

Logan Scott
Presentation to PNT Advisory Board
16 November 2017, Redondo Beach

An Example of Misplaced Trust

The Portland Spoofing Incident

Narrative available at <http://www.insidegnss.com/node/5661>

Portland Spoofing Event

- **Type of Event:** Spoofing by a GNSS signal generator affecting numerous smartphones
- **Date of Occurrence:** 28 September 2017
- **Location:** Portland Convention Center, Exhibition Hall, ION GNSS+2017 Conference

Symptoms People with S2 Phones Noticed On the Exhibition Floor

Position Error Was Mostly Unnoticed

- Inability to fetch e-mail
 - Server Error
 - Failed Attachment
- Very old text messages
- Wrong time & date
 - 12 January 2014



The Hunt

Using a Chronos CTL3520 Borrowed from NavtechGPS

ION GNSS+ Exhibit Hall Map and Information

	118	119	218	217	318	319	418	419	518	519
	116	117	216		316	317	416	417	516	517
	114	115	214	215	314	315	414	415	514	515
Attendee Lounge	108	109	208	B	E	409	508			513
	104	A			D					511
	102			C						509
	100					F				505
										501

Entrance

HALL HOURS

Wednesday:

10:00 a.m.–8:00 p.m.

Exhibit Hall Open

6:00 p.m.–8:00 p.m.

Exhibitor Hosted Reception

Thursday:

9:00 a.m.–6:00 p.m.

Exhibit Hall Open



ION GNSS+ 2017 Exhibitors

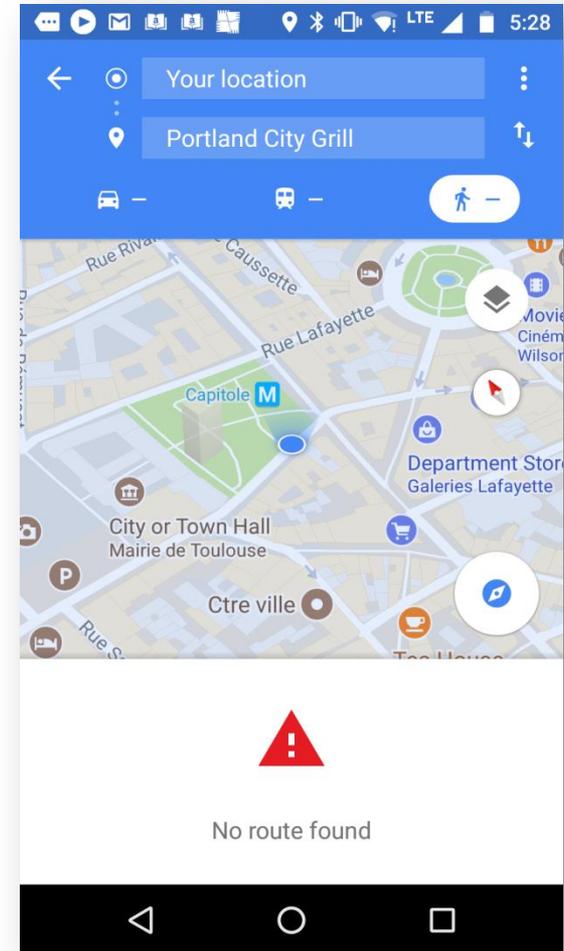
The Culprit Is Found



- GNSS Simulator with 6 Output Ports
 - 1 hooked up to device
 - 5 with plastic covers on
- NO Antenna
 - Range was ~2 Booth Blocks

A lot of people with **non-S2 phones** didn't notice the problem until much later when they tried to navigate

- Phone maintained correct time and date but position was wrong
- One hour after exposure
- ~4 miles removed



Some of the Approaches for Recovery

- Wipe Phone and Reinstall Firmware to Get to Factory Fresh State
 - Lost Data
- Manually Reset Time by Flipping Date ~1348 times
- Expose to Open Sky for Several Minutes



