



+



=



Hackers + Airplanes

No Good Can Come Of This

Defcon 20

Brad "RenderMan" Haines, CISSP

www.renderlab.net

render@renderlab.net

Twitter: [@IhackedWhat](https://twitter.com/IhackedWhat)

HELLO

my name is

inigo montoya
you killed my father
prepare to die

Who Am I?



Who Am I?



**Consultant – Wireless, Physical,
General Security, CISSP**

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

**Trainer – Wireless and Physical
security**



Who Am I?



Consultant – Wireless, Physical, General Security, CISSP

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

Trainer – Wireless and Physical security



Hacker – Renderlab.net

Hacker Group Member – Church of Wifi, NMRC

Defcon Old Timer – Every year since DC7

Who Am I?



First, The Kaminsky Problem

- At multiple cons, over multiple years, speaking in opposite rooms
- Getting rather ridiculous
- I have yet to see any of his talks live
- Summed up as the “RenderMan Birthday Paradox” on his blog
- Ironic since yesterday (27th) was my birthday
- Can someone confirm if they are scheduling this intentionally!

Ass Covering

- For the love of Spongebob, 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 happened and make sure future systems are built secure from the start
- Hackers need to be included in more areas than we are now

Ass Covering

- **I Want To Be Wrong!**; If I am wrong about something, call me on it, publicly!
- I am not a pilot, ATC operator, or in any way associated with the airline industry or aviation beyond flying cattle class. A Lot!
- I may have some details or acronyms wrong, I apologize, feel free to correct me
- This research is ongoing and too important to keep hidden until completion
- I want to prove to myself this is safe, so far I've failed, so I need your help

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 lookup of flights
- This is cool, how does it work?



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
- Also contained info on how the site and App worked

It Went Downhill From There

- Been under-employed for over a year
- When I get bored, bad things happen
- I still fly to a lot of speaking gigs
- Started thinking about airplane tracking
- This is why I should always be employed



Current Air Traffic Control

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



Current Air Traffic Control

- Transponder ID used to communicate situations i.e. emergencies, hijacking, etc
- Transponder provides a higher power return than primary radar reflection, longer range
- Only interrogated every 6-12 seconds, low resolution of altitude
- Pilots get no benefit (traffic, etc)
- Requires large separation of planes (~80miles) which limits traffic throughput in busy areas

Current Air Traffic Control

- IFR flights are way point based, not optimal or direct path
- 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



