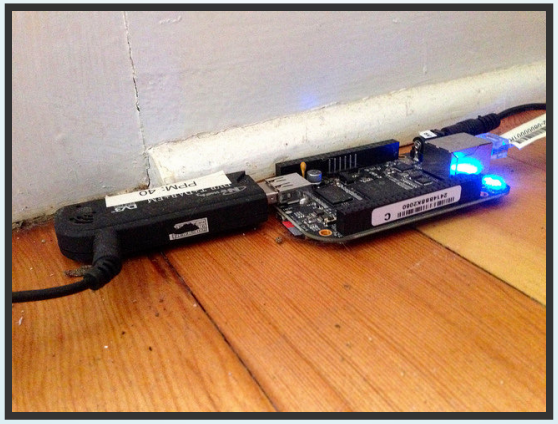
LAW ENFORCEMENT AND AERIAL SURVEILLANCE

- History of aerial surveillance (Sam Richards)
- Technology on spy planes (Jerod MacDonald-Evoy)
- Detecting surveillance aircraft (Jason Hernandez)

NSP
NORTH STAR POST
Independent
Investigative
Journalism

HISTORY OF THE SKY SPIES

- Odd plane patterns noticed, WSJ, Baltimore
- r/conspiracy (John Wiesman - ADSB Detection)
- Citizen journalists (Sam Richards) #FBISkySpies and 100 Tail-numbers, links to FlightRadar24 tracks



SKY SPIES 101

- Sam's story goes viral, a week later AP breaks it into the mainstream
- Sen. Franken calls for investigation (nothing happens)
- FBI Planes hidden behind front companies (FVX Research, et. al)

WHAT WE KNOW


Persistent Surveillance
Systems
Wide Area Surveillance
64 Square Kilometers
½ Meter Resolution
192 Megapixel Color Image
Recorded for analysis

TYPES OF AIRCRAFT

- Small fixed wing (Cessnas)
- Large dual engine (Beechcraft)
- Military style (Pilatus)
- Helicopters
- Drones (Small and Large)

EQUIPMENT

- Wescam by L3 Communications
- FLIR SAFIRE
- IMSI Catchers
- LETC Devices

EXAMPLES OF USE

- FBI Aerial Surveillance of Freddie Grey protests
- FBI Aerial Surveillance of Arizona I-10 shooter suspect's apartment
- Phoenix PD used Pilatus to follow U-haul thief
- 'Persistent Surveillance Solutions'

HIDDEN IN *PLANE* SIGHT

- FBI, CBP, DEA and DOJ use of front companies
- $10 FAA records request reveals equipment
- The Delaware problem

2.0 GENERAL INFORMATION

2.1 DESCRIPTION

This installation provides locates an MX-15HDi EO/IR Sensor in the lower fuselage pressure box previously installed by STC SA1811CE and installs two (2) LETC Antenna Arrays on the lower fuselage skin.

Installation of the LETC Arrays required the relocation of several existing antennas, all current antenna locations are defined in D/N 01890002 Antenna Arrangement.

