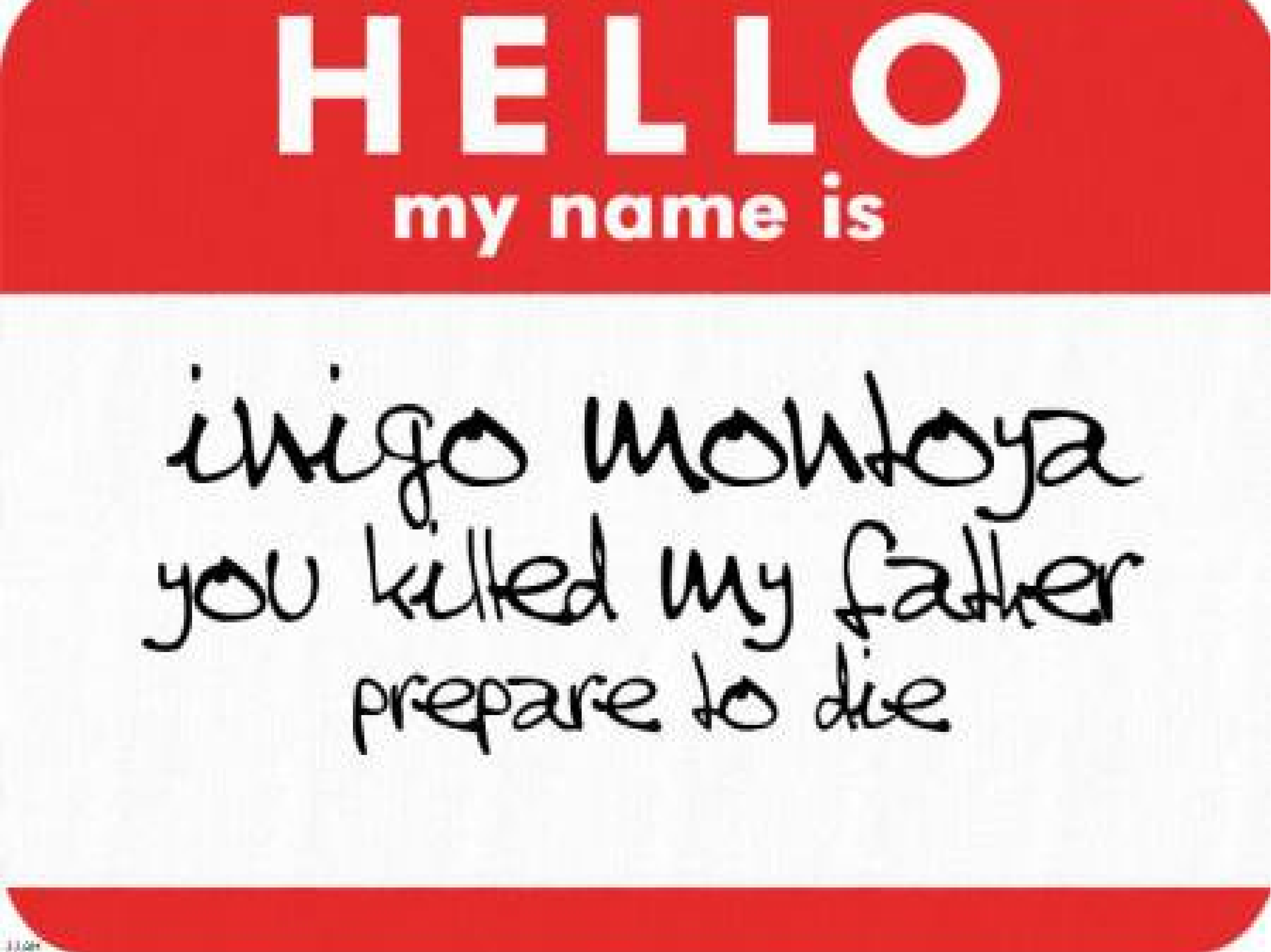
They are doing WHAT! With Air Traffic Control

-OR-

Hackers, Liquor and Commercial Airliners = Fun For All!

RenderMan
www.renderlab.net
render@renderlab.net
Twitter: @IhackedWhat



HELLO
my name is

inigo montoya
you killed my father
prepare to die

Who Am I?

Who Am I?

Pen Tester for ATB Financial

Author – 7 Deadliest Wireless Attacks, Kismet Hacking, RFID Security

Trainer – Wireless and Physical security

Who Am I?

Pen Tester for ATB Financial

Author – 7 Deadliest Wireless Attacks, Kismet Hacking, RFID Security

Trainer – Wireless and Physical security

Hacker – Renderlab.net

Hacker Group Member – Church of Wifi, NMRC

“Notorious Canadian Hacker”

Defcon Old Timer but first Hackfest and first Canadian Hacker con!

Whitehat by trade, Blackhat by fashion

Ass Covering

- For the love of Sponge bob, do not actually try any of the ideas in this talk outside of a lab!!!
- We are talking about commercial airliners and peoples lives here; serious stuff
- Use this information to make air travel safer
- Think about how this was allowed to happen and make sure future systems are built secure from the start
- I want to make air travel safer for everyone, especially for my frequent flying ass

Ass Covering

- Canadian Aeronautic Act
  - Section 302.10: No person shall... (g) at an airport, **knowingly remove, deface, extinguish or interfere with** a marker, marking, light or signal that is used for the purpose of air navigation
- Criminal Code of Canada
  - Section 77: Every one who... (g) endangers the safety of an aircraft in flight by communicating to any other person **any information that the person knows to be false**
  - (e) causes damage to or interferes with the operation of any air navigation facility **where the damage or interference** is likely to endanger the safety of an aircraft in flight
  - is guilty of an indictable offense and liable to imprisonment for **life**.

