

PNT Advisory Board  
Baltimore,  
28-29 June 2017



SPIRENT

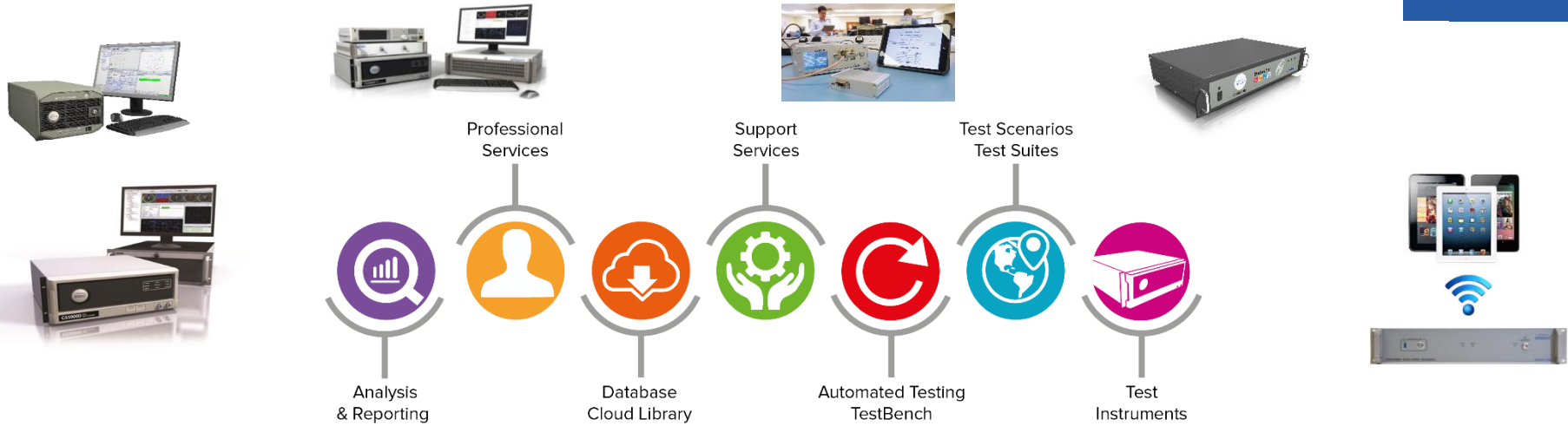


# GNSS Threats, Attacks and Simulations

Guy Buesnel and Mark Holbrow, June 2017



# Overview of Spirent Positioning and Timing



**Mobile Devices**

**Military Applications**

**Commercial Air Travel**

**Automotive**

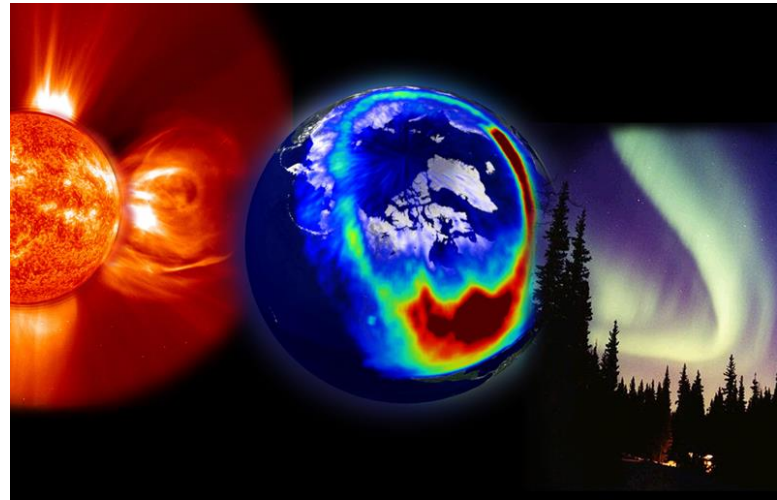
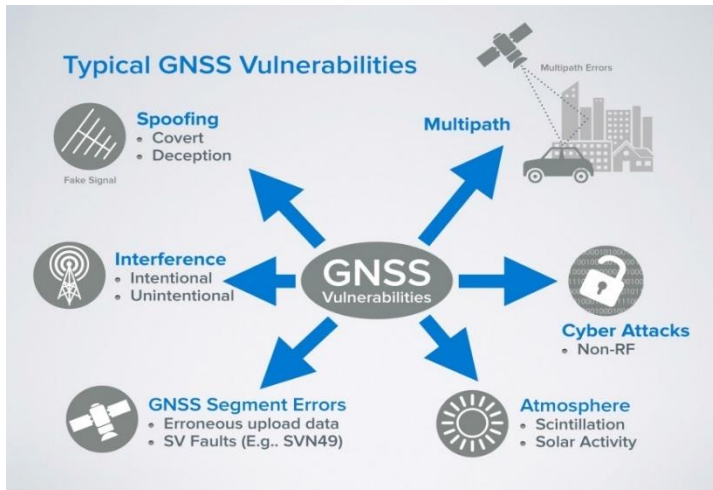
**Space**

