You are not where you think you are

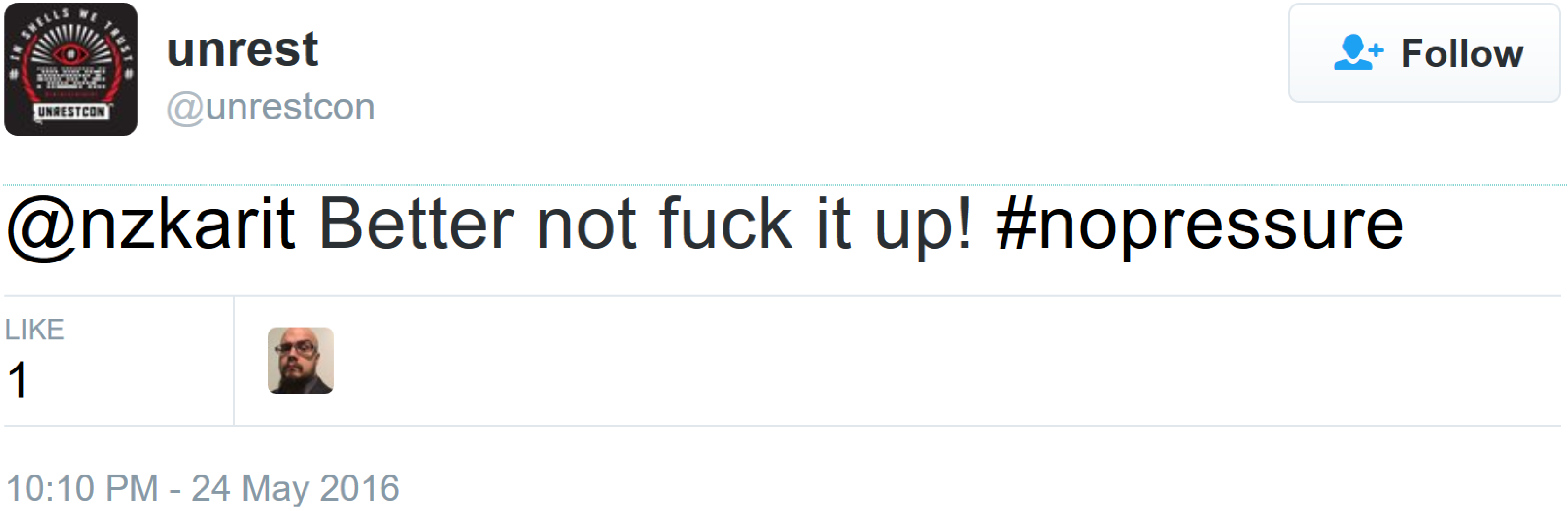
David Robinson/Karit (@nzkarit) – ZX Security

Unrestcon 2016

whoami

- Dave Robinson, Karit, @nzkarit
- Security Consultant/Pen Tester at ZX Security
- Enjoy radio stuff
- Pick Locks and other physical stuff at Locksport

Clear Guidelines for this Talk



unrest
@unrestcon

@nzkarit Better not fuck it up! #nopressure

LIKE
1

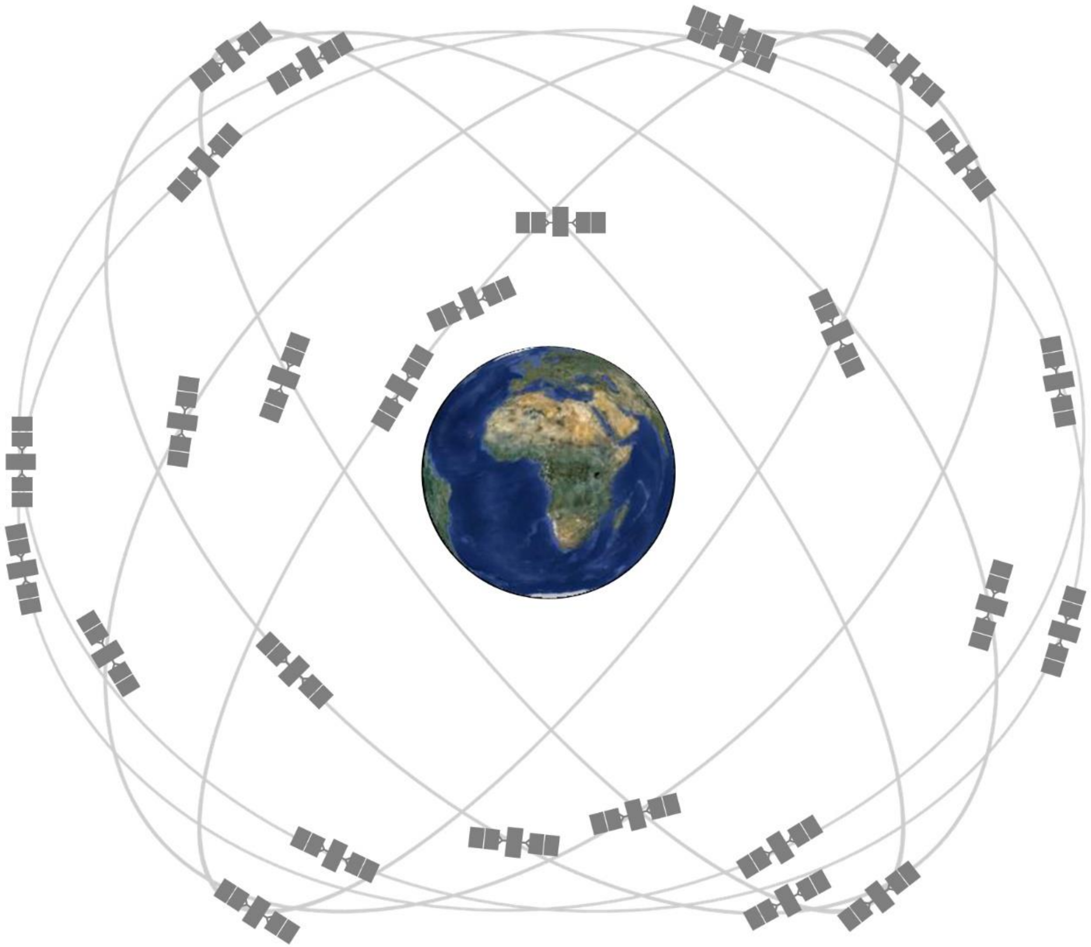
10:10 PM - 24 May 2016

Today

- GPS (Global Positioning System)
- GPS Spoofing on the cheap
- So what?
- How to detect GPS Spoofing

GPS

- Tells us where we are
- Tells us the time



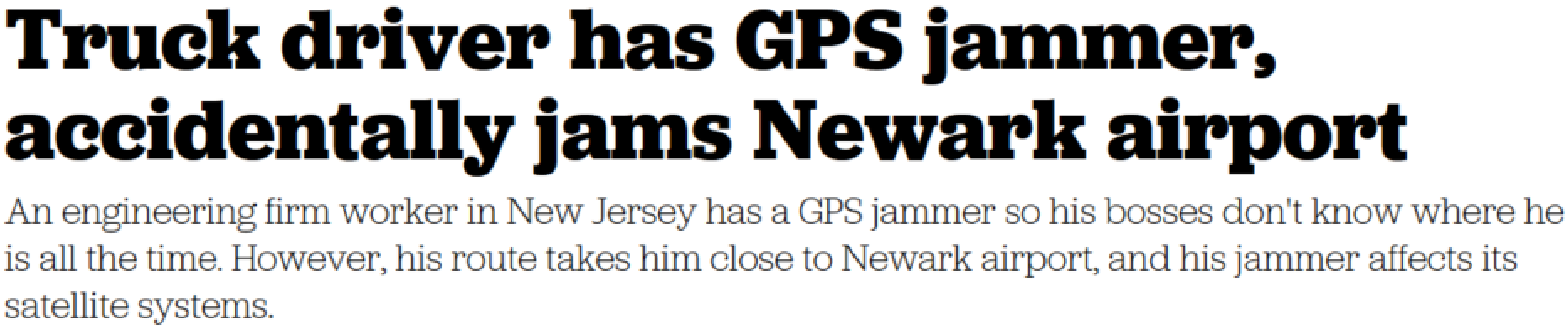
We Trust GPS Right? Right?????

- Anyone in the room not currently trust GPS locations?
- Anyone in the room not currently trust GPS time?

You have to trust it right?

- GPS too important to life?
- GPS must be great and robust? Right?
- Important services rely on it:
  - Uber
  - Tinder
- Also some other things:
  - NTP Time Source
  - Plane Location
  - Ship Location
  - Tracking Armoured Vans
  - Taxi law in NZ no longer knowledge requirement

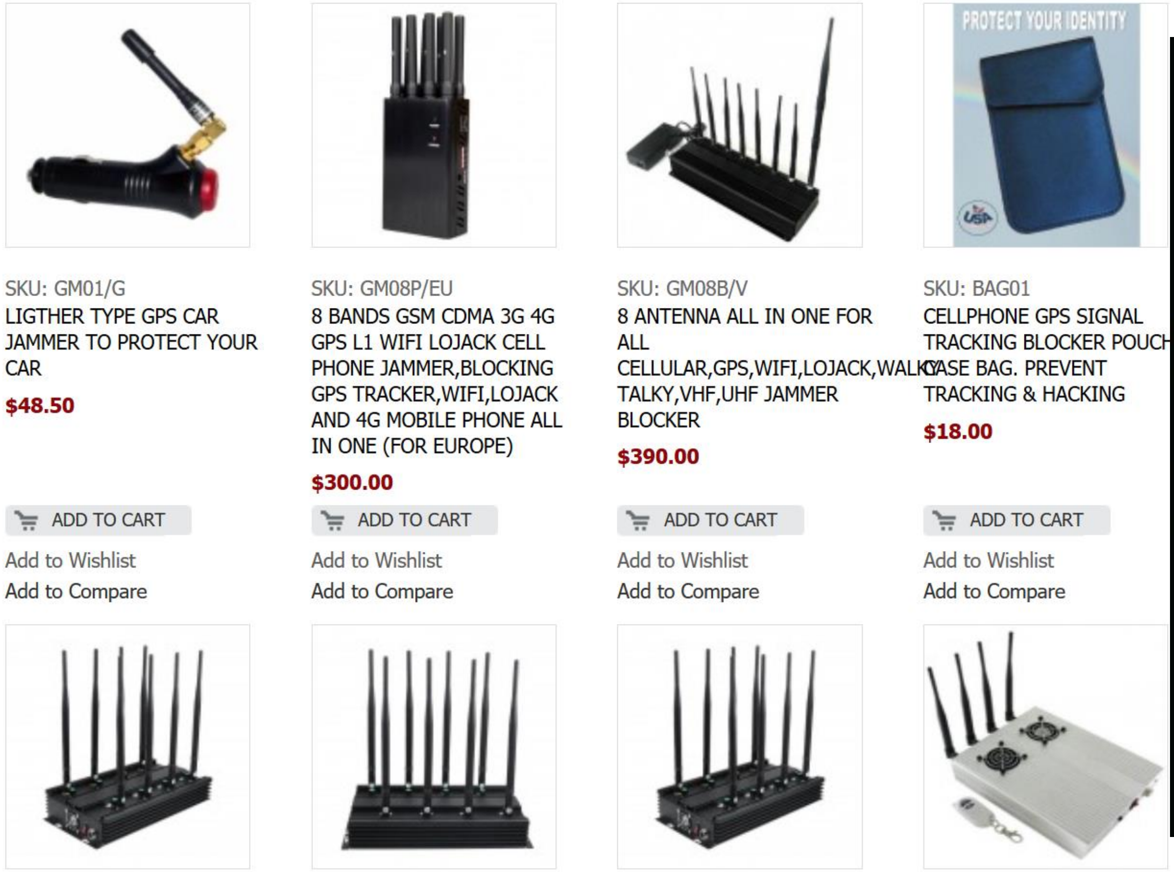
So why don’t I trust it?