Ass Covering

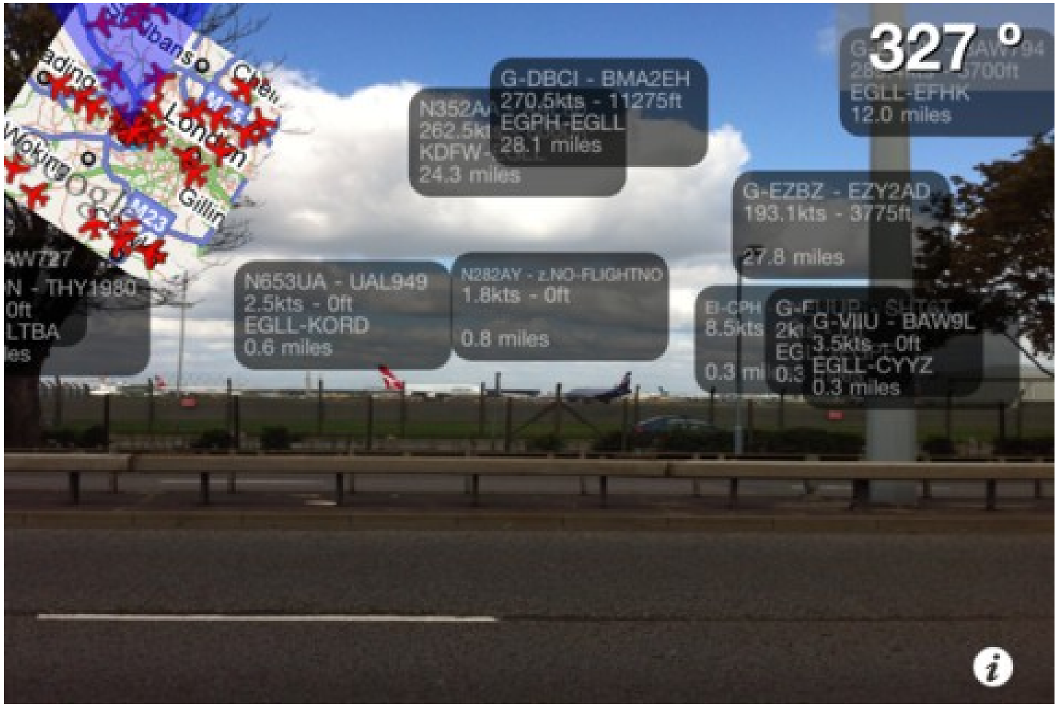
- **I Want To Be Wrong!**; If I am wrong about something, call me on it, publicly! I'm happy to admit if I am wrong - **Be prepared with evidence,** assertions mean nothing to me
- I am not a pilot, ATC operator, or in any way associated with the airline industry or aviation beyond frequent flights in cattle class. I may have some details or acronyms wrong, I apologize, feel free to correct me
- I want to prove to myself that this is safe, so far I've failed
- I need your help to keep up the pressure on the industry and regulators to get answers by asking your own
- My first time presenting this in Canada – I May run a bit long (~70 slides), Theo and Iftach can wait, I'll buy them a beer if they want afterwards

Logic

- I cant prove any of this, and that’s not a bad thing
- 5th version of this talk in 3 years and I'm still asking questions because I have not gotten answers
- NavCanada, et al have still not responded to my satisfaction
- The logic and methods apply to all sorts of systems we use everyday and take for granted
- Go beyond the vuln/exploit/fix cycle and fix the meta level problems of bad system design from the start
- I am providing my evidence for debate and scrutiny. I would hope industry does too in order to prove me wrong and prove the safety of these systems

It All Started With An App

- I got interested purely by accident
- Bought Planefinder AR in October 2010
- Overlays flight information through camera
- GPS location + Direction + web look-up of flights = Neat!

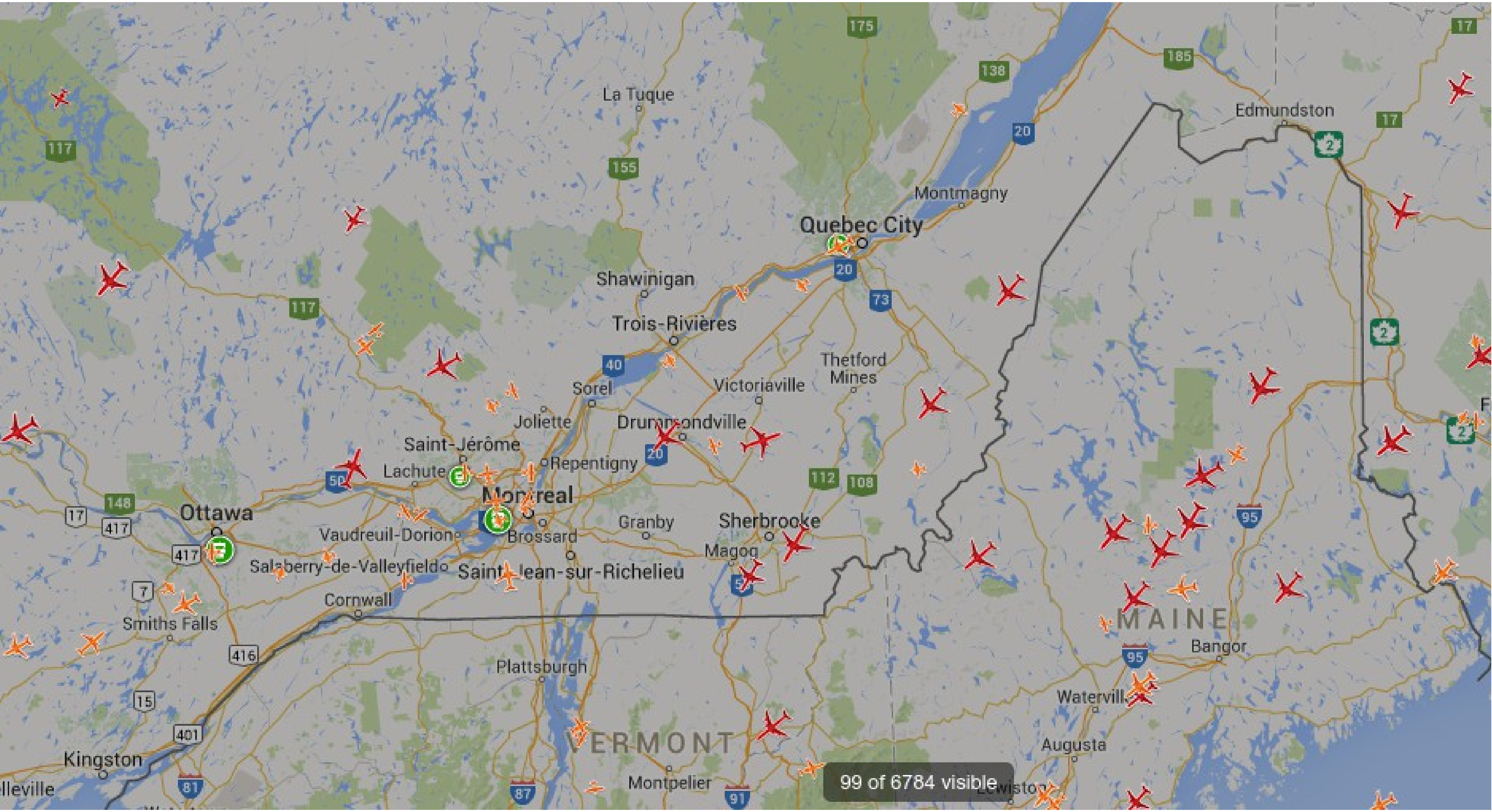


Planefinders

- Planefinder.net, Flightradar24.com, Radarvirtuel.com
- Aggregates data from all over the world
- User provided ground stations and data
- Generates near real time (~10 min delay) Google Map of air traffic
- Supports queries for Airlines, cities, tail numbers, flight numbers, etc. Lots of interesting info for mining
- Allows for very pretty maps and visualizations....