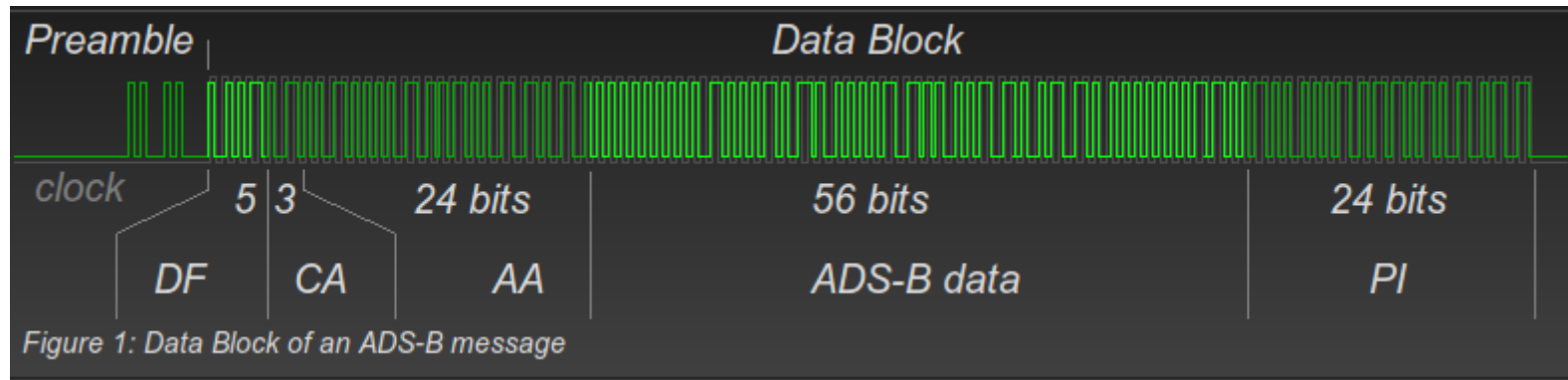
Nextgen Air Traffic Control

- Late 90's FAA initiative to revamp the ATC system in the US, and via ICAO, the world
- Do more with less
- Modernize the ATC system over approximately 20 years
- Save costs on ATC equipment, save fuel, save time, increase capacity
- **ADS-B** is the key feature, the datasource for Planefinder sites and the focus of this talk

ADS-B

- Automatic Dependant Surveillance Broadcast
- Planes use GPS to determine their position, broadcast over 1090Mhz (978Mhz for GA) at 1Hz
- Contains Aircraft ID, altitude, position lat/lon, bearing, speed
- Recieved by a network of groundstations
- Particularly useful over radar 'dead zones', i.e. mountainous regions, Oceans, Hudsons Bay, Gulf of Mexico, Alaskan mountains
- Certainty of location allows for flights to be closer (5 miles)
- Two forms: ADS-B Out and ADS-B In

