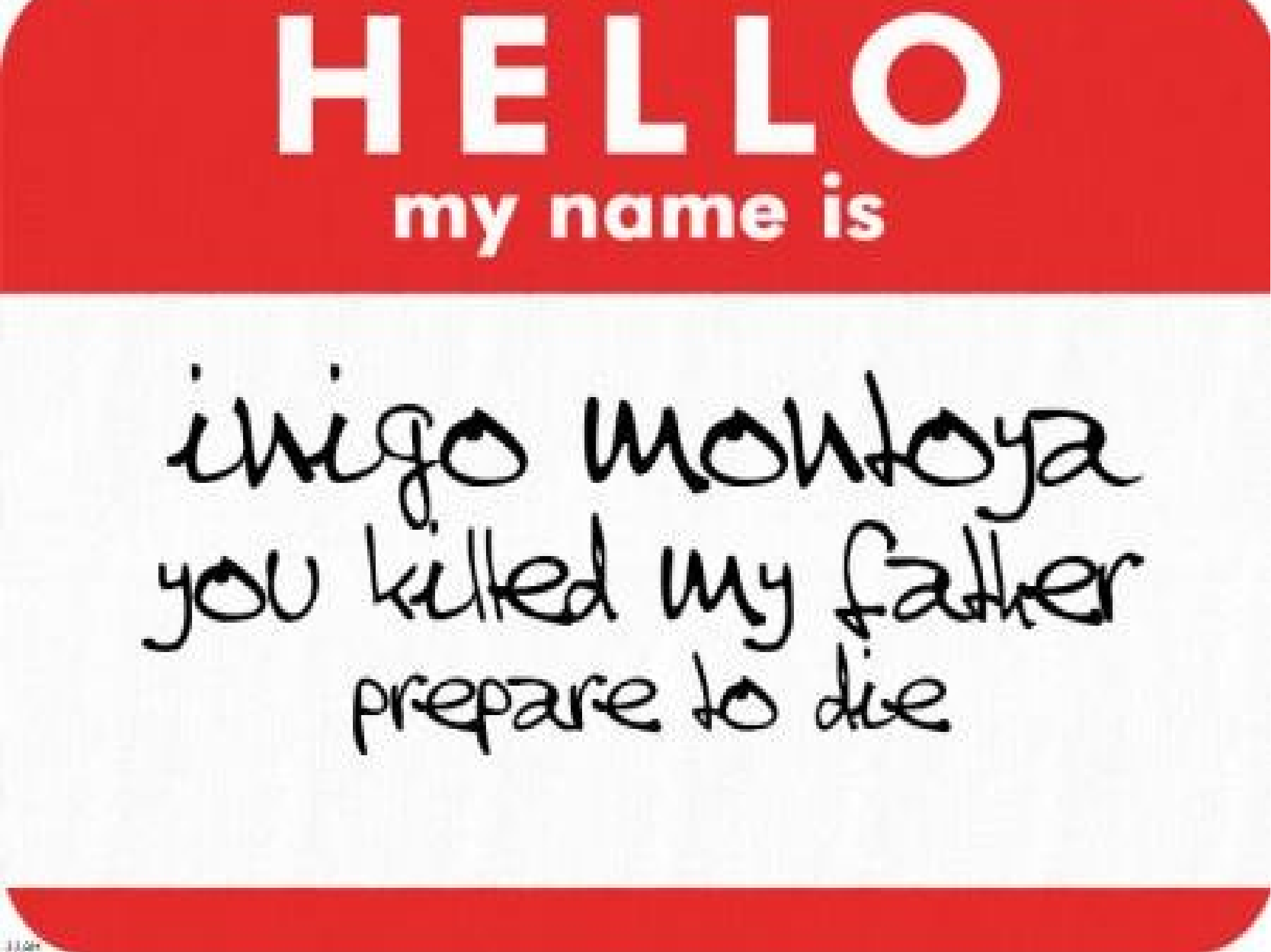
+

=

Hackers + Airplanes

No Good Can Come Of This

Confidence 2012
Brad “RenderMan” Haines, CISSP
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?

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

Frequent Speaker World Wide, 4th time at CONfidence

Who Am I?


