Improving the robustness of GPS Receivers to defend against spoofing/cyber attacks

Guy Buesnel

Contents

- Real GNSS Incidents
- Likely evolution of GNSS Threats
- Overview of GNSS Threat mitigation
- GNSS Spoofing
- GNSS Spoofing attack vectors
- GNSS Spoofing detection
- Considerations for Spoofing test bed
- Integrated detection methods for spoofing
- Final thoughts

Real GNSS Incidents

- **FBI Cyber Division – Private Industry Notification October 2014**

- Auto thieves shipping vehicles to China used GPS jammers placed in shipping containers in an attempt to thwart tracking of the containers, according to July 2014 information from the National Insurance Crime Bureau.
- In 46 reported incidents, the thieves placed one or more GPS jammers in cargo containers with stolen automobiles.

- Cargo thieves in North Florida used GPS jammers with a stolen refrigerated trailer containing a temperature controlled shipment
- In this incident, the hauling tractors were swapped out by the cargo thieves. The Miami based suspects were ultimately stopped and apprehended by the Florida Highway Patrol in mid-Florida on a routine vehicle stop -the shipment was recovered intact.
- Discovered, hidden inside of the trailer's refrigerator unit, were portable GPS jamming devices hooked unobtrusively to a battery located inside the unit

Real GNSS Incidents

GPS leap – second issue January 2014

- On January 21, GPS navigation messages began to include future leap second data indicating an addition to the leap second that will go into effect at the end of June 2015.
- Apparently several brands/models of GPS receivers "seem to be mishandling this information and applying the leap second now," which is creating a negative one-second offset in faulty receivers.
- The U.S. Coast Guard Navigation Center has received reports of these receivers causing synchronization issues with radios, computer systems, and data logging equipment.

- Story from Inside GNSS

Real GNSS Incidents

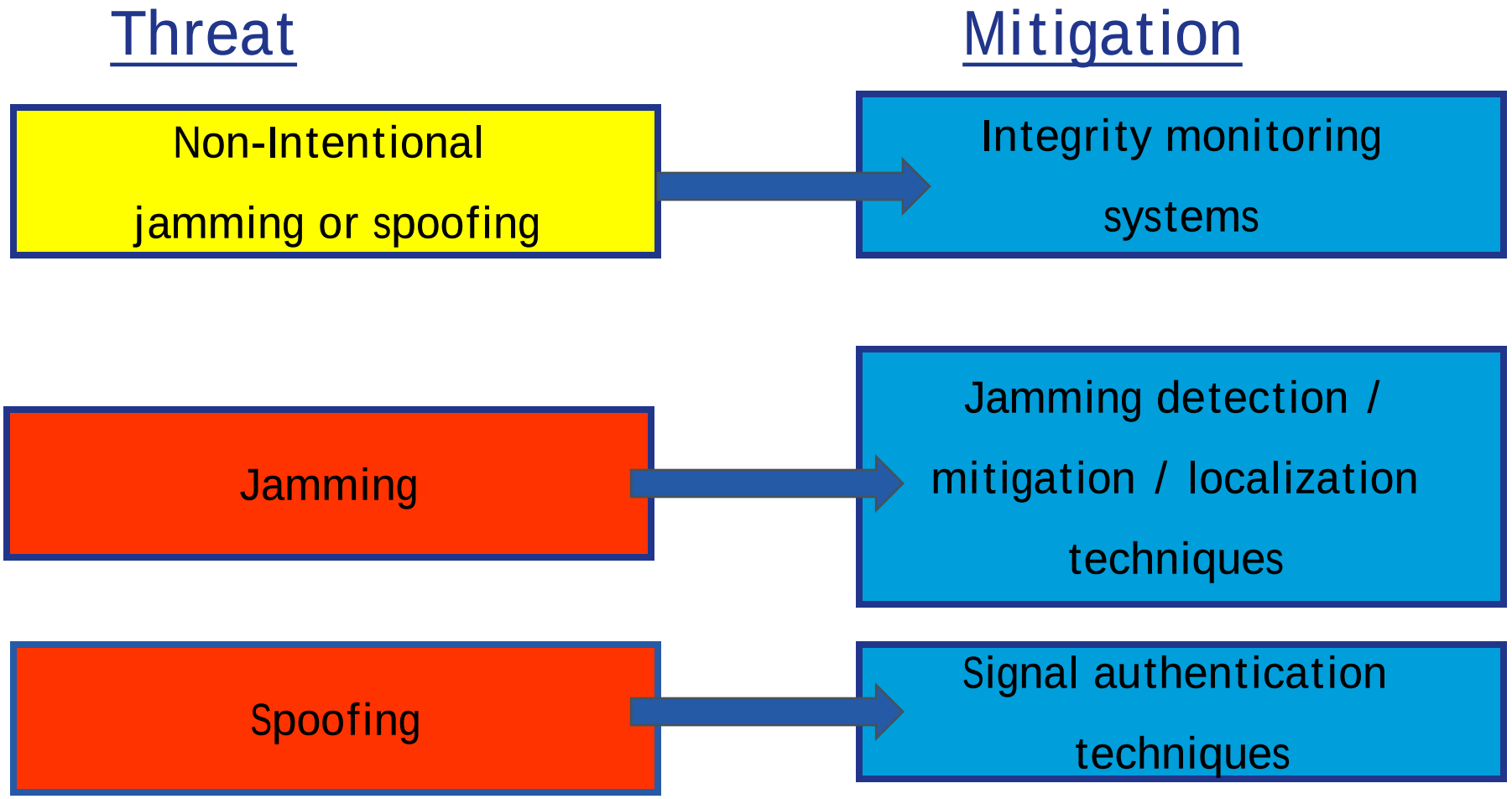
- Global fishing watch project - 2014
- Satellite AIS Receiver – Reception footprint shown (Atlantic Ocean)

