DHS SCIENCE AND TECHNOLOGY

Resilient PNT Reference Architecture:

Applying Cybersecurity Concepts to PNT Resilience

PNT Advisory Board

May 4, 2022

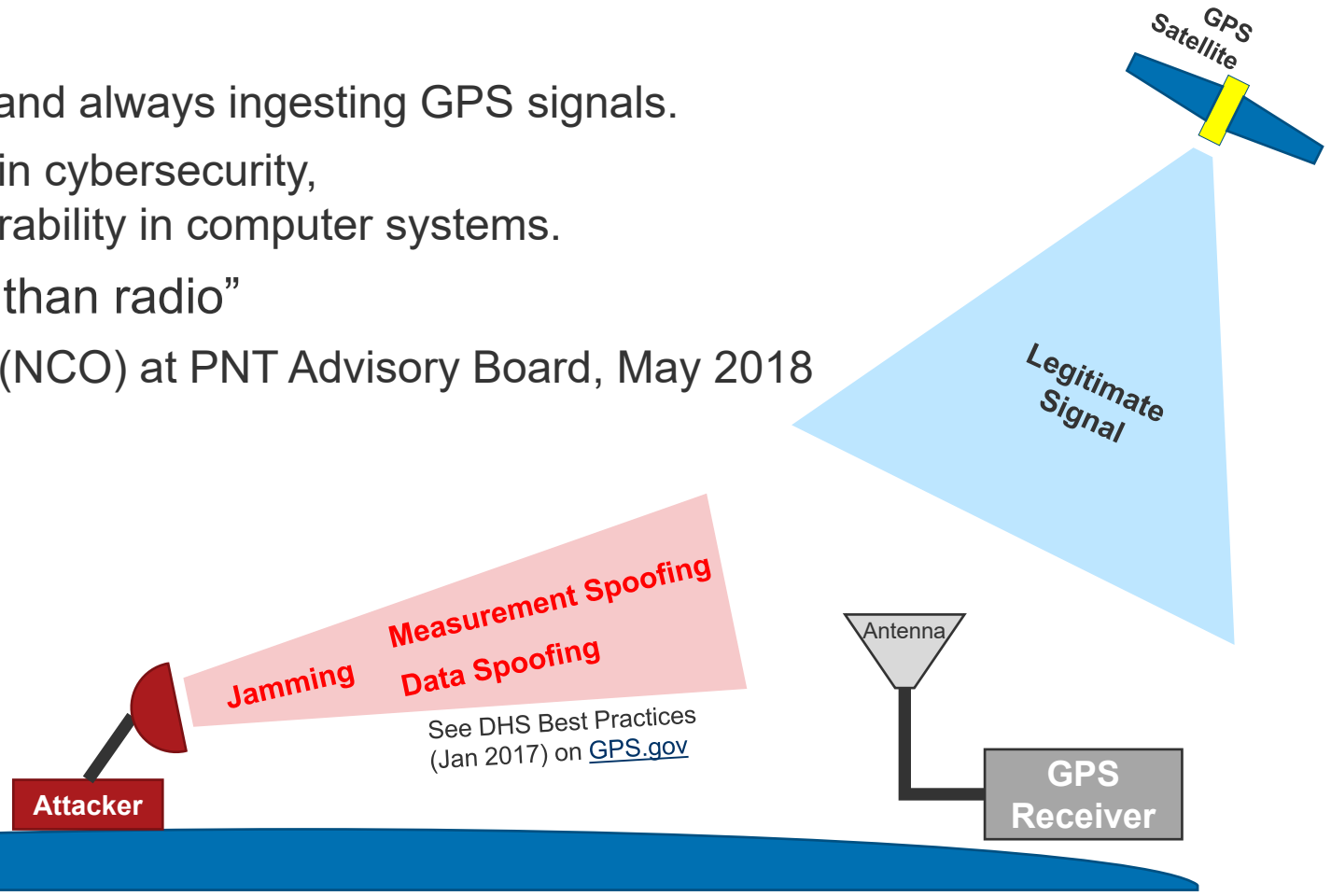
Ernest Wong

Technical Manager, PNT Technical Lead
Technology Centers Division
Science and Technology Directorate

Homeland Security
Science and Technology

Cybersecurity Lens: Open Ports

- "Open Port" Problem:
  - GPS Receiver is always listening and always ingesting GPS signals.
  - This is equivalent to an open port in cybersecurity, which is considered a major vulnerability in computer systems.
- "A GPS receiver is more computer than radio"
  - PNT National Coordination Office (NCO) at PNT Advisory Board, May 2018



Cybersecurity Lens: Attack Surfaces

- Based on industry trends, the future of PNT involves a multitude of signals.
- However, every PNT source is an attack surface.

