REGULUS

GNSS Cybersecurity

First “Anti Virus” software to protect satellite navigation and time

Hi, I’m

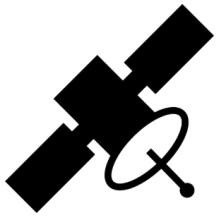
Yoav Zangvil

CTO & Co-Founder

Regulus Cyber

Systems engineer and an expert in telecommunication & navigation.

Holding a B.Sc. in mechanical engineering from the Technion, cum laude.



Regulus Cyber - Cybersecurity for GNSS Timing:

Hardening Accurate Timing Receivers

Against Low-cost 1PPS Spoofing

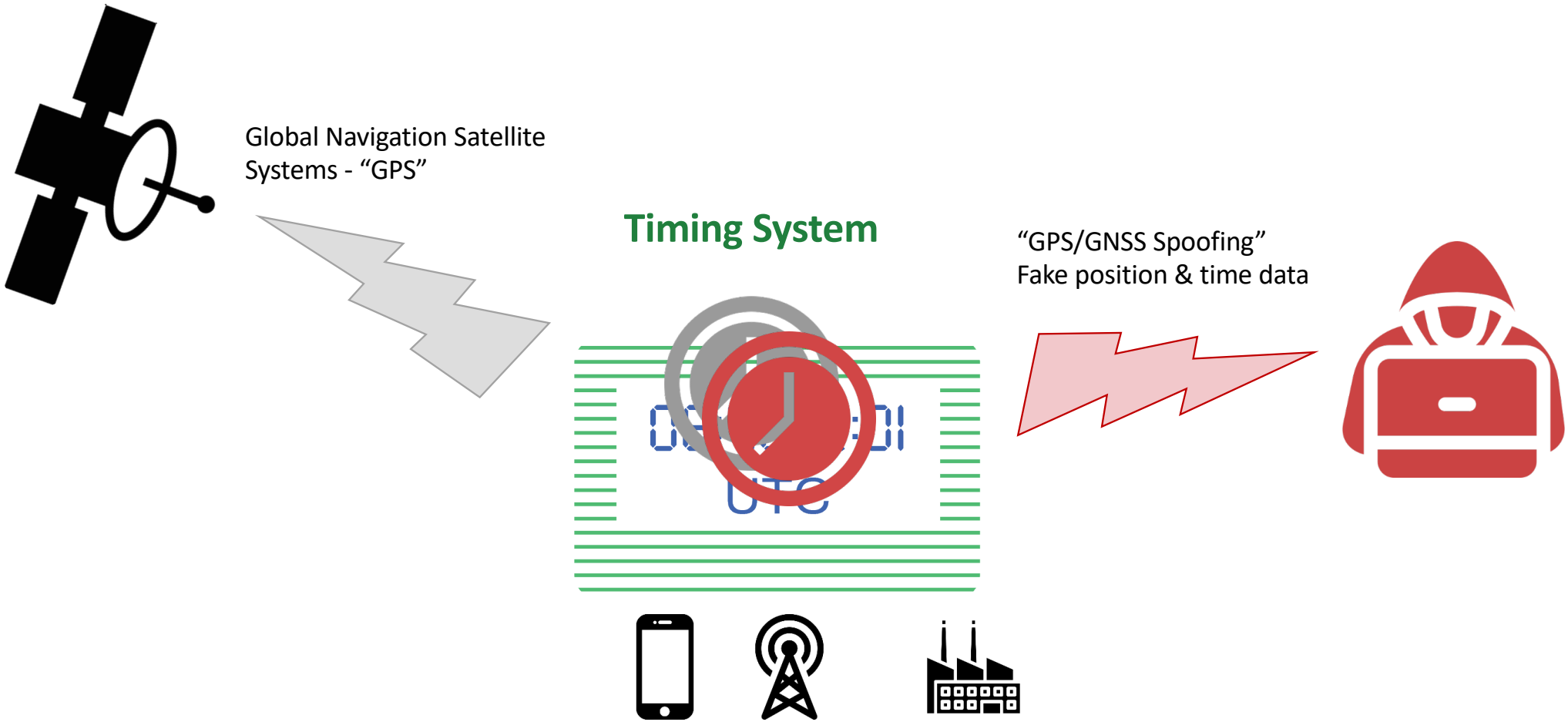
For ITSF Online, Nov 4th 2020

By Yoav Zangvil, CTO

Regulus Cyber

What Is GNSS Spoofing?