- Two ships observed definitely spoofing their position – either spoofing GPS or inserting false data into the AIS transponder

How are GNSS threats evolving?

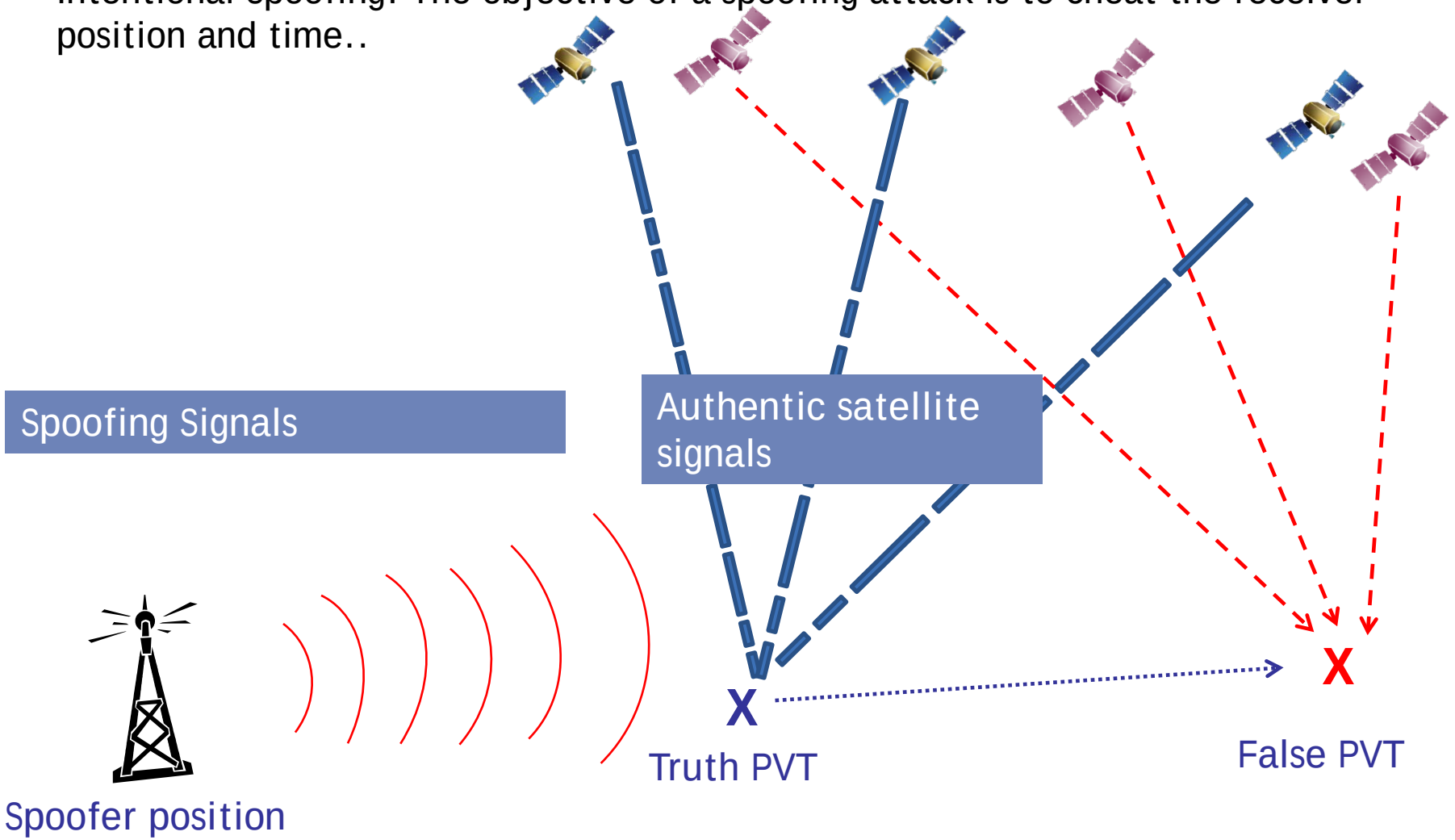
- Interference threat increasing rapidly – Many real jamming events being detected every day
- Spoofing is (in comparison) in its infancy… but – becoming much easier to carry out
- Human error will cause problems (Control centre operators, Software…)
- As in the IP world the threats to GNSS will likely come from the following groups (Source SANS Institute)
  - Unstructured Hacker
  - Structured Hacker
  - Organised crime/industrial espionage
  - Insider
  - Unfunded terrorist group
  - Funded terrorist group
  - Nation State
- Strong parallels with evolution of Information Security threats (Theunissen)