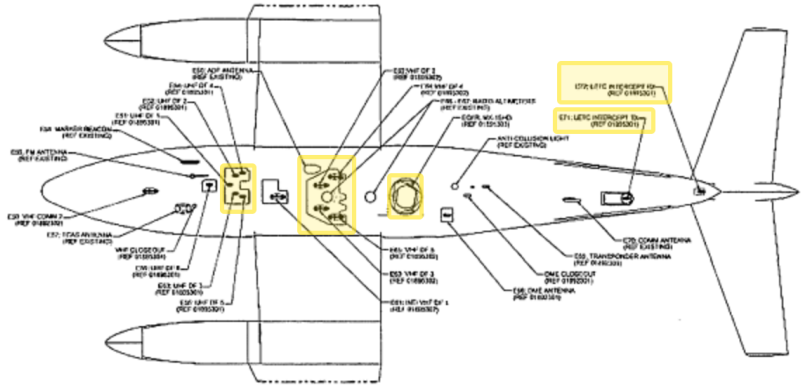
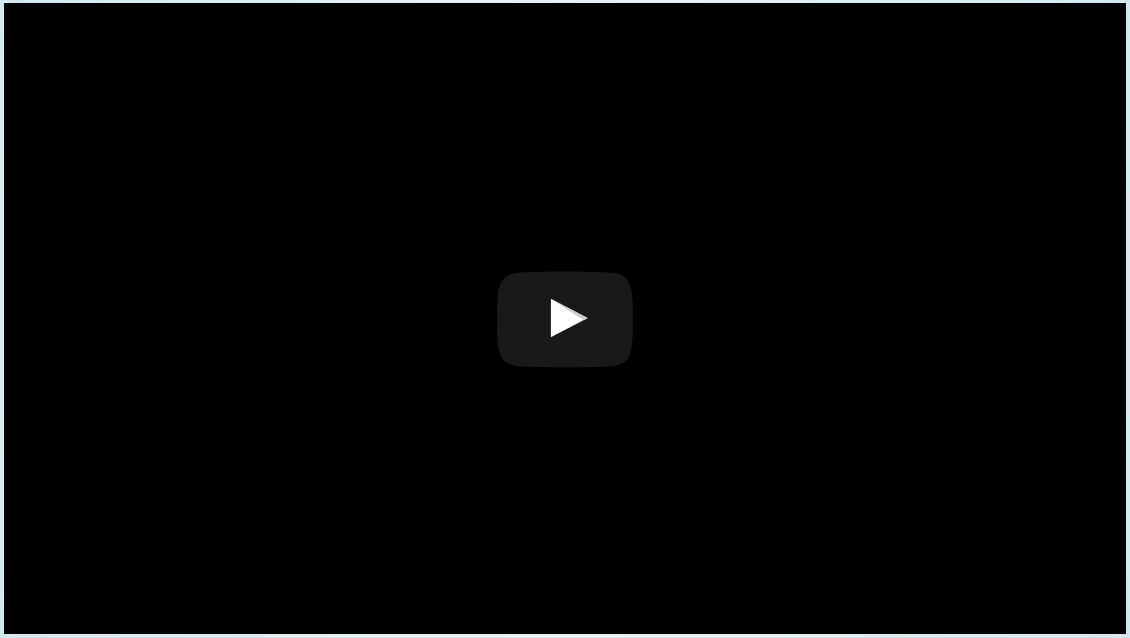


Figure 1: Lower Fuselage

2.2 LOCATION OF ACCESS PANELS

The VHF Comm Antenna is installed on the forward lower access panel, which is utilized for

PHOENIX PD PLANE



FOOTAGE OBTAINED VIA PUBLIC RECORDS REQUEST

TRACKING THE SKY SPIES

- How do we more generally detect surveillance aircraft and activity?
- Registrations can be changed and obscured
- Many surveillance technologies are commercially available
- How much surveillance is happening in other parts of the world?

- Technical and operational requirements dictate flight patterns
- Surveillance flights look very different from most other traffic

HOW DO WE TRACK AIRCRAFT?

- Radar is not practical
- ADS-B messages are the way to go
- Active community of radio / aviation / hacking enthusiasts collect ADS-B data
- Requires a Raspberry Pi 1B+, an RTL-SDR radio, antenna, and internet connection
- Multiple aggregators collect data
  - FlightRadar24.com, FlightAware.com, **adsbexchange.com**
- FAA regulations require an increasing number of aircraft to transmit ADS-B
  - Part of the "NextGen" program
- Similar regulations in .EU, .IN, .AU, elsewhere

ADS-B DATA

- Aircraft transmit a beacon signal with a unique ICAO number
- Positions can be calculated with multilateration
  - Compare time difference of messages arriving at multiple receivers
- Requires 4+ receivers for accurate calculation
- Aggregator networks collect feeds from ADS-B receivers and calculate aircraft positions
- Some aircraft also transmit additional information: (latitude / longitude), call sign, etc.
  - Currently not required, and location may not be accurate

LIMITATIONS TO DATA

- Major commercial flight tracking sites augment their data with FAA radar data
- This data comes with restrictions that tracking sites do not publish positions of aircraft on the FAA's ASDI block list
- Bulk access to data is limited or expensive
- ADS-B Exchange is an exception
- Does not use FAA data, does not censor flights
- Provides free access to live & historical data
  - Data challenges
  - Donation info on their site

PICKING SURVEILLANCE FLIGHTS FROM A FIREHOSE OF DATA

- There are over 80,000 flights a day
- At any given time 8,000~13,000 aircraft are in the air
- Most of these are not surveillance flights
- How do we pick out the surveillance flights?

