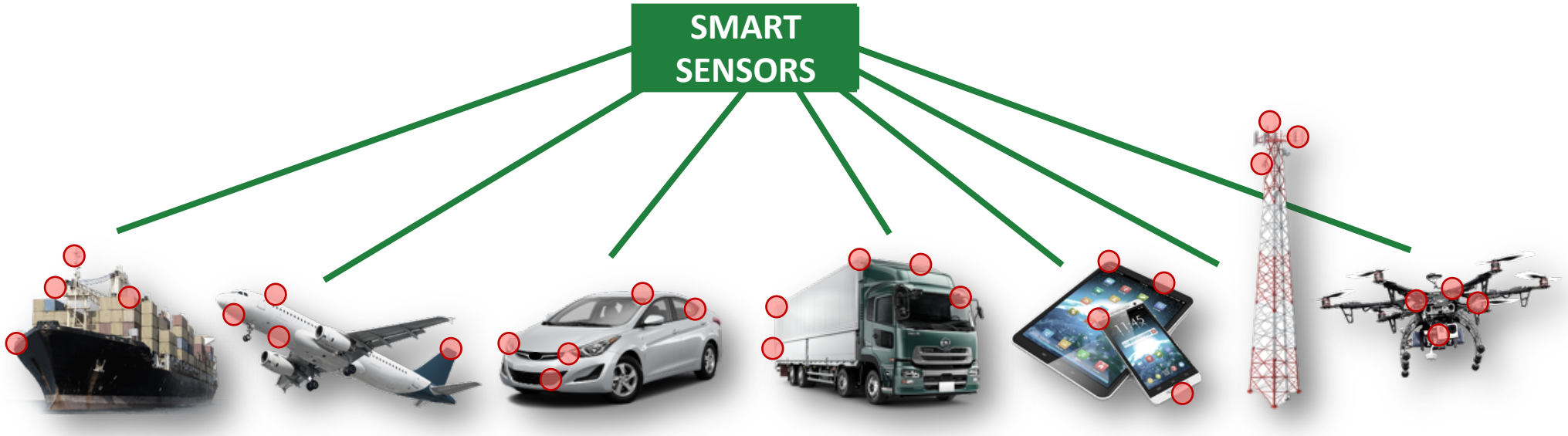
Research on GPS Resiliency & Spoofing Mitigation Techniques Across Applications

Yoav Zangvil, CTO and Co-Founder. Regulus Cyber

Context of our Research



The Eyes and Ears of Modern Systems

- Our focus is on **GNSS**
  - No security
  - Easily spoofed
  - Easily jammed

Yoav Zangvil, CTO and Co-Founder, Regulus Cyber

- B.Sc. degree in Mechanical Engineering from the Technion with major in robotics, dynamics and control systems, Cum laude.
- Military UAV Systems Engineer dealing with telecommunications protocols, encryption and resilient GNSS.
- Prior to Regulus, Elbit Systems, ADT, Rafael Advanced Defense Systems, Comverse and a Technology Division in the IDF.

Context of our Research – GNSS Across Applications

- **LBS –** Over 90% of context-aware apps rely on GNSS.
- **Road –** The need in autonomous driving and ADAS for reliable and accurate positioning.
- **Aviation –** General positioning, ILS/GPS, approaches at airfields, ATC, ADSB.
- **Maritime –** GNSS has become the primary means of obtaining PNT information at sea.
- **Surveying –** GNSS is the backbone in increasingly sophisticated applications.
- **Timing –** Keeping accurate time in sync across multiple locations

https://www.gsa.europa.eu/system/files/reports/gnss_mr_2017.pdf

Why Now?