Past

1 open port

Present & Future

+Non-GNSS Sources

Many open ports

Resilient PNT Reference Architecture

- **Purpose**
  1. Follow-on to Conformance Framework that provides concrete implementation examples. The CF was non-prescriptive in nature. The RA describe more clearly what was intended by the CF.

  2. Introduces how to implement modern cybersecurity principles (including Zero Trust Architectures) into PNT resilience.

  Applying these concepts in the design of NextGen Resilient PNT systems will enable them to be resilient against both current and future threats, through containing the impact of attacks and disrupting exploit chains.

What is Zero Trust?

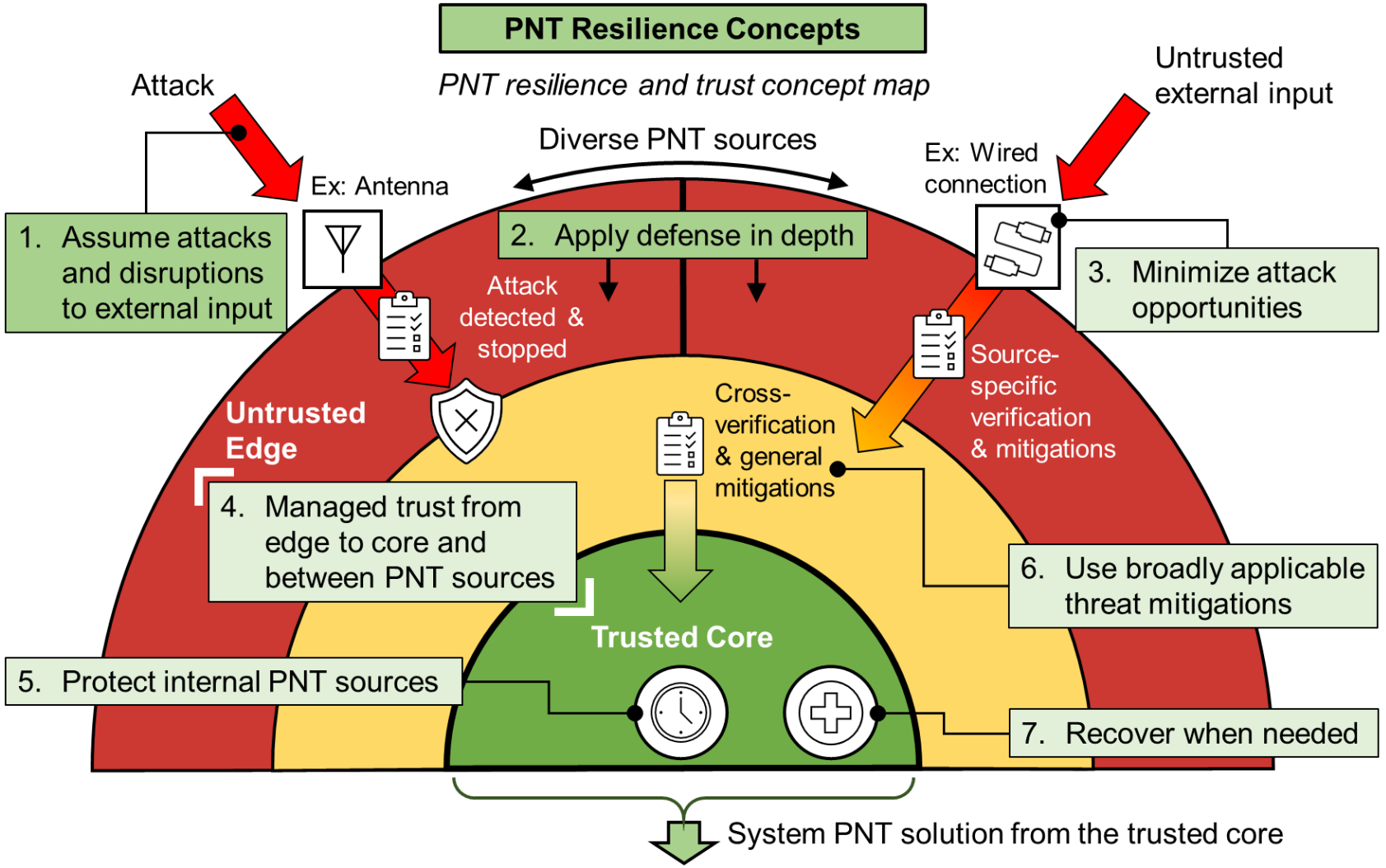
- **Objective of ZTA**: Contain and limit the impact of successful attacks and intrusions.

- **Key Requirements for Applying to PNT**
  - Verification
  - Component Isolation

- **Trusted Core**: If isolated properly, is inherently trusted as it does not require external input.
- **Untrusted Edge**: Inherently untrusted as it sits at the edge of the system and is an attack surface.