ConfidEncE
WAITING FOR RENDERMAN
SAMSUNG
CZYSTA
de Luxe
ŻOŁĄDKOWA
GORZKA
WYBÓROWA
LUKSUSOWA
FINLANDIA

Ass Covering

- For the love of Spongebob, do not actually try any of the ideas in this talk!!!
- 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

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

- IVR 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 and the focus of this talk

ADS-B

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

ADS-B Out

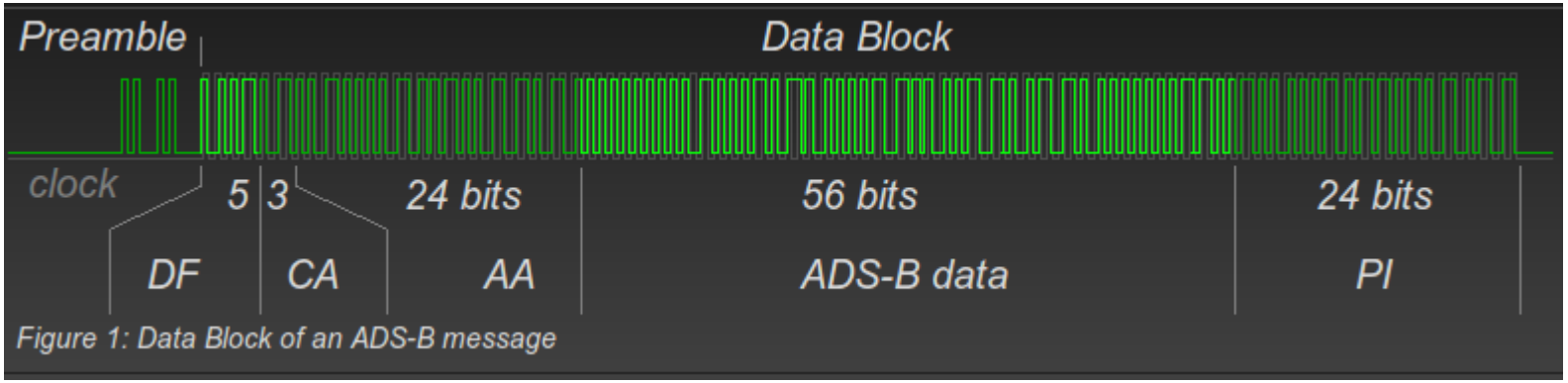
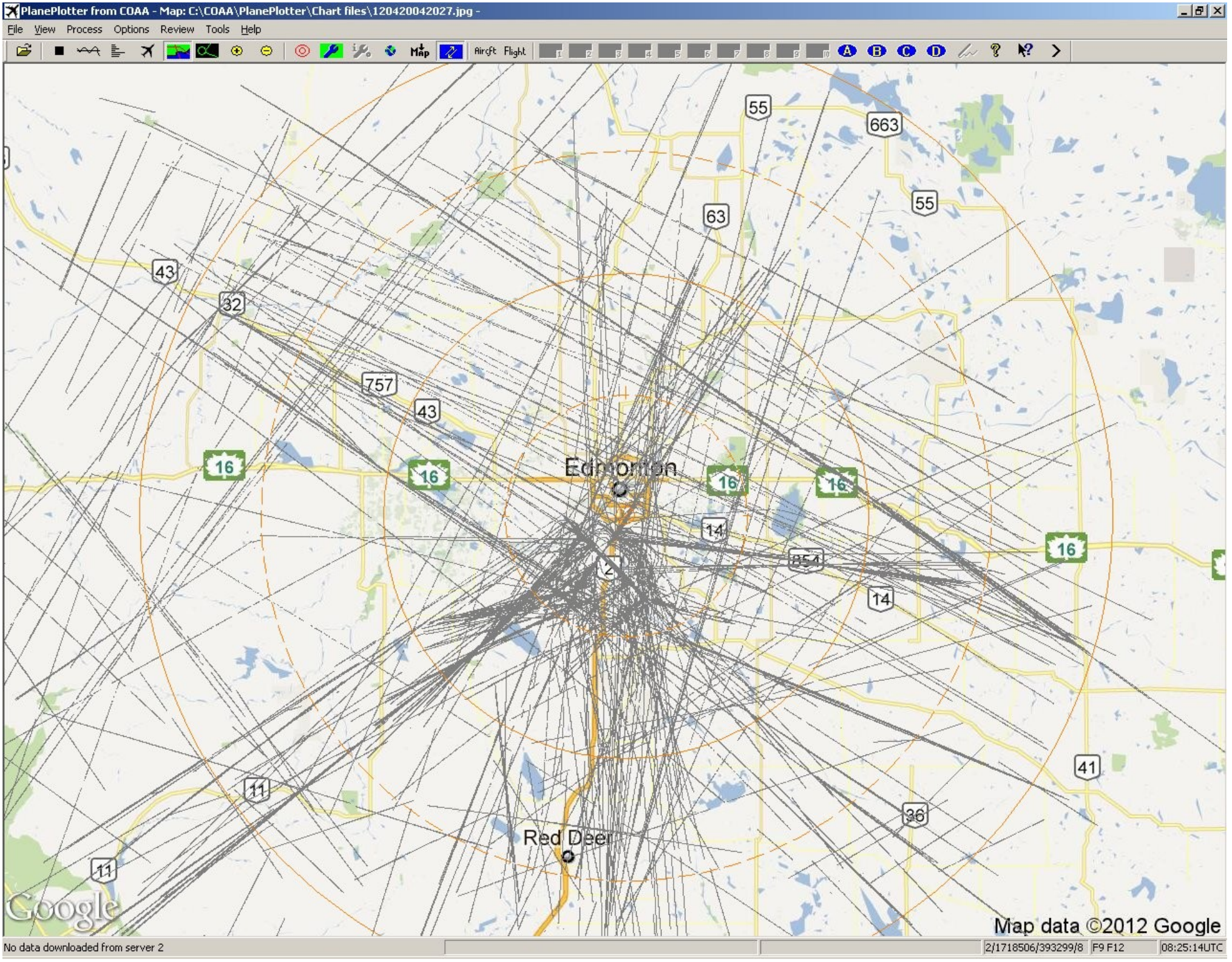