Truck driver has GPS jammer, accidentally jams Newark airport

An engineering firm worker in New Jersey has a GPS jammer so his bosses don't know where he is all the time. However, his route takes him close to Newark airport, and his jammer affects its satellite systems.

Jammers Boring………

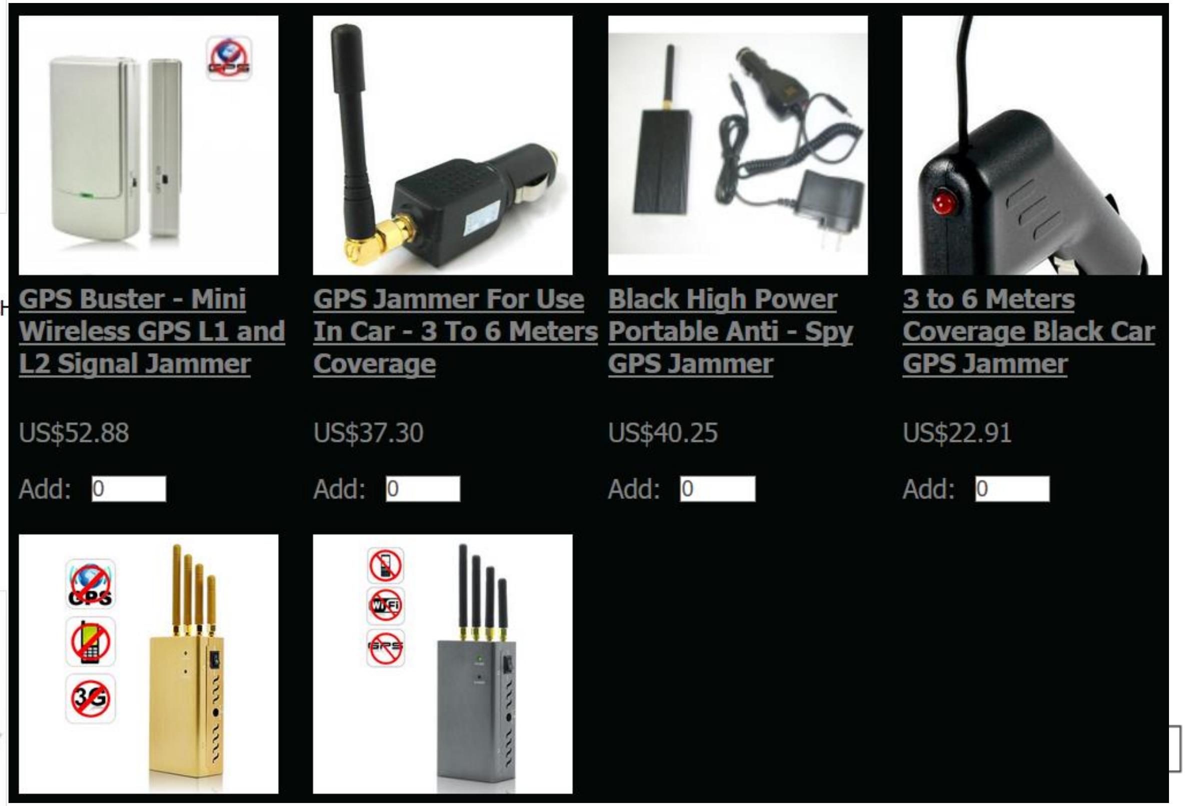


SKU: GM01/G
LIGTHER TYPE GPS CAR JAMMER TO PROTECT YOUR CAR
$48.50
ADD TO CART
Add to Wishlist
Add to Compare

SKU: GM08P/EU
8 BANDS GSM CDMA 3G 4G GPS L1 WIFI LOJACK CELL PHONE JAMMER,BLOCKING GPS TRACKER,WIFI,LOJACK AND 4G MOBILE PHONE ALL IN ONE (FOR EUROPE)
$300.00
ADD TO CART
Add to Wishlist
Add to Compare

SKU: GM08B/V
8 ANTENNA ALL IN ONE FOR ALL CELLULAR,GPS,WIFI,LOJACK,WALKY TALKY,VHF,UHF JAMMER BLOCKER
$390.00
ADD TO CART
Add to Wishlist
Add to Compare

SKU: BAG01
CELLPHONE GPS SIGNAL TRACKING BLOCKER POUCH CASE BAG. PREVENT TRACKING & HACKING
$18.00
ADD TO CART
Add to Wishlist
Add to Compare



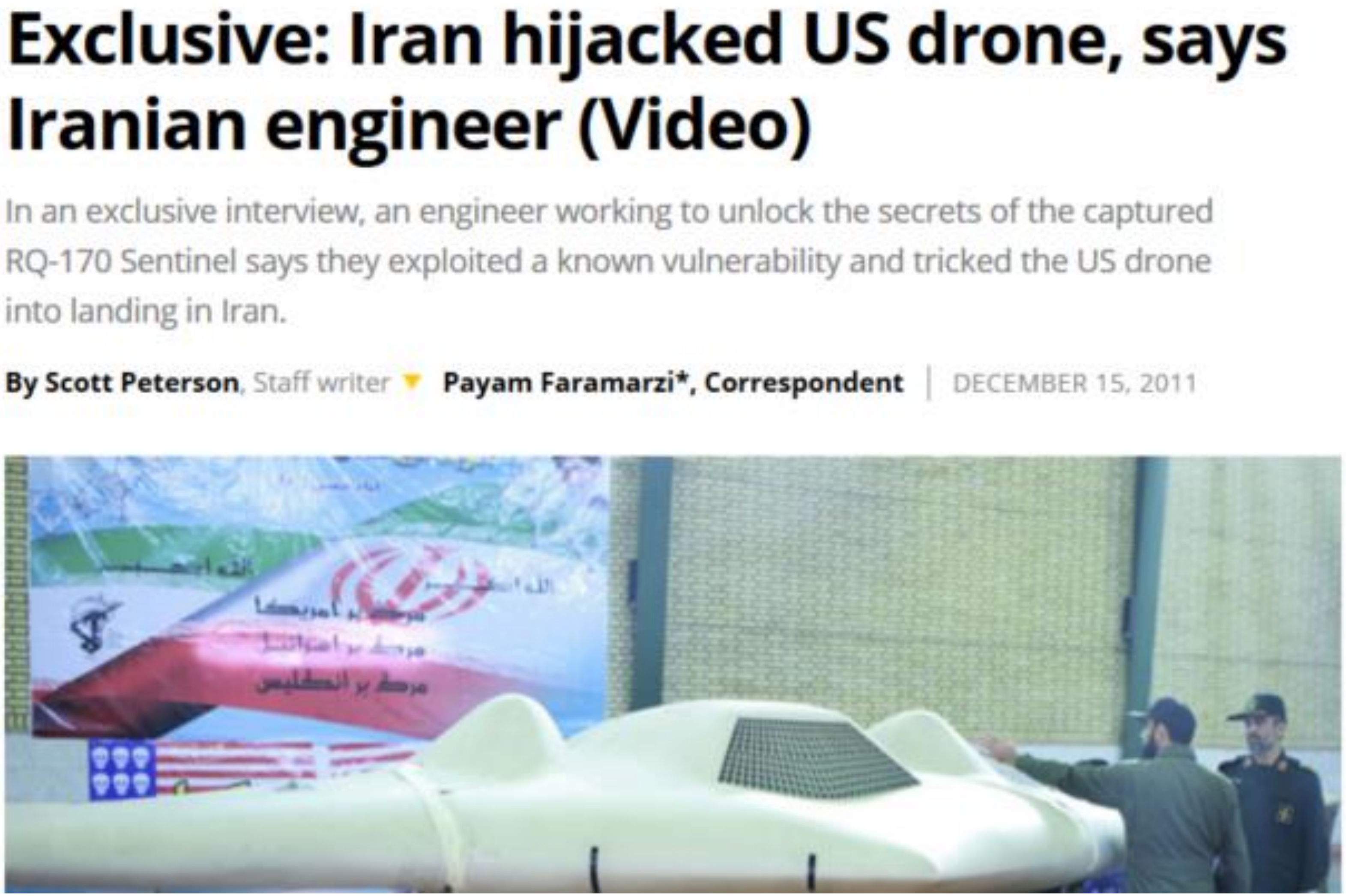
GPS Buster - Mini Wireless GPS L1 and L2 Signal Jammer
US$52.88
Add: 0

