U.S. Department of Homeland Security | Science and Technology Directorate

A Cybersecurity Perspective to Addressing PNT Vulnerabilities

Civil GPS Service Interface Committee

Science and Technology

Ernest Wong
PNT Technical Lead
Technology Centers Division
September 19, 2022

Agenda

- The Communication Challenge

- The Cybersecurity Angle
  - For End-Users: Conveying PNT Vulnerabilities to Non-PNT SMEs
  - For Designers: Traditional Approach vs. Cybersecurity Approach to Mitigations

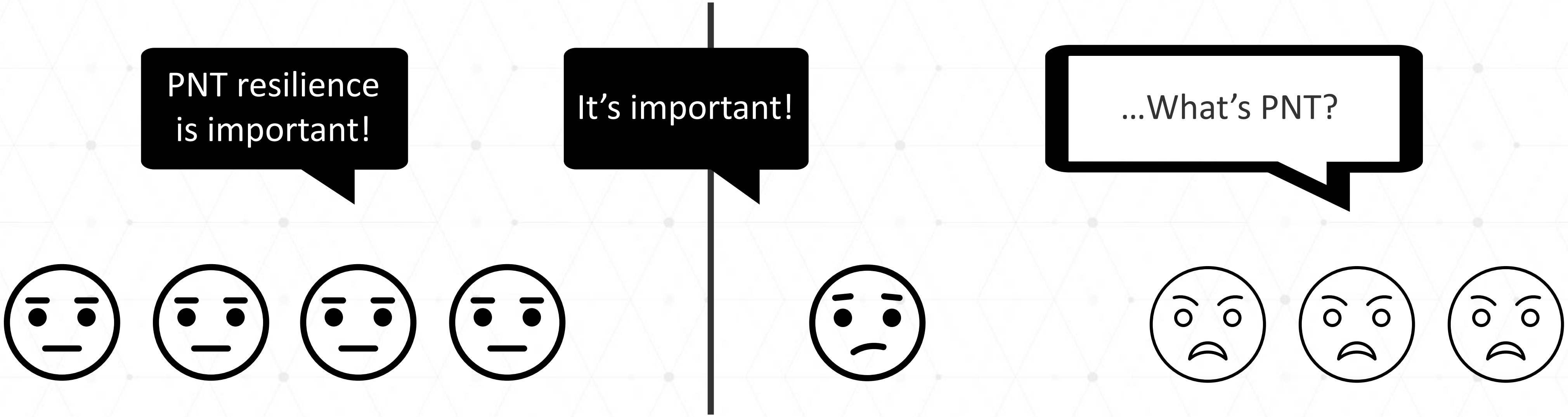
- DHS Resilient PNT Reference Architectures: Applying ZTA concepts to PNT

Acronyms

- PNT: Positioning, Navigation, and Timing
- GPS: Global Positioning System
- GNSS: Global Navigation Satellite System
- UE: User Equipment
- ZTA: Zero Trust Architectures

The Challenge: Asymmetric Expertise

- Importance of PNT vulnerabilities and resilience well understood within PNT industry.
- However, understanding across end-user community is less consistent.