GNSS Spoofing – The Threat is Evolving

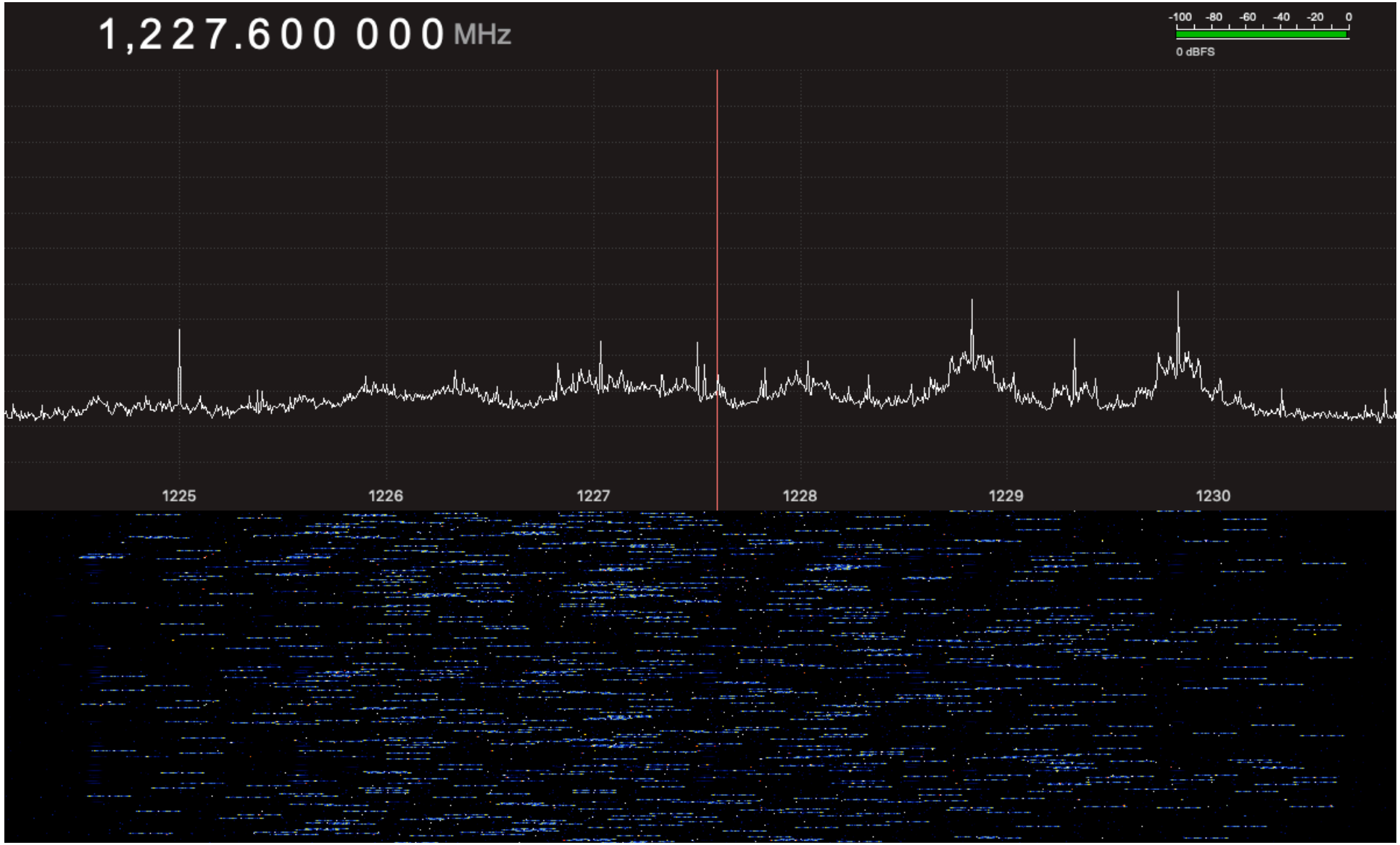
Until 5 years ago

A GNSS spoofing attack would require expensive, high-end equipment in the $50K - $500K range

Today

Software Defined Radios and open source software allow anyone to spoof for as little as $100

Jamming GPS L2 with a low cost SDR



GNSS Spoofing – Intermediate Setup

- Setup Price - $250 + laptop
- Capabilities
  - Real time spoofing static/dynamic scenarios
  - Reply recorded and generated files
  - Smart jamming

