Ensuring PNT Robustness, Resiliency, & Interoperability: the upcoming Galileo Signal Authentication services & Anti-spoof Techniques.

Dr. Oscar Pozzobon

National Space-Based Positioning, Navigation, and Timing Advisory Board

November 21st, Cocoa Beach, Florida
Our background

System Engineering & Cybersecurity R&D
Scientific Missions

Advanced Navigation Systems

GNSS simulation
Universal Threat Management

Cyber attack detection & response

Security Testbed

GNSS SDR

Cybersecurity Simulation

Jam/Spoof monitoring

UNCLASSIFIED – FOR PUBLIC USE
All rights reserved © 2019 Qascom S.r.l.
The evolution of attacks in ICT

Cybercrime is the most growing threat in the network and computer security domain

ICT cyber attacks

- Cyber Crime: 49%
- Hacktivism: 7.4%
- Cyber Espionage: 4.3%
- Cyber Warfare: 27.7%

Source: web

GNSS cyber attacks (2018-2019)

- Cybercrime: 67%
- Hacktivism: 6%
- Cyber Warfare: 17%
- Intentional: 10%

Source: web
A motivational risk analysis perspective

- Computer networks: 400 to 500 millions attack per year.
  - 18M$ cost per service as average
  - Total world wide cost expected to reach 6 trillion$

- GNSS: 10 to 20 attacks per sector reported annually in the public?
  - What is the total cost of GNSS spoofing attacks to date?

- Growth of attacks mainly proportional to:
  - Political Cyberwarfare context
  - Financial payments that rely on GNSS

- Shall we consider the risk probability mainly proportional to a potential motivation of the attacker?
Currently there are two trends:

- User protection, with autonomous anti-spoofing techniques
  Implementations available since the last 5 years in the market
- System based services
  - Galileo Authentication services
  - SBAS Authentication
  - Others: GPS CHIMERA proposals

- Autonomous Anti-spoofing
- Galileo OSNMA
- Galileo CAS
- Antenna Techniques
- Receiver Techniques
- Other Sensors integration
Galileo Authentication developments foresee signals on
- E6C: Galileo Commercial Authentication Service (CAS)
- E1B: Galileo Open Service Navigation Message Authentication (OSNMA)

Future Authentication Signals under investigation

Date TBD

IOT starting in 2020
Overall Spoofing likelihood of success

- The probability of success for the spoofing attacker is the combination of:
  - The probability to enter at the right power in the first radio stage
  - The probability to capture the right dynamic in the acquisition and tracking and shift with intelligence
  - The probability to bypass all sanity and integrity checks in the navigation solution, and to stay within the other nav and time systems accuracy boundaries
Autonomous anti-spoofing techniques can provide detection and mitigation in a number of stages of a navigation system. They are evaluated by statistical, detection timing and security performances.
Data authentication provides assurance that the data is coming from the satellite, and position solution is performed with the right data.

The Open Service Navigation Message Authentication (OSNMA) will be available in 2020.

Ongoing activities for SBAS.
Data and signal authentication provides assurance that the data and signals are coming from the satellites, and position solution is performed with the right data and ranging.

The Galileo Commercial and Authentication (CAS) Service is under definition.

- Ongoing activities for OS auth evolutions
Conclusions: Benefits of Combined GPS Galileo

- Combined GPS Galileo solutions provides advantages in a number of domains:
  - Space and deep space applications, capability to track more signals and perform longer integration on combined GPS and Galileo signals
  - Increase robustness in critical applications by:
    - Use of Galileo upcoming Galileo signals
    - Slightly increased difficulty for attackers to simulate 3 frequencies, dual constellations, with a total of up to 100 signals (at least with SDR)
    - The need to hide more live constellations without jamming the receiver
  - Increased availability indoor and urban canyons, backup in case of outages (The recent Galileo one, and previous short GPS ground time glitch)
  - Use of future Galileo CS signals in snapshot mode, both for ground and space applications
Thank you!

Oscar Pozzobon
info@qascom.com

National Space-Based Positioning, Navigation, and Timing Advisory Board
Date: November 21st
Cocoa Beach, Florida