Maps

Planefinder.net - Quebec City/Montreal, Nov 8, 2014, 1:36pm



Pretty Visualizations

Play Europe 24 video here

Getting Slippery...

- Some sites also contained info on how the site and Apps worked
- Some things should not be told to a hacker like me
- I turned into a dog with a bone; ended up pissing of most if not all Air Traffic Control authorities, airlines and aircraft manufacturers worldwide since Defcon 20
- But first, some background....

It Went Downhill From There

- I was under-employed for over a year
- Flying to a lot of speaking gigs worldwide
- Started thinking about airplane tracking and how it worked
- When I get bored, bad things happen
- This is why I should always be employed

DANGER

YOU ARE IN A METAL TUBE 6 MILES ABOVE THE SURFACE OF THE EARTH TRAVELLING FASTER THAN EVOLUTION COULD POSSIBLY HAVE PREPARED YOU TO GO

www.says-it.com/safety

H/T to https://xkcd.com/1075/

Current Air Traffic Control

- ATC has not changed much since 1970's
- Primary radar provides range and bearing, no (accurate) altitude
- Transponder system (Secondary Radar) queries the plane > plane responds with a 4-digit identifier + Altitude
- ID number attached to flight on radar scope, great deal of manual communication and work required

Current Air Traffic Control

- SSR only interrogated every few seconds, low resolution of altitude
- Pilots get no benefit (traffic maps, etc)
- Low resolution requires large separation of planes which limits traffic throughput in busy areas
- Many other systems at play obviously (hugely complex system)
- But until recently, a fairly manual process between Pilots and ATC

Current Air Traffic Control

- IFR (Insturment) flights are way point based, not optimal or direct paths, waste of fuel
- Air travel is increasing, capacity is limited
- Weather and other events (i.e. Volcano's) can cause havoc around the world
- Something needed to change to make things safer and more efficient

NextGen Air Traffic Control

- Late 90's ICAO initiative to revamp the ATC system worldwide
- Do more with the same or less equipment
- Modernize the ATC system over approximately 20 years?
- Save costs on ATC equipment, save fuel, save time, increase capacity at already busy airports
- **ADS-B** is the key feature, the data source for Plane finder sites and the focus of this talk

ADS-B

- Automatic Dependent Surveillance Broadcast
- Planes use GPS to determine their position
- Broadcast over 1090Mhz (978Mhz for GA) at 1Hz to ATC
- Contains Aircraft ID, altitude, position lat/lon, bearing, speed
- Received by a network of ground stations (even sea based!)
- Particularly useful over radar 'dead zones', i.e. mountainous regions, Oceans, Hudsons Bay, Gulf of Mexico, Alaskan mountains, etc
- Certainty of location allows for flights to be closer much closer
- Two forms: ADS-B Out and ADS-B In

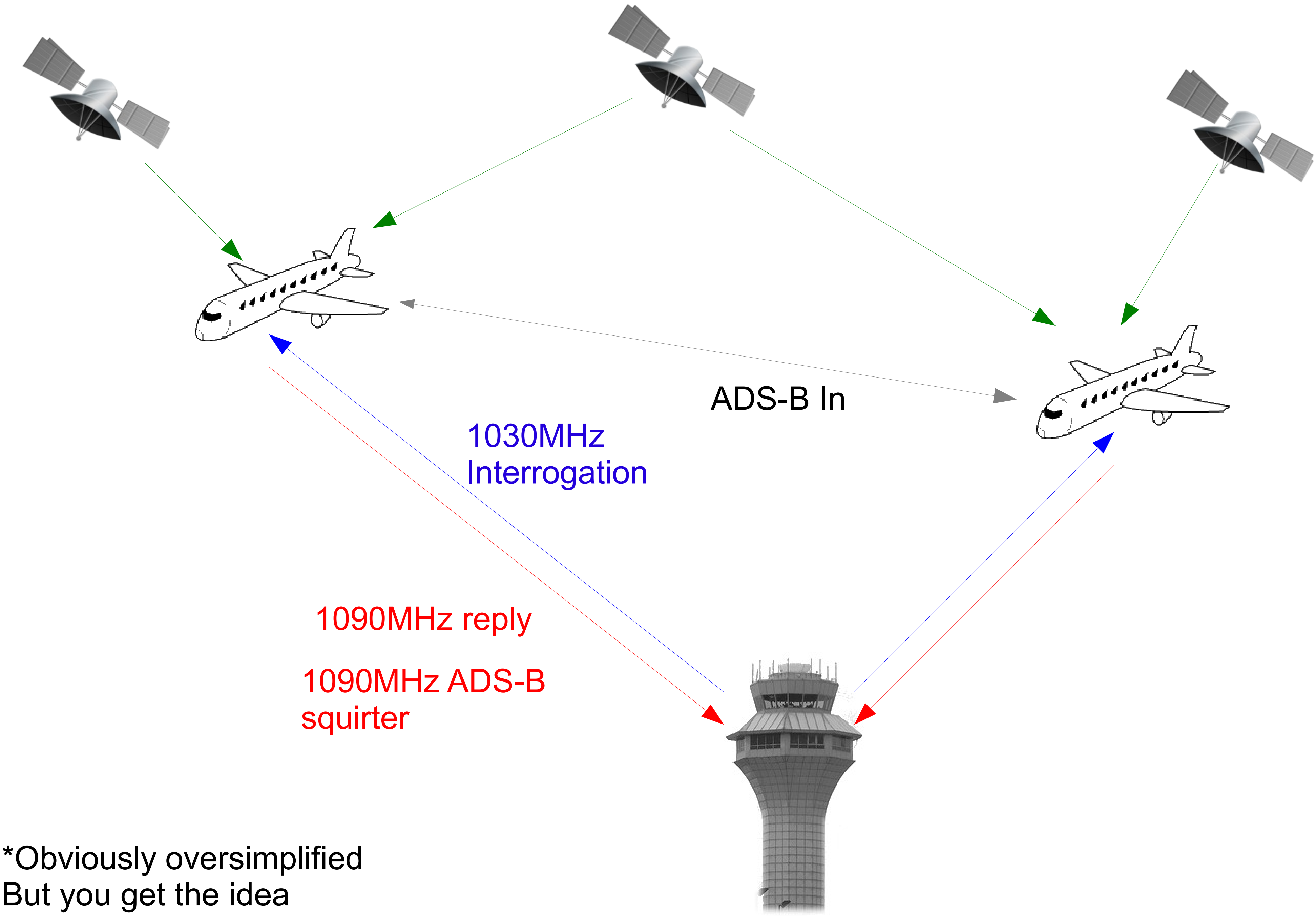
ADS-B Out

- Out – Out from the aircraft
- No interrogation needed (Automatic)
- Instead of primary/secondary radar, planes report their location from GPS (Dependent)
- Sent omni-directionally from aircraft to ground stations and other aircraft (Broadcast)
- ATC's scope is populated from received signals
- Uses 1090Mhz for commercial (big stuff), 978Mhz for General aviation (small stuff)
- 978Mhz uses different link format (UAT), but is effectively the same beast