GNSS Spoofing – Sophisticated Setup

- Four different constellation
- Four different frequencies
- Accurate OCXO
- 1PPS Sync from a GNSS Receiver
- Multi frequency antenna
- Start with valid navigation messages
- Transition to corrupted messages, rendering NMA useless

GNSS Spoofing and Jamming – Proposed Categories for Civil Aviation

Jamming
J1 - Collateral Jammers
J2 - High Power Interferers
J3 - Targeted Jammers
J4 - Targeted Sophisticated Jammers

Spoofing
S1 – Repeaters
S2 – Errant signals
S3 - Collateral Spoofers – Simulators
S4 - Collateral Spoofers – Re-radiators
S5 - Targeted Spoofers – Simulators
S6 - Targeted Spoofers – Re-radiators
S7 - Targeted Sophisticated Spoofers

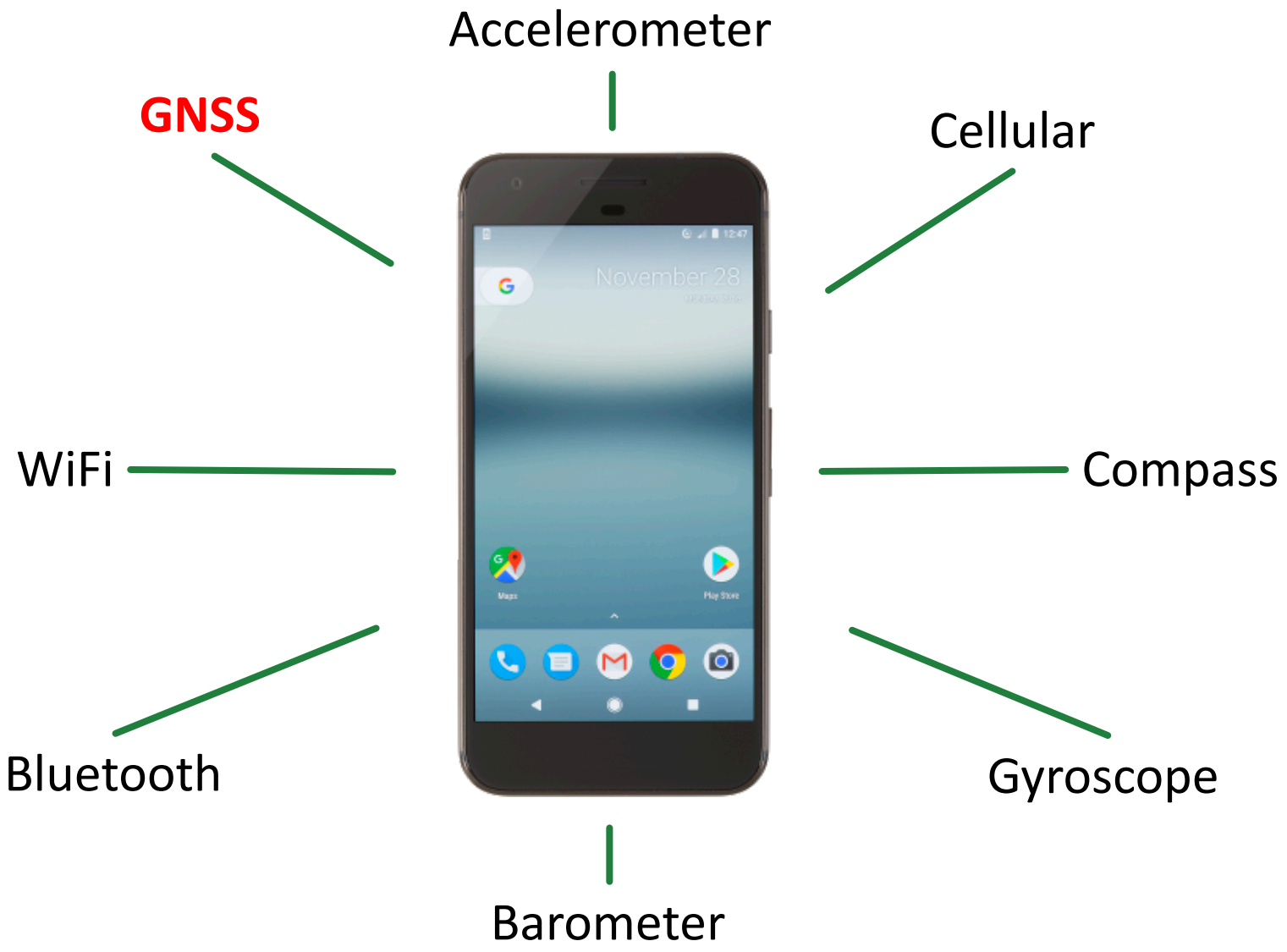
Table 1 – New Interference Types (Jamming, Spoofing) and Categories (J1-J4, S1-S7)