GPS Jammer For Use In Car - 3 To 6 Meters Coverage
US$37.30
Add: 0

Black High Power Portable Anti - Spy GPS Jammer
US$40.25
Add: 0

3 to 6 Meters Coverage Black Car GPS Jammer
US$22.91
Add: 0

Nation State

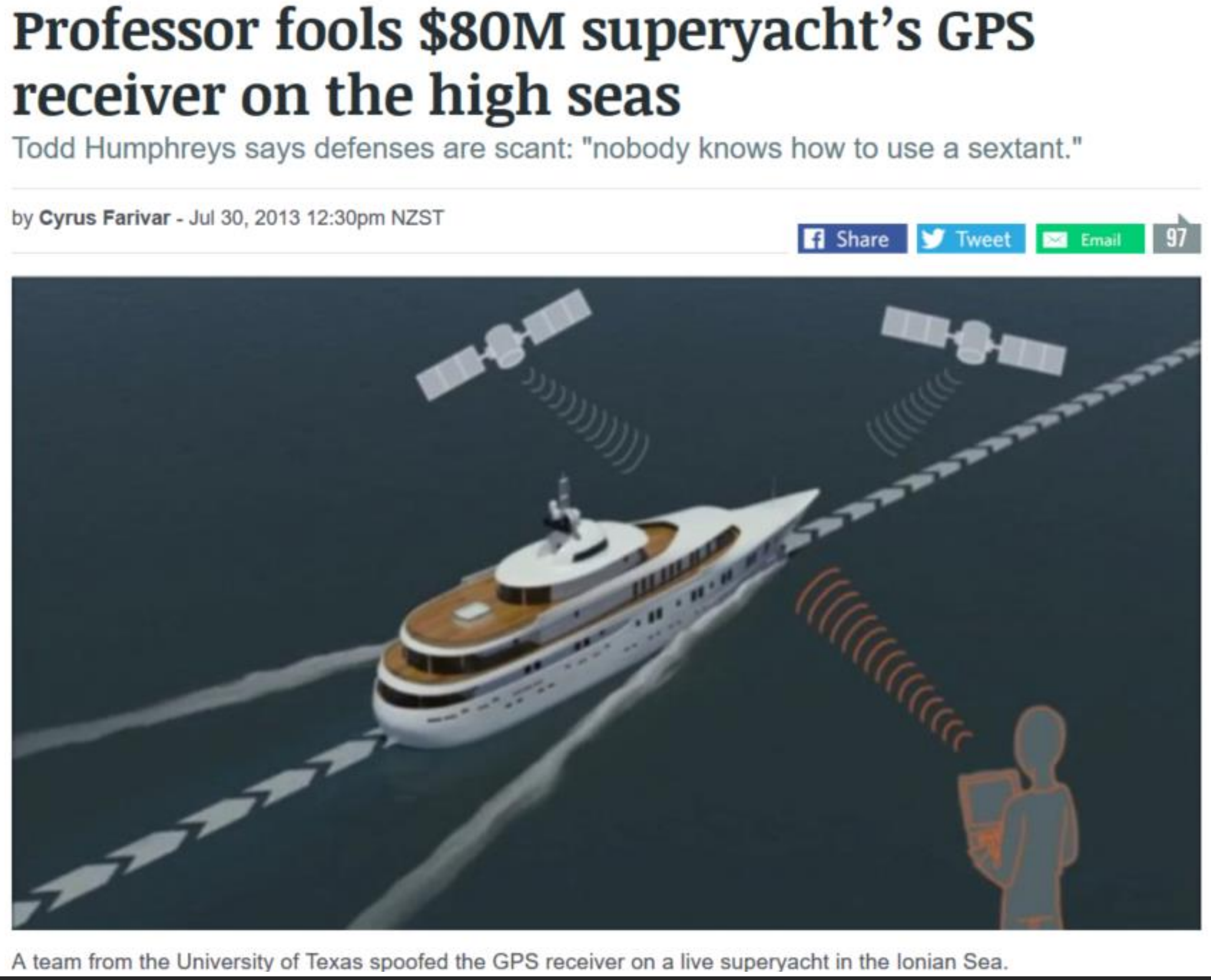


Exclusive: Iran hijacked US drone, says Iranian engineer (Video)

In an exclusive interview, an engineer working to unlock the secrets of the captured RQ-170 Sentinel says they exploited a known vulnerability and tricked the US drone into landing in Iran.

By Scott Peterson, Staff writer ▼ **Payam Faramarzi*, Correspondent** | DECEMBER 15, 2011

A University



Professor fools $80M superyacht’s GPS receiver on the high seas

Todd Humphreys says defenses are scant: "nobody knows how to use a sextant."

by **Cyrus Farivar** - Jul 30, 2013 12:30pm NZST

A team from the University of Texas spoofed the GPS receiver on a live superyacht in the Ionian Sea.

The Chinese are in the NTPs

Time is on my side

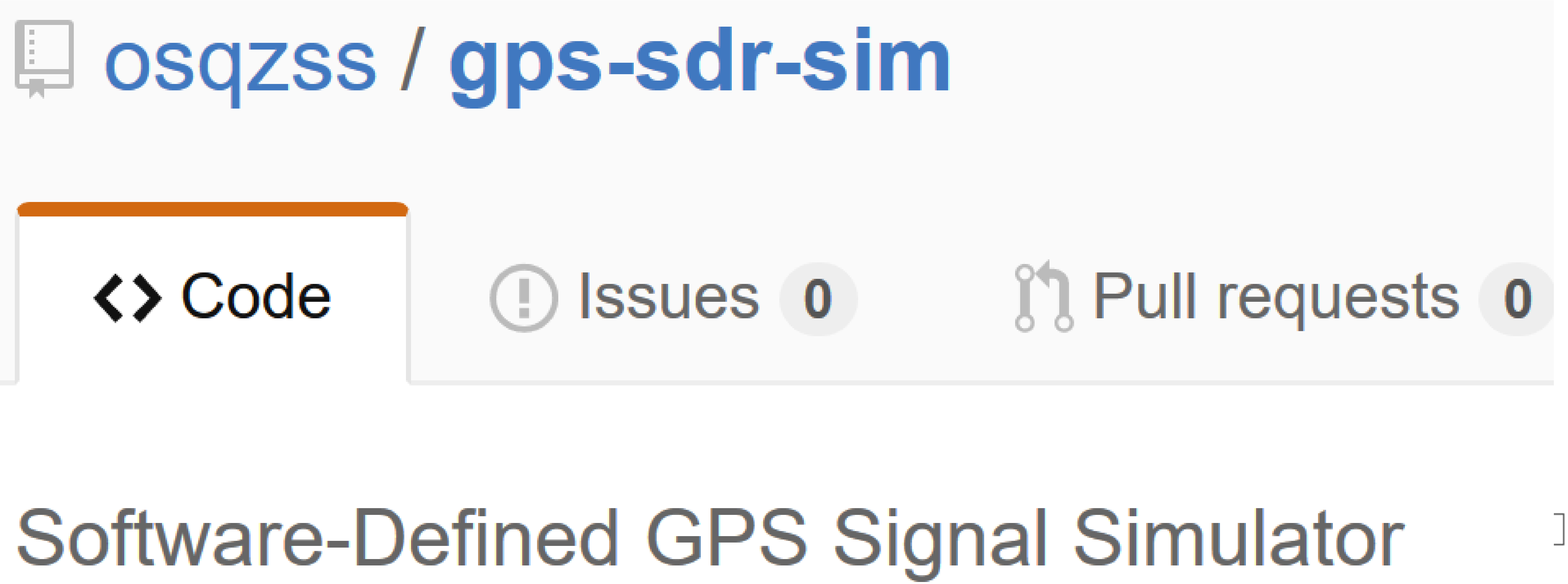
Forging Wireless Timing Signals to Attack the NTP Server

Yuwei Zheng @HITB
Haoqi Shan @HITB
From: Qihoo360 Unicorn Team

Time is on my side

HITB
360UNICORNTEAM

Now we are talking



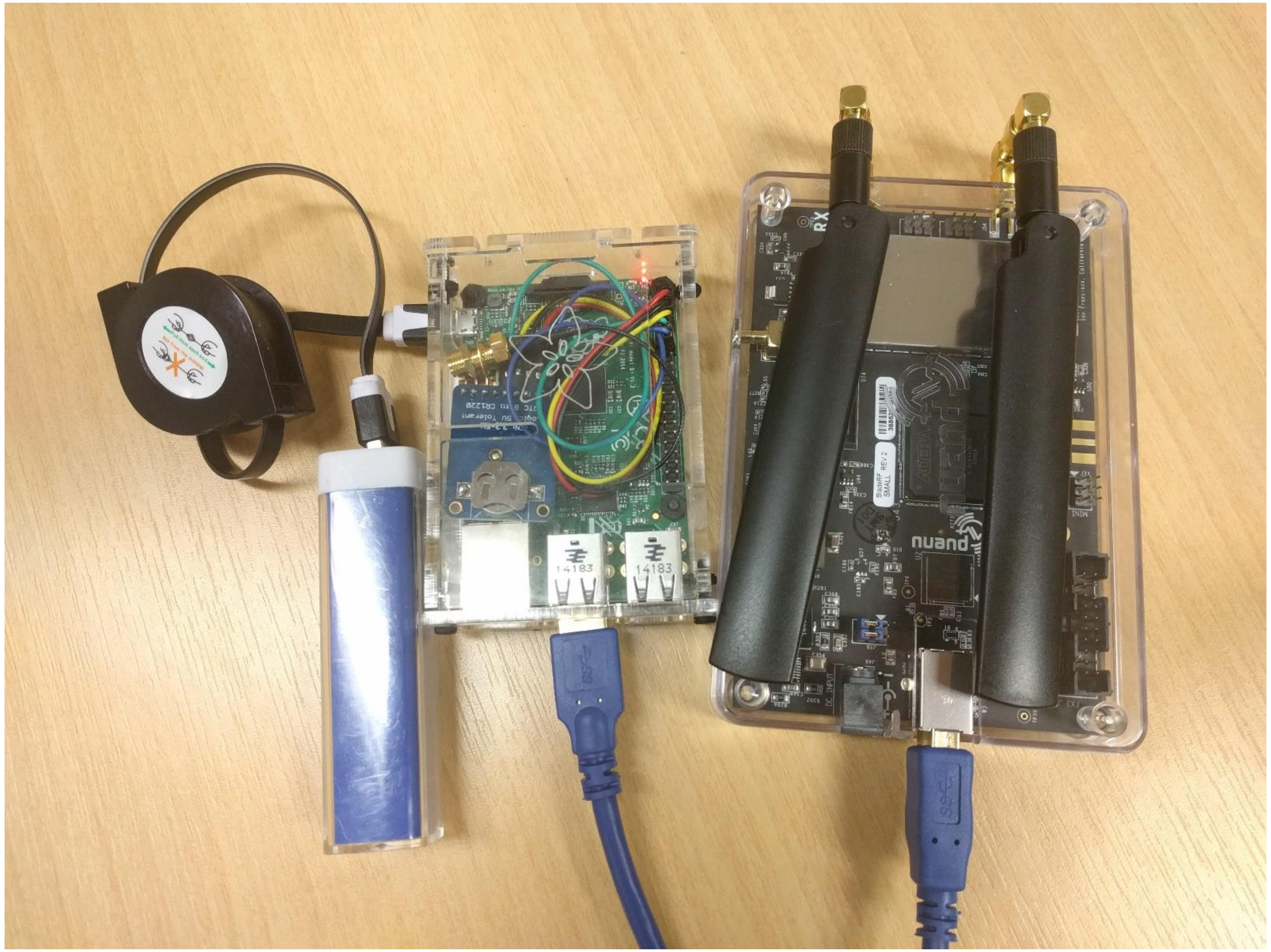
osqzss / gps-sdr-sim

Software-Defined GPS Signal Simulator

What we need

- A box
- An SDR with TX
  - I used a BladeRF
  - HackRF in theory works but need external clock source
    - Internal clock not stable enough
  - USRP someone want to buy me one to check???
- So US$420 in hardware
- Also some aluminium foil to make a Faraday Cage
- So it is now party trick simple and cheap
  - This is the big game changer from the past

