DHS SCIENCE AND TECHNOLOGY

A Cybersecurity-based Vision for NextGen Resilient PNT

Civil GPS Service Interface Committee

September 21, 2021

Ernest Wong

Technical Manager
Technology Centers Division
Science and Technology Directorate

Homeland Security
Science and Technology

Agenda

- Re-Framing the Problem
- Initial Efforts: Resilient PNT Conformance Framework
- Going Further: Resilient PNT Reference Architecture
- Related S&T Products
  - GPS Whitelist Development Guide
  - PNT Integrity Library + enhancement
- Links & Resources

Acronyms

- PNT: Positioning, Navigation, and Timing
- GPS: Global Positioning System
- GNSS: Global Navigation Satellite System
- IEEE: Institute of Electrical and Electronics Engineers

Re-Framing the Problem to Cybersecurity

- PNT receivers are always listening, ingesting, and processing PNT signals.
- This is equivalent to an “open port” in cybersecurity, which is a major vulnerability in computer systems.

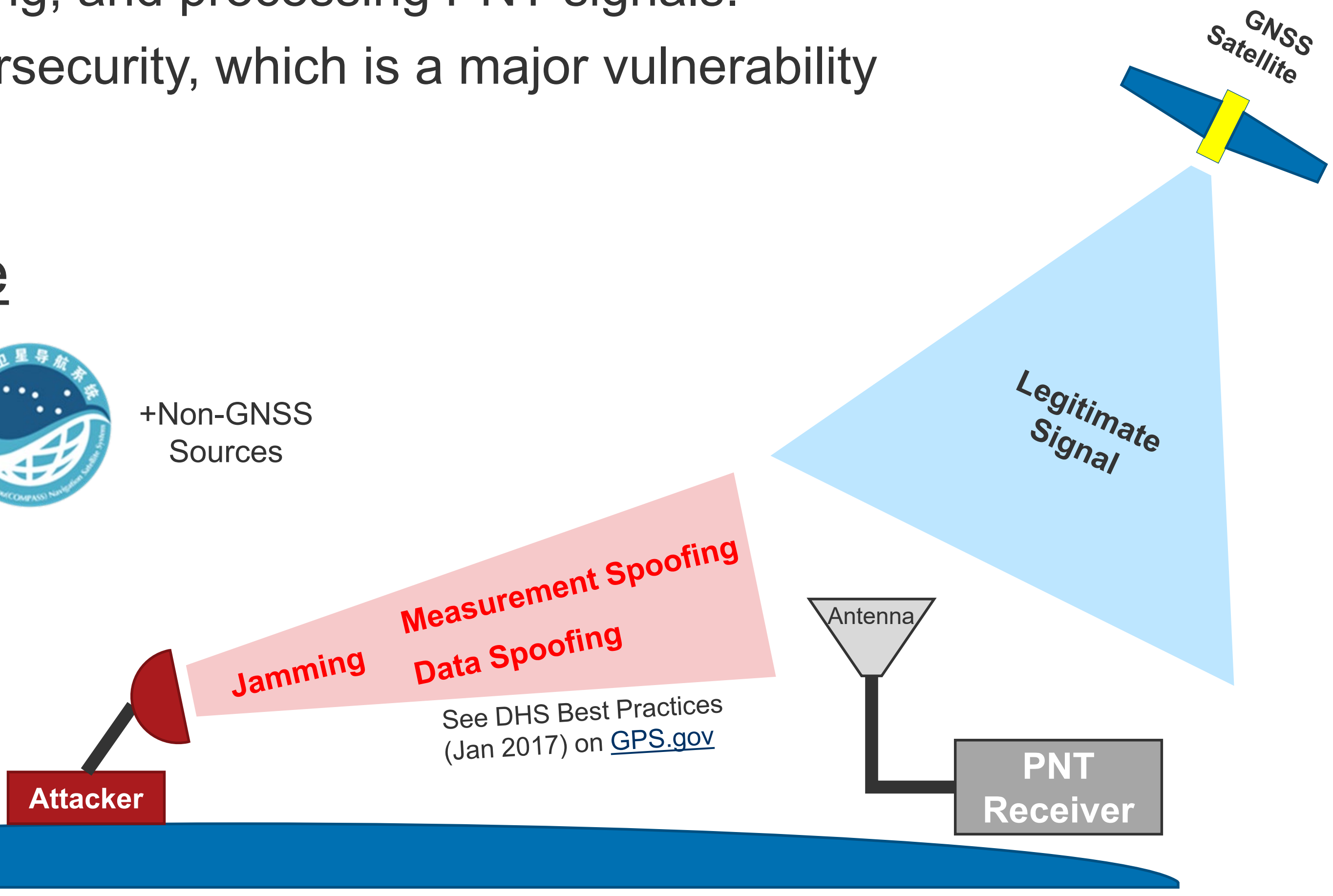
Past

1 Attack Surface

Present & Future

+Non-GNSS Sources

Many Attack Surfaces



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

Resilient PNT Conformance Framework

Background

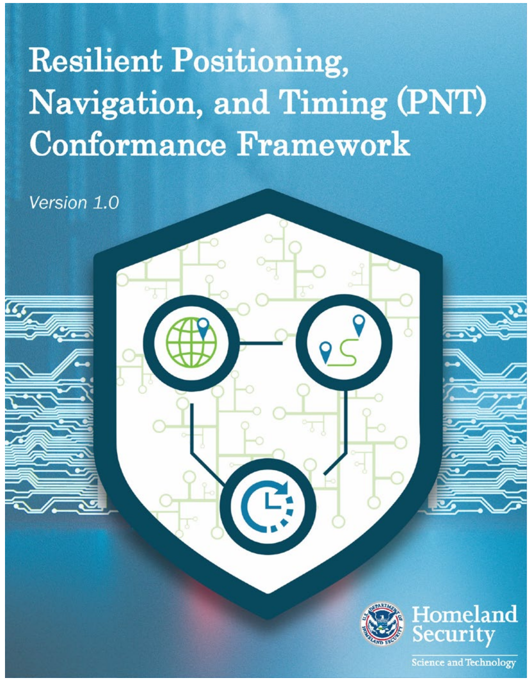
- Outcome-based and solution agnostic framework for defining expected behaviors from resilient PNT equipment across four levels of resilience. Published Dec 2020.
- Developed in collaboration with industry and federal interagency partners.

Initial Cybersecurity Steps

- Initial step for introducing cybersecurity concepts to PNT resilience.
- Concepts limited by the outcome-based and agnostic nature of the framework.

IEEE P1952

- Transitioned to IEEE in May 2021 for standards development (P1952).
- https://sagroups.ieee.org/p1952/



Resilient Positioning, Navigation, and Timing (PNT) Conformance Framework

Version 1.0

Homeland Security
Science and Technology

Resilient PNT Reference Architecture

- **Holistic Cybersecurity-based Approach to Resilient PNT Architectures**
  - Focuses on future paradigm of multi-PNT ecosystems and complex threat environments.
  - Fully embraces cybersecurity principles for a holistic approach for dealing with present and future PNT threats.

- **Resilient PNT Reference Architecture**
  - Beyond the scope of the Conformance Framework
  - More concrete application of cybersecurity concepts

- **Status**
  - Document planned for publication by January 2022.

