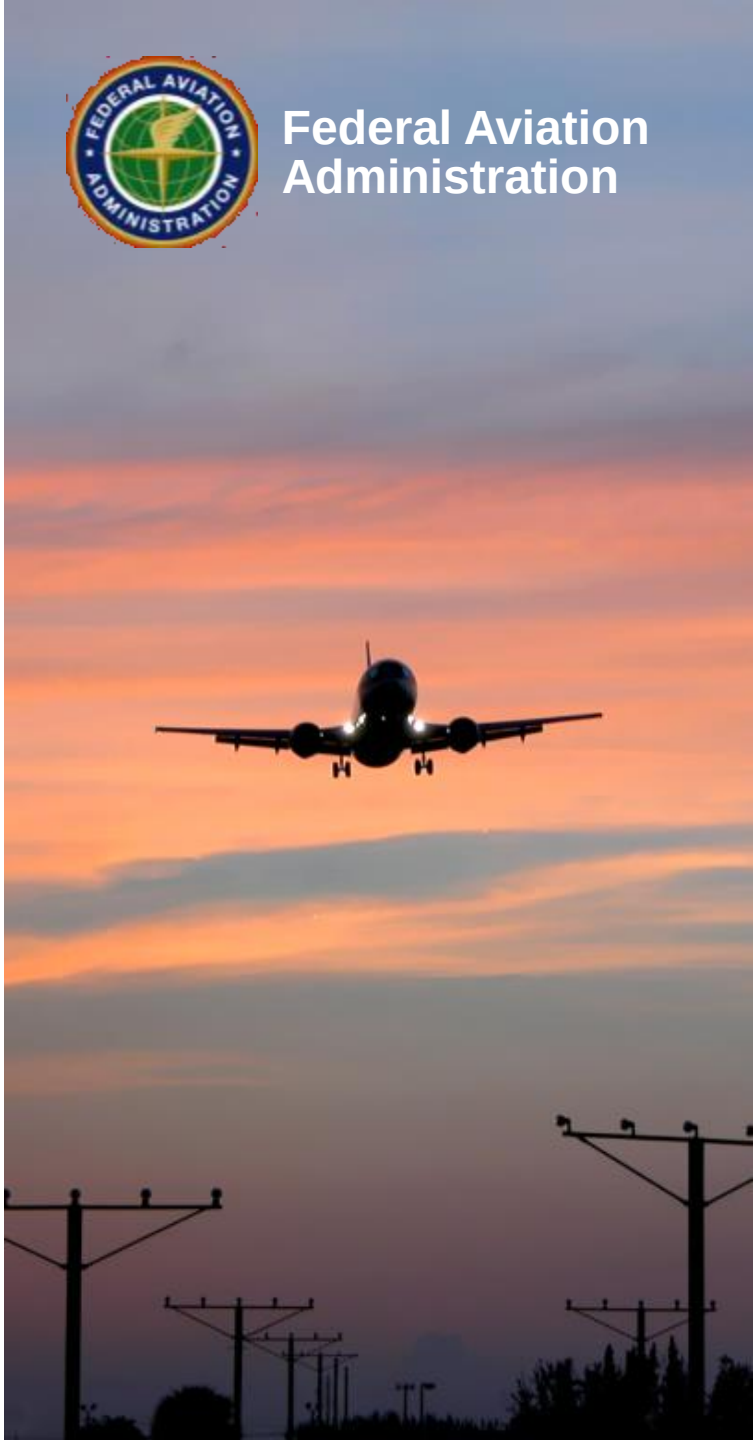
GNSS Intentional Interference and Spoofing

By: Ken Alexander and Deborah Lawrence

Date: October 2015

Federal Aviation Administration



Background

- **GNSS is vulnerable to intentional interference and spoofing**
  - Capabilities exist to adversely impact safety, security, and capacity of the NAS
  - Topic is subject of growing public awareness
- **FAA Navigation Programs and Aircraft Certification established Study Team in Oct. 2012 to**
  - Examine threat assessments, studies, and data
  - Develop specific, actionable recommendations

National Policies

- ***"It is the policy of the United States to strengthen the security and resilience of its critical infrastructure against both physical and cyber threats."*** **—Presidential Policy Directive (PPD-21)**
- **Deputy Secretary-level Executive Committee (NSPD-39, 2004) approved a plan in 2013 to:**
  - Leverage PPD-21 and updates of the National Infrastructure Protection Plan framework and Sector-Specific Plans for engaging the private sector and critical infrastructure owners and operators
  - Leverage Executive Order for Improving Critical Infrastructure Cybersecurity (E.O. 13636, 2013) to further examine the relationship between the federal provided GPS and cyber threats, dependencies and vulnerabilities to civil infrastructure
  - Leverage cyber statutes to protect vital position, navigation, and timing (PNT) data provided by GPS and its augmentations to civil users
    - 18 U.S.C. § 1030(a)(5) prohibits damaging a computer system: "Damage" is defined as "any impairment to the integrity or availability of data, a program, a system, or information"