Figure 1: Data Block of an ADS-B message

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

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
- Not a lot of used market yet (problem for researchers)


PlanePlotter from COAA - Map: C:\COAA\PlanePlotter\Chart files\120420042027.jpg -
File View Process Options Review Tools Help
Aircft Flight
Edmonton
Red Deer
55
663
63
43
32
757
16
14
2
41
36
11
Google
Map data ©2012 Google
No data downloaded from server 2
2/1718506/393299/8
F9 F12
08:25:14UTC

Planefinder AR

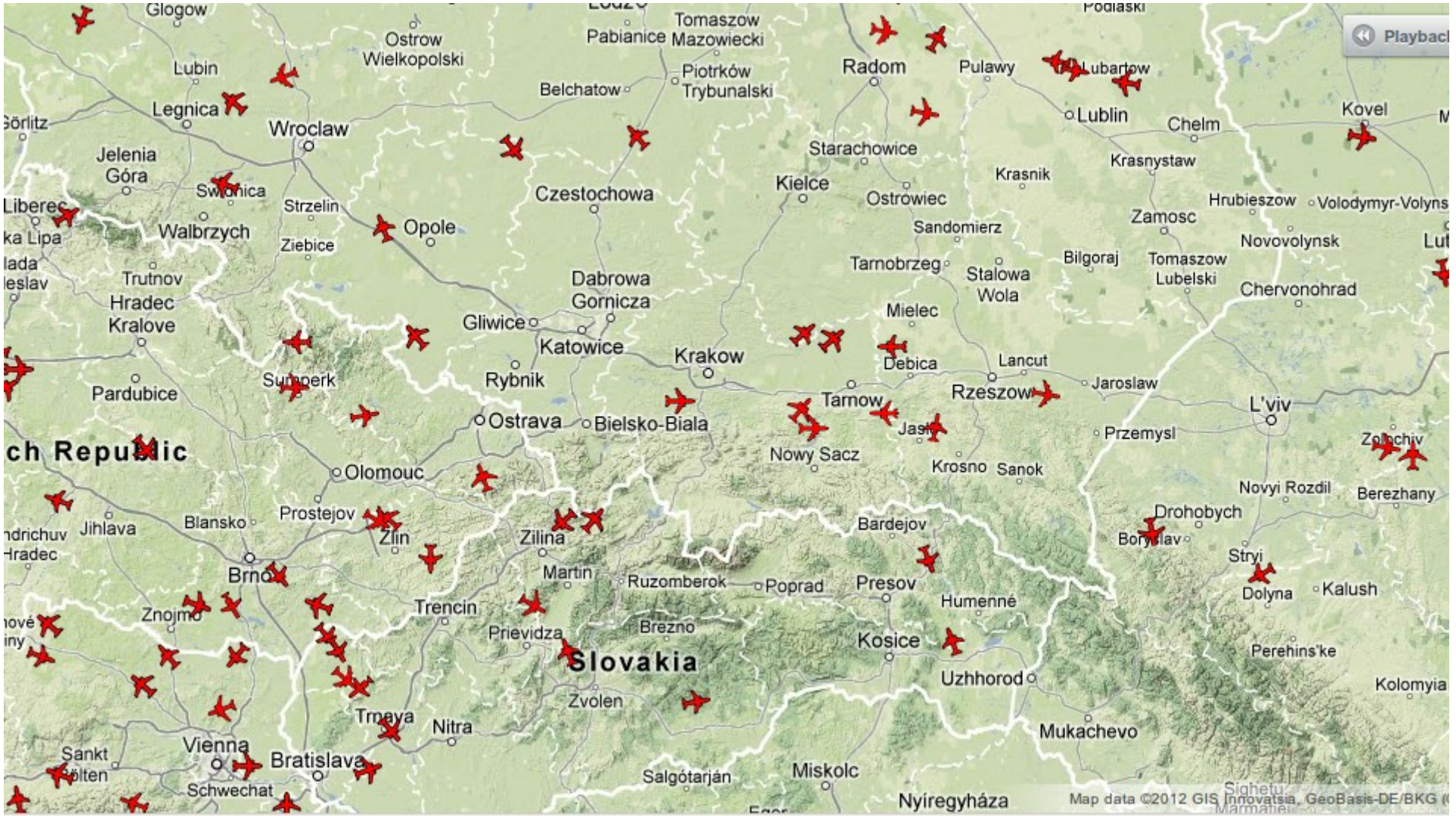
- I got interested purely by accident
- Bought in October 2010
- Overlays flight information through camera
- GPS location + Direction + web lookup of flights
- This is cool, how does it work?
- Huge world opened up of aircraft enthusiasts

Planefinder.net

- Planefinder.net
- 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

Planefinder.net

(and others)



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 (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
- Righter 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

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; Corporate jets, known passenger flights (celebs), general traffic patterns
- Combine with other stations and have your own, cheap ATC view of a country or continent
- FAA Block Aircraft Registration Request (BARR) – Block aircraft from FAA provided flight data feed
- We are watching the raw data. Correlate hidden flights to raw data, sell to TMZ or worse

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 one or many 'ghosts' into ATC
- Introduce slight variations in real flights
- Generally cause confusion at inopportune moments (weather, major travel hubs, Olympics)
- Create regular false flights, train the system (smugglers)

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

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?
- No ATC involvement, no radar fusion

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

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
- Very difficult to do outside of lab
- Iran may have used this technique to capture US drone
- May get easier with time

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 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?

ADS-B Threats

- Basically “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
- Hackers looking at ATC will get a response
- Also want disclosure of procedures for 'weird crap'