- **Implementation**: Ideal case is full isolation in a CF Level 4 receiver. But can scale down the concepts to lower levels.

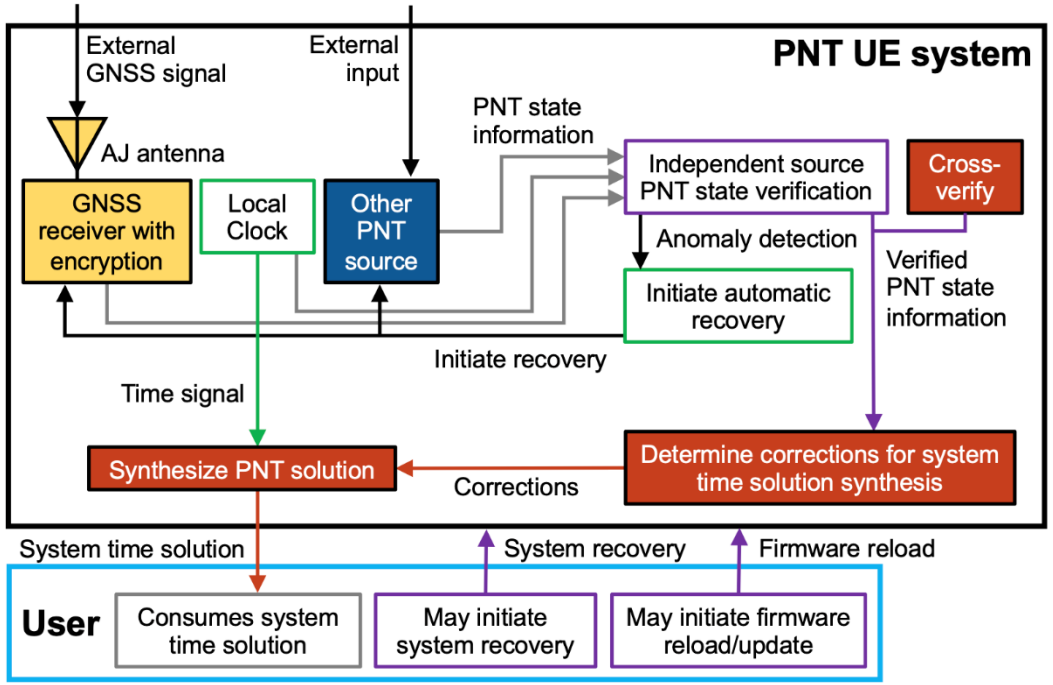
Applying Zero Trust Concepts to PNT



Homeland Security
Science and Technology

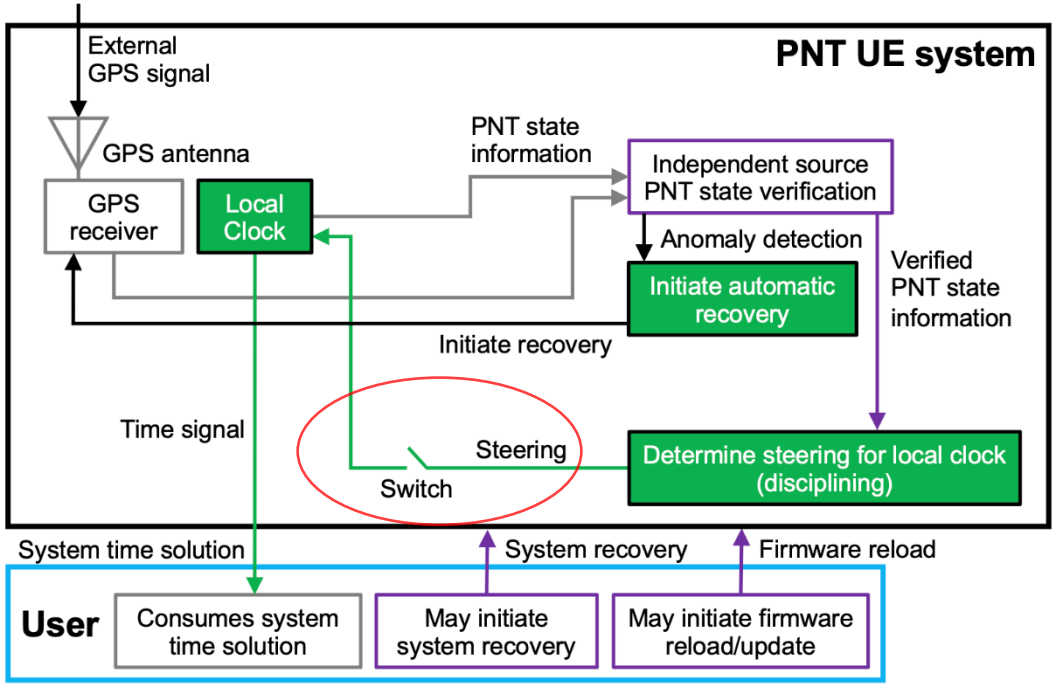
Level 3-4 Implementation Example

- Internal clock = primary source (b/c it's trusted the most—vs. GNSS source on the untrusted edge)
- Internal clock fully isolated. Corrections applied at solution synthesizer.