**Rail**

**Survey**

# Real world threats to GNSS

## Impacting Time and Position



Spirent Paignton, UK



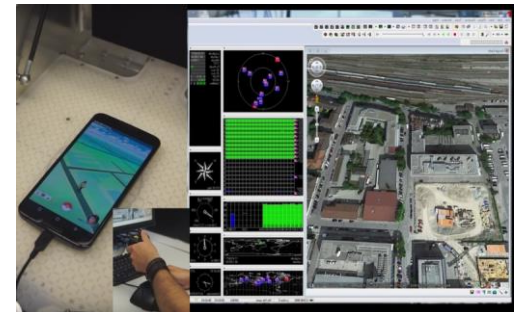
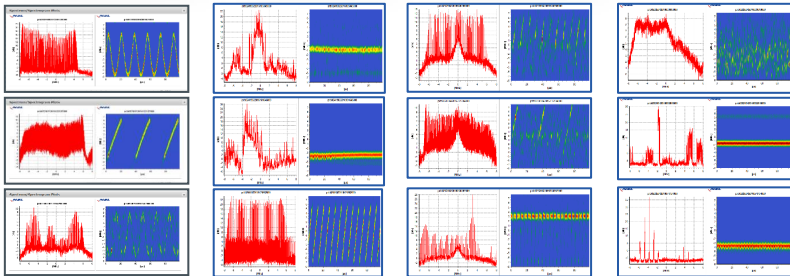
German Airport



Spirent San Jose, US



JAPAN



# The spread of GNSS jamming



**Author:** PatrickMiles November 27, 2012

**Quality:** ★★★★★

I like that jammer because it is simple. You don't have to be a rocket scientist if you want to use it. Nothing special is here, just plug it in and it is done. Another thing I like about this small gadget is that it has precisely calculated output signal power so it never comes out of my car and that is just perfect because nobody can spot and track that jammer.

**Author:** AndyDecker November 7, 2012

**Quality:** ★★★★★

I'm a truck driver and I'm working with one company for almost four years and we've trusted each other. I hauled their cargo and everything was ok, until they have decided to install a tracker in my lorry. I was really angry and I've decided to protect my privacy myself. Now I just plug that thing in my car lighter slot and enjoy my ride!

**Author:** Stewie October 2, 2012

**Quality:** ★★★★★

I'm using this GPS jammer for almost a month. I like it, it jams GPS and leaves everything else untouched, exactly what I needed. With it I'm sure I won't be tracked, and it fits my budget!

## Drines jamming system

Total RF output power : **550W** (Adjustable output power for each band)

Quadcopters/Drones remote controls frequency tapye 6 bands:

1. 5.8Ghz 5500-5900MHz (or 5.0-5.9Ghz) -50W
2. 2.4Ghz 2400-2500 MHz - 100W
3. Remote Control 433 MHz -100W
4. Remote Control 868 Mhz - 100W
5. GPS L2 1227.60 MHz - 100W



Long distance drones jammer Take down drones



drones jammer

**Drines jamming system Range: 1500-3000 meters(-75dBm@Omnidirectional antennas).**  
**The jamming distance will be varied depending on the signal strength and location.**  
Power supply: AC adapter (AC220V-DC27V or 24V/ 40-50 Amp)  
Adjustable Output Power each Band, Stand-alone modular design and individual power control.  
Temperature over protection.