Setup



@amm0nra patented Faraday Cage

- Make sure you measure signal outside to ensure none is leaking
- Be careful

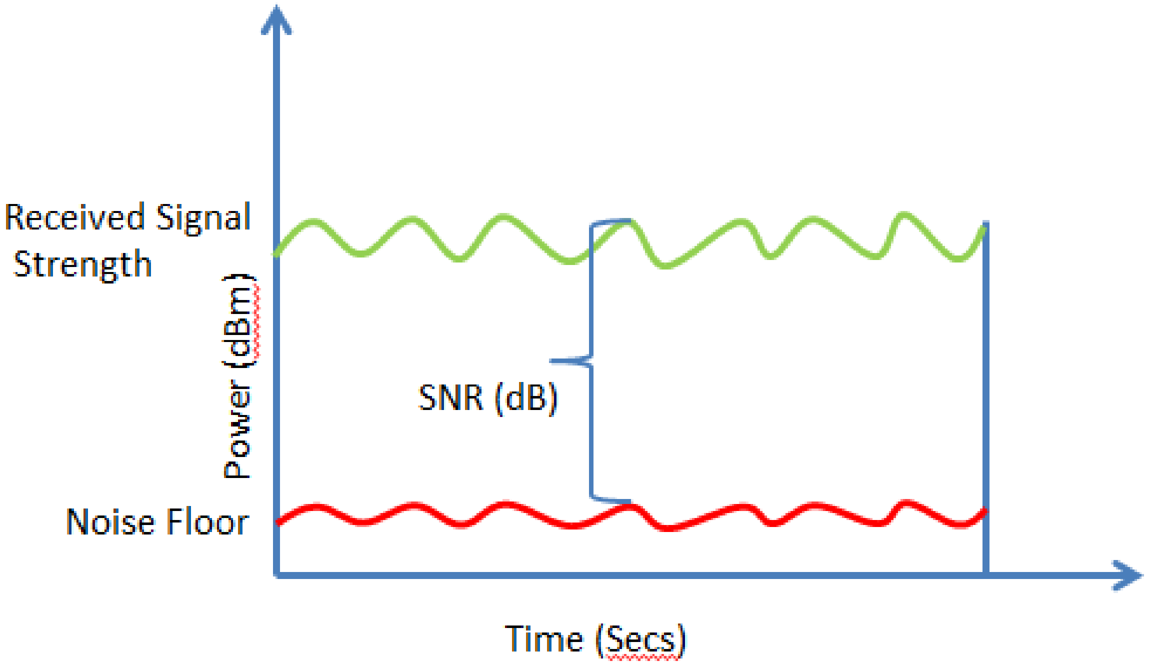
The Law

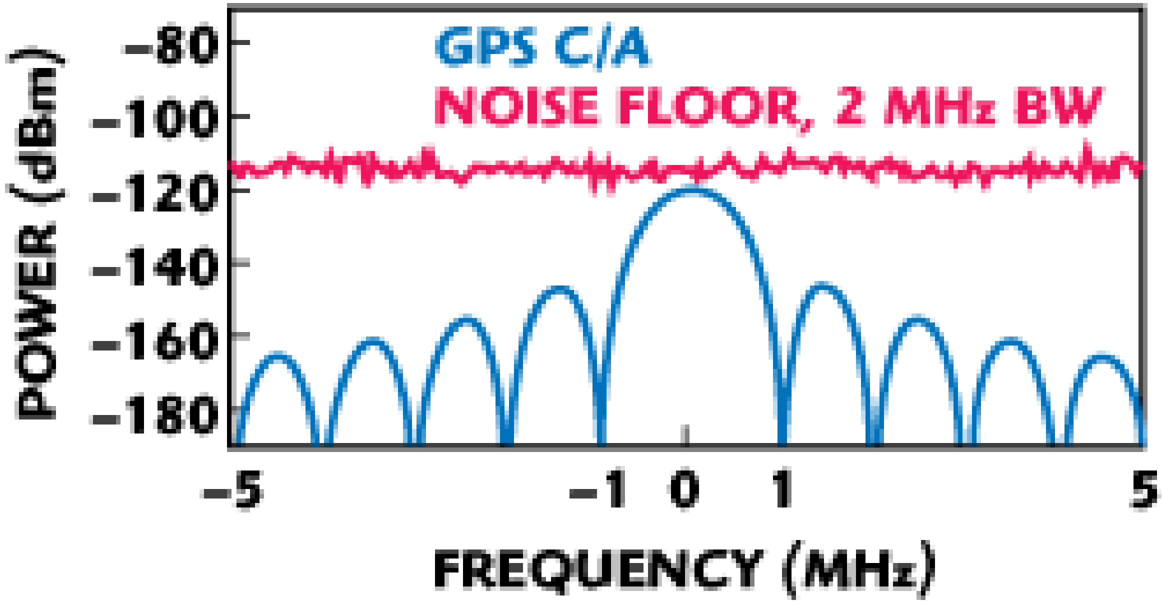
- INAL (I’m not a lawyer)
- GPS isn’t Open Spectrum
- So Faraday Cage
  - Keep all the juicy GPS goodness to yourself

Remember

- Your SDR kit is going to be closer to the device
  - So much stronger signal
  - Got to have line of sight though
- GPS Orbits ~20,000 km
  - So signals weak
  - Signal is weaker than the noise floor

Noise Floor

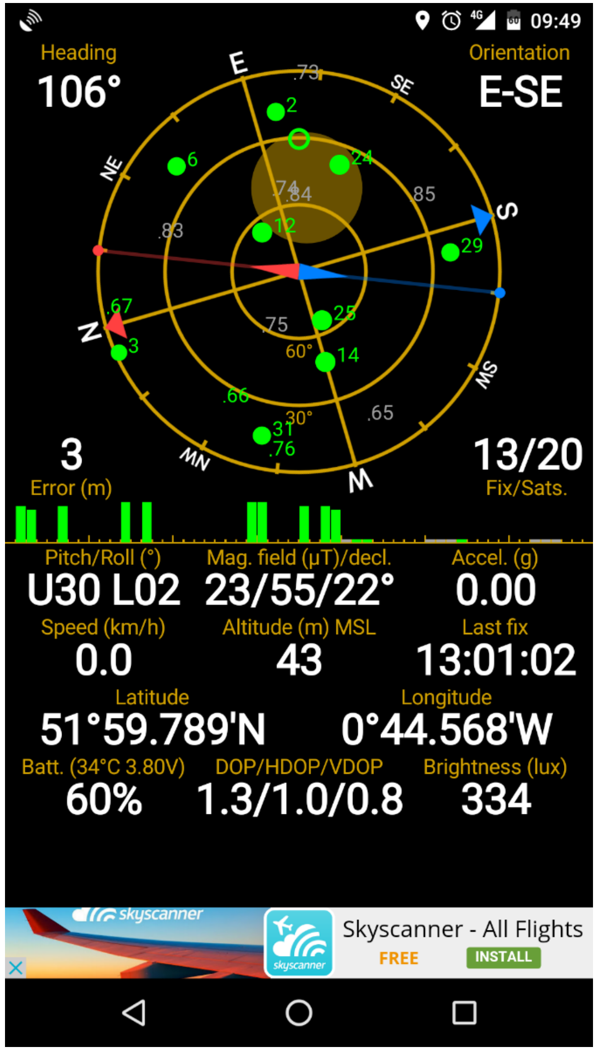

Received Signal Strength
Power (dBm)
SNR (dB)
Noise Floor
Time (Secs)


GPS C/A
NOISE FLOOR, 2 MHz BW
POWER (dBm)
−80
−100
−120
−140
−160
−180
−5
−1
0
1
5
FREQUENCY (MHz)

Right so what can we do?

- Got some simulator software and a bladeRF what could people get up to?

A trip to Bletchley Park?



09:49

Heading 106°

Orientation E-SE

3 Error (m)

13/20 Fix/Sats.

Pitch/Roll (°) U30 L02

Mag. field (µT)/decl. 23/55/22°

Accel. (g) 0.00

Speed (km/h) 0.0

Altitude (m) MSL 43

Last fix 13:01:02

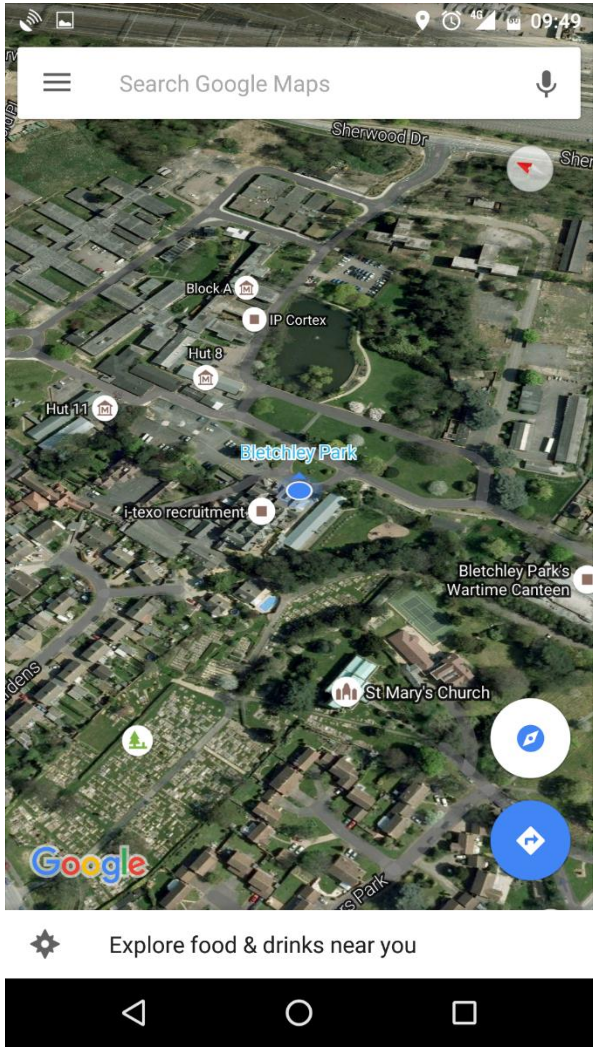
Latitude 51°59.789'N

Longitude 0°44.568'W

Batt. (34°C 3.80V) 60%

DOP/HDOP/VDOP 1.3/1.0/0.8

Brightness (lux) 334



09:49

Search Google Maps

Explore food & drinks near you

How does the tool work?

- Two Methods
- First one two steps
- 1. Generate the data for broadcast
  - About 1GB per minute
  - Static location or a series of locations to make a path
  - Has an Almanac file which has satellite locations
    - Need to get each day as is what GPS broadcast time is based off this (from NASA FTP Server)
  - Uses Almanac to select what satellites are required for that location at that time
- 2. Broadcast the data

How does the tool work?