A real-world attack sending fake time information to GPS / GNSS based timing systems



Why Now?

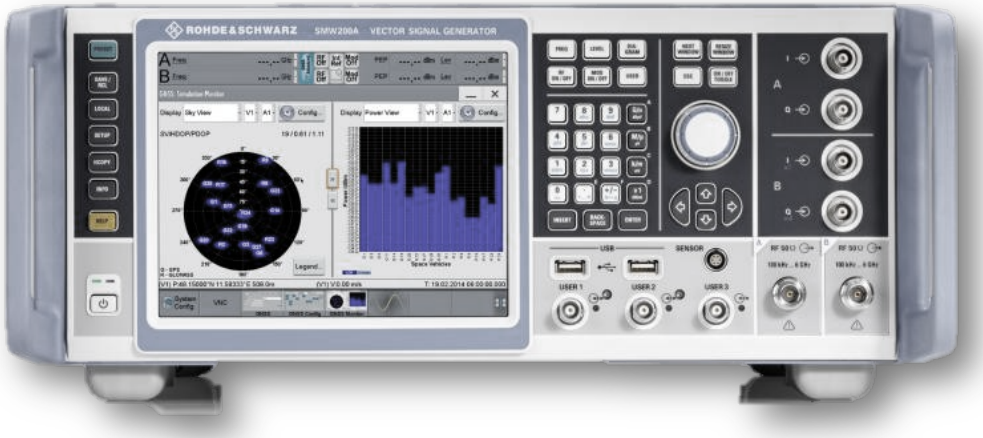
GPS hacking (spoofing) - a paradise for Hackers