ADS-B IN

- In – Into the aircraft
- ADS-B IN: Optional equipment can be installed in aircraft to listen to ADS-B out from planes and ATC
- Allows planes to be aware of each other without ATC intervention (TIS-B traffic), augmenting TCAS, ACAS, etc.
- Also allows for real time weather data for GA over UAT (FIS-B)
- Situational awareness increases dramatically, allows more flights operate simultaneously, closer together
- Expensive!! $5-10K+ for ADS-B out, $20K+ for ADS-B In on commercial aircraft
- GA market getting cheap though (few $100 + Ipad)
- Not a lot of used market yet (problem for researchers like me with no budget) but getting accessible

ADS-B enhanced ATC system



*Obviously oversimplified
But you get the idea

Multilateration

- Now, before the NavCanada et. al freak out on me (again!)
- Multilateration; time differential between signal receiving stations; Inverse of triangulation
- Supposed to provide correlation that ADS-B data matches signal source
- No indication this will be used everywhere, not much public on how it deals with errors
- Many other systems/checks in place of course
- More on this later

Starting To Get Scary

- The hacker side of my brain took over the more I researched
- Started to investigate how this worked and what measures may be in use to mitigate obvious threats
- Could not immediately find answers (Answer: trust us!)
- Previous experience shows no answer usually means hadn't thought of it, or have thought of it, but too late, so lets hide the answer
- Started digging deeper and found I'm not the only one looking, and we were all on the same page

Others

- Others have begun to look and question ATC security
- Righter Kunkel - Defcon 18 Talk
- Balint Seeber - spench.net – SDR research (and ISEE-3 reboot badass!)
- USAF Maj. Donald L. McCallie – Graduate research project
- Nick Foster – SDR radio hax0r, professional badass
- Andrei Costin, Hugo Teso – Various talks and research
- All reached similar conclusions independently and have not found any answers

And Now The Scary Part

- Anyone can listen to 1090Mhz (or 978Mhz) and decode the transmissions from aircraft in real time
- Simple PPM (Pulse Position Modulation)
- No data level authentication of data from aircraft, just simple check sums
- Some correlation of primary radar sighting to received data (changing to multilateration)
- ADS-B is **unencrypted** and **unauthenticated**

Say What Now?

Unencrypted and Unauthenticated

ADS-B Out

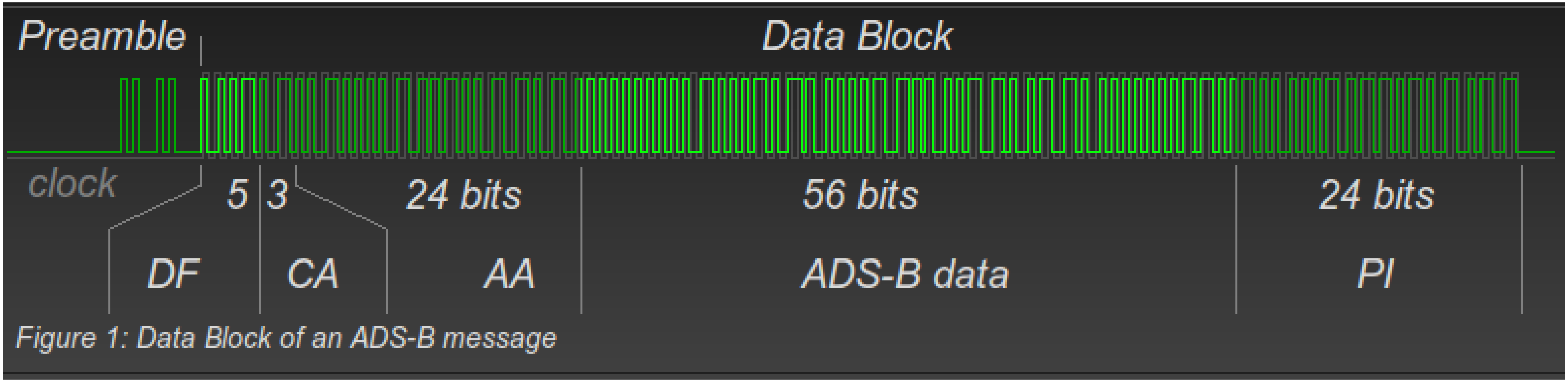
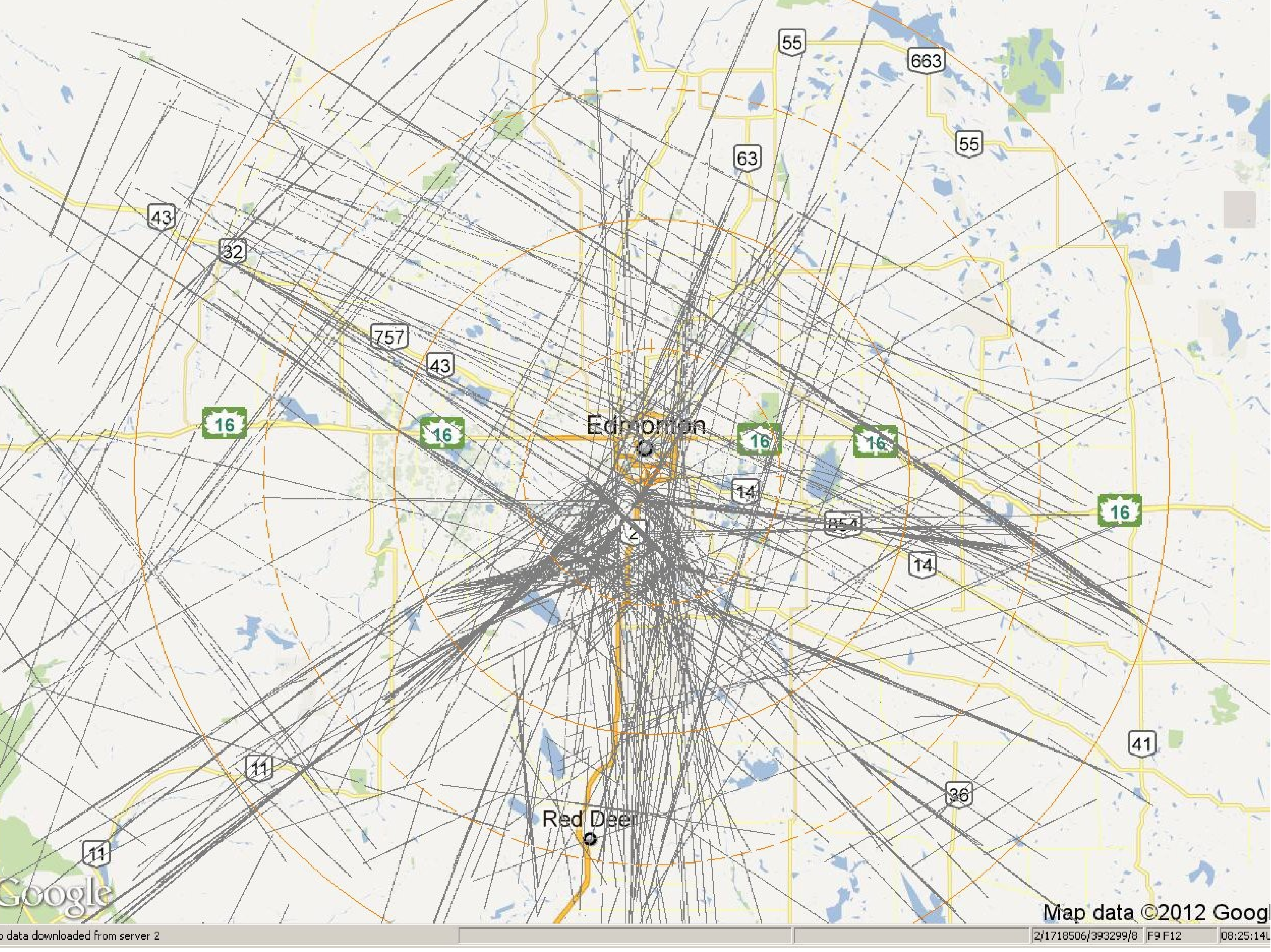


