Time Travel and GPS F*ckery

Larry Pesce, Technical Operations Manager & Director of Research
Mike Poor, President, Senior Security Analyst

Wild West Hackin' Fest - Way West 2020

WHO THE F*CK ARE YOU?

Mike Poor, InGuardians

President & Senior Security Analyst

- Consiglieri
- Detection and analysis expert
- Professional speaker/educator
- Bladesmith extraordinaire
- Foodie & cook

Larry Pesce, InGuardians

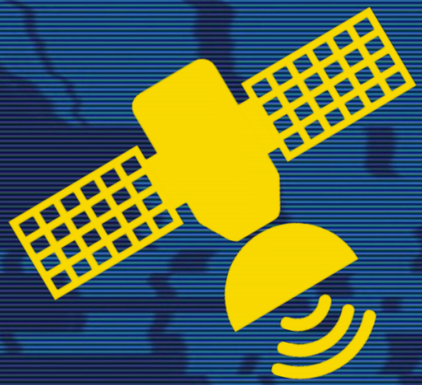
Technical Operations Manager & Director of Research

- IoT, WiFi, SDR
- Star Wars fan
- SANS author/instructor (SEC617)
- Amateur sawdust and knife maker
- Ham Radio operator (KB1TNF)

SATELLITE NAVIGATION – THE FUNDAMENTALS

- Multiple satellites in orbit transmitting to earth with known position
- Transmissions include:
  - A pseudorandom code
  - Current Time of Transmission (TOT) aka epoch
  - Satellite position at TOT
- Upon receipt, the receiver:
  - Aligns the “packet” reception with the pseudorandom code
  - Compares TOT to Time of Arrival (TOA) from 4 satellites
  - Computes 4 Time of Flight (TOF) values with the TOT and TOA
  - Uses the 4 TOF values, satellite positions and the speed of light to calculate position

SATELLITE NAVIGATION – THE HARD PART



For *n* satellites, the equations to satisfy are:

$$d_i = (t_i - b - s_i)\, c,\ i = 1, 2, \ldots, n$$

where d_i is the geometric distance or range between receiver and satellite *i* (the values without subscripts are the *x, y,* and *z* components of receiver position): * **

$$d_i = \sqrt{(x - xi)2 + (y - y_i)^2 + (z - z_i)^2}$$

* https:// https://en.wikipedia.org/wiki/Global_Positioning_System#Navigation_equations
** Microsoft Office products suck for math equations!

SATELLITE NAVIGATION – TL;DR

InGuardians™
Advanced Persistent Testing™

Space Force, Maths, and Magic

SATELLITE NAVIGATION – THE SERVICES

- Multiple satellite systems deployed, all with similar math, collectively referred to as GNSS:
  - GPS (US)
  - BeiDou (China)
  - Galileo (EU ++)
  - GLONASS – Russia, operational worldwide
  - IRNSS - India
  - QZSS - Asia-Oceania, Japan
- All systems feature:
  - Civilian and encrypted military applications
  - Multiple position resolution enhancements
- Can be used for time synchronization, NTP…

SATELLITE NAVIGATION – THE PROBLEMS

- Satellite transmissions are weak
  - They come from space!
  - Low power transmitters, solar power
- Deriving location relies on unauthenticated signal reception
  - Transmissions can be spoofed/crafted
  - Technically illegal, licensed transmission bands
  - Reception only provides no method for mutual authentication
- Deriving time from GPS is easier with arguably less math
  - Time encoded in transmission…
  - …just spoof the transmissions
- Yes, spoofing mitigations do exist, some expensive to implement

A JOURNEY THROUGH TIME AND SPACE

- Easy for civilians to spoof over a short distance
  - Again, illegal, but possible!
- Needs a Software Defined Radio (SDR) and Software
  - Hackrf
  - gps-sdr-sim from from osqzss (Takuji Ebinuma)

We can spoof *location* or *time…*

- Why do we trust GPS and who would f*ck with it?
- Nation states with more advanced capabilities may be highly motivated…

RISKY BUSINESS? YOU TELL ME!