ADS-B Out



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

ADS-B Out

- No interrogation needed (Automatic)
- Instead of primary/secondary radar, planes report their location from GPS (Dependant)
- Sent omni-directionally 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)

ADS-B In

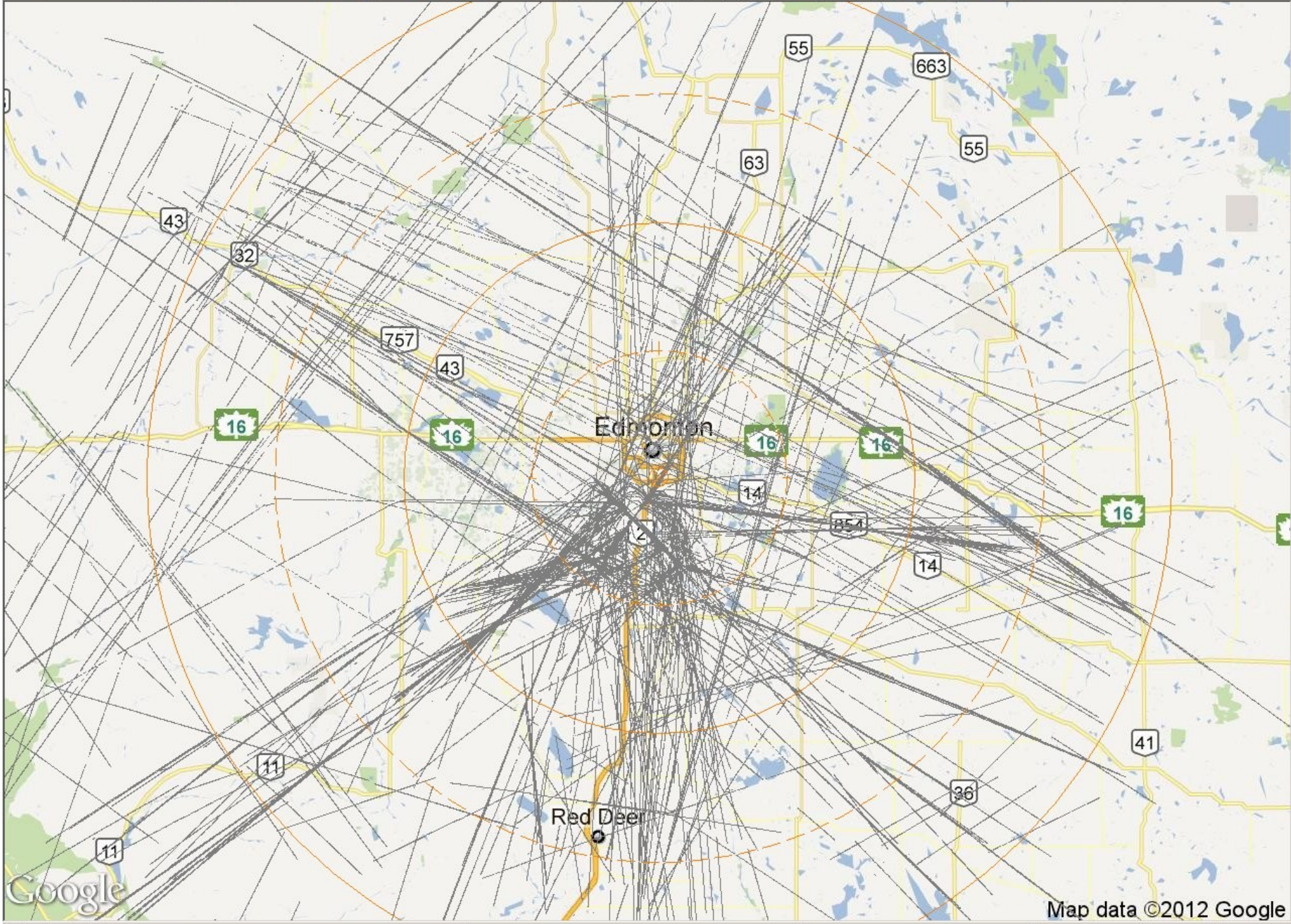
- ADS-B IN: Optional equipment can be installed in aircraft to listen to ADS-B out from planes and ATC
- Allows planes to be aware of each other without ATC intervention (TIS-B)
- Also allows for real time weather data (FIS-B)
- Situational awareness increases dramatically, allows more flights operate simultaneously
- Also works for ground equipment and taxiing aircraft
- Expensive!! \$5-10K for ADS-B out, \$20K for ADS-B In
- GA market getting cheaper though
- Not a lot of used market yet (problem for researchers)