Figure 1: Data Block of an ADS-B message

Looks a lot like any other network packet doesn't it?

- Any idiot has access to raw ATC data
- I am running a ground station in Edmonton covering northern Alberta for Plane finder Sites



o data downloaded from server 2 | 2/1718506/393299/8 | F9 F12 | 08:25:14U

Why This Matters

- Being utilized all over the world, adopted wider yearly, mandatory in N. America in 2020
- UPS equipped all of their fleet for initial testing
- ADS-B equipped planes are in the air over your head right now
- The inevitable direction of ATC for the next couple decades
- I fly a lot and want to get home from here safely!
- I'm sure you do too....
- A multitude of threat vectors to look at....

ADS-B Out Threat #1

- Eavesdropping: Easily capture clear text data of air traffic
- Home brew multilateration to track non-cooperative flights (I.e encrypted military, Air Force One)
- Data mining potential; We know whats in the air, where it is and when as well as historical data to mine (Remember the extraordinary rendition flights?)
- Attacker has the raw data for whatever purpose they want or can imagine

ADS-B Out Threat #2

- Injection: Inject 'ghost' flights into ATC systems
- Documents that discuss fusing ADS-B with primary radar, also discusses discontinuing primary radar!
- Introduce slight variations in real flights or generally cause confusion at inopportune moments (weather event, busy holidays, major travel hubs, special events like the Olympics)
- Create regular false flights, train the system (smugglers?)
- Some documentation discussing multilateration, nothing denoting its mandatory use or alert generation policies
- Multilateration is the constant public excuse from the FAA, et al. For why the system is 'secure'
- Multipoint broadcast could defeat multilateration with a bit more work
- Some evidence that ATC systems may not filter correctly anyways....

ADS-B Out Threat #2

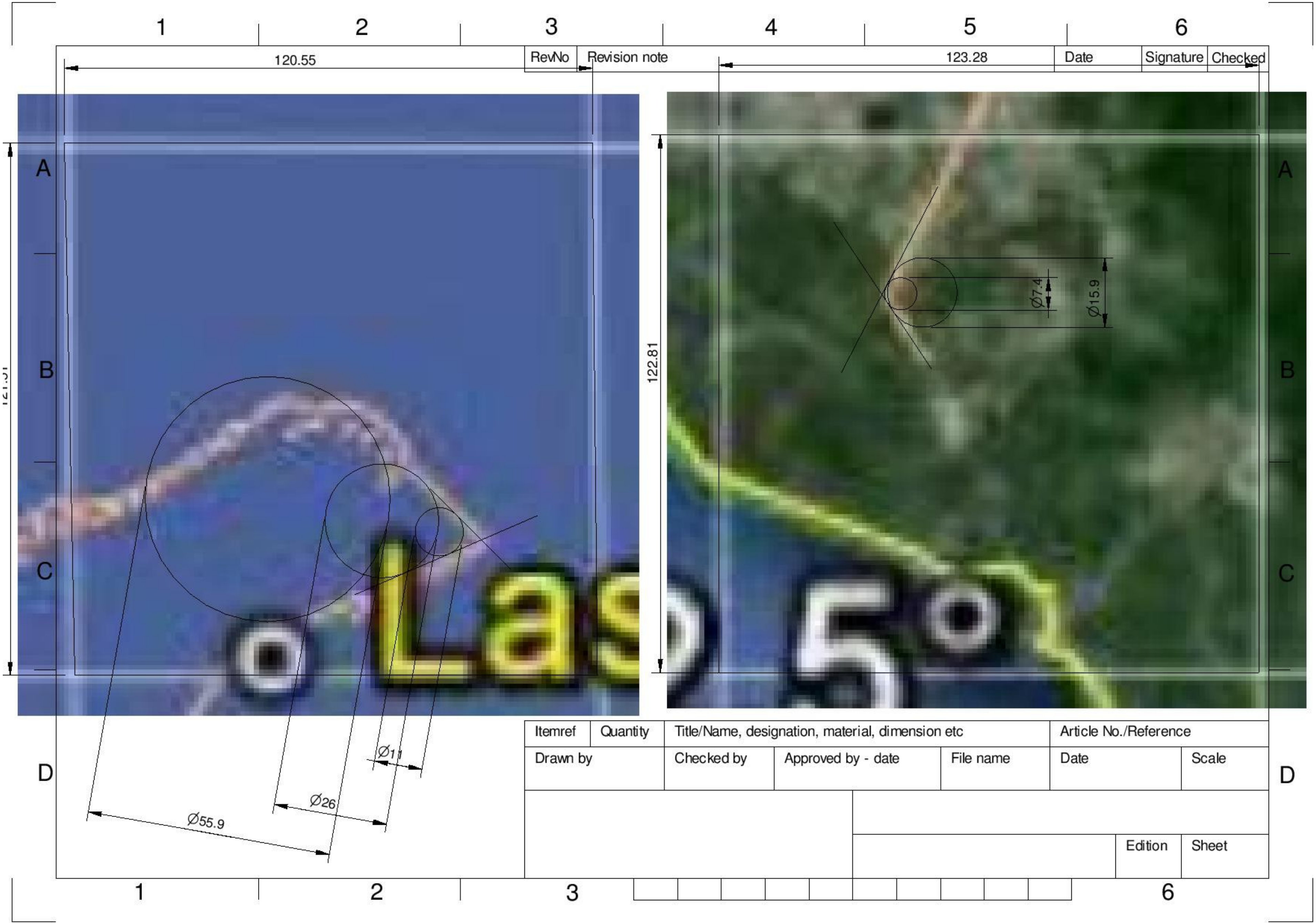
- EASA Safety Information Bulletin 2011-14
- …when two (or more) aircraft with the same (duplicate) ICAO 24-bit aircraft address are operating within range of a specific Mode S interrogator, then potentially hazardous situations can arise...
- … aircraft involved may be assessed by the Mode S interrogator to be a false or reflected echo, and subsequently ignored. **These aircraft will not then be displayed to air traffic controllers**.