GNSS Threat Mitigation – an overview



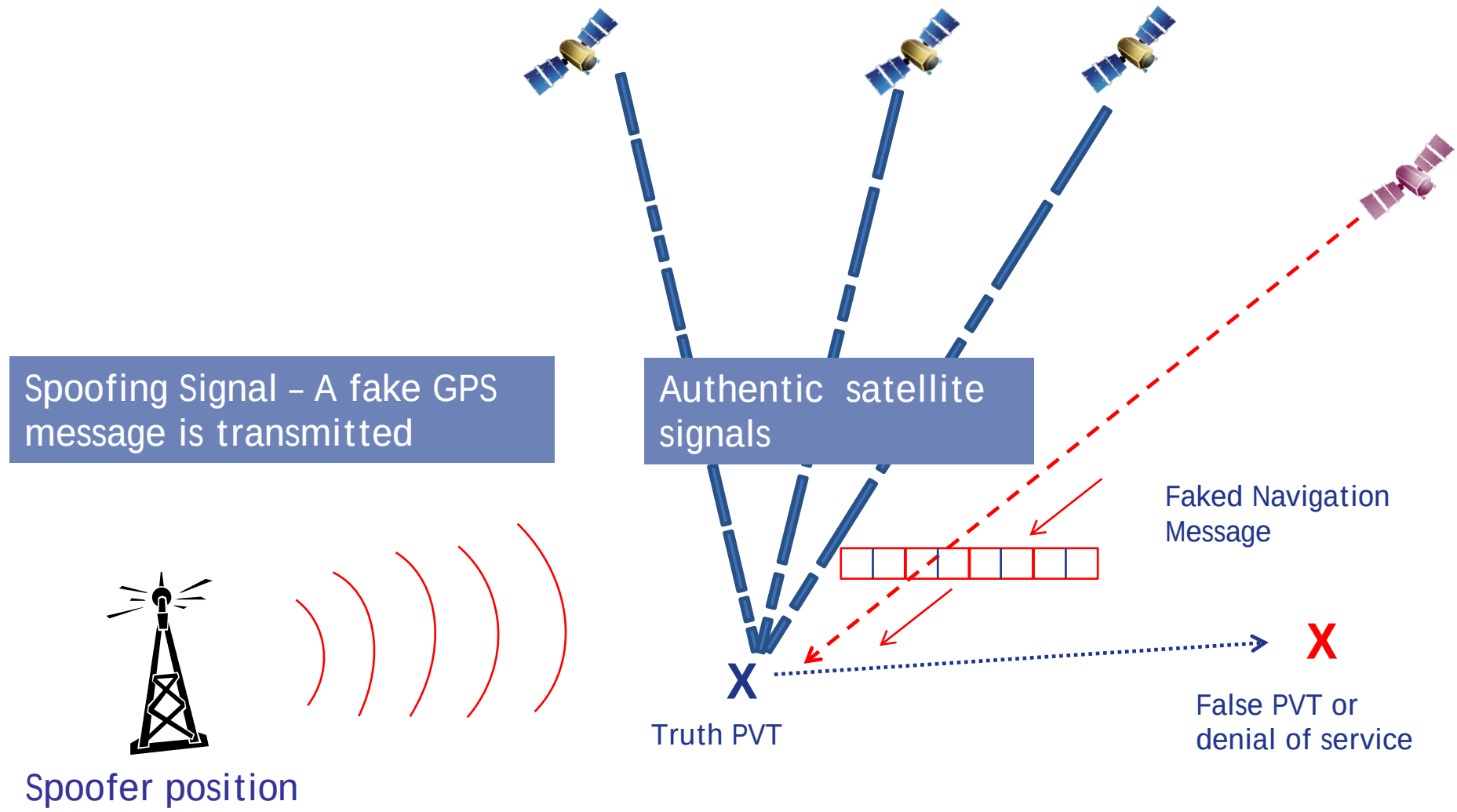
GNSS spoofing

- Intentional Spoofing: The objective of a spoofing attack is to cheat the receiver position and time..