- Why do we trust GPS and who would f*ck with it?
- Nation states with more advanced capabilities may be highly motivated…and even those with reduced capabilities have motive
- What happens when *location* changes:
  - On critical, fixed assets
  - For shipments in transit, now delivered to the wrong destination
  - And re-direction of VIPs, family into dangerous situations
  - …and you can capture that rare Pokémon
- What happens when *time* changes:
  - For servers/devices using time-based authentication (TOTP, OATH)
  - System time out of sync for ICS/SCADA/IIoT automation
  - Financial systems reliant on precise timing for transactions
  - Systems connected to NTP or local WWVB re-transmissions

"A hypothetical disruption to GPS could result in $30 billion to $45 billion in economic losses over a 30-day period." – NIST

CASE STUDY: THE RUSSIAN PREDICAMENT

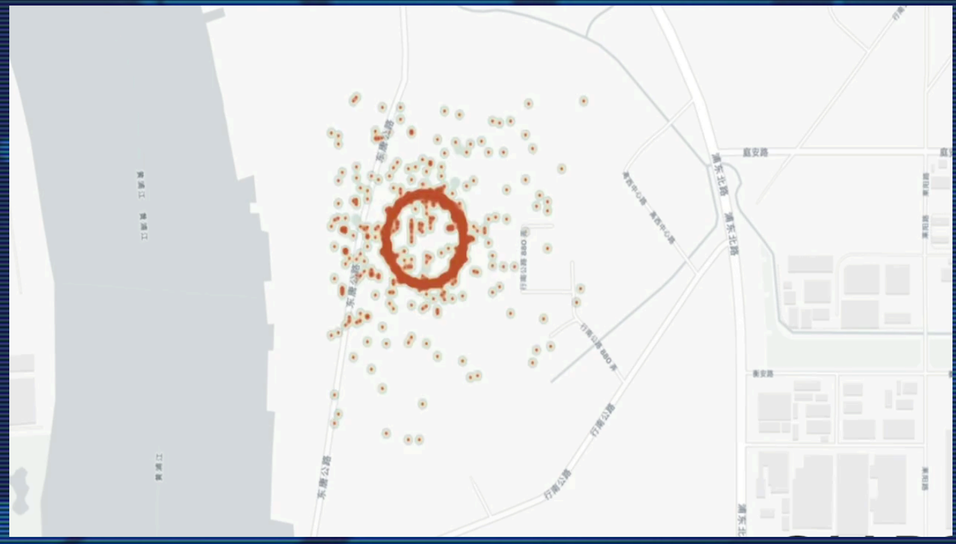
- C4ADS and The University of Texas at Austin study of Russian GNSS spoofing activity
- 500+ ships, military targets untold number of civilian devices affected with “false locations”
- Intended to provide protection/masking making attacks, drone strikes difficult or impossible
  - Used in areas of “protected airspace”
  - Diversions from VIPs (Putin and others)
  - In defense of strategic government and military facilities
  - Protection of military assets abroad (Syria)
- Rumored to be delivered though both mobile and fixed position transmitters
  - Theorized to perform RF jamming on L2 and L5 transmitters, forcing fallback to spoofed L1

Locations of observed GNSS spoofing, C4ADS
https://www.c4reports.org/aboveusonlystars

“[Syria is] the most aggressive electronic warfare environment in the world.”
– General Tony Thomas

CASE STUDY: WE'VE BEEN SHANGHAIED!

- C4ADS, The University of Texas at Austin study of GNSS spoofing activity at the Port of Shanghai, China and the Huangpu river
- Alleged AIS sailing vessel navigation spoofing
- Unknown number of affected vessels, but many life-threatening conditions reported
- Determined to not be an AIS problem but GPS f*ckery…
  - AIS location broadcasts are derived from GPS
  - Navigation decisions made on AIS data, which was erroneous
- GPS spoofing confirmed through Strava aggregated data
  - Many bicycles, many fitness trackers, all spoofed
  - Statistically all spoofed to a central location, Sinopec Shanghai Petrochemical Company, a large chemical manufacturer
- Unknown motivation at this time… ¯_(ツ)_/¯
  - …how ever it is odd that China allegedly "attacked" their own assets (Huangpu Maritime Safety Administration, MSA) for long periods of time
  - Potential attempt to thwart smuggling, illegal sand mining



Time-lapse of spoofed GPS data from Strava. C4ADS
https://www.technologyreview.com/s/614689/ghost-ships-crop-circles-and-soft-gold-a-gps-mystery-in-shanghai/

"Captains and pilots have become very dependent on GPS, because it has been historically very reliable. If it claims to be working, they rely on it and don't double-check it all that much."