ADS-B Out Threat #2

- In the case of aircraft whose flight paths cross, **the identification labels of those aircraft may inadvertently ‘swap’** (i.e. replace one another) on air traffic controllers displays, thereby presenting controllers with **incorrect information and creating the possibility of misidentification.**
- The performance of ACAS II systems (Collision Avoidance) could be seriously degraded or even <u>disabled</u>

http://ad.easa.europa.eu/blob/SIB_201114_Incorrect_Setting_of_ICAO_24Bit_Address.pdf/SIB_2011-14_1

ADS-B Out Threat #2



ADS-B Out Threat #3

- Jamming: Outright Jam ATC reception of ADS-B signals (obvious threat)
- Could be detected and DF'd quickly, but are facilities available for that on short notice?
- Proper target location and timing could cause mass chaos (Sochi Olympics?) and pants browning
- Coordinated jamming across many travel hubs? Accidental or intentional?
- Single point failures can be bad enough (i.e. Chicago ATC sabotage in September...)
- Simple frequency congestion already a problem, no contention protocol, so planes can stomp on each other

ADS-B In Threat #1 (Plane to Plane)

- Injection: Inject data into aircraft ADS-B In displays
- Inject confusing, impossible, scary types of traffic to illicit a response (sphincter variety)
- Introduce conflicting data between ATC and cockpit displays
- Aircraft have no source for multilateration, no secondary verification of received data
- FAA has never addressed this issue publicly to my satisfaction

ADS-B In Threat #2

- GPS Jamming - Block planes ability to use GPS
- North Korea currently jamming GPS along border
- UK tests found widespread use along highways
- Newark airport caused grief daily by truck mounted jammer
- ~$20-30 on Dealextreme.com
- Easily tucked into baggage on a timer
- Removes ADS-B advantages, causes delays, confusion, etc
- Many pilots rusty on IFR (instrument) flight rules

ADS-B In Threat #3

- GPS Spoofing: Introduce manipulated signal to generate false lat/lon reading
- Aircraft location no longer reliable
- Best case, fall back to traditional navigation
- Worst case, remote steering of aircraft
- Iran may have used this technique to capture US drone
- Utexas team shown to be able to screw with US made drones (sub ~$1000)

ADS-B Unknown Threats

- Some threats are total unknowns. The ATC system is huge and hard to parse from public docs
- Has anyone got a full understanding of the whole thing?
- Has anyone fuzzed a 747 or a control tower? Buffer overflow at 36,000 feet?
- Verification of ADS-B chip level code. Could it be used as a control channel?

New, Unknown Threats

- Drone autopilot integration with ADS-B has been tested for domestic drone use
- http://bit.ly/PoFDe4
- Drone automatically adjusts course without human interaction from ADS-B input
- Start remote piloting your own drone!
- What happens when a predator size drone drops in on a suburb?

New, Unknown Threats

- US 2013 Sequestration budget cuts threatened 173 tower closures
- Smaller towers, small airports, but valuable intermediaries between large airports
- More work for already overworked ATC controllers means more reliance on technology
- Congress restored funding, but such closures may happen again

ADS-B Threat Mitigations?

- You hope that the engineers, FAA, DHS, everyone else looked at these threats
- FAA submitted ADS-B to NIST for Security Certification, but.....
- “ the FAA specifically assessed the vulnerability risk of ADS–B broadcast messages being used to target air carrier aircraft. This assessment contains Sensitive Security Information that is controlled under 49 CFR parts 1 and 1520, and **its content is otherwise protected from public disclosure**”

ADS-B Threat Mitigation

- It gets worse: “While the agency cannot comment on the data in this study, it can confirm, for the purpose of responding to the comments in this rule making proceeding, that using ADS–B data does not subject an aircraft to any increased risk **compared to the risk that is experienced today**” - Docket No. FAA–2007–29305; Amdt. No.91–314
- What threats are those? No list anywhere I've found yet
- What about threats of tomorrow? Why not threats we haven't thought of yet?

NIST

- Sounds a lot like Security by Obscurity?
- "System security should not depend on the secrecy of the implementation or its components" - NIST guide to general server security
- http://1.usa.gov/cwbYhH
- Something about a goose and a gander....

ADS-B Threat Mitigation

- Multilateration (back to this again)
- How does the ATC UI indicate a mismatch?
- Liability issues for ATC equipment vendors ignoring data? A great many unknowns in policy and process (working on getting more of this)
- FAA says they have never detected a ghost flight: Maybe no one has tested it yet? Maybe they have just not caught it?
- Plane spotters have cataloged 1770 'oddities' in ICAO24 addresses (duplicates, etc) http://www.airframes.org/oddities.php
- Previous mentioned EASA doc shows that someone has tested it officially and found issues....

ADS-B Threats

- Basically response is always; “Trust Us”
- I don't know about you, but I never trust anyone who says 'Trust Me”
- Not trying to spew FUD, but to raise awareness and pressure to disclose more information about threat mitigation technology and procedures (if any)
- Hackers looking at ATC security has gotten a response of sorts
- Have heard reports of many meetings being held where my name came up and changes are being made
- I'm not going away until I get full, public answers

Hackers and ADS-B

- Office of the Inspector General of the Department of Transport has initiated an audit of the security controls of ADS-B - https://www.oig.dot.gov/sites/default/files/ADS-B%20Announcement%20Memo_5-14-12.pdf
- POTUS specifically mentioned securing Air Traffic Control system as part of cyber security in 2013 SOU address - http://1.usa.gov/XDNTKX
- Recently many academics have been reaching out and starting their own research with access to resources I lack