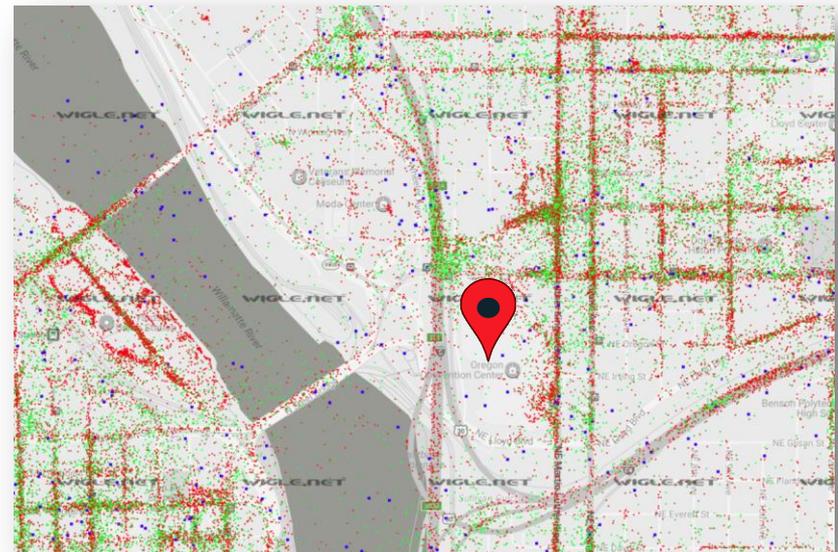
Lessons Learned

- **Spoofting is very confusing** with symptoms that may appear unrelated to GNSS
- **Different model phones react differently**
 - “S2” in particular experienced difficulty since it bought into wrong time
- **Recovery was not fast**
 - Phones did not use all available information

Numerous Location and Time Sources Were Available to Affected Phones

Too Much Trust in the GPS Receiver?

- Cellular Base Station Location & Time was Available
 - 3G/4G Basestations Authenticate to the Handset
 - $\overline{52}$ Phones Probably Got Time from Basestations
- WiFi Access Points
 - Just Hearing a Particular Access Point provides Location Clues



So the Phone Should Always Trust Basestation Time? It Is Not Always a Good Idea to Trust a Basestation

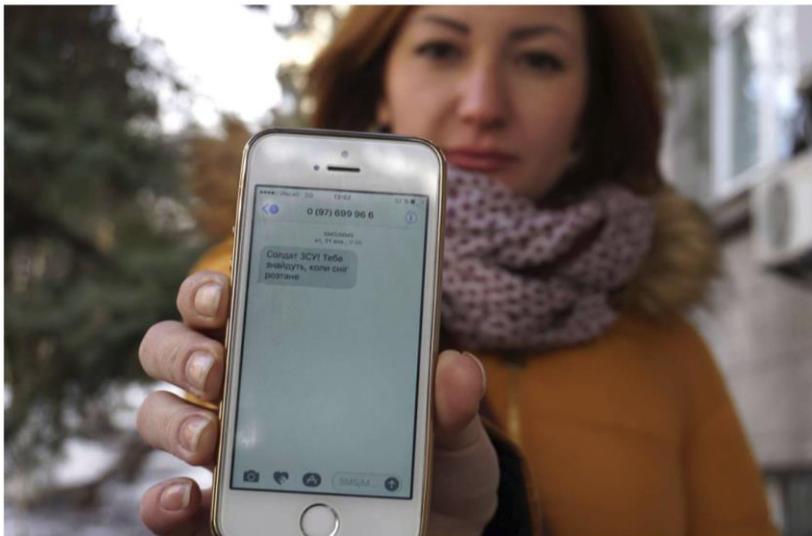
A given model of smartphone operates in many countries.
Need to learn how to provide & access authenticatable time sources.



eLoran can play an important role

Ukraine soldiers bombarded by 'pinpoint propaganda' texts

AP By The Associated Press
May 11, 2017 6:24 pm



In this photo taken Wednesday, Feb. 22, 2017, television journalist Julia Kirienco holds up her smartphone to show a text message reading "Ukrainian soldiers, they'll find your bodies when the snow melts", in Kiev, Ukraine. Ukrainian soldiers fighting pro-Russian...