Until 3-4 years ago

$250,000 for a spoofer

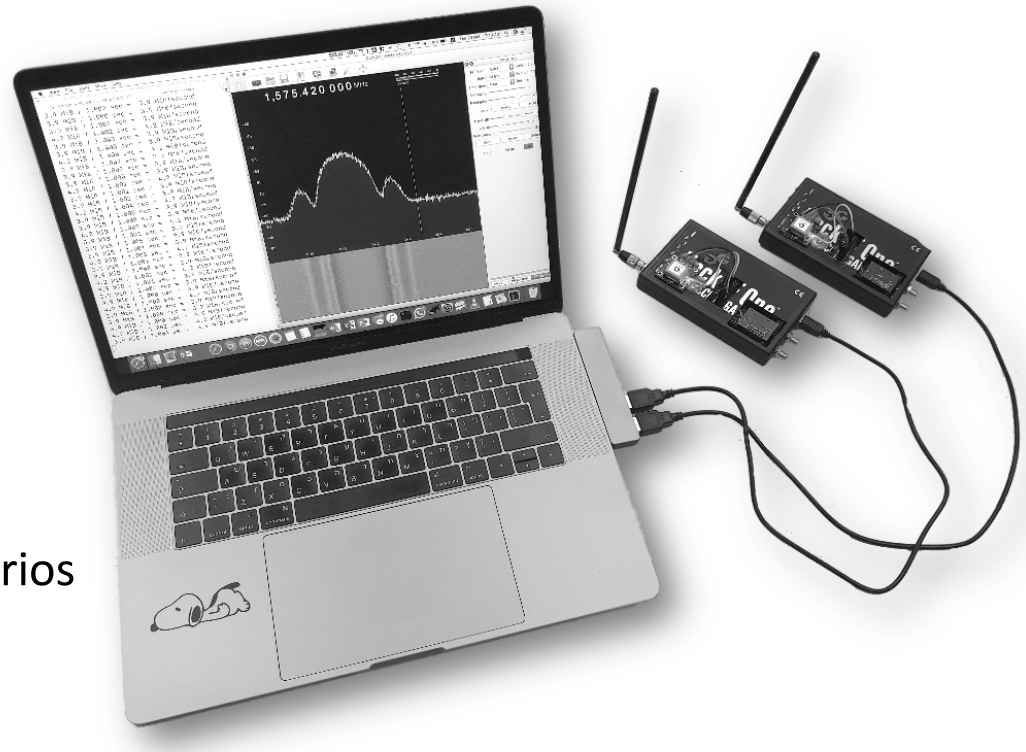
Today

SDR spoofer - $100



GNSS Spoofing – Intermediate Setup, HackRF

- Setup Price - $200 + laptop
- Specification:
  - Dual frequency
  - 1PPS Sync from GPS
  - TCXO
- Capabilities:
  - Real time spoofing static/dynamic scenarios
  - Reply recorded and generated files
  - Smart jamming



Why Now?

GNSS Cybersecurity Attacks Are Increasing Worldwide

Bogus Satellite Nav Signals Send Autonomous Cars Off the Road

At the Black Hat security conference, a researcher demonstrated how making tweaks to navigation signals could send a self-driving car careening off the road.

By Max Eddy August 8, 2019 2:12PM EST

NJ Man Jammed Newark Airport GPS Signals, FCC Says

Paul Milo 04/19/2019 2:23 p.m.

SHARE TWEET PIN IT EMAIL PRINT 0 COMMENTS

Drivers use GPS spoofing, fake apps to defraud Grab, says ride-sharing firm

Published 2 months ago on 17 May 2019

Silicon Valley & Technology

Ben Gurion Incident Exposes West's Vulnerability to GPS Disruption

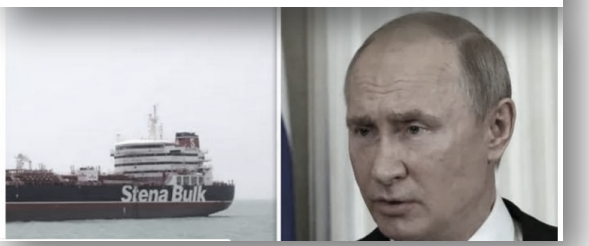
By Oksana Bedratenko
July 3, 2019 03:33 PM

circuit breaker

This Pokémon Go GPS hack is the most impressive yet

15

MI6 probe if seized British tanker was given 'spoofed' Iran coordinates by Russian spies



A $225 GPS spoofer can send sat-nav-guided vehicles into oncoming traffic *

* Some restrictions apply.

DAN GOODIN - 7/18/2018, 2:30 PM

Tesla Model S and Model 3 Prove Vulnerable to GPS Spoofing Attacks, Research from Regulus Cyber Shows

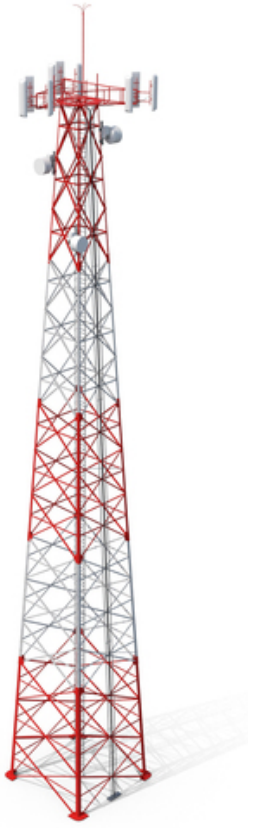
BY INSIDE UNMANNED SYSTEMS

And much more…

Telecom

Telecommunication applications

GNSS is at the core of network synchronization. Interferences and cyber attacks can cause major network disruptions and denial of service at various points in the system:



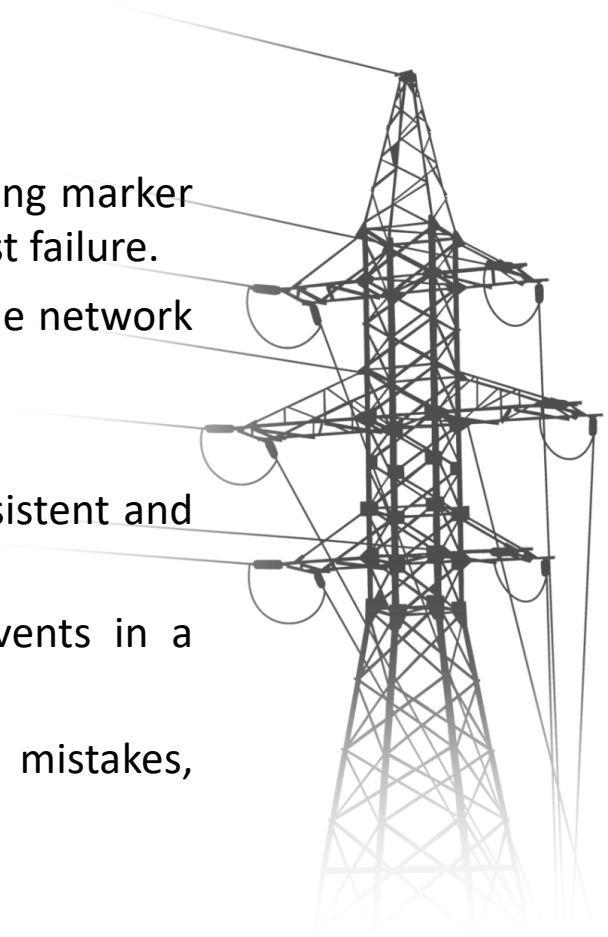
- **Telecom operators -** require accurate time and a consistent frequency at distant points of AD Telematics - spoofing is a major threat
- **Professional Mobile Radio (PMR) -** GNSS is used for synchronization of time slots and handovers between base stations.
- **Satellite Communication (SATCOM) -** GNSS is typically used in Satellite Control Stations and Telecommunications Gateways, mostly for frequency control.
- **Small Cells -** GNSS is used to provide frequency and phase alignment in small cell networks.

Additional applications depending on network synchronization:

- **Emergency Service Sector -** relies on a stable network in order to support emergency calls, first responders, law enforcement and correctional technologies like ankle monitors.
- Disruption of the network may result in the collapse of emergency services.

Critical Infrastructure Applications

- **Energy applications:**
  - Phasor Measurement Units (PMU): GNSS is used to provide a precise timing marker at nodal points of the networks to ensure monitoring and protection against failure.
  - Manipulation of the accurate time source may affect the energy flow of the network with serious consequences.
- **Finance applications:**
  - Financial institutions are legally required to trace operations within a consistent and accurate time scale.
  - Bank applications: GNSS is used for time-stamping functions to log events in a chronological manner, and therefore be able to establish causal links.
  - A manipulation of the timing within financial applications can cause mistakes, disruptions and collapse of the system.