SURVEILLANCE FLIGHTS VS. OTHERS

- Most non-surveillance traffic goes from point A to B as quickly and directly as possible
- Minimizes flying over populated areas and crossing in to airports' controlled airspace
- Exceptions - holding patterns, flight schools, aerial surveys

TECHNICAL CONSTRAINTS OF SURVEILLANCE FLIGHTS

- Technical and economic constraints result in relatively unique flight patterns for surveillance
- Cell site simulators - range of ~2 miles
- FLIR (infrared) cameras
- Surveillance flights often take off and land at the same airport
- Cover densely populated metro areas
- Visual surveillance - needs daylight
- Electronic surveillance - cover of night preferred
- Altitude "sweet spot"

PATTERN BASED DETECTION

- Surveillance flights make a large number of turns
- Most flights with 30+ turns "look" like surveillance flights
- Limitations & future improvement

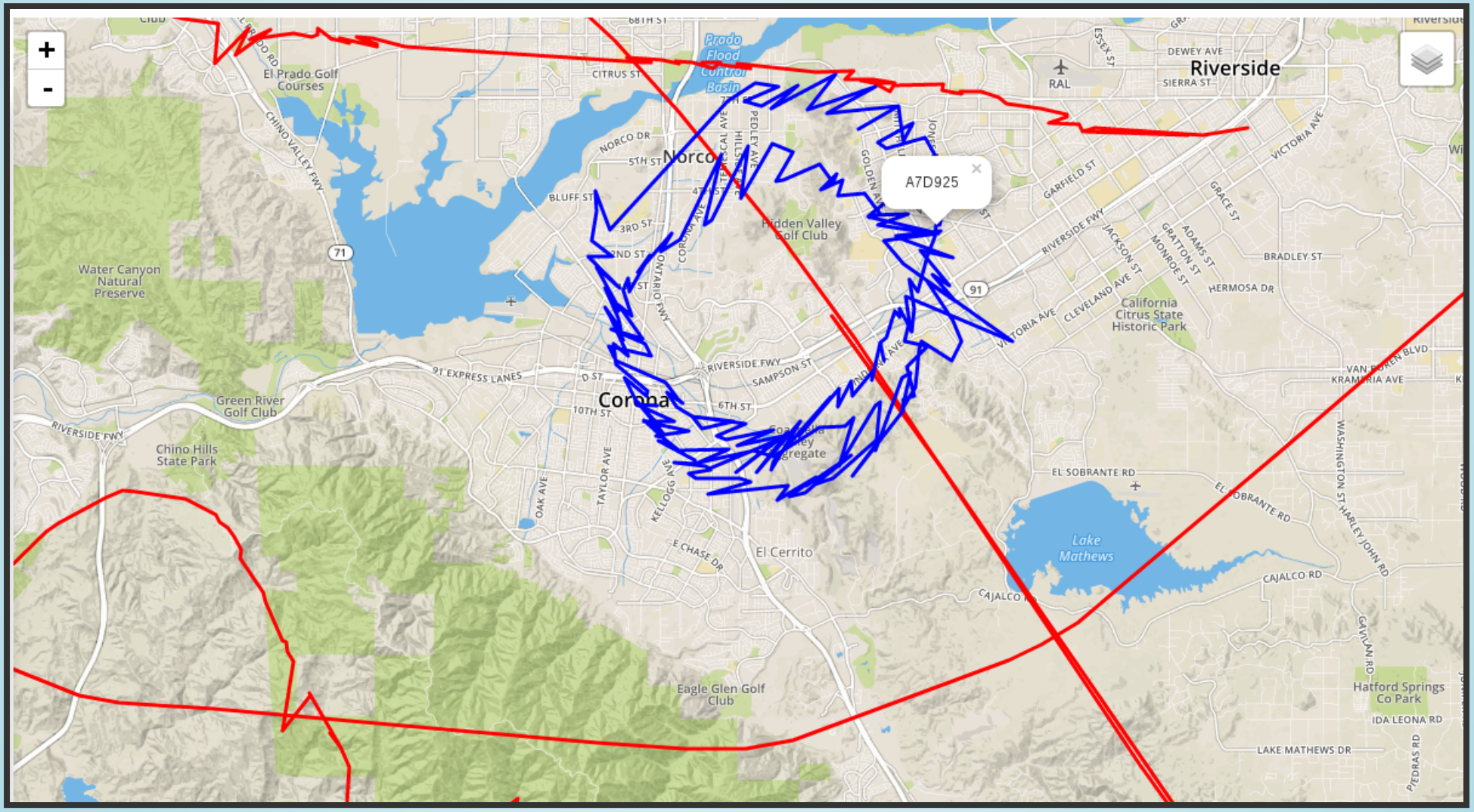
SURVEILLANCE SCORE METHODOLOGY

- Calculate headings of each aircraft and increase the score each time it changes > 90 degrees
- Conditional based on altitude
  - Sweet spot is appx. 6,000 - 12,000 ft
- Future refinements:
  - Consider proximity to airports and controlled airspace (needs good airspace data, may be compute intensive)
  - Score based on aircraft model
  - Additional geometric calulations to filter out survey activity
  - Compare flights to interesting geography -- borders, events, etc.

IMPLEMENTATION

- Virtual Radar Server (http://www.virtualradarserver.co.uk) with connection to adsbexchange.com 's live data feed
- Analysis / tracking code to be released today pulls flight trails from local Virtual Radar Server JSON endpoint