Scary Stuff

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

And Now The Scary Part

- ADS-B is unencrypted and unauthenticated
- Anyone can listen to 1090Mhz and decode the transmissions from aircraft in real time
- Simple Pulse Per Second modulated
- No data level authentication of data from aircraft, just simple checksums
- Some correlation of primary radar sighting to received data (changing to Multilateration, More on that later)
- I am running a ground station at home, monitoring all traffic in and out of Edmonton



Others

- Others have begun to look and to question
- Richter Kunkel, Defcon 18
- Balint Seeber, spench.net – SDR research
- USAF Major Donald L. McCallie – Graduate research project
- Nick Foster – SDR and radio enthusiast
- No one has come up with solid security answers in several years of research

Why This Matters

- Largely a N. America problem but being utilized all over the world, adopted wider yearly
- UPS equipped all of their fleet
- 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
- A multitude of threat vectors to look at

ADS-B Out Threat #1

- Eavesdropping: Easily capture cleartext data of air traffic
- Data mining potential; We know whats in the air and when
- See the talk after mine: Busting the BARR: Tracking “Untrackable” Private Aircraft for Fun & Profit
- They will go more into it

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
- Generally cause confusion at inopportune moments (weather, Holidays, major travel hubs, Olympics)
- Create regular false flights, train the system (smugglers)
- Some documentation discussing Multilateration, nothing denoting its mandatory use

ADS-B Out Threat #3

- Jamming: Outright Jam ATC reception of ADS-B signals
- Could be detected and DF'd quickly, but are facilities available for that?
- Proper target location and timing could cause mass chaos (London Olympics?)
- Co-ordinated jamming across many travel hubs? Accidental or intentional?
- Simple frequency congestion already a problem, no contention protocol

ADS-B In Threat #1

- Injection: Inject data into aircraft ADS-B In displays
- Inject confusing, impossible, scary types of traffic to illicit a response
- Introduce conflicting data between ATC and cockpit displays
- Autopilot systems using ADS-B In data for collision avoidance?
- Aircraft have no source for multilateration

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

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
- Already shown to be able to screw with US drones recently (sub ~\$1000)

ADS-B Unknown Threats

- Some threats are total unknowns. The ATC system is huge and hard to parse from public docs
- What about injecting data for a flight on the west coast, into a ground station on the east coast?
- Has anyone fuzzed a 747 or a control tower? Buffer overflow at 36,000 feet?
- Look into Chris Roberts of One World Labs work on embedded control systems on planes, ships, cars, etc. Mix in ADS-B.....Scary stuff.
- Verification of ADS-B chip level code. Could be used as a control channel?