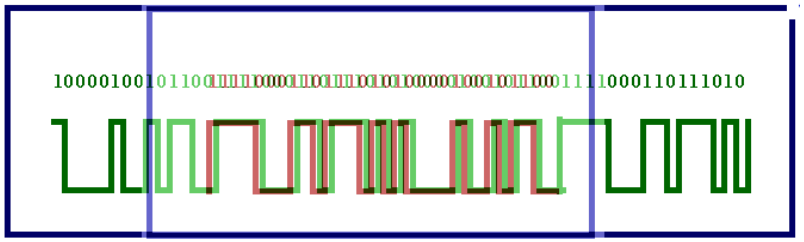
GNSS spoofing

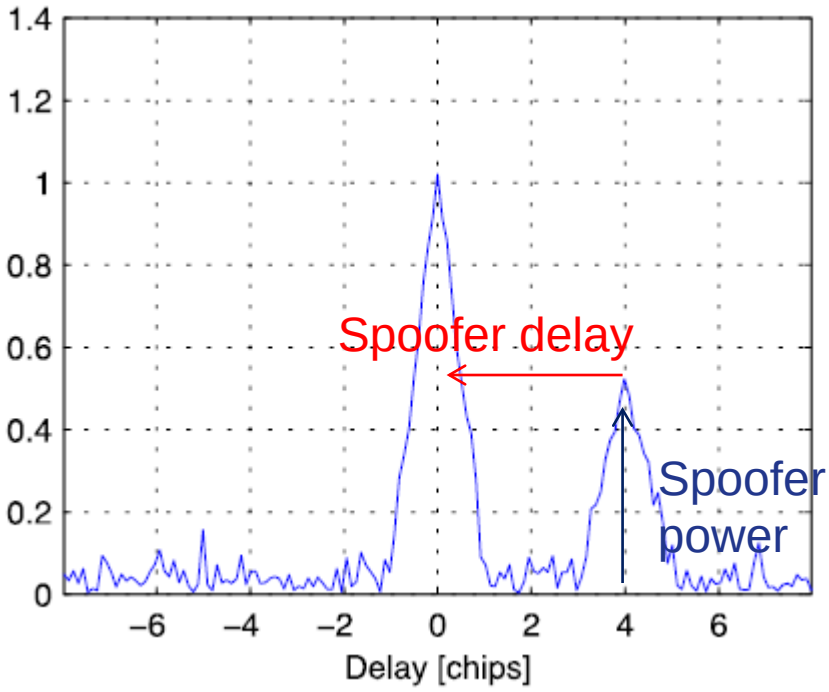
Spoofing the navigation message…



GNSS spoofing attack vectors

- The attacker might attempt to align code and power to the real signal to avoid jumps / lock loss
- The attacker might attempt to replay space navigation data in order to bypass data verification mechanisms
- The attacker might attempt to force the receiver to acquisition mode in order to cheat spoofing detection implemented in tracking loops
- The attacker might attempt to modify navigation data (e.g. EGNOS)





Spoofing detection – Power levels

- Monitor signal power of each Satellite
  - Spoof Signal is likely to have noticeably higher power
- Monitor signal power rate of change as vehicle moves
  - Proximity of Spoof Signal will cause higher power changes on movement
- Monitor relative power of each GNSS signal per Satellite
  - L1/L2/L5, P(Y), C/A and C should be a relatively fixed power offsets

Spoofing detection – Signal Changes

- Bound and Compare range rates
  - Code and Carrier range rate changes will be different for a Spoof Signal
- Doppler Shift Check
  - Spoof Signal is likely to be from a fixed position so Doppler is likely to be incorrect
- Cross-Correlation of L1/L2
  - Use Codeless tracking to check L1/L2 delay, and match to other satellites
- Range Differences L1/L2/L5 signals
  - Range should be the same only Atmosphere should cause delays

Spoofing detection - other

- Verify Received Navigation Data
  - Compare Almanac/Ephemeris to known data
  - Check for ‘missing/default’ Navigation data
- Jump Detection
  - Observable should remain within a tolerable range, check for sudden changes
- Check GNSS Position with other sensors (GPS/IMU)
  - IMU position will drift over time but look for rate of drift changes
- Compare GPS Position with other GNSS (Glonass, Galileo, etc.)
  - Positions from all GNSS systems should be similar so large variations could indicate a Spoof Signal is being used
- Angle of Arrival determination
  - Multi element antenna technology can determine the angle of arrival of received signals. The spoofed signal channels will all appear from one source