Level 2 Implementation Example

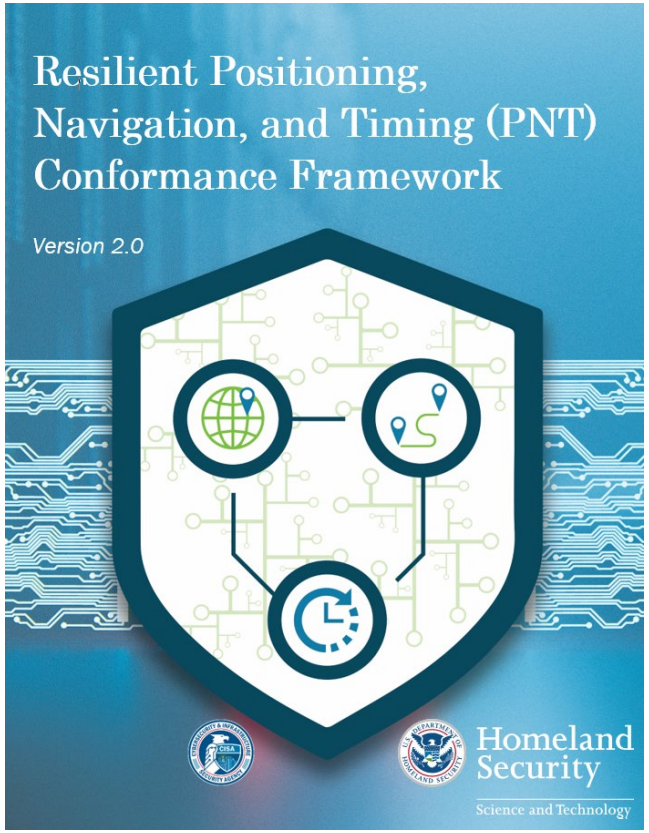
- Internal clock still primary source (b/c of trusted core vs. untrusted edge)
- Less isolation but can achieve some degree of it through the FLIP method (limit exposure to attack surface).

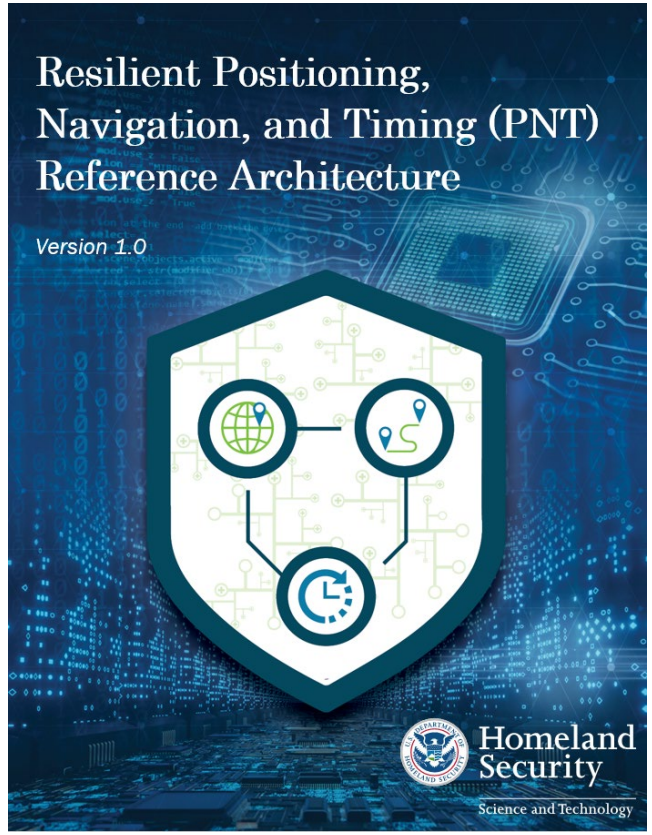


Upcoming Publications

- Planned publication in next 1-2 months:
  - Resilient PNT Conformance Framework v2.0
  - Resilient PNT Reference Architecture 1.0

- Will be posted to S&T website and GPS.gov





Resource Links

- GPS.gov Resilience Repository
  - https://www.gps.gov/resilience/
- 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

Homeland Security

Science and Technology

DIVERSE PERSPECTIVES + SHARED GOALS = POWERFUL SOLUTIONS