ENGLISH TRANSLATIONS

Address your questions about payment for housing services to: 0501691294 Moskal

The balance of your account was reduced by 10 hryvnias. Thank you for supporting the Anti-Terrorism Operation

From June 1st, an 8 percent tax on IT equipment will be assessed at the border

Hacks Will Happen, Be Prepared

Core Recommendations

- Don't Be Too Trusting
 - Validate Measurements (e.g. Spoof/Jammer Detection)
 - Do Cross Checks Between Dissimilar Systems and Sensors
- Do Penetration Testing with Certifications
 - Provide Purchase Selection Criteria for the User Community
- Do Cryptographically Sign Critical Data for Authentication
 - Ephemeris, Differential Corrections, Reported Position etc.
 - Watermarking to a Chip Level is a Crucial Step
 - Trusted Platform Module (TPM) IP is Inexpensive
- Do Protect Spectrum for ALL GNSS Systems (US and Foreign)
 - Makes Spoofing Detection Easier

Zero to Operational in 10 minutes With No GPS Expertise

Step By Step Instructions by a Script Kiddie

"I Wear Cool Sunglasses"

The screenshot shows a YouTube video player. The video content features a person wearing sunglasses and a headset, sitting at a desk. On the desk, there is a computer monitor displaying a terminal window with green text on a black background, and a software-defined radio (SDR) interface. The SDR interface shows a frequency spectrum plot and a map of a location. The video player interface includes the YouTube logo, a search bar with the text 'gps spoofer sdr', and a play button. The video title is 'GPS Spoofing w/ BladeRF - Software Defined Radio Series #23'.

"I'm in Cuba"

GPS Spoofing w/ BladeRF - Software Defined Radio Series #23



Crazy Danish Hacker

Subscribe

5,296 views

+ Add to Share ... More

54 0

<https://www.youtube.com/watch?v=VAmbWwAPZZo>
danish bladerf videoplayback.mp4

BACKUP

Spoofting is a Growing Threat

Zero to Operational in 10 minutes With No GPS Expertise

Step By Step Instructions by a Script Kiddie

"I Wear Cool Sunglasses"

The video player shows a YouTube video titled "gps spoofer sdr". The video content includes a terminal window with code, a person wearing sunglasses, and a smartphone displaying a map. The video title is "GPS Spoofing w/ BladeRF - Software Defined Radio Series #23" by "Crazy Danish Hacker". The video has 5,296 views.

"I'm in Cuba"

GPS Spoofing w/ BladeRF - Software Defined Radio Series #23

 Crazy Danish Hacker [Subscribe](#)