"INCREASING INTERNATIONAL CIVIL AVIATION RESILIENCE: A PROPOSAL FOR NOMENCLATURE, CATEGORIZATION AND TREATMENT OF NEW INTERFERENCE THREATS", January 28 - 31, 2019

GNSS Spoofing – Countermeasures and Rebuttals

Detection Methods	Spoofer
Check Time Shift	Hacker can be perfectly aligned with real-time signals
Check Position Shift	Hacker can start spoofing to current position and drift to the position
Multi Constellation Receiver	Hacker can spoof other constellations or jam them
Multi Frequency Receiver	Hacker can jam other frequencies
Accurate Receiver Clock	Hacker can use a TCXO or a OCXO in the spoofer
Navigation Message Authentication (NMA)	Replay attacks with a time shift or corrupted CRC

Sensors in Mobile Phones



Multiple Sensor Inputs – Can That Solve Spoofing?

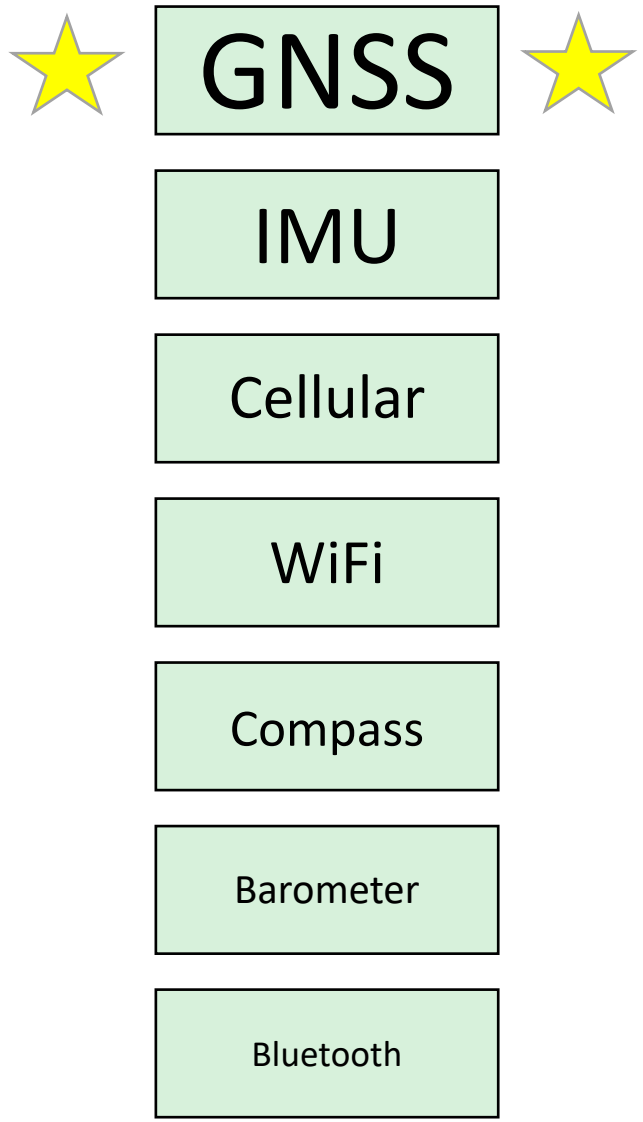
- Accelerometer is not reporting movement but the GPS does
- Compass is reporting a conflicting heading
- Barometer is reporting a change in altitude
- Connection to WiFi did not change while GPS reports a far away location
- Connection to a cell tower did not change while GPS reports a far away location
- In a car, the odometer reports a different velocity