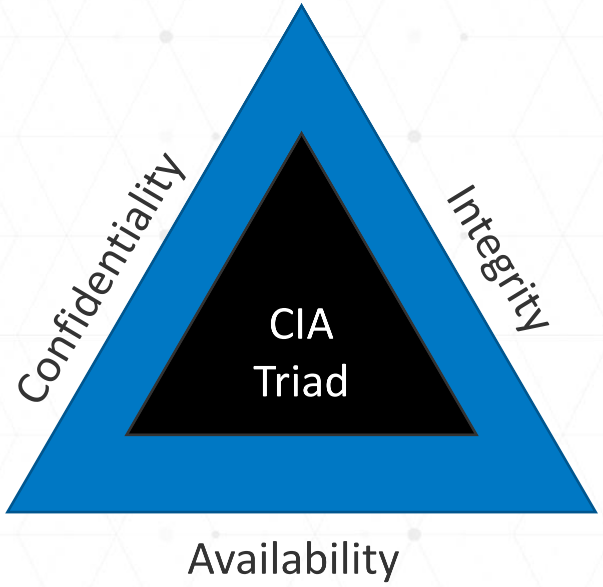
The Cybersecurity Angle

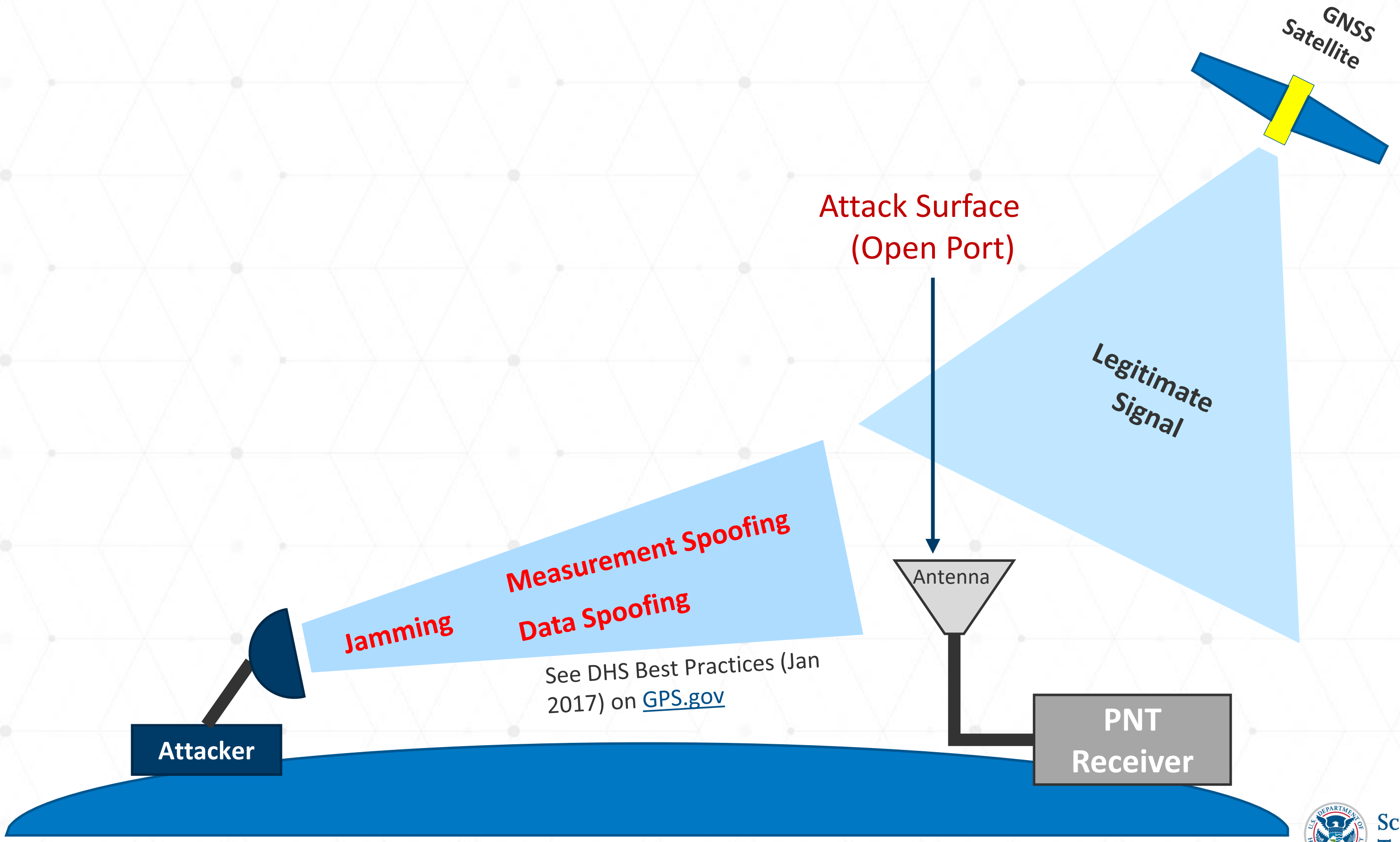
- PNT industry should consider the cybersecurity perspective both when discussing PNT resilience and designing mitigation measures.

- **Reasons to Adopt a Cybersecurity Perspective to PNT Resilience:**
  - Cybersecurity concepts & terminology fit the problem well and is more widely understood by end-users.
  - Cybersecurity perspective to designing PNT resilience (user system) provides a holistic approach.

Translating the Vulnerabilities

- **Objective**: Enable discussion of PNT issues beyond the PNT SME community.