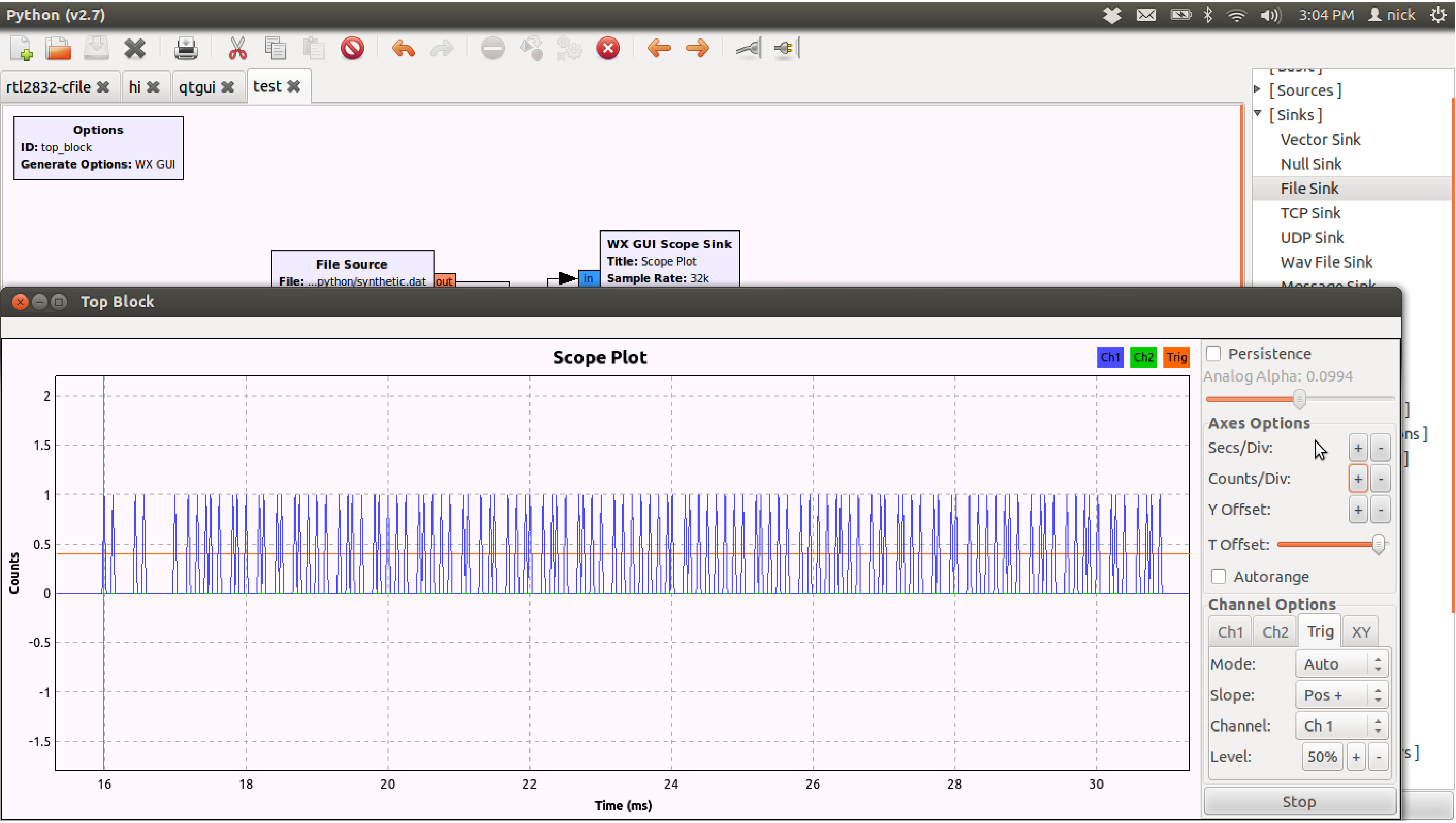
ADS-B Threats

- A common response is that 'It's too expensive/complex for the common man to feasibly attack”
- ~$20 USB TV tuner can be made into a software defined radio and used to receive ADS-B (rtl-sdr)
- HackRF ($300) - BladeRF ($420-650) - USRP ($880-$6K)
- With some additional equipment (amps, antennas), all suitable for mischief, all available via retail channels

ADS-B Threats

- Got word while in the air en route to Poland
- Nick Foster implemented ADS-B Out in Gnu Radio
- A synthetic report generated and decoded by the Gnuradio ADS-B receiver: (-1 0.0000000000) Type 17 subtype 05 (position report) from abcdef at (37.123444, -122.123439) (48.84 @ 154) at 30000ft
- It's not theory any more, we can do it

ADS-B Out Gnu Radio



Python (v2.7)