- Generate in real time
- Need a fast enough computer
- 1. Generate and broadcast
- In author’s words this is an experimental feature

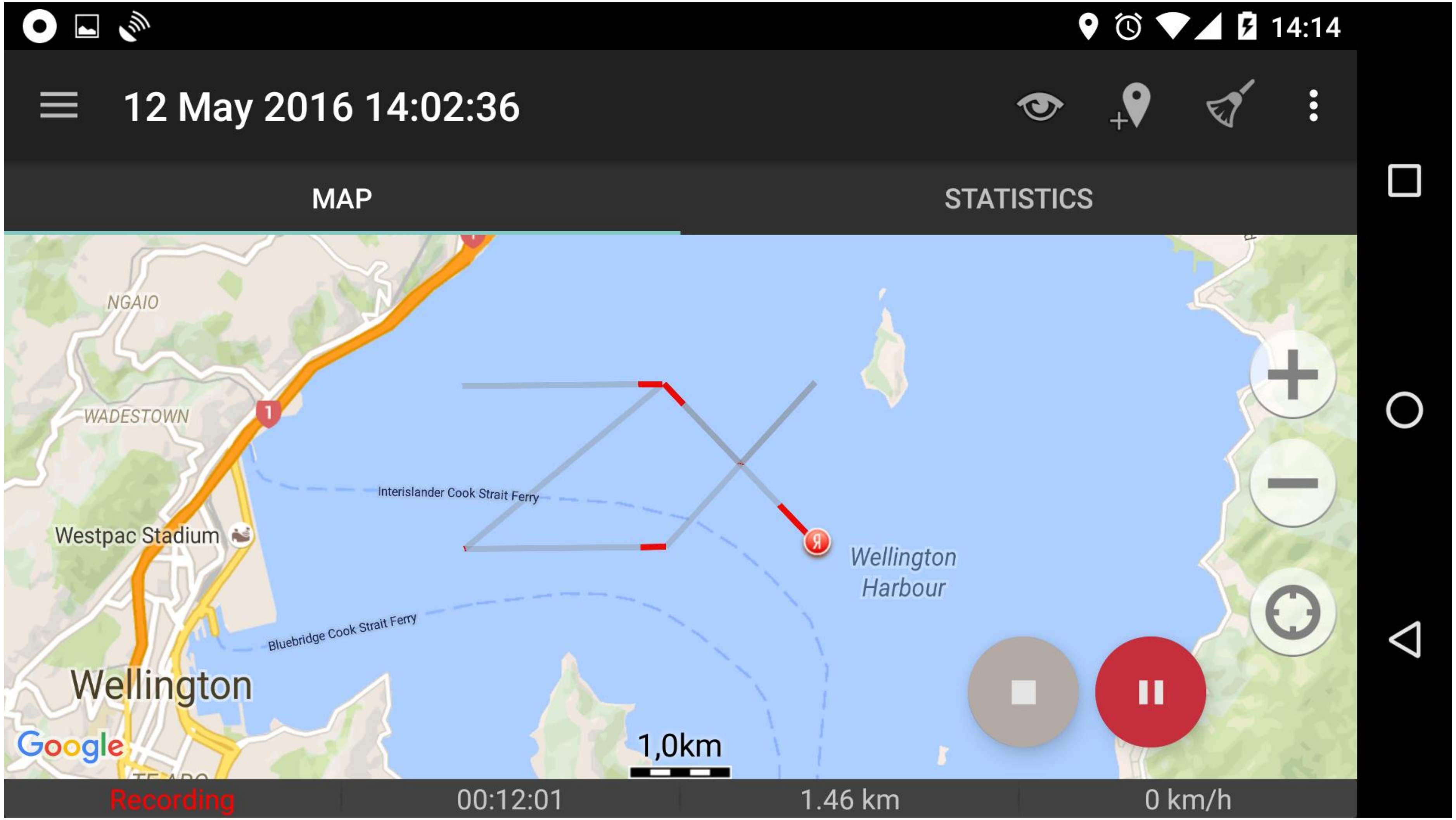
Limitations of tool

- Have to get almanac files each day
  - Else time will be for historic timestamp
- Can only do dates you have the almanac for
- By default only 5 mins of transmit data
  - Need to change a value in code for longer
  - Approx. 1GB a minute hence the limit
- Pi3 about three times slower than real, so not fast enough to real time must precompute
  - Pi3 there is a file size limit
    - <4GB from my experience, so 4-5 minutes of broadcast per file

Generate a Path

- To do the path give the generator a series of locations at 10Hz
- Can’t just give a series of lat/long in a csv ☹
  - ECEF Vectors or
  - NMEA Data rows

A Path



12 May 2016 14:02:36

MAP | STATISTICS

Recording | 00:12:01 | 1.46 km | 0 km/h

What are the Impacts? Location

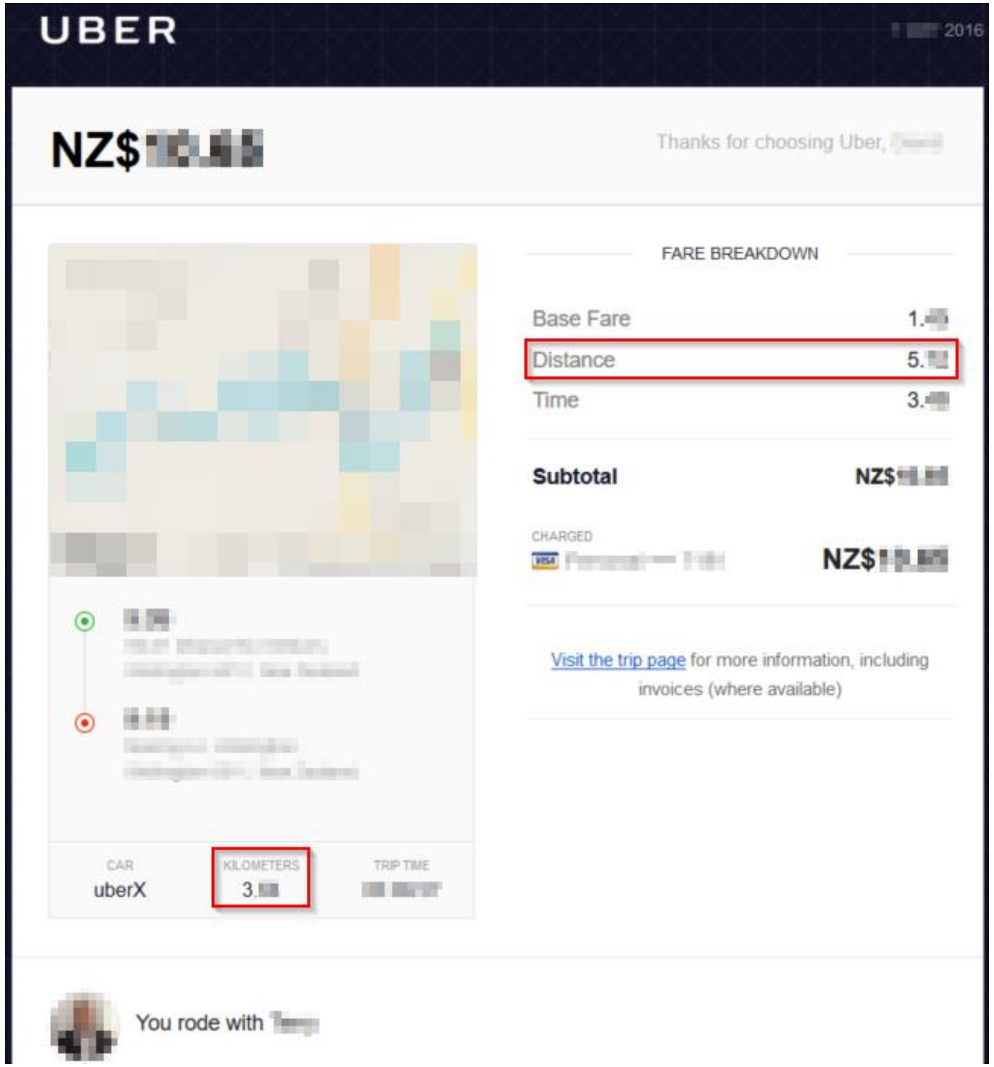
- What are the impacts of GPS spoofing being so simple?
- Sit on a hill next to the Harbour Entrance while ships trying to stay in the channel?
  - At night, while foggy, etc so no visual references
  - Hope they are cross referencing with RADAR

$$$

- Keep an armoured van on track as you take to you secret underground lair
  - Have a track following its normal route while drive it somewhere else

ACM
CURRENCY MANAGEMENT
THIS VEHICLE PROTECTED BY GPS SATELLITE & CAMERA SURVEILLANCE
THIS VEHICLE PROTECTED BY GPS SATELLITE & CAMERA SURVEILLANCE

Uber trip with no distance?



UBER

[redacted] 2016

NZ$[redacted]

Thanks for choosing Uber, [redacted]

FARE BREAKDOWN

Base Fare	1.[redacted]
Distance	5.[redacted]
Time	3.[redacted]
Subtotal	**NZ$[redacted]**
CHARGED [redacted]	**NZ$[redacted]**

Visit the trip page for more information, including invoices (where available)

[redacted]

[redacted]

CAR	KILOMETERS	TRIP TIME
uberX	3.[redacted]	[redacted]

You rode with [redacted]

Evidence

- Blessie Gotingco murder case used GPS Bracelet as evidence
- The defence tried to question the evidence
  - High speed
  - Tracks through buildings
  - Crown acknowledge issues
    - but said was normal to have jumps and high speeds
- So in NZ GPS outliers in Evidence are just Meh, just what suits the Crown