See DHS Best Practices (Jan 2017) on GPS.gov

Translating the Vulnerabilities (Examples)

GPS Threat Example	Cybersecurity Equivalent	Effect (CIA Triad)
GPS Jamming	Denial-of-Service Attack	Loss of Availability (Transient) Recovers after removal of threat
GPS Data Spoofing Example: 2017 ION GNSS+	Ransomware / Wiper	Loss of Availability (Persistent) Persists after removal of threat
GPS Measurement Spoofing	Data Manipulation (MITRE ATT&CK Framework T1565)	Loss of Integrity

Traditional UE Resilience Measures

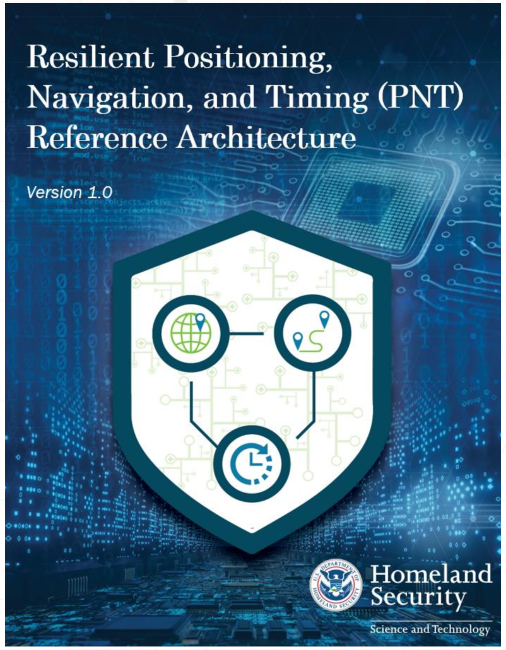
- **Scope of Traditional PNT Resilience:**
    - Anomaly Detection
    - Holdover Devices (e.g., oscillator)
    - Additional PNT sources

- ***Incorporating Cybersecurity Angle***
    - Uncovers dynamics of how threats enter a system.
    - Informs architecture design on how to mitigate.

Cybersecurity-Informed Approach

- **Additional UE Considerations:**
  - Attack Surfaces: Identifying and minimizing
  - Edge vs. Core: Importance of placement of verification/detection
  - Defense-in-Depth: Variety of threat dynamics requires defenses at multiple points from edge to core.
  - Component Isolation: To prevent impacts to lateral sources
  - Software Assurance: Reduce vulnerabilities from implementation errors

- **Example**: DHS Resilient PNT Reference Architecture
  - Incorporates Zero Trust Architectures concepts into design of Resilient PNT UE System
  - Emphasis on verification & isolation (see May 2022 PNT AB for full brief)
    - https://www.gps.gov/governance/advisory/meetings/2022-05/



