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
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

- Spoofing 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
  - S2 Phones Probably Got Time from Basestations

- WiFi Access Points
  - Just Hearing a Particular Access Point provides Location Clues
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

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 Kiddy

“I Wear Cool Sunglasses”

“I’m in Cuba”

https://www.youtube.com/watch?v=VAmbWwAPZZo
danish bladerf videoplayback.mp4
BACKUP
Spoofing is a Growing Threat
Zero to Operational in 10 minutes With No GPS Expertise
Step By Step Instructions by a Script Kiddy

“I Wear Cool Sunglasses”

“I’m in Cuba”

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:

<table>
<thead>
<tr>
<th>Function</th>
<th>Component</th>
<th>Cost (€)</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>Up Board</td>
<td>89.00</td>
</tr>
<tr>
<td>Transmitter</td>
<td>HackRF One</td>
<td>280.00</td>
</tr>
<tr>
<td>WiFi Dongle</td>
<td>LB-Link</td>
<td>9.00</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td></td>
<td><strong>378.00</strong></td>
</tr>
</tbody>
</table>
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.

According to AIS: all ships in the area are next to each other. There were actually no radar echo there.
Objective May Have Been to Ground Geofenced Commercial Drones
Limit Surveillance, IED etc.

“Position Is Good”
46 km
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

RAIM is Not Possible Using any One Constellation

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

Probability of Capturing All Signals
Probability of Capturing One Signal

Higher Power