Embracing Cybersecurity Concepts

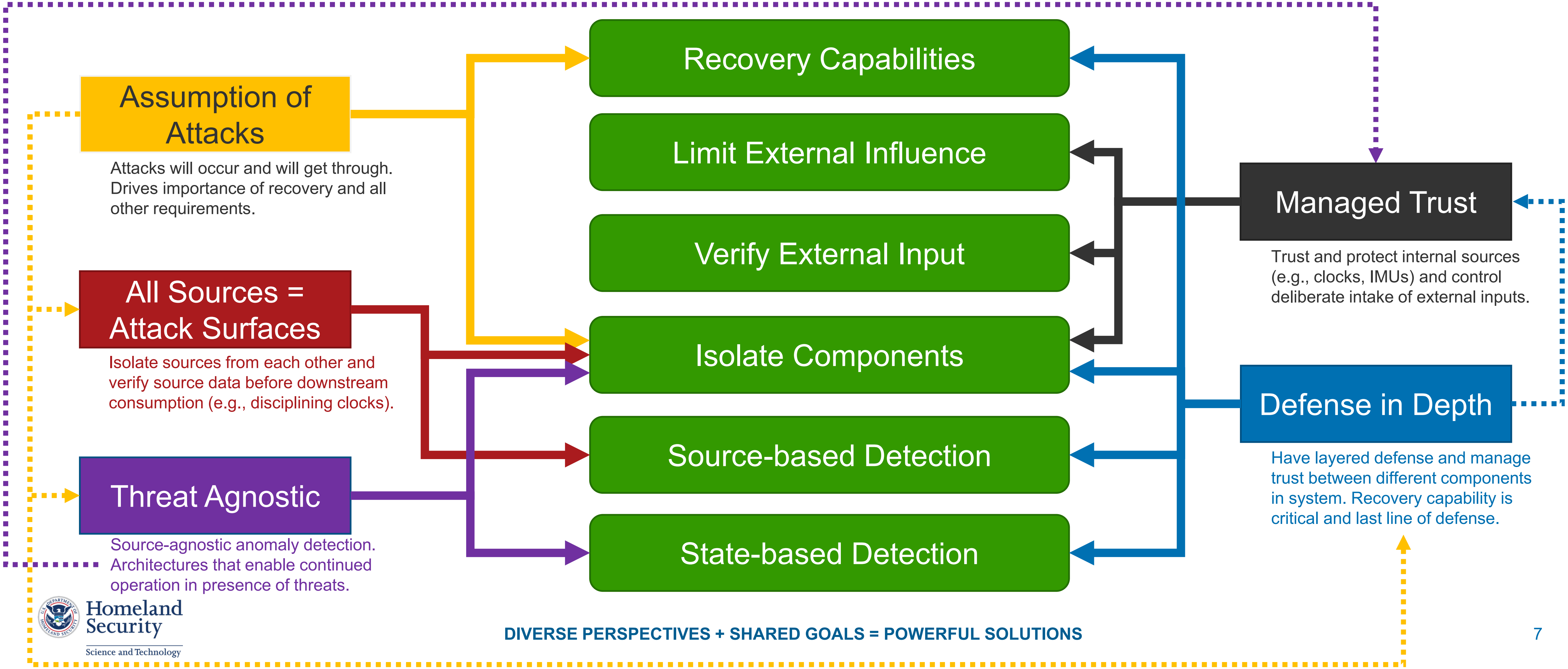
Current (Initial) Generation of Resilient PNT

- Emphasis on detection and validation.
- Automated responses to threat detection.

Additional Concepts for NextGen Resilient PNT

- Assuming attacks will occur and get through
- Recognizing every external PNT sources as an attack surface
- Adapting “Zero Trust Architecture” concepts → Managed Trust of PNT Components
- Defense in Depth
- Proactive and Agnostic Approach to Threats (signature-based detection difficult to scale)

Holistic Approach to Resilient Architectures



Assumption of Attacks

Attacks will occur and will get through. Drives importance of recovery and all other requirements.

All Sources = Attack Surfaces

Isolate sources from each other and verify source data before downstream consumption (e.g., disciplining clocks).

Threat Agnostic

Source-agnostic anomaly detection. Architectures that enable continued operation in presence of threats.

Recovery Capabilities

Limit External Influence

Verify External Input

Isolate Components

Source-based Detection

State-based Detection

Managed Trust

Trust and protect internal sources (e.g., clocks, IMUs) and control deliberate intake of external inputs.

Defense in Depth

Have layered defense and manage trust between different components in system. Recovery capability is critical and last line of defense.