## Commercial Aviation

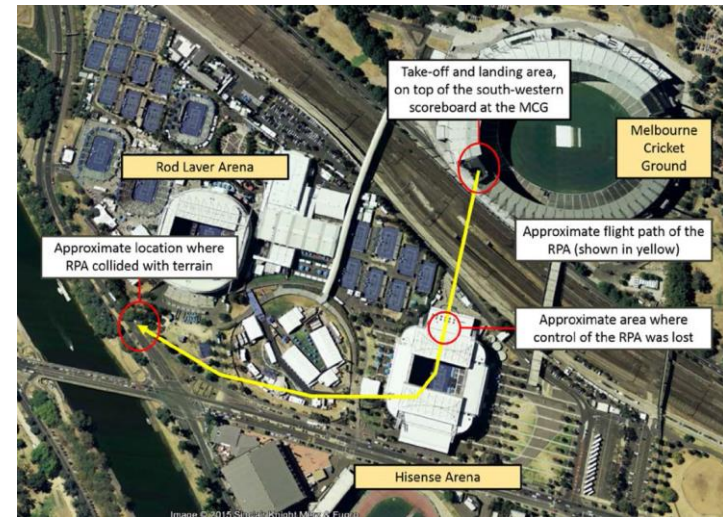
- Over 90 incidents of GPS jamming reported by pilots through NASA's Aviation Safety Reporting System (ASRS) since 2013
  - Philadelphia North East Airport (PNE) – FCC Agents detected a GPS jammer that was operating in a nearby car park – and causing intermittent jamming of a GPS approach procedure.
  - Clark Regional Airport (JYV) - Android tablet frozen showing the aircraft approx. 10 nm to NW of JYV....The PIC visually identified what he mistakenly thought was JYV and proceeded to fly Southbound towards the field.....noted the runway configuration did not appear consistent with the airport of intended landing.
  - “Complete GPS loss of signal as we crossed the coast in point to RPLL (Manila). Signal was lost for remainder of flight. Also on takeoff from RPLL we had a complete loss of GPS signal until coast out. No notice on NOTAMs viewed. No notices on RPLL ATIS.”
  - Mexico City MMMX – Several ASRS reports of GPS Receiver outages whilst on final approach to the international airport – thought to be caused by jamming

## Telecoms

- Complaint from a cell provider in Florida that its cell phone tower sites had been experiencing interference: Forfeiture Order affirms proposed \$48,000 forfeiture against a man for using a cell phone signal jammer in his car while commuting to and from work on a Florida highway over a 16-24 month period (*Source COPUOS Scientific and Technical Subcommittee Meeting presentation, Feb 2017*)

## *Loss of operator control involving a remotely piloted aircraft at MCG*

- Drone failed to respond to “Return to home” function and manual overrides.
- **Post assessment concluded RFI interference was most likely**



**With a GNSS signal the drone should have returned to home, without a GNSS signal the Drone should have maintained position and then descended slowly**



# GNSS jamming – Detection in the real world



Spirent Paignton, UK



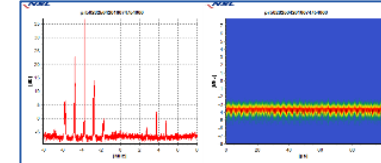
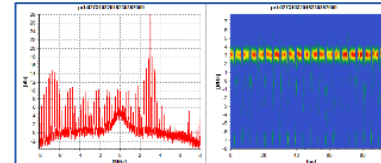
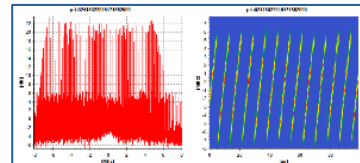
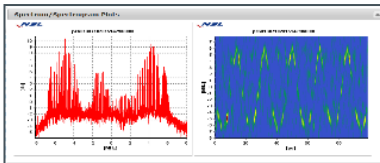
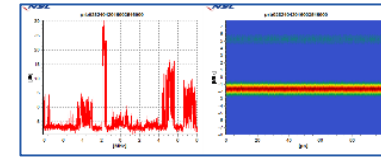
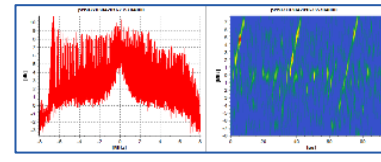
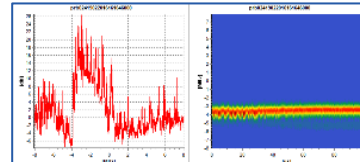
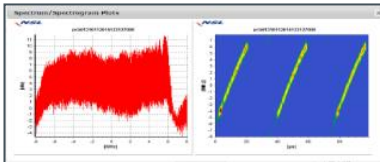
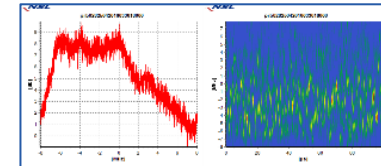
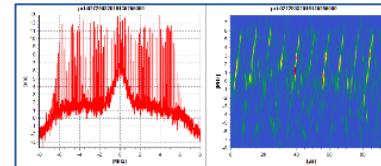
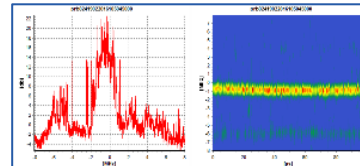
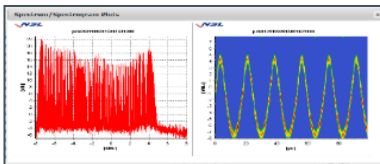
German Airport