Queenstown Airport Approach

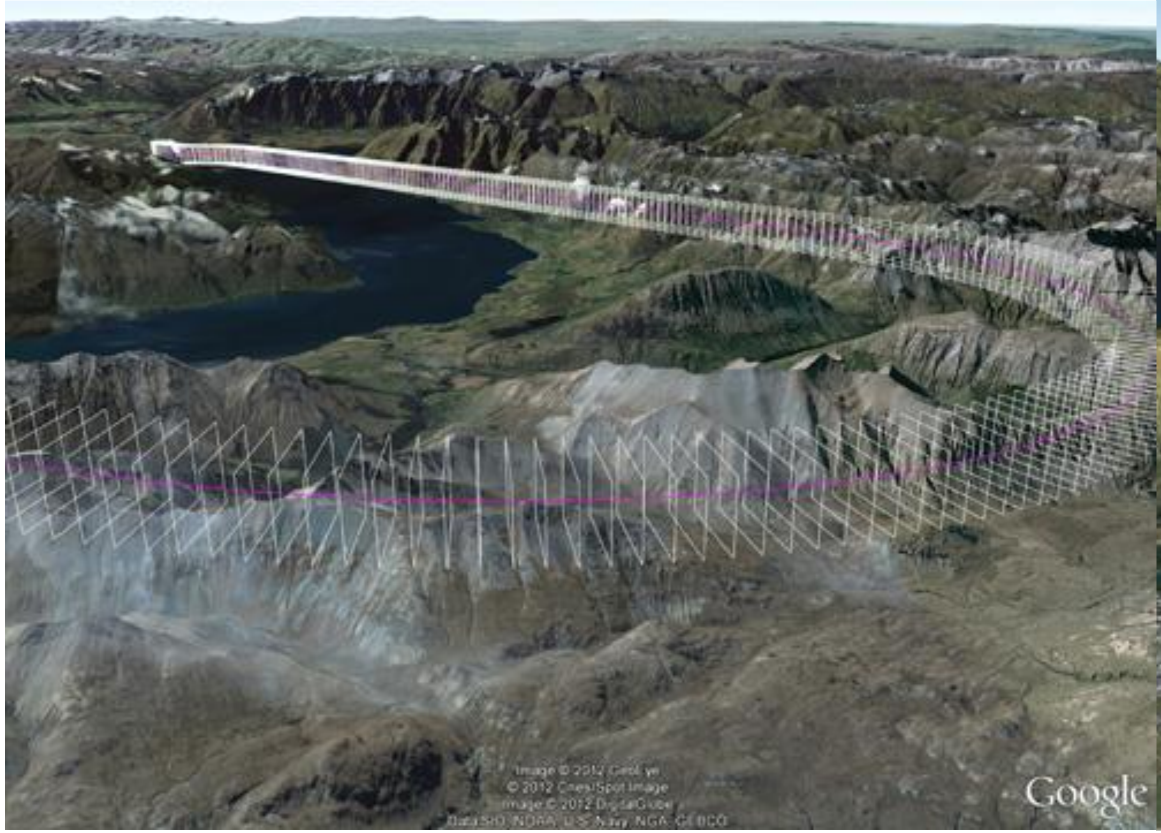
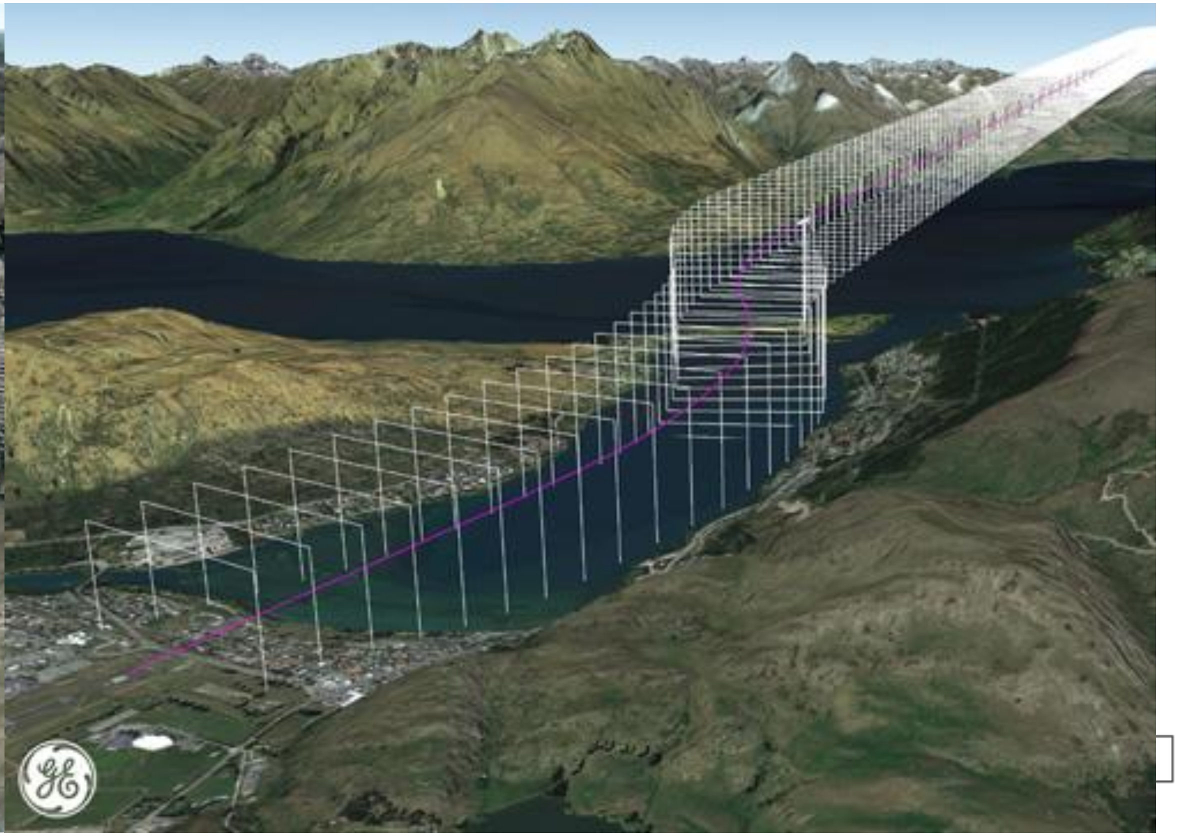


Image © 2012 GeoEye
© 2012 Cnes/Spot Image
Image © 2012 DigitalGlobe
Data SIO, NOAA, U.S. Navy, NGA, GEBCO
Google



Planes

- For places like Queenstown planes have Required Navigation Performance Authorisation Required (RNP AR)
  - When not visual conditions
- As approach is through valleys
  - Can’t use ground based instrument landing systems
- If go off course going to hit the ground

Planes

- RAIM
  - Receiver Autonomous Integrity Monitoring
  - Pre calculates availability in Mountainous Terrain
    - Based on restricted view of sky
  - When flying in a valley with cloud, margin of error low
- Requires more than 4 satellites so can rule out bad Satellite
  - Although spoofing spoofs all the satellites ☺
  - Documentation from Airbus etc, doesn’t mention spoofing
    - Only covers loss of signal

Mitigations for Location

- Use multiple satellite systems
  - GLONASS
  - Galileo
  - Would have to spoof all of them
- Cross reference with Cell Site and WiFi
  - Requires a data connection
  - Though Android trusts GPS over these
  - Not in air or at sea
- Inertial Navigation System
  - 0.6 Nautical Miles per hour and tenths of a degree per hour
  - Resynced from GPS (when was last trusted fix?)

Mitigations for Location

- Next GPS and Galileo have some integrity and safety of life aspects,
  - Which may stop the spoofing if signing, details hard to find
  - But not replay protection
  - Military is encrypted and signed

What are the Impacts? Time

- There are NTP servers which use GPS as time source
- Can change the time
  - So all your time is off in network
  - Can you correlate your logs?
  - Will transactions fail because of time skew?
  - Time Based 2FA?
  - Time based windows for trades
- Infrastructure
  - Power Grids use GPS time in their monitoring
  - Some LTE sites use GPS time for coordination of timing signal

Mitigations For Time

- With NTP don’t rely solely on GPS
- Make sure have multiple NTP servers
  - 3 or more to cover the bad ticker problem identification
  - Make sure some upstream is not GPS
- With GPS NTPs make sure they have some setting for detecting big jumps in time
  - Need a good internal time crystal
- Segmented direction antenna
  - If all signals from one direction know something is up

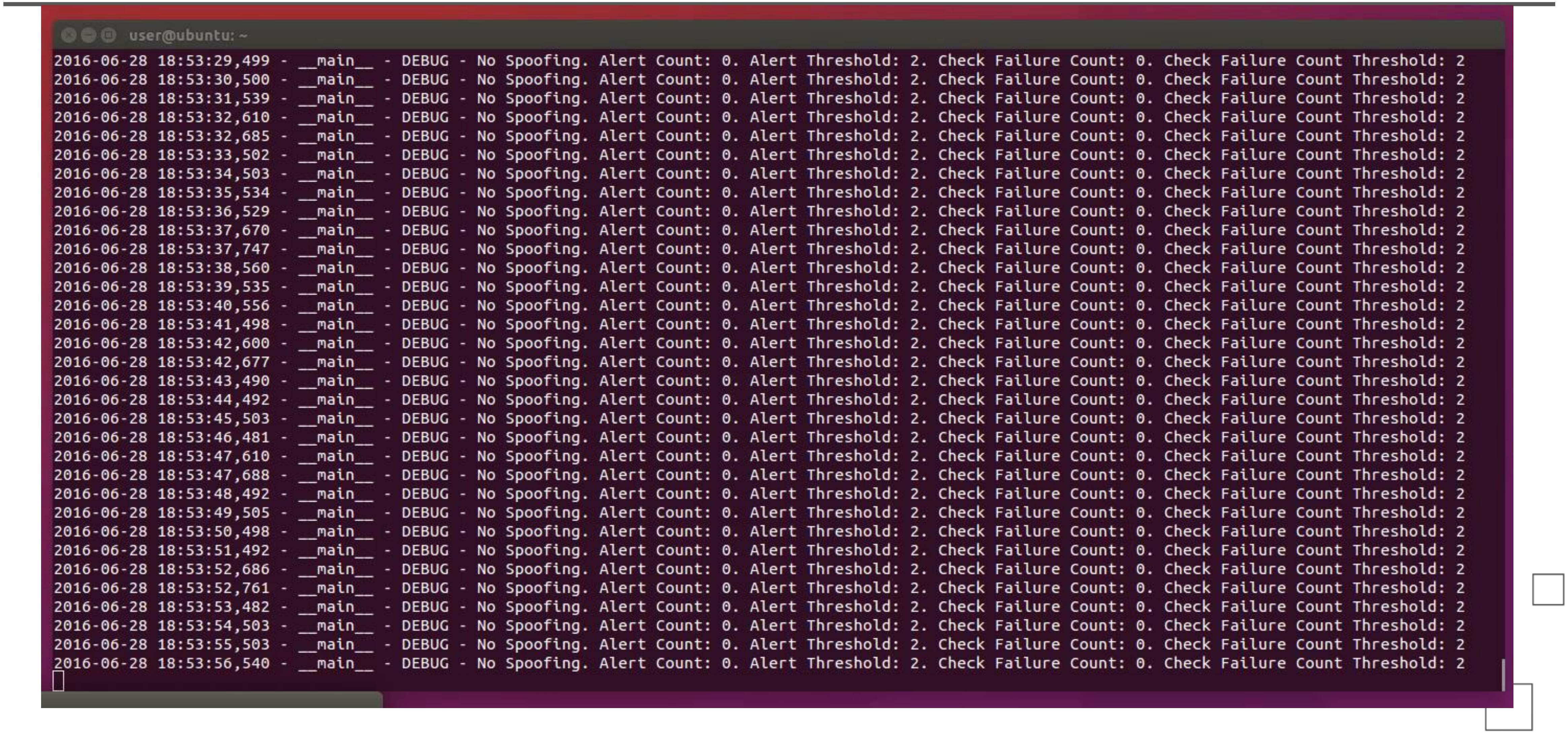
Detecting Spoof

- Does time suddenly change?
- Are the signals too strong?
- Are the signals from all the satellites the same strength?
- Does location change?
  - If stationary

Introducing

- The GPS Spoofer Checker
  - The GPS IDS
- I have a POC
- The other work is academic and they don’t seem to follow POC or GTFO
- I will put the Python script on GitHub or something