Spoofing a time server using an SDR and open source software

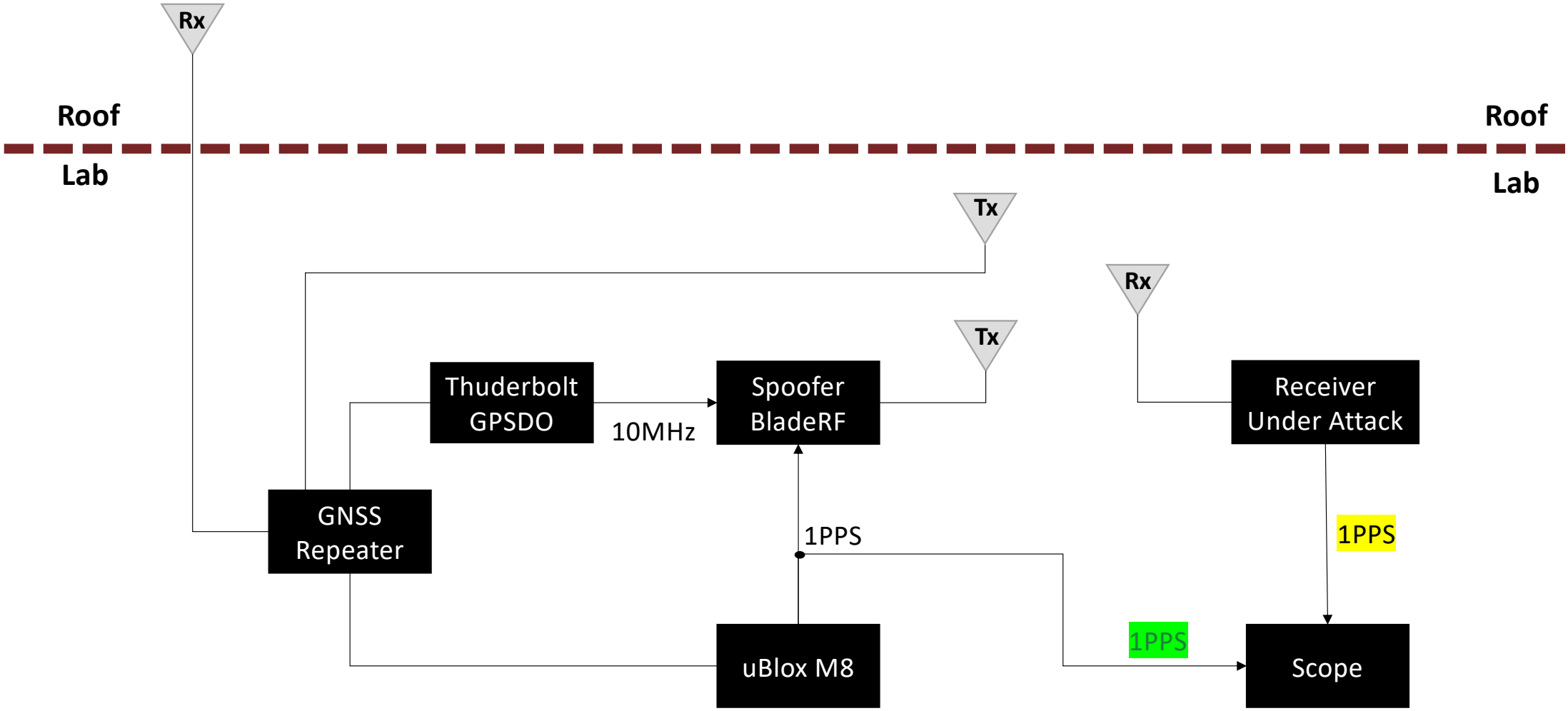
GNSS Spoofing is used to move time back and forth

Experiments

Spoofing Time common GNSS receiver

Experiments

High Accuracy 1PPS Spoofing



Experiments

High Accuracy 1PPS Spoofing

Solution - Automotive

Pyramid GNSS

Phase 1

Detection Software

Detection

Level 2, Level 3 - Driver in the loop

- Simple flexible software-only integration
- Affordable solution
- Protects the system from GNSS hacking
- Connected and stand-alone capabilities

Mitigation Software

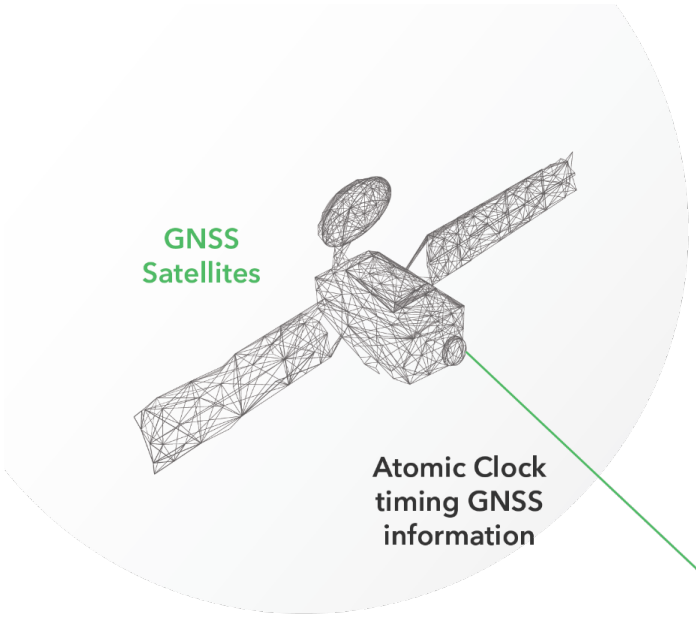
Detection & Mitigation

Level 4, Level 5 - Autonomy

- High-end solution
- Adds mitigation
- Requires additional system resources
- For continuous PNT under spoofing