5,296 views

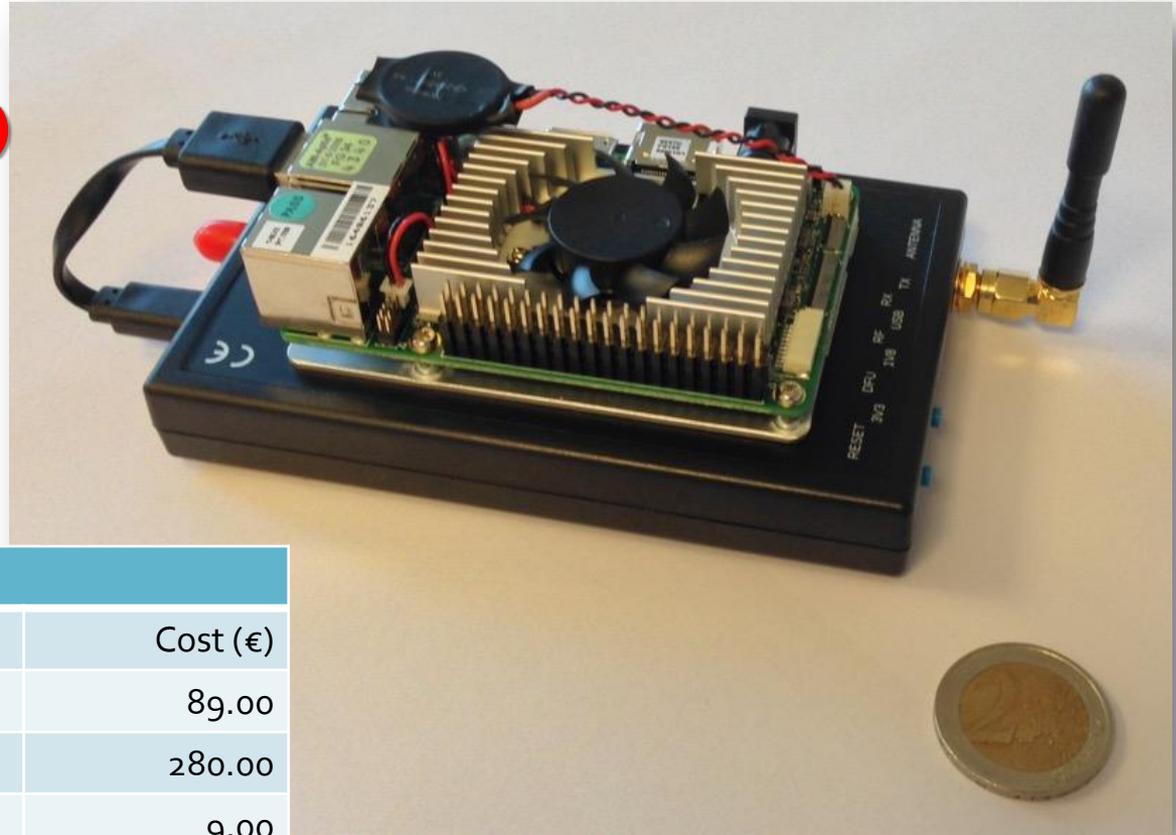
<https://www.youtube.com/watch?v=VAmbWwAPZZo>
danish bladerf videoplayback.mp4

Standalone GNSS Signal Generators are Inexpensive Curtesy of James Curran

€378

(€200 using Lime Mini)

18 channels



Bill of materials:

Function	Component	Cost (€)
CPU	Up Board	89.00
Transmitter	HackRF One	280.00
WiFi Dongle	LB-Link	9.00
Total		378.00

Persistent Location Spoofing Incident June 2017

Similar to Moscow incidents near the Kremlin starting October 2016



NEWS FEATURES MAGAZINE NEWSLETTER BLOGS DIRECTORY SUBSCRIBE

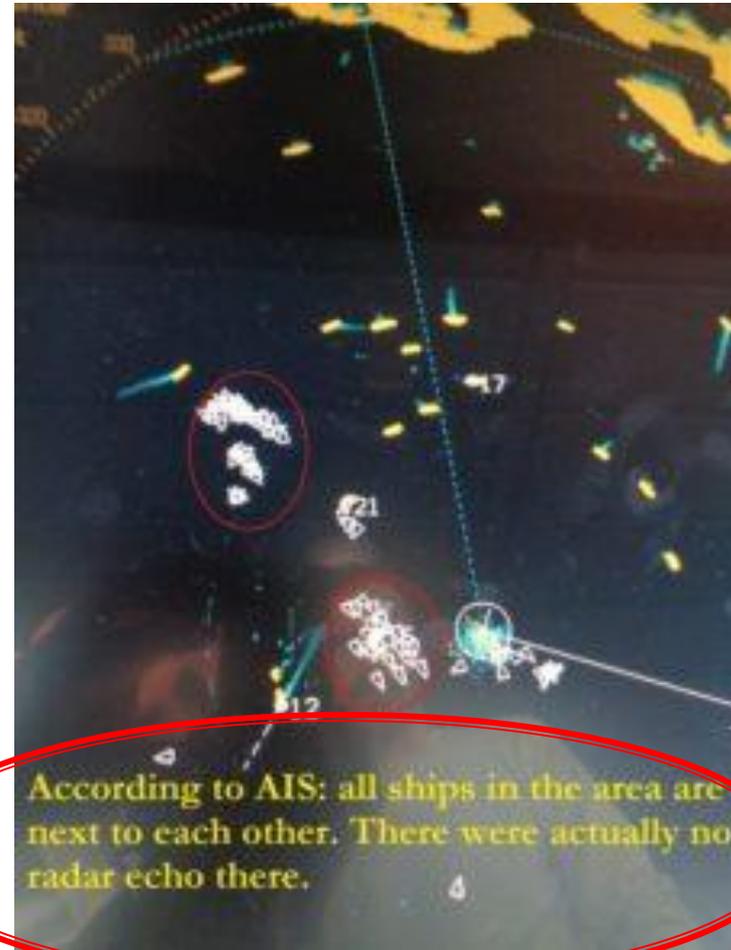
Tweet Share 110 G+ 0 reddit this! Like 216 Share