Spirent San Jose, US



JAPAN



- Spirent has seen over 15000 GPS L1 interference events since fielding sensors in 2015
- Our interest is in the characterization and replay of threat waveforms in a simulated environment (impact assessment)

# GNSS Spoofing – its emergence as a real threat



- DEFCON 23, Las Vegas, August 2015
- Huang and Yang Spoofing Demonstrations



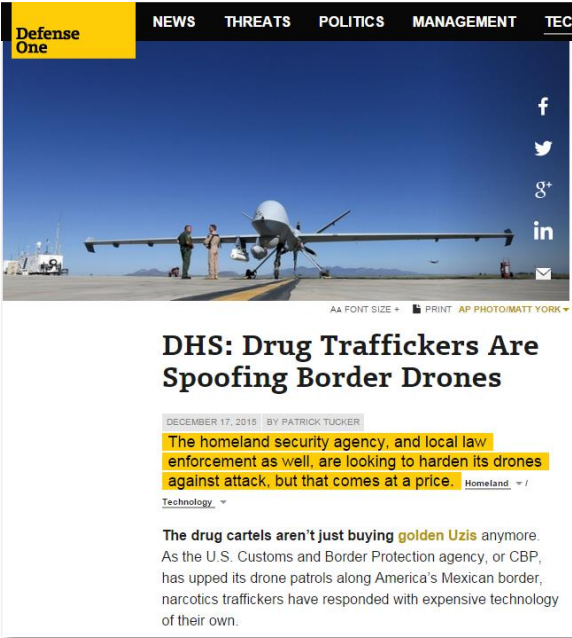
Spoofed a drone's GPS co-ordinates  
Drone is geo-fenced & cannot fly in a forbidden area....  
**But with spoofed co-ordinates it can!**

...Also spoofed a car's position....  
Car is positioned in a car park but Sat-Nav shows that it is in the centre of a lake....  
First time (known) that non-GPS specialists have spoofed navigation signals successfully



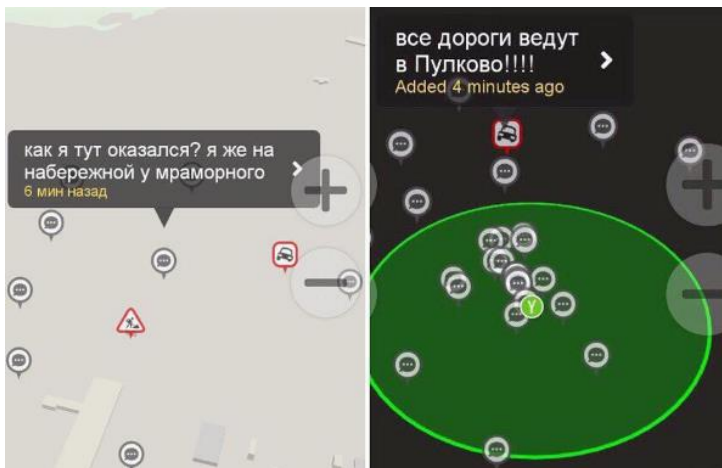


# Real GNSS Spoofing reported



Reported in press 17<sup>th</sup> December 2015

- Highlighted attempts to jam and spoof drones patrolling US/Mexico border
- Attempted GPS spoofing in the real world reported for the very first time
- Criminals using technology to attempt to disrupt GNSS



Reported in press 27 December 2016

- Car drivers experience “strange problems” in St Petersburg
- Car Sat navigation systems show location near Pulkovo airport when they are actually in city centre
- Possible GNSS spoofing by government?