- Todd Humphreys, Radionavigation Laboratory Director, UT Austin

GPS SPOOFING FOR THE MASSES

InGuardians™
Advanced Persistent Testing™

Location

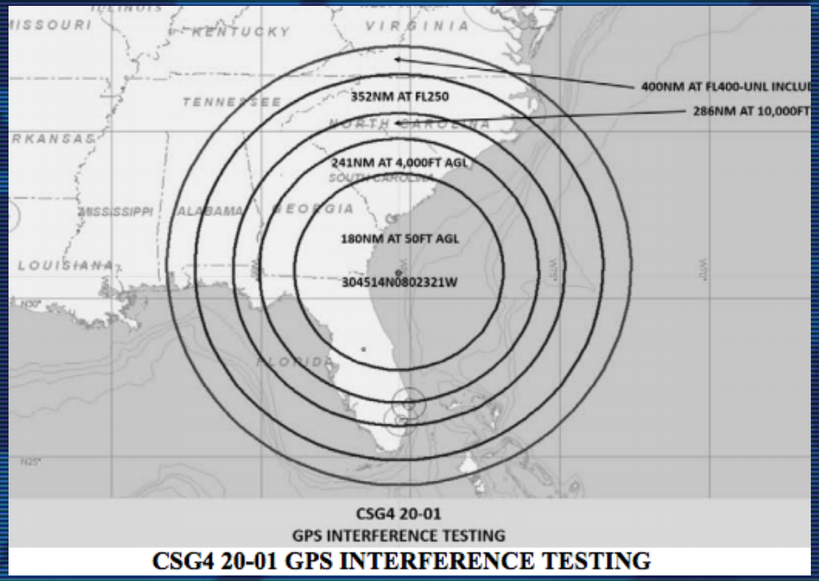
```
gps-sdr-sim -e <ephemerides.brdc> –l 30.286502,120.032669,100
```

Time

```
gps-sdr-sim -e <ephemerides.brdc> -t 2020/02/29,01:23:45 -T
2020/02/29,01:23:45
```

DETECTING GPS F*CKERY

- There is no method for civilians to detect unusual GPS time/location behavior
- Projects to determine the health of satellites exist
  - GALMON (https://galmon.eu/)
- Some info available, largely in academia
- Notifications from various agencies on “testing”
  - Only for “legitimate” f*ckery!
  - US Government executive order to test outages - more to come!
- There is no method for civilians/enterprise to detect unusual GPS time/location behavior
- So, we built one…
  - Hardware and software-based mechanism for detecting GPS f*ckery



Area affected by January 16-20, 2020 interference testing
https://www.faasafety.gov/files/notices/2020/Jan/CSG4_20-01_GPS_Flight_Advisory.pdf

INTRODUCING WAILIN

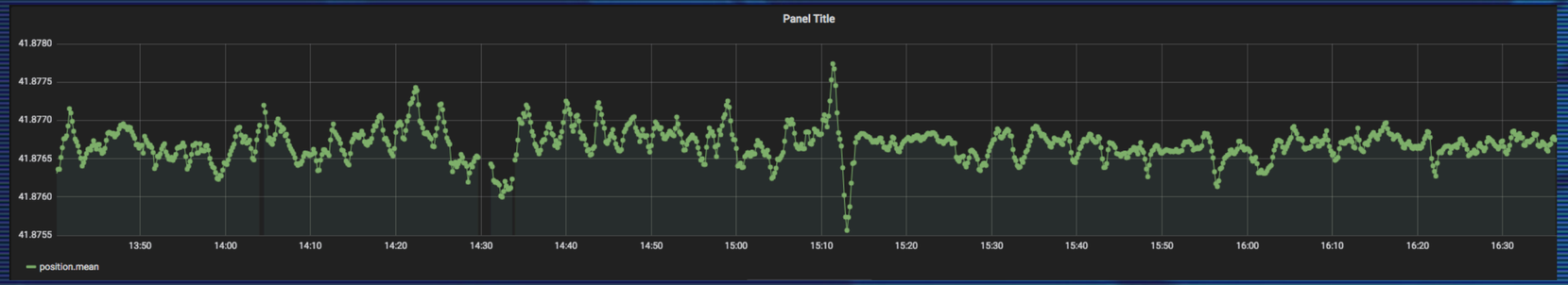
WHAT THE F*CK IS WAILIN?

- A method for aggregating separate and distinct satellite location and time datapoints to look for outliers
  - Distinct systems in order to determine if one or many are being disrupted
  - Raspberry Pi image and manual install methods
- WaiLin is:
  - A citizen approachable GPS f*ckery detection platform
  - Open source
  - Extensible
  - Expandable
  - Inexpensive
- Build your own!
  - https://www.amazon.com/hz/wishlist/ls/2S55SRUKHFHCR

https://github.com/inguardians/WaiLin

CURRENT STATE OF WAILIN

- Hardware
  - Raspberry Pi 4
  - 2x RTL-SDR (ADS-B, AIS) (optional)
    - Expandable for other time sources, IE WWVB
  - 3x Satellite Navigation receivers (uBlox 8M)
    - With 3x serial to TTL converters
    - GPS, GLONASS, Galileo, configurable for others/more/less
  - Multiple points of location/time for independent confirmation
- Software
  - Ingestion of data to a local InfluxDB instance
  - Post-processed with Grafana for visualization
  - Alerting to Discord, customizable for other DIY methods



InGuardians™
Advanced Persistent Testing™

Huge thanks to Faith @InGuardians: She did so much of the heavy lifting with the code!