Mass GPS Spoofing Attack in Black Sea?



By Dana Goward 2017-07-11 20:22:39

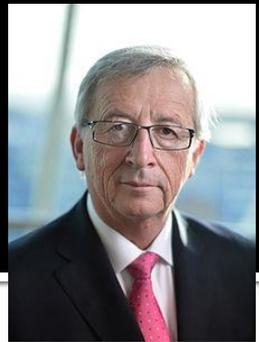
An apparent mass and blatant, GPS spoofing attack involving over 20 vessels in the Black Sea last month has navigation experts and maritime executives scratching their heads.



Objective May Have Been to Ground Geofenced Commercial Drones Limit Surveillance, IED etc.



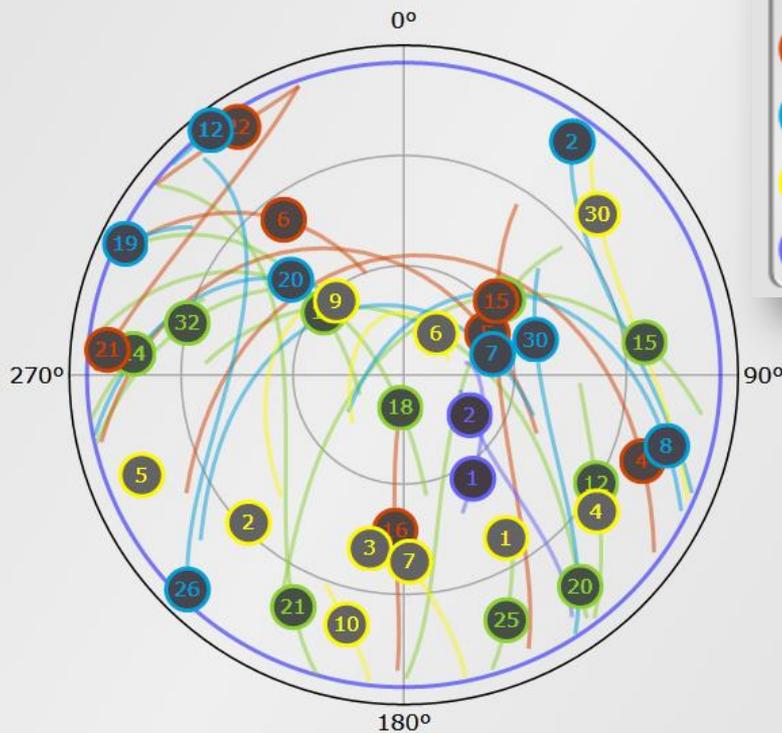
Galileo Signals Will Have Authentication Features That Prevent Signal Generator Attacks



- COMMISSION IMPLEMENTING DECISION (EU) 2017/224 of 8 February 2017
 - Signed at Brussels by Jean-Claude Juncker, President of the European Commission
- “The authentication capacity should increase the degree of safety and prevent risks of falsification and fraud in particular. **Additional features must therefore be incorporated into satellite signals** in order to assure users that the information which they receive does come from the system under the Galileo programme and not from an unrecognised source.”

Multi-Constellation GNSS Provides Coverage, Integrity and Resiliency Benefits

5° Elevation Mask



45° Elevation Mask



www.gnssplanningonline.com

Even One Inconsistent Signal Should Raise Suspicions

Multiconstellation GNSS Makes Spoofing Harder and More Detectable By Forcing Spoofer to Use Higher Power

Successful Spoof Requires Capturing All Signals
Otherwise the Event is RAIM Detectable