# Real examples of GPS Spoofing – Pokemon GO



Follow

my little brother literally has his phone attached to the ceiling fan so he can hatch his eggs on Pokemon Go...



RETWEETS 38 LIKES 65



4:42 AM - 13 Jul 2016



So i heard if u tie your phone on a fan it counts as if ur walking on pokemon, but no one said it could fly off n break your samsung tablet 😂😂  
#ofallthechances



Pokémon GO News  
@PokemonGoNews

Follow

When you're too lazy to hatch your own eggs in #PokemonGo



RETWEETS 2,632 LIKES 5,532



7:56 AM - 12 Jul 2016

133 2.6K 5.5K



# Real examples of GPS Spoofing


## Spoofing at Application Layer

- Programs can be modified to “offset” a position
- Applications can be used to “fake” position information inside android, which is then presented to the Pokemon Go! Application
- These are actually mainly developer applications that were developed to test location aware applications
- Pokemon Go Developers were quick to implement checks in their application to ensure only “real” GPS locations were used.



CopterSafe

NFZ - Att - Sport - FLIR - Drop - News - Contacts - Cart



**NFZ mod for Inspire 1**  
\$300.00

**Disable no-fly zone limitation mod**  
Mod is easily integrated inside your Inspire 1. Just open upper cover, connect a couple of cables and your drone is ready. You can activate and configure NFZ mod by pressing button. By default NFZ is disabled. Control your current NFZ offset from your phone. Details...

In stock (can be backordered)

1 **ADD TO CART**

Categories: Inspire, NFZ

**Description** | **Reviews (2)**

**Description**  
NFZ mod board allows you to fly using GPS positioning inside NFZ zones. By default NFZ mod is not activated therefore you can use your Inspire 1 as usual. No NFZ correction will be applied.

You can activate NFZ mod using button. Click red button between 2 and 4 seconds after power on of the battery. It has six offset modes. One click mode is most useful in most situations.

- 1 click -10km south west
- 2 clicks -10km nord east
- 3 clicks -90m south west
- 4 clicks -90m nord east
- 5 clicks -200km south west
- 6 clicks -200km nord east

You can see position offset at your DJI Go screen after satellite position is fixed. Ensure that there is no fly zone near your false position otherwise restart battery and select other NFZ mode.

**What's included**

- NFZ Inspire 1 board
- 8 pin cable

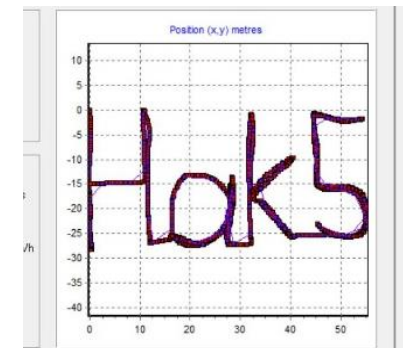
# Real examples of GPS Spoofing – Pokemon Go