rtl2832-cfile ✖ hi ✖ qtgui ✖ test ✖

Options
ID: top_block
Generate Options: WX GUI

File Source
File: ...python/synthetic.dat

WX GUI Scope Sink
Title: Scope Plot
Sample Rate: 32k

Top Block

☐ Persistence
Analog Alpha: 0.0994

Axes Options
Secs/Div: + -
Counts/Div: + -
Y Offset: + -
T Offset:
☐ Autorange

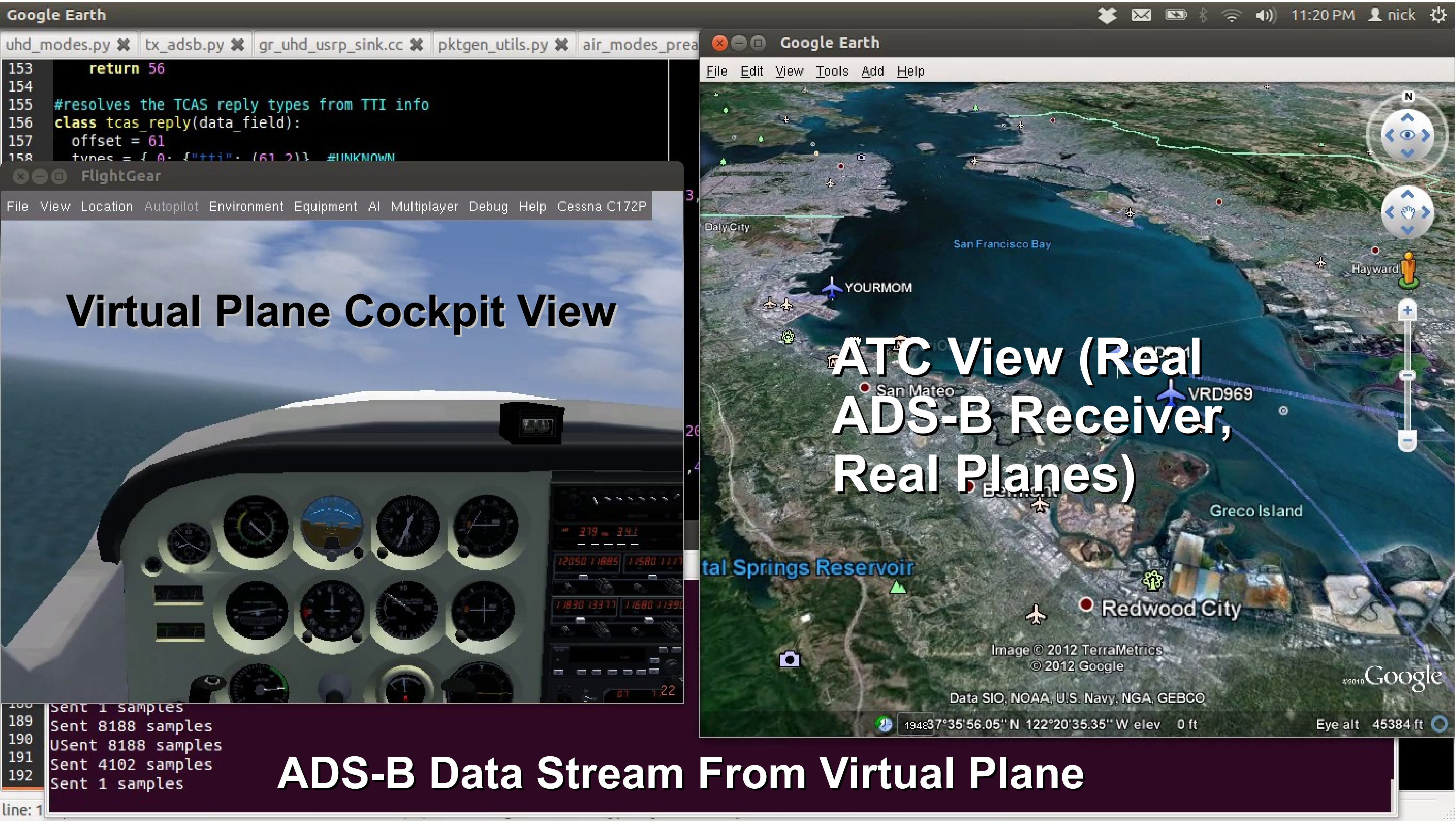
Channel Options
Ch1 Ch2 Trig XY
Mode: Auto
Slope: Pos +
Channel: Ch 1
Level: 50% + -

Stop

ADS-B Threats

- Nick Foster raised his game to badass
- ADS-B In to Flightgear (OSS Flight sim), populates simulator environment with real planes
- ADS-B data generated by your virtual plane, fed into an SDR and put out over the “real” air
- Your virtual world is now transmitting into the real world!
- Flight characteristics now pseudo-matches a real planes behavior......

Movie Time!



```
    return 56

#resolves the TCAS reply types from TTI info
class tcas_reply(data_field):
  offset = 61
  types = { 0: {"tti": (61,2)},  #UNKNOWN
```

```
Sent 1 samples
Sent 8188 samples
USent 8188 samples
Sent 4102 samples
Sent 1 samples
```

Google Earth
11:20 PM
nick
uhd_modes.py
tx_adsb.py
gr_uhd_usrp_sink.cc
pktgen_utils.py
air_modes_prea
FlightGear
File View Location Autopilot Environment Equipment AI Multiplayer Debug Help Cessna C172P
Virtual Plane Cockpit View
Google Earth
File Edit View Tools Add Help
Daly City
San Francisco Bay
YOURMOM
Hayward
ATC View (Real ADS-B Receiver, Real Planes)
San Mateo
VRD969
Greco Island
tal Springs Reservoir
Redwood City
Image © 2012 TerraMetrics
© 2012 Google
Google
Data SIO, NOAA, U.S. Navy, NGA, GEBCO
1948 37°35'56.05" N 122°20'35.35" W elev 0 ft
Eye alt 45384 ft
ADS-B Data Stream From Virtual Plane
line: 1

Play modes_tx.mp4 here

ADS-B Threats

- We have the capability to generate arbitrary packets, anyone else could easily do this
- Took Nick a weekend and my prodding
- All major testing was at 900Mhz ISM band over coax cable from injector to reciever
- Power dialed down to 1/10 milliwatt
- Easy to adjust for UAT ADS-B for GA
- We chose not release the code for safety/legal reasons....

ADS-B Threats

- ...But others have working ADS-B out code on Github now:
  - github.com/JiaoXianjun/GNSS-GPS-SDR
- Working ADS-B flight path generator:
  - github.com/kapman28/ADSB_Radar
  - Socket server output to whatever connects...
- Basically, an exploit is in the wild to generate arbitrary ADS-B data

Other Threats

- Tailored arrival (ATC upload landing plan to aircraft), ACARS, other protocols
- Aircraft are huge, complex systems
- Air Traffic Control is even larger and more complex
- Reading on one system leads you to many others, all tightly integrated and prone to unforeseen interactions

We are Making A Difference!

- “In accordance with the recommendations mentioned in the AIGD, it is proposed that working group within the ADS-B Task Force could be formulated to look into specific security measures with respect to identify potential encryption and authentication techniques, so that the ADS-B security issues could be addressed uniformly across the states, instead of implementing respective state-wise policies”
- From April 2014!!!!!!
- http://www.icao.int/APAC/Meetings/2014%20ADSBSITF13/WP19_India%20AI.7%20-%20Security%20Issues%20of%20ADS-B%20operations.pdf

I've Caused A Ruckus, We are Making A Difference!

- Security has been added to the ADS-B Implementation and Operations Guidance Document (AIGD)!
- http://www.icao.int/APAC/Documents/edocs/cns/ADSB_AIGD7.pdf
- Many more documents (2 years later!) finally doing risk assessments and asking these questions
- Lots of fun documents found recently, make for amusing reading
- Hackers putting pressure on an industry does work, but we need to maintain it

Future

- ADS-B will be mandatory in US by 2020
- Equipped planes are flying overhead for the foreseeable future
- Aircraft industry is very insular and does not think like a hacker. Safety Engineering =! Security Engineering
- Still time to develop countermeasures i.e. don't turn off primary radar! Train ATC operators for 'weird stuff', etc
- Let outsiders have access to test these systems - Offer up proof to shut me up once and for all
- If you have a 747 or similar and/or an air traffic control tower that I can borrow for a while, please let me know

Future

- http://www.atca.org/cyber
- Air Traffic Controllers Association Aviation Cyber Security Day – November 13, Arlington, VA
- Anyone feeling generous (or mischievous) and can pay to send me there?
- Never been contacted by any agencies or groups. You'd think a phone call would be a good idea?

Thanks - Questions

Please Prove Me Wrong!

Email: render@renderlab.net
Twitter: @ihackedwhat
Website: www.renderlab.net

Big thanks to Nick Foster, the EFF, and the other researchers mentioned.

Huge thanks to several anonymous pilots, academics and industry insiders who have been feeding me info!