- Flight data queued in RabbitMQ and composed in Redis
- Uses multiple cores and flight analysis can be distributed to multiple machines
  - Completed flights stored for retrospective analysis
- Flight paths for each suspicious aircraft exported as JSON files
- Upload to object storage (AWS S3)
  - Viewable in a basic leaflet.js web map

EXAMPLE


A7D925
Riverside
Norco
Corona
El Cerrito
Lake Mathews
Prado Flood Control Basin
El Prado Golf Courses
Water Canyon Natural Preserve
Hidden Valley Golf Club
California Citrus State Historic Park
Green River Golf Club
Chino Hills State Park
Eagle Glen Golf Club
Hatford Springs Co Park
RAL
CITRUS ST
NORCO DR
5TH ST
BLUFF ST
3RD ST
2ND ST
D ST
6TH ST
10TH ST
SAMPSON ST
RIVERSIDE FWY
91 EXPRESS LANES
CHINO VALLEY FWY
ONTARIO FWY
DEWEY AVE
SIERRA ST
GARFIELD ST
VICTORIA AVE
JACKSON ST
ADAMS ST
GRATTON ST
MONROE ST
GRACE ST
BRADLEY ST
HERMOSA DR
CLEVELAND AVE
VAN BUREN BLVD
KRAMERIA AVE
EL SOBRANTE RD
CAJALCO RD
HARLEY JOHN RD
WASHINGTON ST
GAVILAN RD
IDA LEONA RD
LAKE MATHEWS DR
PEDLEY AVE
HILLSIDE AVE
OAK AVE
TAYLOR AVE
KELLOGG AVE
E CHASE DR
71
91

CONCLUSION

- Many surveillance technologies improve with Moore's Law
- Policies and oversight have not moved as quickly
- You can work on tracking spy planes
- Use, fork, and improve our application
- Set up your own receiver and feed to adsbexchange.com and any future open ADS-B aggregators

MORE INFO:

- https://www.nstarpost.com
- github.com/nstarpost
- twitter.com/nstarpost

For the most accurate / up to date copy of this presentation, see https://www.nstarpost.com/defcon-25/