## Spoofing the RF Channel

With the developer tools blocked, people started looking at spoofing GPS

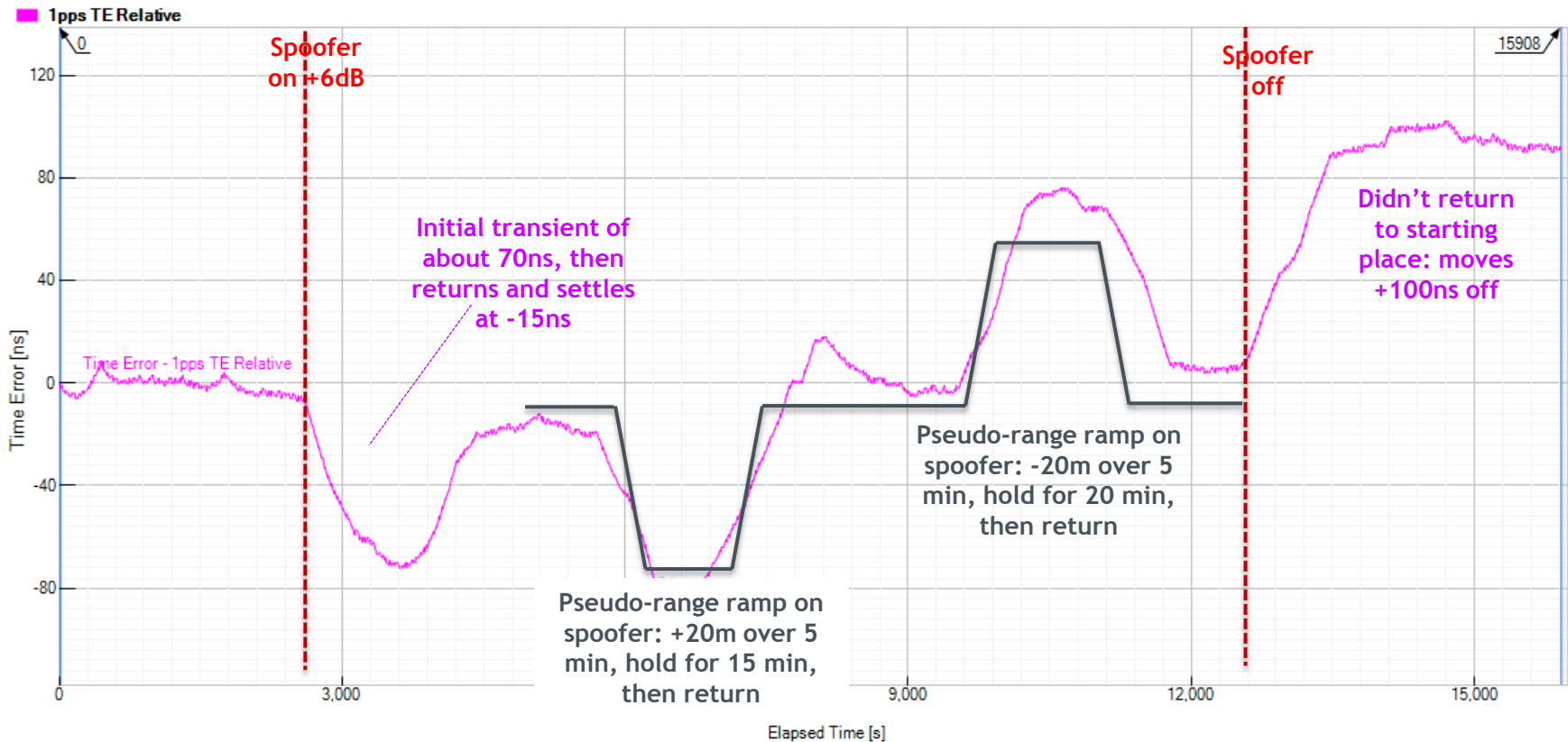


- Quick and dirty using
  - HackRF
  - GPS-SDR-SIM
- Pokemon Spoofing setups were being shared within weeks of release
- Spoofing now becoming available to a new generation of hackers....