It can help a lot but it is not the holy grail

Multiple Sensor Inputs

- GNSS is a great technology!
- We want to use GNSS when we need it
- Giving GNSS a lower priority over other sensors makes a solution more complicated

Too many “edge cases” to address



Spoofing Techniques – From Simple (1) to Complex (7)

1. Meaconing – replay recorded sky
2. Spoof using a generated scenario on L1
3. Add 1PPS sync to allow real-time spoofing
4. Add TCXO and OCXO
5. Since L1 and E1 are the same frequency, we developed a selective jammer that allows us to jam E1 (BOC) but allows us to spoof L1 (BPSK)
6. Spoof GPS L1 and jam everything else
7. Multi constellation and multi frequency spoofing

Research: GNSS Resiliency Report

- Developing Pyramid GNSS technology – spoofing detection for commercial GNSS receivers.
- Lab and field tests to verify reliability of detection technology.
- Advanced GNSS spoofing capabilities, using open source hardware and modified software
- Reveal vulnerabilities of commercial GNSS receivers.
- Aid development of mitigation techniques.

What is the status of commercial GNSS security?

GNSS Resiliency Report – Scenarios

Indoor Tests: **Standalone Receivers and Mobile Phones**

Inside a lab, where no external GNSS signals are available

Indoor Tests: **Cars**

Inside underground parking garage, where no external GNSS signals are available.

100% vulnerable

Outdoor Test, **Scenario A**:

Spoofing attack is initiated after the target has locked on a real GNSS signal

Outdoor Test, **Scenario B:**

Spoofing attack is initiated before the target is powered on.

Since a mobile phone is always on, it was not a part of this scenario.

GNSS Resiliency Report – Findings

Standalone Receivers

- Reports wrong position and/or time
- No spoofing alarm is activated
- No jamming alarm is activated
- Additional effect are system dependent

Mobile Phones

- All LBS are not useable
- Find My iPhone
- Photo geo-tagging
- Unable to plan or follow a route
- Unable to use navigation apps
- Unable to use ride hailing apps like Uber, DiDi and Lyft.

Major privacy implications where a user can be "placed" in a location that he is not.

GNSS Resiliency Report – Findings in Cars

Safety:

- Exit at the wrong interchange.
- Aggressive braking and steering.
- Accelerate to 100 km/h in a 30 km/h zone.
- Slowed down to 50 km/h on a 100 km/h road.
- Failed to slow down before intersections.
- Braked on main road thinking an intersection is close.
- Height of the car's suspension changed while driving.
- SOS feature reports wrong position to dispatch.
- Confusing and distracting navigation cues while trying to follow a planned route.

Non-safety:

- The car's built-in navigation system displays wrong position on the map.
- Car's clock displays wrong time.
- Unable to plan or follow a route.
- Unable to activate adaptive cruise control.
- GPS-based alarm services do not work.

100% vulnerable

Our employee was genuinely frightened while holding the wheel, and despite the fact he could manually control the car and regain control, the split second of speeding, turning, and other aggressive maneuvers resulted in panic on a highway. This proves that regulation has to be actively involved in ensuring PNT resiliency for public safety.

GNSS Resiliency Report – Responsible Disclosure

Mixed reactions from major corporations across industries:

Negative:

- More often than not, companies did not take visible responsibility for vulnerability of their product
- Referred to it as a ‘Global problem across industries’
- Impression that Spoofing threat is beyond their reach and realm of responsibility

Positive:

- Number of companies asked for extension
- Some indicated interest in cooperating towards testing their technology and finding a solution

Responsibility for GPS vulnerabilities and their effects on platforms and users need to be defined. Government needs to take lead in this matter. Still early – Now is the time to act.