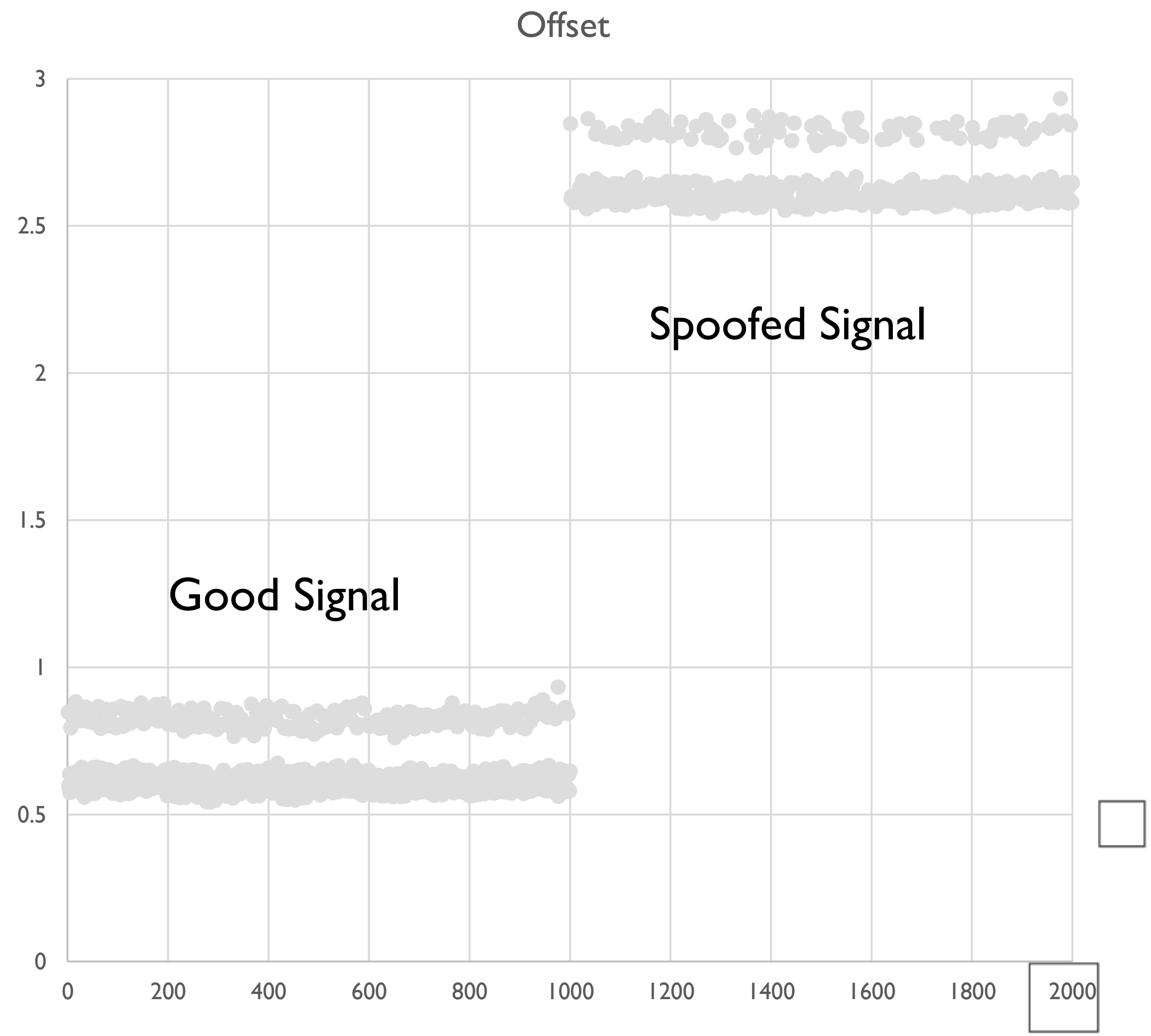
Demo



```
2016-06-28 18:53:29,499 - __main__ - DEBUG - No Spoofing. Alert Count: 0. Alert Threshold: 2. Check Failure Count: 0. Check Failure Count Threshold: 2
2016-06-28 18:53:30,500 - __main__ - DEBUG - No Spoofing. Alert Count: 0. Alert Threshold: 2. Check Failure Count: 0. Check Failure Count Threshold: 2
2016-06-28 18:53:31,539 - __main__ - DEBUG - No Spoofing. Alert Count: 0. Alert Threshold: 2. Check Failure Count: 0. Check Failure Count Threshold: 2
2016-06-28 18:53:32,610 - __main__ - DEBUG - No Spoofing. Alert Count: 0. Alert Threshold: 2. Check Failure Count: 0. Check Failure Count Threshold: 2
2016-06-28 18:53:32,685 - __main__ - DEBUG - No Spoofing. Alert Count: 0. Alert Threshold: 2. Check Failure Count: 0. Check Failure Count Threshold: 2
2016-06-28 18:53:33,502 - __main__ - DEBUG - No Spoofing. Alert Count: 0. Alert Threshold: 2. Check Failure Count: 0. Check Failure Count Threshold: 2
2016-06-28 18:53:34,503 - __main__ - DEBUG - No Spoofing. Alert Count: 0. Alert Threshold: 2. Check Failure Count: 0. Check Failure Count Threshold: 2
2016-06-28 18:53:35,534 - __main__ - DEBUG - No Spoofing. Alert Count: 0. Alert Threshold: 2. Check Failure Count: 0. Check Failure Count Threshold: 2
2016-06-28 18:53:36,529 - __main__ - DEBUG - No Spoofing. Alert Count: 0. Alert Threshold: 2. Check Failure Count: 0. Check Failure Count Threshold: 2
2016-06-28 18:53:37,670 - __main__ - DEBUG - No Spoofing. Alert Count: 0. Alert Threshold: 2. Check Failure Count: 0. Check Failure Count Threshold: 2
2016-06-28 18:53:37,747 - __main__ - DEBUG - No Spoofing. Alert Count: 0. Alert Threshold: 2. Check Failure Count: 0. Check Failure Count Threshold: 2
2016-06-28 18:53:38,560 - __main__ - DEBUG - No Spoofing. Alert Count: 0. Alert Threshold: 2. Check Failure Count: 0. Check Failure Count Threshold: 2
2016-06-28 18:53:39,535 - __main__ - DEBUG - No Spoofing. Alert Count: 0. Alert Threshold: 2. Check Failure Count: 0. Check Failure Count Threshold: 2
2016-06-28 18:53:40,556 - __main__ - DEBUG - No Spoofing. Alert Count: 0. Alert Threshold: 2. Check Failure Count: 0. Check Failure Count Threshold: 2
2016-06-28 18:53:41,498 - __main__ - DEBUG - No Spoofing. Alert Count: 0. Alert Threshold: 2. Check Failure Count: 0. Check Failure Count Threshold: 2
2016-06-28 18:53:42,600 - __main__ - DEBUG - No Spoofing. Alert Count: 0. Alert Threshold: 2. Check Failure Count: 0. Check Failure Count Threshold: 2
2016-06-28 18:53:42,677 - __main__ - DEBUG - No Spoofing. Alert Count: 0. Alert Threshold: 2. Check Failure Count: 0. Check Failure Count Threshold: 2
2016-06-28 18:53:43,490 - __main__ - DEBUG - No Spoofing. Alert Count: 0. Alert Threshold: 2. Check Failure Count: 0. Check Failure Count Threshold: 2
2016-06-28 18:53:44,492 - __main__ - DEBUG - No Spoofing. Alert Count: 0. Alert Threshold: 2. Check Failure Count: 0. Check Failure Count Threshold: 2
2016-06-28 18:53:45,503 - __main__ - DEBUG - No Spoofing. Alert Count: 0. Alert Threshold: 2. Check Failure Count: 0. Check Failure Count Threshold: 2
2016-06-28 18:53:46,481 - __main__ - DEBUG - No Spoofing. Alert Count: 0. Alert Threshold: 2. Check Failure Count: 0. Check Failure Count Threshold: 2
2016-06-28 18:53:47,610 - __main__ - DEBUG - No Spoofing. Alert Count: 0. Alert Threshold: 2. Check Failure Count: 0. Check Failure Count Threshold: 2
2016-06-28 18:53:47,688 - __main__ - DEBUG - No Spoofing. Alert Count: 0. Alert Threshold: 2. Check Failure Count: 0. Check Failure Count Threshold: 2
2016-06-28 18:53:48,492 - __main__ - DEBUG - No Spoofing. Alert Count: 0. Alert Threshold: 2. Check Failure Count: 0. Check Failure Count Threshold: 2
2016-06-28 18:53:49,505 - __main__ - DEBUG - No Spoofing. Alert Count: 0. Alert Threshold: 2. Check Failure Count: 0. Check Failure Count Threshold: 2
2016-06-28 18:53:50,498 - __main__ - DEBUG - No Spoofing. Alert Count: 0. Alert Threshold: 2. Check Failure Count: 0. Check Failure Count Threshold: 2
2016-06-28 18:53:51,492 - __main__ - DEBUG - No Spoofing. Alert Count: 0. Alert Threshold: 2. Check Failure Count: 0. Check Failure Count Threshold: 2
2016-06-28 18:53:52,686 - __main__ - DEBUG - No Spoofing. Alert Count: 0. Alert Threshold: 2. Check Failure Count: 0. Check Failure Count Threshold: 2
2016-06-28 18:53:52,761 - __main__ - DEBUG - No Spoofing. Alert Count: 0. Alert Threshold: 2. Check Failure Count: 0. Check Failure Count Threshold: 2
2016-06-28 18:53:53,482 - __main__ - DEBUG - No Spoofing. Alert Count: 0. Alert Threshold: 2. Check Failure Count: 0. Check Failure Count Threshold: 2
2016-06-28 18:53:54,503 - __main__ - DEBUG - No Spoofing. Alert Count: 0. Alert Threshold: 2. Check Failure Count: 0. Check Failure Count Threshold: 2
2016-06-28 18:53:55,503 - __main__ - DEBUG - No Spoofing. Alert Count: 0. Alert Threshold: 2. Check Failure Count: 0. Check Failure Count Threshold: 2
2016-06-28 18:53:56,540 - __main__ - DEBUG - No Spoofing. Alert Count: 0. Alert Threshold: 2. Check Failure Count: 0. Check Failure Count Threshold: 2
```