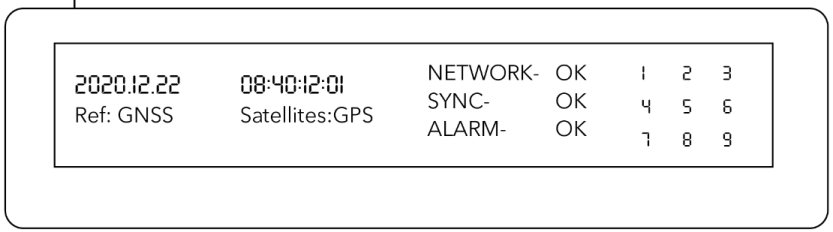
Phase 2

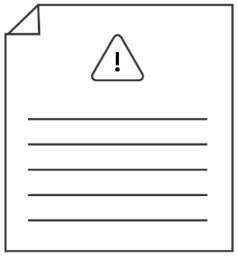
Next Generation Resilient GNSS Receiver



Fake timing transmission
causing offset that leads
to catastrophic failure

GNSS
Antenna

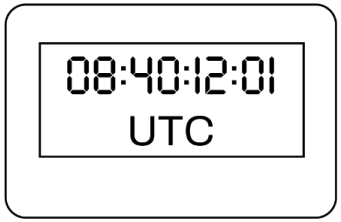




Connected Pyramid solution
provides real time alert of
ongoing spoofing attack and
records the logs

Timing System with Pyramid
GNSS Software that Monitors
all incoming signals

Holdover
Clock



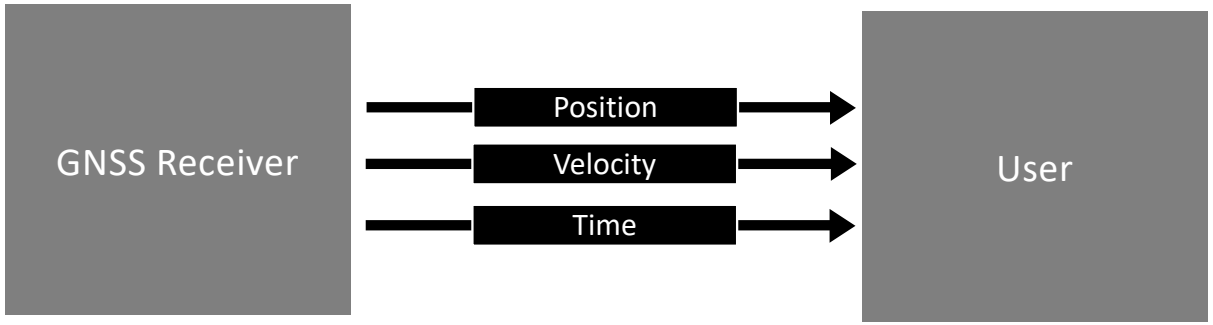
Pyramid engages backup timing system
until it identifies a secure GNSS signal
is available again preventing any
harm to the critical infrastructure

Software Library

Software Library & Authentication Service

Current Receiver's Data Provision

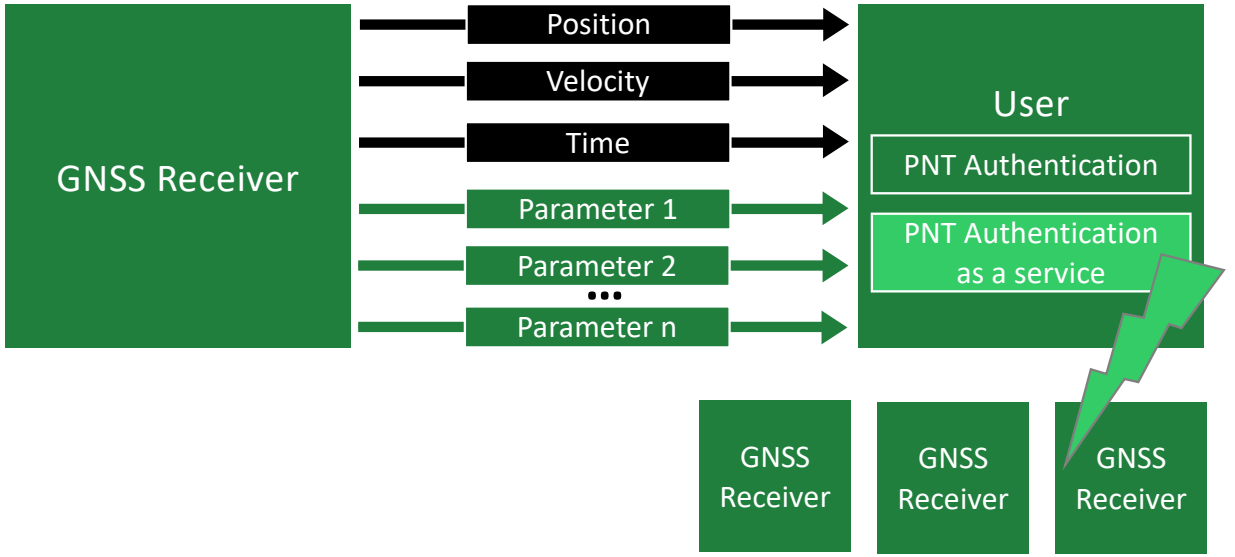
Today, users are using only limited data provided by the GNSS receiver.