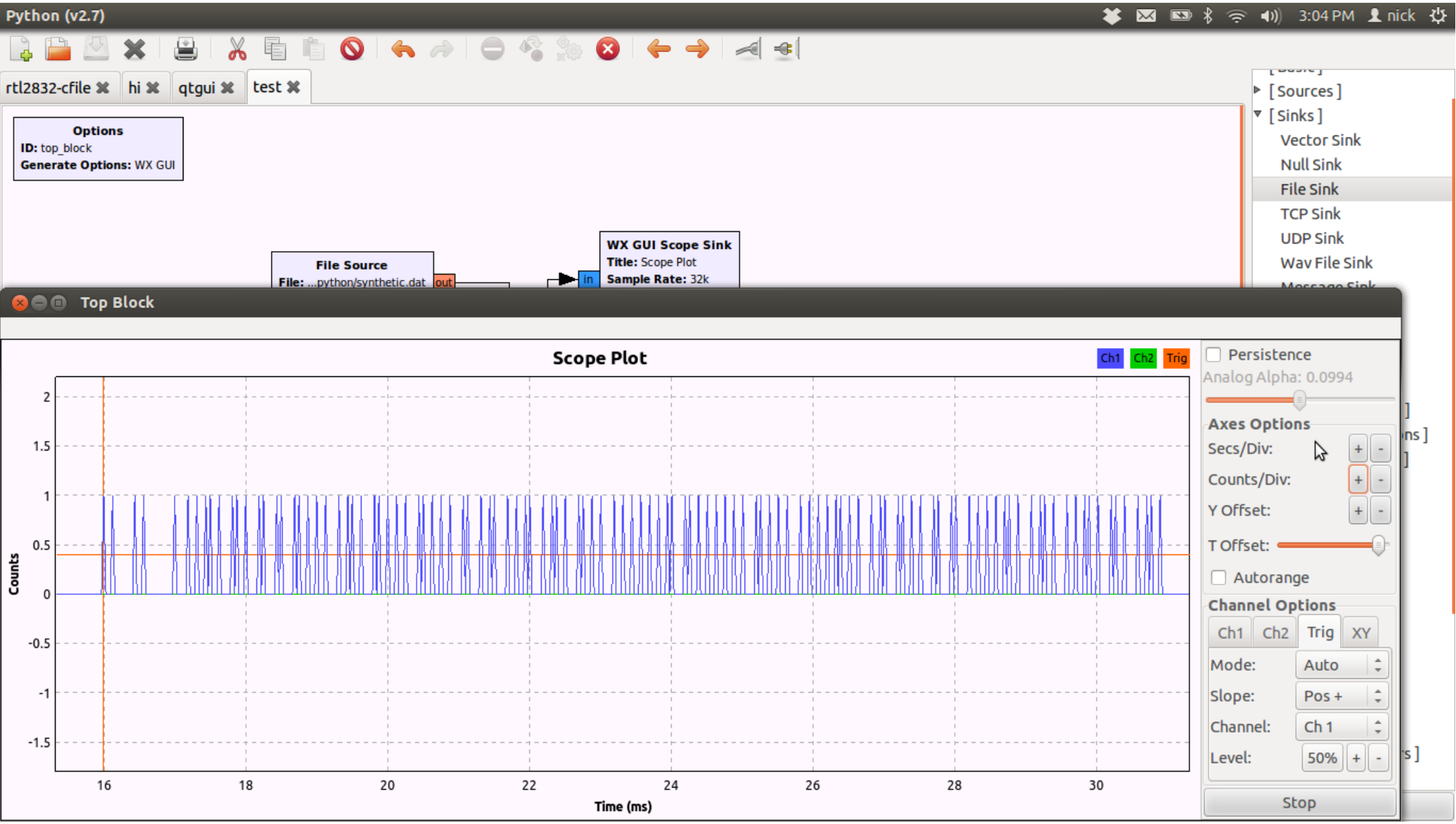
ADS-B Threat

- 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 coming here!
- Nick Foster has implemented ADS-B Out on 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”
- Other ADS-B protocols coming soon
- Honeymoon is over, exploit #1 is here

ADS-B Out Gnu Radio



ADS-B Threats

- Plan is to release the software
- Need to run past the EFF first to make sure we don't get shot
- We have the capability to generate arbitrary packets, anyone else could do this
- We at least looking to access a safe target, rather than something 'live'
- The next guys might not be so nice

Future

- ADS-B will be mandatory by 2020
- 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 access to a 747 or similar and/or an air traffic control tower that I can hack away at, 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
- We should all be working on solving problems like this, I cant do it all
- Significant investment has been made already
- If anyone has a 747 or an airport I can borrow, talk to me afterwards
- I want to hear your comments and your ideas on further threats and research. Lets work on this together!

Thanks - Questions

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