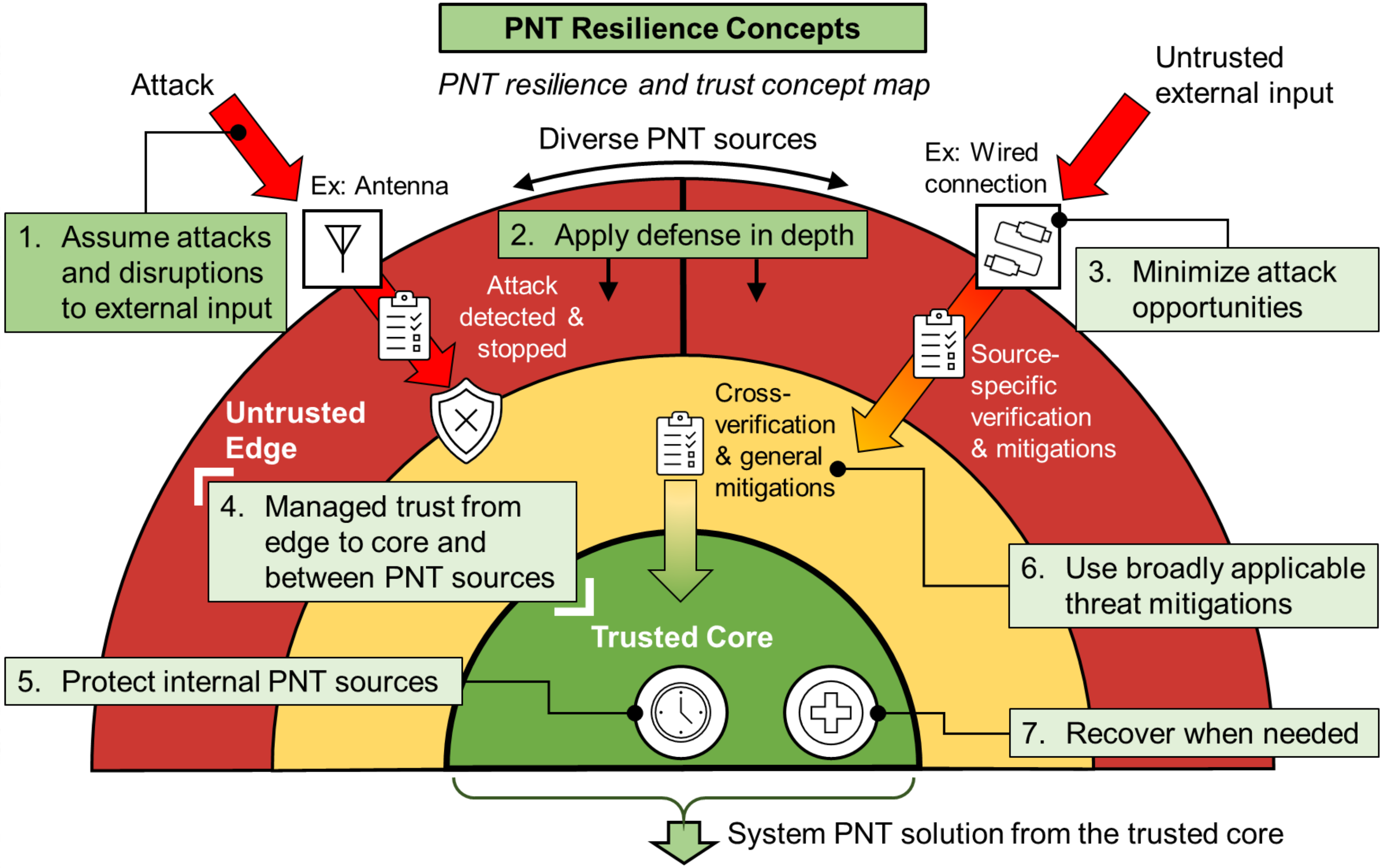
Resilient Positioning, Navigation, and Timing (PNT) Reference Architecture