GNSS Resiliency Report – Responsible Disclosure

Mixed reactions from major corporations across industries:

Negative:

- More often than not, companies did not take visible responsibility for vulnerability of their product
- Referred to it as a ‘Global problem across industries’
- Impression that Spoofing threat is beyond their reach and realm of responsibility

Positive:

- Number of companies asked for extension
- Some indicated interest in cooperating towards testing their technology and finding a solution

Responsibility for GPS vulnerabilities and their effects on platforms and users need to be defined. Government needs to take lead in this matter. Still early – Now is the time to act.

Easy To Execute Spoofing Scenarios

- At the base of operations
- Inside an office building or a mall
- Disrupt ride-sharing and mobility services (potential theft)
- Inside an airport/maritime port
- Target single car by tailing (Cargo theft)
- Initiate spoof in parking lot
- Unintentional (taxi drivers, Pokémon Go)

So What Can We Do?

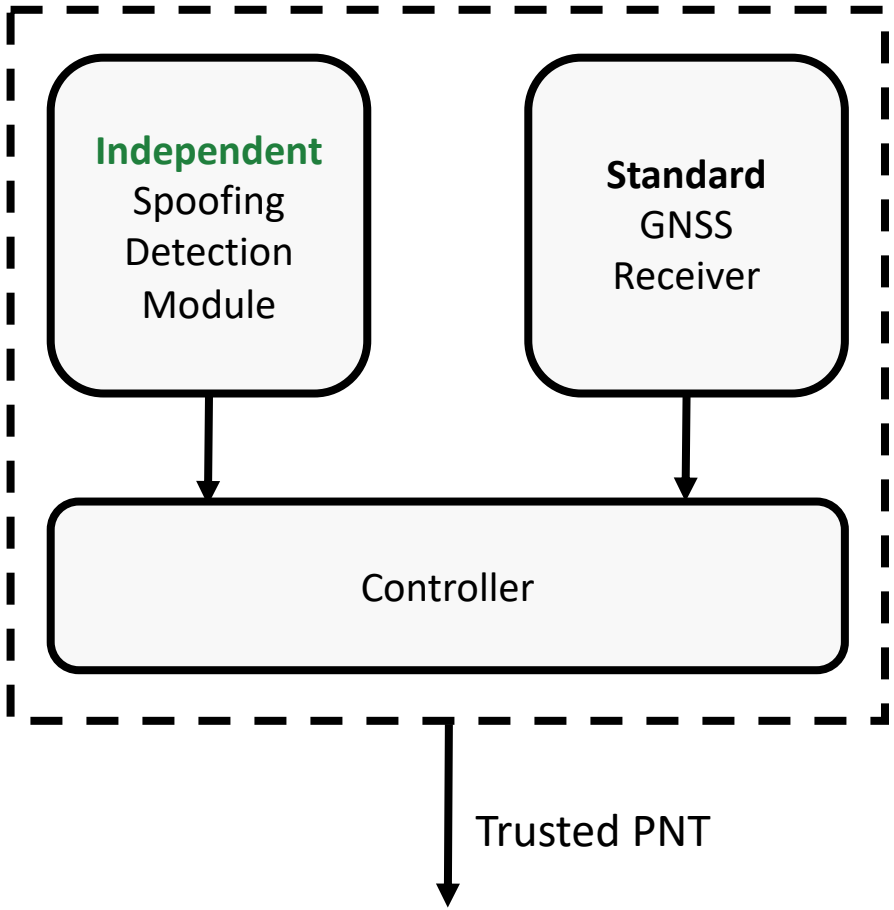
Short-term Solution

Long-term Solution

- **Detection and Prevention**
  - Prevent false PNT effects
  - Fortify existing receivers
  - Solution at the SW level
  - Use today’s GNSS chips

- **Mitigation**
  - Provide valid PNT under spoofing
  - For new receivers
  - Solution at the chip level
  - Re-design GNSS chips