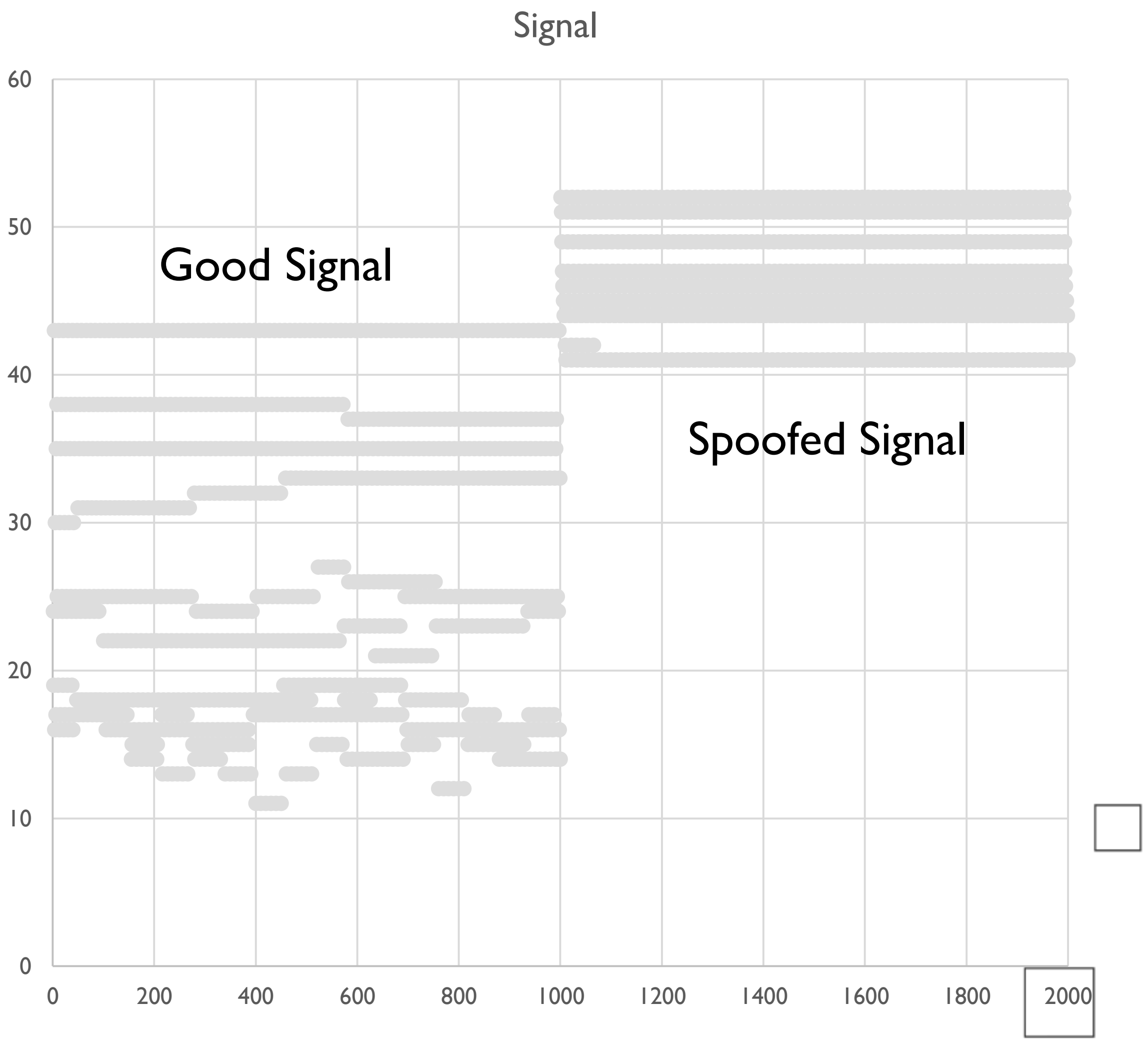
Time

- Easy to detect spoofing, as hard to get broadcast the exact time right
- Assumes you have an NTP source



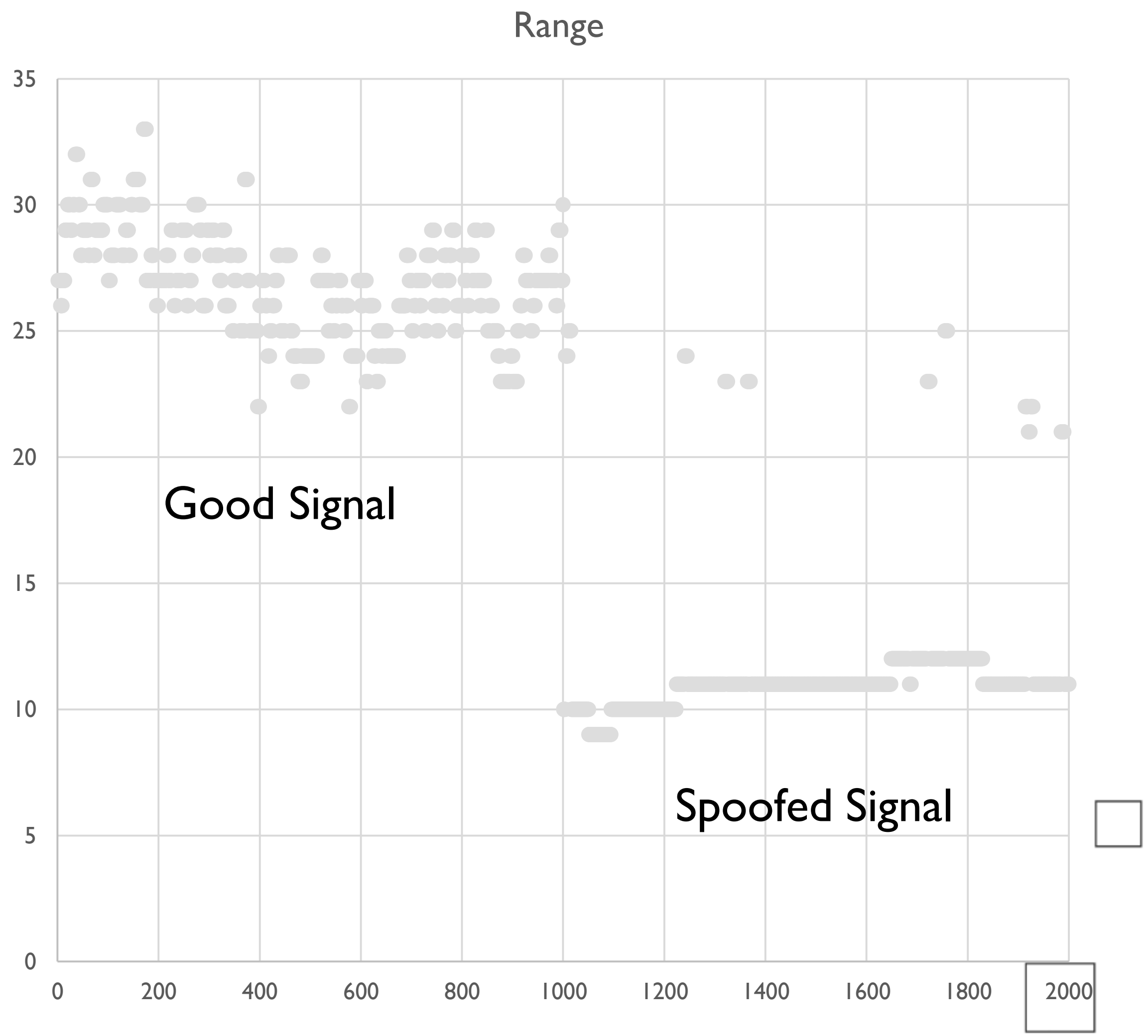
Signal Strength

- The Signal from the bladeRF was stronger than of directly overhead
- If it is stronger than an overhead satellite know it is a fake
- Theoretically anything closer than the satellite



Signal Range

- All the satellites should have different strengths given different locations
- If all the signal strengths are too closely group likely to not be real



Movement

- Currently only looking at static location
  - Don’t have accelerometer for Inertial Navigation
- If move away from the datum more than error
  - Possible spoofing

False Positives

- There were some
- Filtered out using
  - 2 checks per iteration must fail and
  - 3 iterations in a row must fail
- View of sky was important
  - At home good view of sky with plenty of satellites
    - Better
  - At work not much sky and buildings not many satellites
    - Worse

Improvements thinking about

- Inertia Navigation
  - With an accelerometer
  - So can cross reference movement
  - Does the change in location from inertia match the change in GPS?
- Directional Antenna
  - Where are the signals coming from?
- Cross reference location with WiFi SSIDs
- Needs some LEDs
  - Because everything is better with coloured LEDs

Future Work

- Get a plane (or a real sim) with RNP and have a go
  - Can the plane's system detect a spoof?
  - Or does it only detect loss/jamming?
- Get an NTP box and see what behaviour is
  - Are there some that assume GPS is always good?
  - Internal integrity checking?
- Fuzzing the data sent to the receivers
- If can change Almanac file to future or past dates
  - 1970 (for iOS), 2038 and week roll over points

Thanks

- bladeRF – Awesome customer service and great kit
- Takuji Ebinuma – for GitHub code
- @amm0nra – General SDR stuff and Ideas
- @bogan & ZX Security – encouragement, kit, time and flights
- Fincham – GPS NTP Kit
- Unicorn Team – Ideas from their work
- Everyone else who has suggested ideas / given input
- Unrestcon – For having me
- You – For hanging around and having a listen
- GPSd – Daemon to do the GPS stuff
- GPS3 – Python Library for GPSd

Questions?

- Penetration Testing
- Information Security / Phishing Awareness Training
- NZISM / PSR Review
- Open Source Intelligence Training

How To

- Code
  - https://github.com/osqzss/gps-sdr-sim/
  - https://github.com/osqzss/bladeGPS
- Blog
  - http://en.wooyun.io/2016/02/04/41.html
- Lat Long Alt to ECEF
  - http://www.sysense.com/products/ecef_lla_converter/index.html

Libraries Used

- GPS3 Python Library
  - https://github.com/wadda/gps3
- GPSd Daemon
  - http://www.catb.org/gpsd/

References

- http://www.csmonitor.com/World/Middle-East/2011/1215/Exclusive-Iran-hijacked-US-drone-says-Iranian-engineer-Video
- http://www.cnet.com/news/truck-driver-has-gps-jammer-accidentally-jams-newark-airport/
- http://arstechnica.com/security/2013/07/professor-spoofs-80m-superyachts-gps-receiver-on-the-high-seas/
- http://www.gereports.com/post/75375269775/no-room-for-error-pilot-and-innovator-steve/
- http://www.ainonline.com/aviation-news/air-transport/2013-06-16/ge-extends-rnp-capability-and-adds-fms-family

References

- http://www.theairlinepilots.com/forumarchive/aviation-regulations/rnp-ar.pdf
- http://www.stuff.co.nz/auckland/68493319/Blessie-Gotingco-trial-GPS-expert-explains-errors-in-data
- https://conference.hitb.org/hitbsecconf2016ams/materials/D2T1%20-%20Yuwei%20Zheng%20and%20Haoqi%20Shan%20-%20Forging%20a%20Wireless%20Time%20Signal%20to%20Attack%20NTP%20Servers.pdf
- http://www.securityweek.com/ntp-servers-exposed-long-distance-wireless-attacks
- http://www.gps.gov/multimedia/images/constellation.jpg

References

- https://documentation.meraki.com/@api/deki/files/1560/=7ea9feb2-d261-4a71-b24f-f01c9fc31d0b?revision=1
- http://www.microwavejournal.com/legacy_assets/images/11106_Fig1x250.gif
- https://pbs.twimg.com/profile_images/2822987562/849b8c47d20628d70b85d25f53993a76_400x400.png
- https://upload.wikimedia.org/wikipedia/commons/4/49/GPS_Block_IIIA.jpg