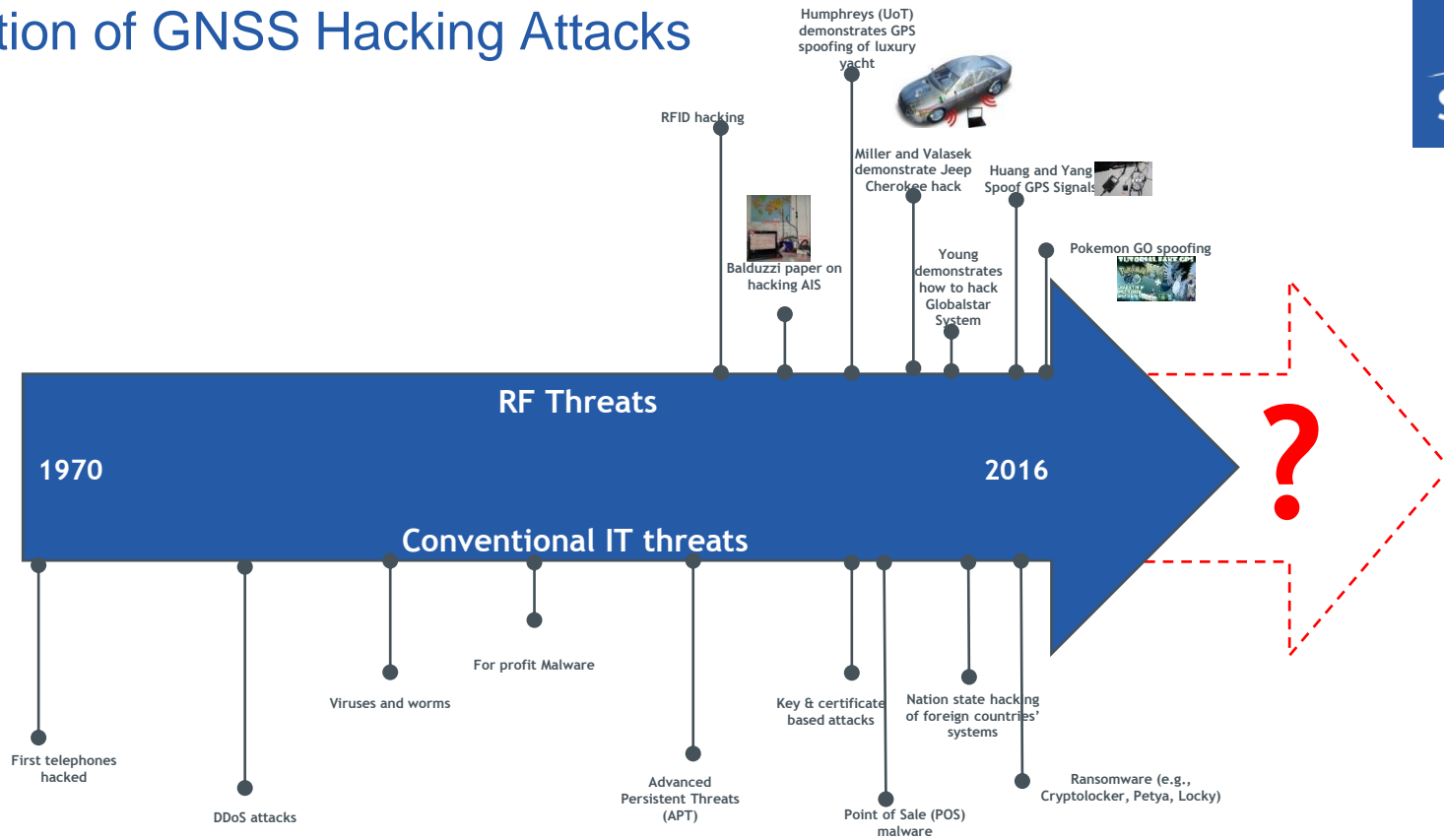


# The importance of testing Spoofing performance



- Performance of a timing receiver subjected to introduction of Spoofed GPS L1 frequency signals using SimSAFE

# Evolution of GNSS Hacking Attacks



- IT threats were seen early on – lots of warnings, eventually many significant events
- GPS threats much more recent – but warnings are there to see....
- As an industry we can't afford to wait for a significant event to occur that could easily have been avoided



# Evaluating Resilience – top level approach



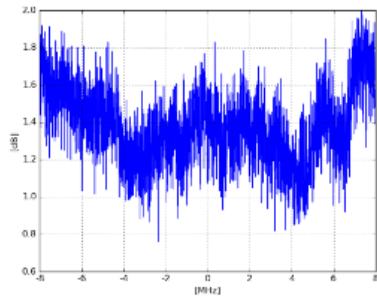
Risk Assessment

Test vs threats

Implement mitigation strategy

Characterisation of environment – derive requirements for operation in degraded/denied GNSS

2D Plots 3D Plot Datafile Download



Real world threat test of systems and devices



Evaluate performance – repeat risk assessment periodically



- GPS / GNSS has unique advantages and will remain as a key component for Position, Navigation and Timing for the foreseeable future
- Interference threats are widespread – the GNSS spectrum isn't clean
- Other threats are also important to consider – e.g, Solar Weather, Scintillation, Spoofing, Segment errors, Cyber
- Our evidence shows that real world GNSS threats can affect PNT systems in very unexpected ways
- Too much talk, not enough “do something about it”
  - A lot of talk about impacts of threats but there are actions that can be taken today to improve the robustness of GNSS systems
  - Need for the Responsible Disclosure of vulnerabilities in Commercial sector
  - Use GPS/GNSS in the Protect Toughen Augment (PTA) framework (Bradford Parkinson)





When trust breaks down...

[guy.buesnel@spirent.com](mailto:guy.buesnel@spirent.com)

<http://www.spirent.com/Solutions/Robust-PNT>



Join the GNSS Vulnerabilities group on LinkedIn to find out more about GNSS jamming and spoofing