With Regulus

The Regulus Pyramid SW library uses a wealth of unused data, analyzing, comparing and combining it to be able to detect and protect against a wide range of sophisticated spoofing attacks.

By adding an Internet connectivity service, more parameters are used in real time to allow even better results in a fleet environment.



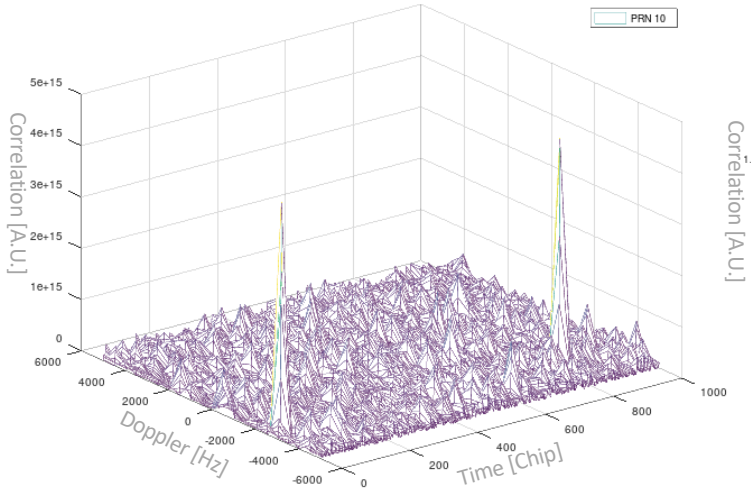
About Mitigation

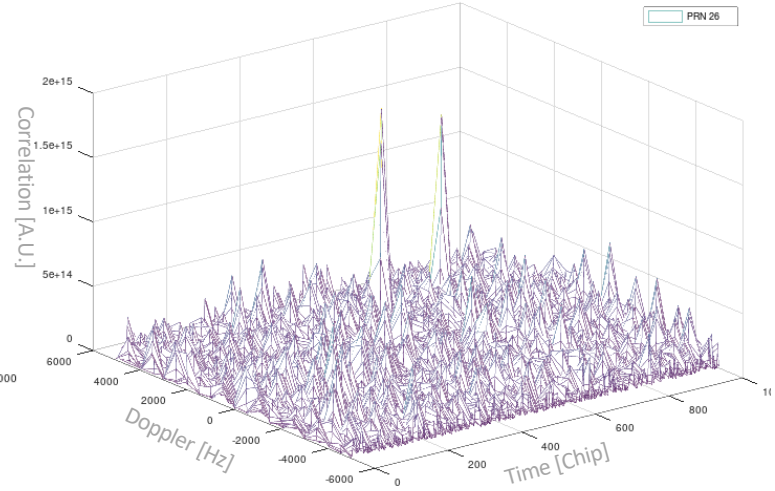
Mitigation - A smart algorithm is able to track all signals of all satellites received by the GNSS receiver and to classify them using signal processing methods into two groups: signals from satellites and signals from SDRs (software defined radios). This enables the mitigation software to solve and display two positioning solutions.