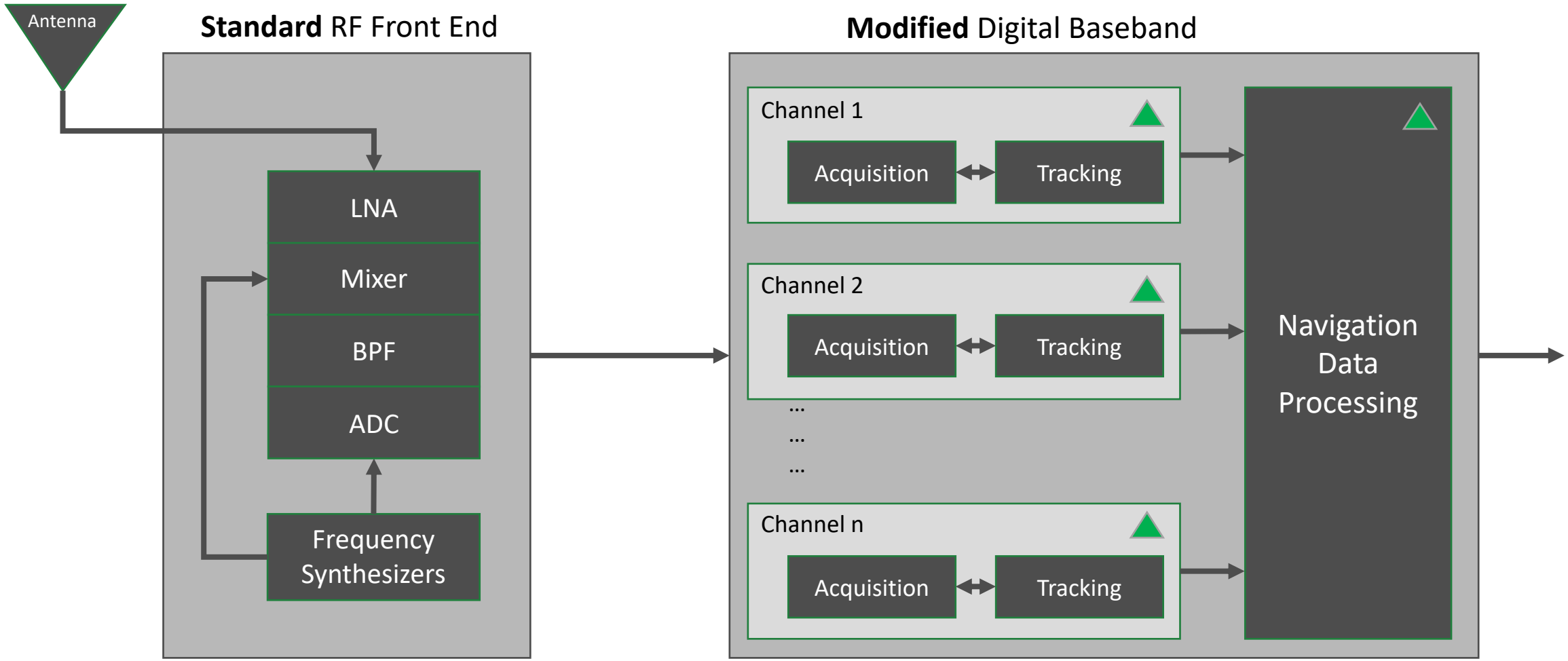
Short Term Solution – Software Level



Long Term Solution – Chip Level

- Multi constellation should not be mandatory
- Multiple correlation peaks tracking – clear sign of spoofing
- Instead of throwing away these PRNs, use them!
- Need a smart way to group those peak
- Once grouped, two converging PNT solutions can be found

Long Term – Pyramid IP Core



Summary

- The new goals of the industry – **security and reliability**
- Sensor fusion helps but is not the holy grail – the receiver must deal with spoofing
- The threat evolves – we must solve the **future** threat today
- Providing a PNT with a confidence level does not tell if you are spoofed – a fully deterministic solution must be used
- Deploy a Red Team capable of testing the effects of interference, jamming, and spoofing
- **Define and enforce GNSS security standards**