Version 1.0

Homeland Security

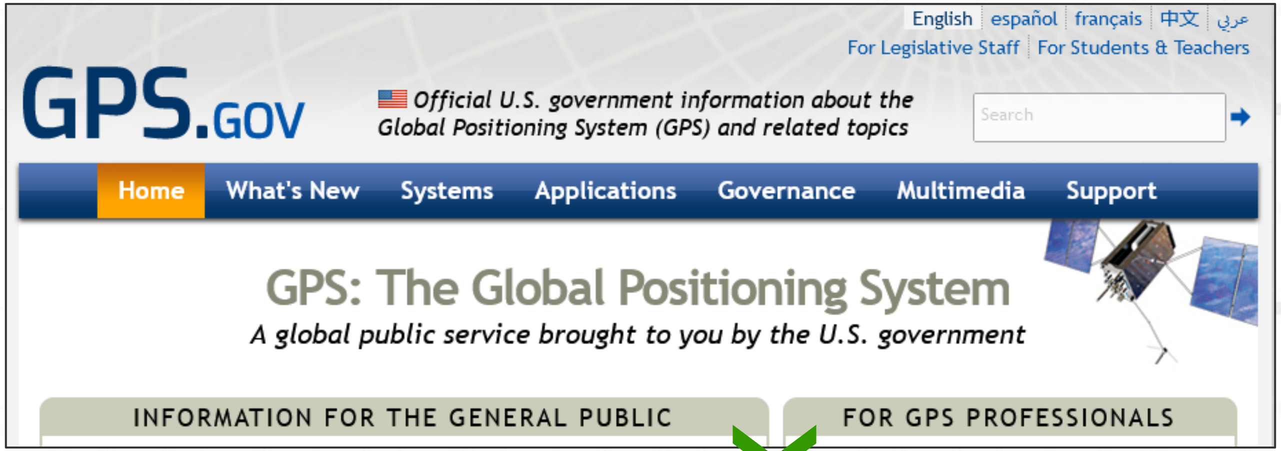
Science and Technology

Applying Zero Trust Concepts to PNT


PNT Resilience Concepts
PNT resilience and trust concept map
Attack
Ex: Antenna
Diverse PNT sources
Ex: Wired connection
Untrusted external input
1. Assume attacks and disruptions to external input
2. Apply defense in depth
3. Minimize attack opportunities
Attack detected & stopped
Source-specific verification & mitigations
Untrusted Edge
Cross-verification & general mitigations
4. Managed trust from edge to core and between PNT sources
6. Use broadly applicable threat mitigations
Trusted Core
5. Protect internal PNT sources
7. Recover when needed
System PNT solution from the trusted core

Resource Links

- GPS.gov Resilience Repository
  - https://www.gps.gov/resilience/
- DHS Resilient PNT Reference Architecture
  - https://www.dhs.gov/science-and-technology/publication/resilient-pnt-reference-architecture
- DHS Resilient PNT Conformance Framework
  - https://www.dhs.gov/publication/st-resilient-pnt-conformance-framework
- PNT Integrity Library
  - https://github.com/cisagov/PNT-Integrity
- Epsilon Algorithms
  - https://github.com/cisagov/Epsilon
- DHS S&T PNT Program
  - https://www.dhs.gov/science-and-technology/pnt-program
- DHS CISA PNT Program Management Office
  - https://www.cisa.gov/pnt


English | español | français | 中文 | عربي
For Legislative Staff | For Students & Teachers
GPS.GOV
Search
Home
What's New
Systems
Applications
Governance
Multimedia
Support

Official U.S. government information about the Global Positioning System (GPS) and related topics

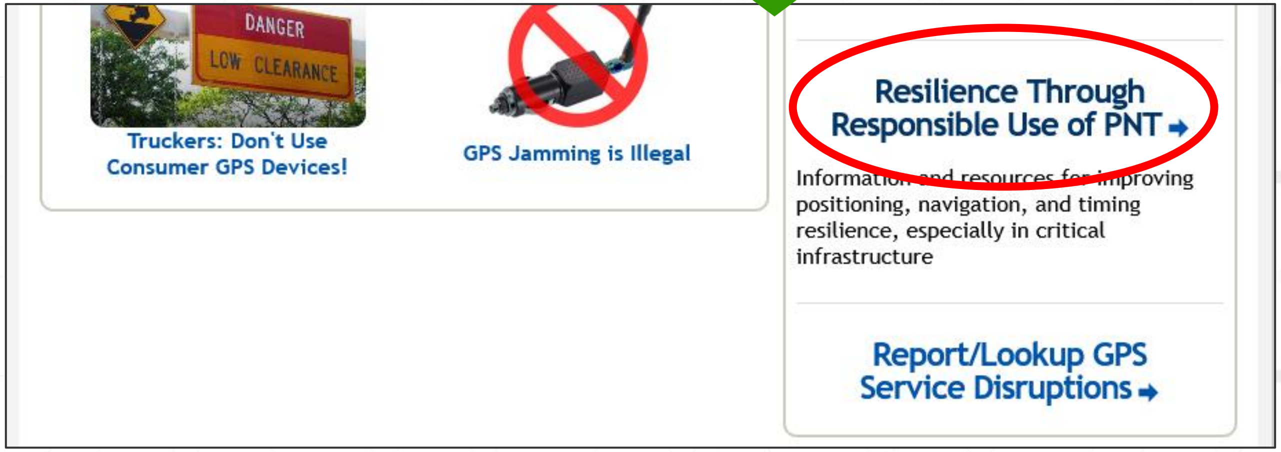
GPS: The Global Positioning System

A global public service brought to you by the U.S. government

INFORMATION FOR THE GENERAL PUBLIC

FOR GPS PROFESSIONALS

Scroll to lower right corner



Truckers: Don't Use Consumer GPS Devices!

GPS Jamming is Illegal

Resilience Through Responsible Use of PNT →

Information and resources for improving positioning, navigation, and timing resilience, especially in critical infrastructure

Report/Lookup GPS Service Disruptions →

Science and Technology

[SCIENCE AND TECHNOLOGY DIRECTORATE]

Engage with us:

scitech.dhs.gov

SandT.Innovation@hq.dhs.gov

@dhsscitech

Science and Technology