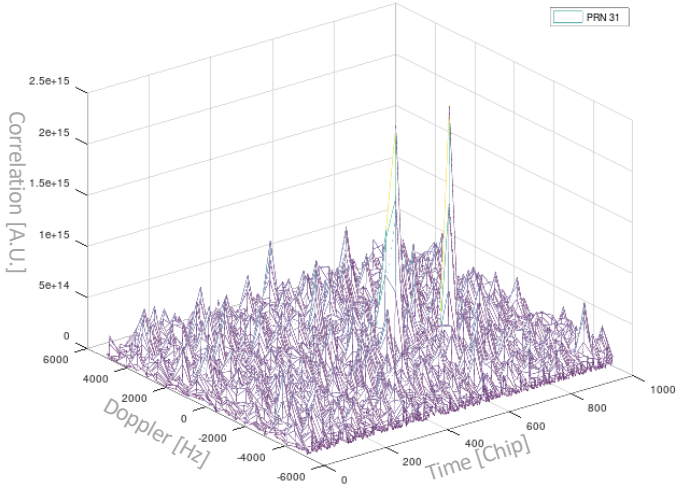
The GNSS time and positioning mitigation algorithm solver builds REAL and SPOOFED solutions.

```
Position 0: 2019-Sep-23 01:03:16.320000 UTC using 10 satellites: lat = 30.288838047º long = -97.735454498º height = 214.177m
Position 1: 2019-Sep-23 01:03:17.320000 UTC using 7 satellites: lat = 30.289230446º long = -97.736413713º height = 213.402m
Position 0: 2019-Sep-23 01:03:16.820000 UTC using 10 satellites: lat = 30.288848393º long = -97.735460708º height = 215.857m
Position 1: 2019-Sep-23 01:03:17.820000 UTC using 7 satellites: lat = 30.289219688º long = -97.736412624º height = 212.467m
```

While spoofing is happening, a double correlation peak appears for each satellite in the doppler time domain. The spoofing mitigation algorithm classifies the correlation peaks to “real” and “spoofed” peaks and solves the positioning and time equations for each group.







Regulation

PNT Resilience for Critical Infrastructure

February 12, 2020 Executive Order 13905

Goal: Creation of cybersecurity guidelines and responsible usage profiles for PNT and GPS services in the critical infrastructure sectors.

- NIST is responsible for creating one basic user profile that will be further defined by Sector Specific Agencies (SSA)
- Published RFI in July **to gather information about managing cybersecurity risks, to systems, networks, and assets dependent on PNT services**
  - Close to 40 submissions, over 50% addressing GNSS spoofing as a threat to PNT systems.
  - PNT and GNSS resiliency against spoofing often addressed within timing synchronization context, primarily regarding: Telecommunications, Datacentres, Financial Institutions, and Energy Sector among others.
- Displays consensus within industry that resilient timing and synchronization solution require hardening of GNSS receivers and advances technology for authentication and integrity checks.

Timing Security

GPS resiliency at the heart of the 5G revolution

The Telecommunication sector is using a variety of technologies to achieve synchronized timing and hold over capabilities, however with advanced LTE and 5G synchronization requirements are evolvingly stringent.

- With advanced LTE and 5G, it is necessary that the timing reference source (GNSS) is deployed close enough to any PTP/NTP client or end point within the network, in order to ensure the needed quality of the time stamp.
- NTP/PTP technology and atomic clocks are efficient ways to ensure the ongoing timing synchronization provided by GNSS receivers and hold-over capabilities **but cannot provide protection against cybercriminals that may generate distorted satellite signals and disrupt services.**
- GNSS technology projected to be deployed more frequently in order to meet the synchronization requirements.
- With the growing reliance on ultra timing synchronization, the implicated risks due to deliberated attacks on timing reference sources needs to be addressed.

For the 5G revolution to be successful GNSS based timing synchronization technology needs to be reliable and resilient against cybersecurity attacks.

In the future, 5G network disruptions can have massive impacts on smart cities and connected services, extending from mass transportation systems to mobility and location-based services.

We are ready for integration!

yoav@regulus.com

More info @
www.regulus.com

DOWNLOAD

DOWNLOAD