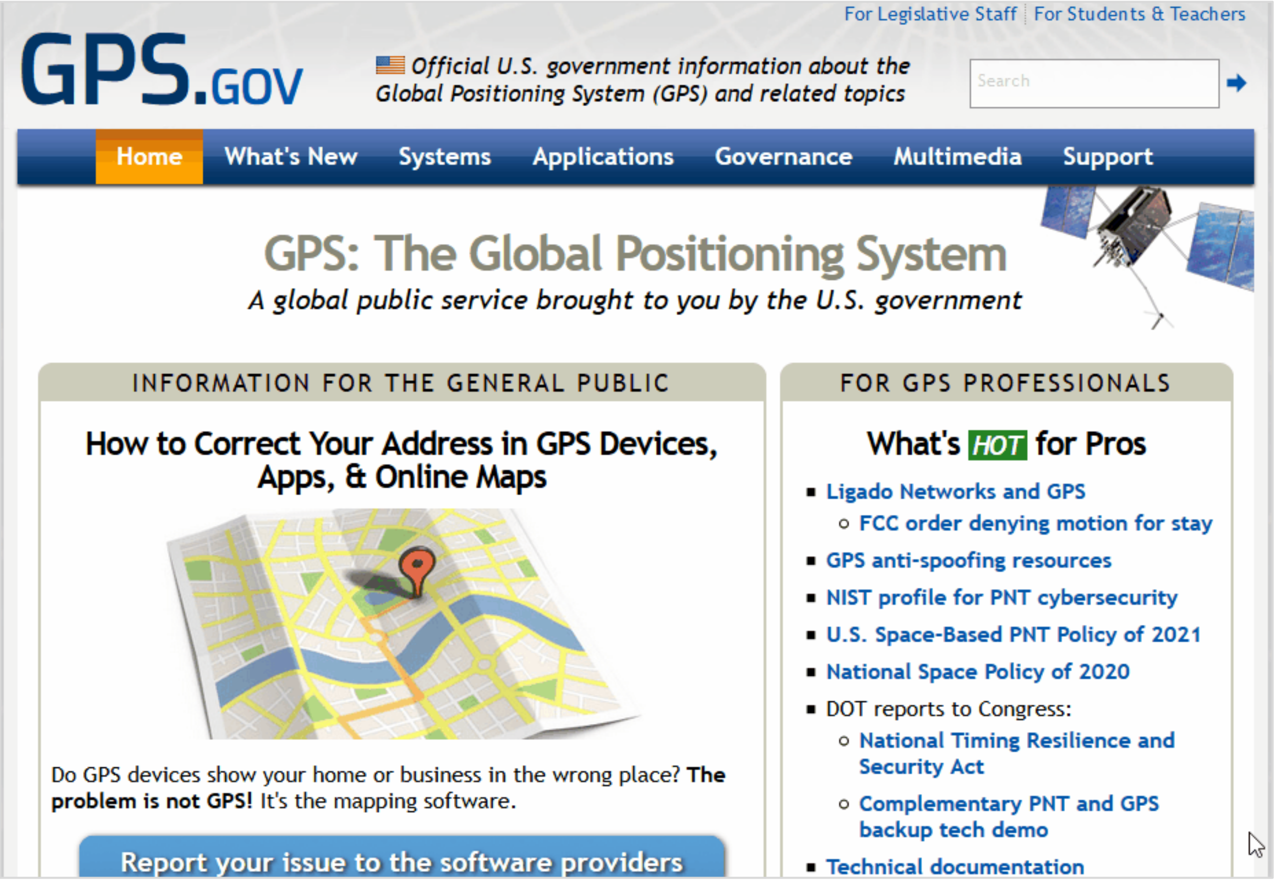
Related S&T Products

- **GPS Whitelist Development Guide**
  - Software assurance approach to addressing potential vulnerabilities & increasing GPS receiver reliability
  - Can help with implementation of data-related requirements in the Resilient PNT Conformance Framework
  - https://www.dhs.gov/publication/gps-receiver-whitelist-development-guide

- **PNT Integrity Library**
  - Modular solution providing end-to-end spoofing detection capability
  - Recent v1.1 release adds GPS data message whitelist checks
  - DIY Demonstration Toolkit release planned for October
  - https://github.com/cisagov/PNT-Integrity

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
- GPS Whitelist Development Guide
  - https://www.dhs.gov/publication/gps-receiver-whitelist-development-guide
- PNT Integrity Library
  - https://github.com/cisagov/PNT-Integrity
- IEEE P1952 Page
  - https://sagroups.ieee.org/p1952/
- DHS S&T PNT Program
  - https://www.dhs.gov/science-and-technology/pnt-program


For Legislative Staff | For Students & Teachers
Search
Home
What's New
Systems
Applications
Governance
Multimedia
Support
Report your issue to the software providers

GPS.GOV

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

How to Correct Your Address in GPS Devices, Apps, & Online Maps

Do GPS devices show your home or business in the wrong place? **The problem is not GPS!** It's the mapping software.

FOR GPS PROFESSIONALS

What's HOT for Pros

- Ligado Networks and GPS
  - FCC order denying motion for stay
- GPS anti-spoofing resources
- NIST profile for PNT cybersecurity
- U.S. Space-Based PNT Policy of 2021
- National Space Policy of 2020
- DOT reports to Congress:
  - National Timing Resilience and Security Act
  - Complementary PNT and GPS backup tech demo
- Technical documentation

Homeland Security

Science and Technology

DIVERSE PERSPECTIVES + SHARED GOALS = POWERFUL SOLUTIONS