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 rulemaking 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? Why not threats of tomorrow? Why not threats we have'nt thought of yet?

ADS-B Threat Mitigation

- Multilateration; time differential between signal receiving stations
- Provides correlation that ADS-B data matches signal source
- No indication this will be used everywhere
- What about if the data doesn't match?
- How does the ATC UI indicate a mismatch?
- Liability issues for ATC equipment vendors ignoring data?

ADS-B Threats

- Basically reponse is; “Trust Us”
- Second time I ran across this excuse. Last time was RFID passports (look how that turned out)
- I dont 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 existing threat mitigation technology
- Also want to see disclosure of procedures for 'weird crap'
- Hackers looking at ATC will get a response

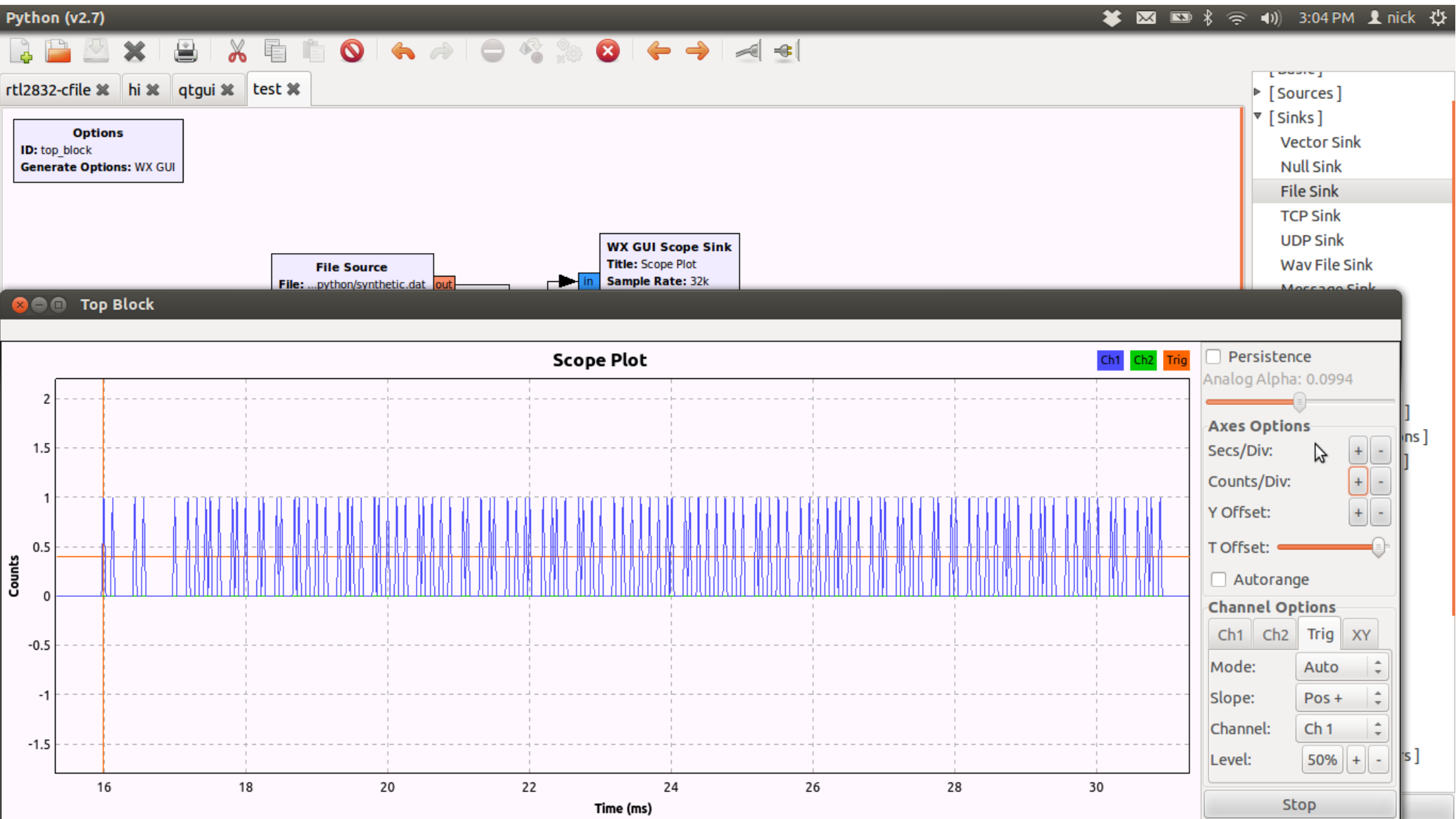
ADS-B Threats

- A common response will be 'It's too expensive for the common man”
- ~\$20 USB TV tuner can be made into a software defined radio and used to receive ADS-B
- Helping Dragorn get cheap receivers working on Kismet and ADS-B support (wardriving for aircraft!)

ADS-B Threats

- Got word while in the air en route to Poland
- Nick Foster implemented ADS-B Out on Gnu Radio
- A synthetic report generated and decoded by the Gnuradio ADS-B receiver: (-1 0.00000000000) Type 17 subtype 05 (position report) from abcdef at (37.123444, -122.123439) (48.84 @ 154) at 30000ft
- Honeymoon is over, exploit #1 is here

ADS-B Out Gnu Radio



ADS-B Threats

- Nick Foster raised his game
- ADS-B In on Flightgear (OSS Flight sim) populates sim environment with real planes
- ADS-B data generated by your virtual plane, fed into GNU radio and put out over the real air
- Your virtual world is now transmitting into the real world.
- Output now pseudo-matches a real planes behaviour
- Flightgear also has an intercept course feature

ADS-B Threats

- Plan is to release the software
- Need to run past the EFF first to make sure we don't get shot, disappeared, etc
- We have the capability to generate arbitrary packets, anyone else could easily do this
- All testing was at 900Mhz ISM band
- Easy to adjust for UAT ADS-B for GA
- The next guys might not be so nice

Other Threats

- Autopilot integration of ADS-B
- Collision avoidance systems
- Tailored approach (ATC upload landing plan to aircraft)
- Aircraft are huge, complex systems
- Reading on one system leads you to many others

Future

- ADS-B will be mandatory by 2020
- Europe delaying till 2030
- Already in use in N. America, Europe, China, Australia
- Even if not in use at airports, equipped planes are flying overhead
- Still time to develop countermeasures (don't turn off primary radar!)
- 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

Suggested Reading

- <https://federalregister.gov/a/2010-19809> - FAA Rulemaking on ADS-B
- <http://www.hsdl.org/?abstract&did=697737> - USAF graduate research project on ADS-B Vulnerabilities
- <http://www.radartutorial.eu> - Good overview of radar tech and ADS-B format
- http://www.oig.dot.gov/sites/dot/files/ADS-B_Oct%202010.pdf - OIG report on other risks to ADS-B

Conclusion

- This is pretty scary to consider
- How many people want to take the bus home?
- We should all be working on finding and solving problems like this
- If I can find this stuff, so can bad guys
- Significant investment has been made already
- I want to hear your comments and your ideas on further threats and research. Lets work on this together!

Thanks - Questions

Please Prove Me Wrong!
I will post responses if I am wrong!

Email: render@renderlab.net

Twitter: [@ihackedwhat](https://twitter.com/ihackedwhat)

Website: www.renderlab.net