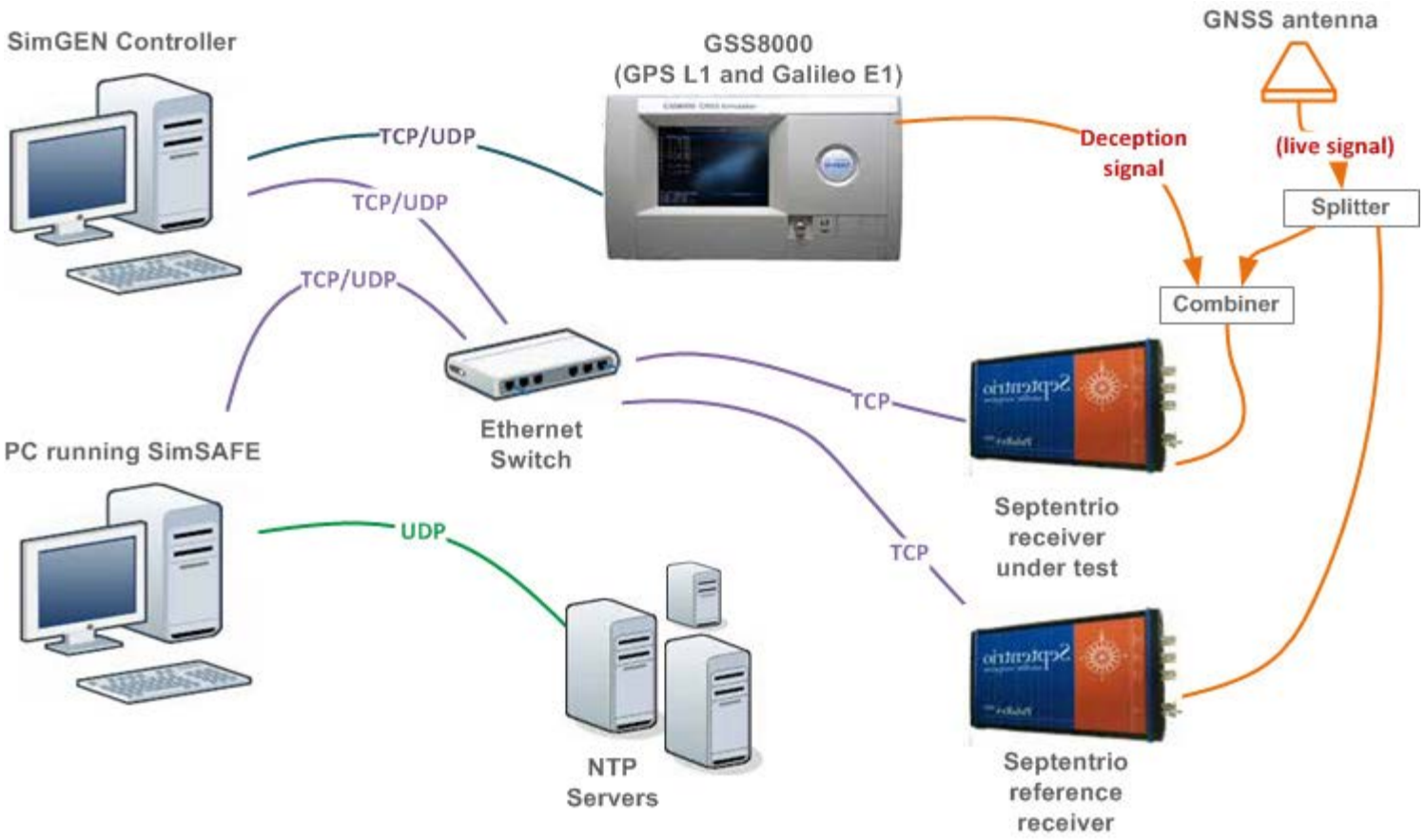
Considerations for a GNSS spoofing test bed

- Pseudorange ramp
- Signal strength
- Power ramp
- Transmitting status
- Navigation data replica
- Navigation data modification
- Sinusoidal deception signal
- Receiver/Simulator data comparison
- Multi-path/Line of Sight data comparison
- Receiver configuration
- Apply an offset to the antenna position

Integrated detection mechanisms for spoofing

- Detection using receiver output data
  - Pseudorange step detection
  - C/N0 step detection
  - Clock bias step detection
  - RAIM
  - Loss of lock on channel
- Detection comparing data with a trusted receiver
  - Navigation data monitoring
  - PVT Solution

Live Sky/Simulated test set-up



Final thoughts..

- GNSS spoofing is an emerging and real threat
  - All attacks on GNSS are cyber-attacks – and have the same consequences, ranging from a Denial of Service, a Distributed Denial of Service, to manipulation of important data (eg timing information through insertion of a fake message0
  - GNSS attacks will evolve in the same way as they have in the information security community (internet)
  - We must learn to deal with them using the experience in the Information Security domain
- Spoofing can be detected
  - Some attacks are much easier than others to defend against
  - Good system design makes things much harder for the hacker
- Understand likely risks and impact of GNSS spoofing on business
  - Which groups of hackers might target your system? What would their motivation be?
  - What resources might they have? What would be the consequences on your business of a successful GNSS spoofing attack?

Improving the robustness of GPS Receivers to defend against spoofing/cyber attacks

Thank you

spirent.com