FUTURE STATE OF WAILIN

- Currently limited to your own, localized data
  - Expansion for sharing of data on a global scale
  - World-wide trending
  - DShield, but for GPS! (Geolocation Reporting Engine Goodness, GREG)
- Further support for additional time/location sources
  - Implementation/analysis of ADS-B, AIS for location
  - Comparison to other time sources such as WWV/JJY/DCF77/DVB/ATSC
- Improved alerting methods
  - Support for additional platforms
  - Near-real time, as opposed to batch processing

HOW CAN YOU HELP?

- Install, use and contribute to the Global GREG
  - We still have some development work left…
- Submit alerts from your fixed-point location to Discord
- Pull requests with new features

…BUT WAIT, THERE'S MORE!

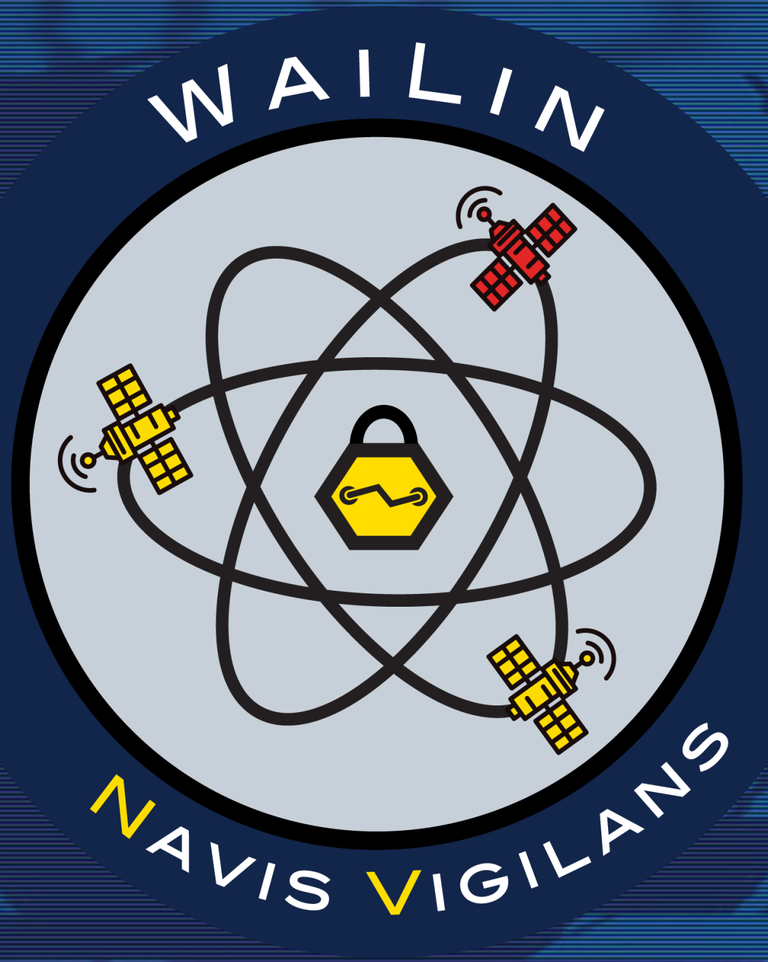
- We've just scratched the surface with GPS
- How many other sources of RF do we rely on for our day to daily lives, or in our enterprise?
- How many of these signals do we blindly trust?
  - GSM? ATSC? FM Radio with RDS? 433 MHz?
- Our challenge to you:
  - Think about those other transmissions
  - Think about how false transmissions would affect you or your enterprise
  - Build (and share) your own detection mechanism

We've become increasingly more reliant on technology and "Magic RF". It is time to verify, monitor and detect the previously unknown f*ckery!

CONCLUSIONS

- GPS spoofing is possible by nation states, or civilians
- GPS spoofing can be damaging to civilians/enterprise
  - Location and time can have drastic effect on operations, authentication
- Few opportunities exist for civilians to, inexpensively perform detection
- WaiLin helps solve the lack of detection
  - We implore you to stand up stations and contribute code
- We've become reliant on technology that can be f*cked with
  - We need to up our detection game for other non-network technologies

THANKS



mike@inguardians.com
@mikepoor

larry@inguardians.com
@haxorthematrix

https://github.com/inguardians/WaiLin