Importance of Resiliency

- **Need for aviation resiliency to GNSS effects is not new, e.g.:**
  - 1999 Johns Hopkins University Applied Physics Lab (APL) Risk Assessment Study
  - 2001 DOT Volpe Vulnerability Assessment
- **What has changed?**
  - Non-aviation critical infrastructure is increasingly dependent upon GPS for vital PNT data
  - Government and private sector are using risk management strategies to identify and address risks associated with GPS dependence, including dependencies across sectors
  - Increase in interest/availability of intentional interferers

Study Team Process

- **Identified and evaluated various aviation threat scenarios**
- **Identified and characterized current and future GNSS uses within the National Airspace System (NAS)**
  - Aircraft and ground systems
- **Assessed threat scenario impacts**
- **Identified potential mitigations**
  - Technical and operational

Threat Scenarios

Scenario	Examples of Experienced Events
Low Power Mobile Interference	Interference at airport caused by personal privacy devices in vehicles on adjacent roadways
Low Power Stationary Interference	Interference at airport caused by stationary personal privacy device in aircraft operations area
High Power Interference	Misuse or unplanned use of military equipment results in jamming
Unintentional Re-radiator	Improper use of aviation GPS test equipment
Pinpoint Spoofing Attack	Partially demonstrated (research, test for hovering UAV with non-aviation grade equipment and pre-determined knowledge of vehicle position/time)
Coordinated Spoofing Attack	No known event for civil, approved, aviation applications
Coordinated Interference and Spoofing Attack	No known event for civil, approved, aviation applications

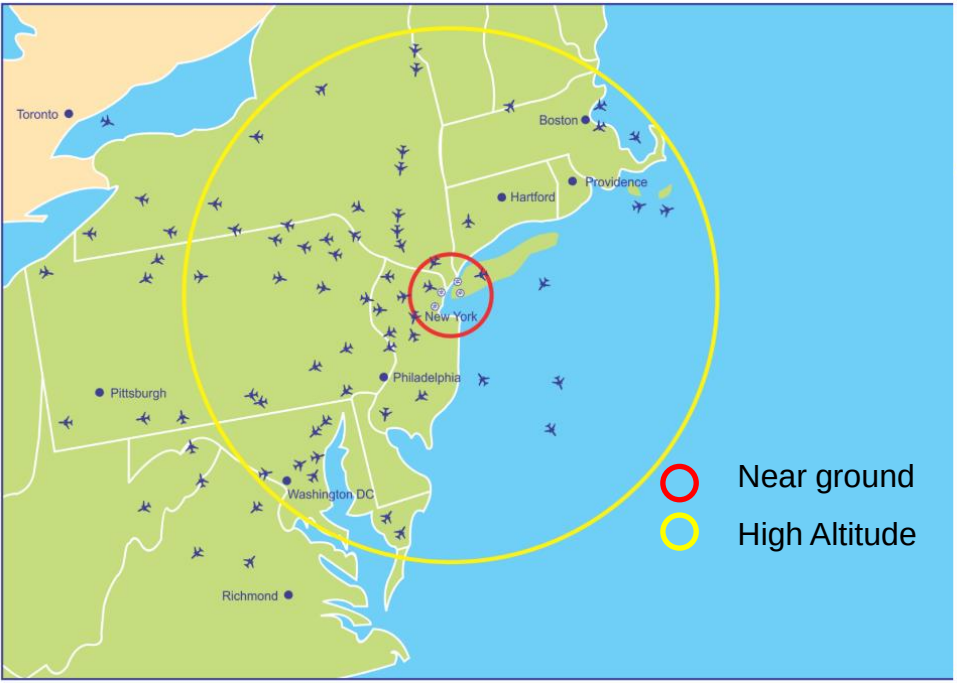
Impacts on Aircraft GNSS Navigation

Intentional Interference Scenarios	GPS/SBAS/GBAS Avionics Impacts
Low Power Mobile Interference	Little effect due to aircraft speed and short exposure to interference; short loss of GPS tracking
Low Power Stationary Interference	Limited loss of availability and continuity depending on location of jammer
High Power Interference	Loss of availability and continuity

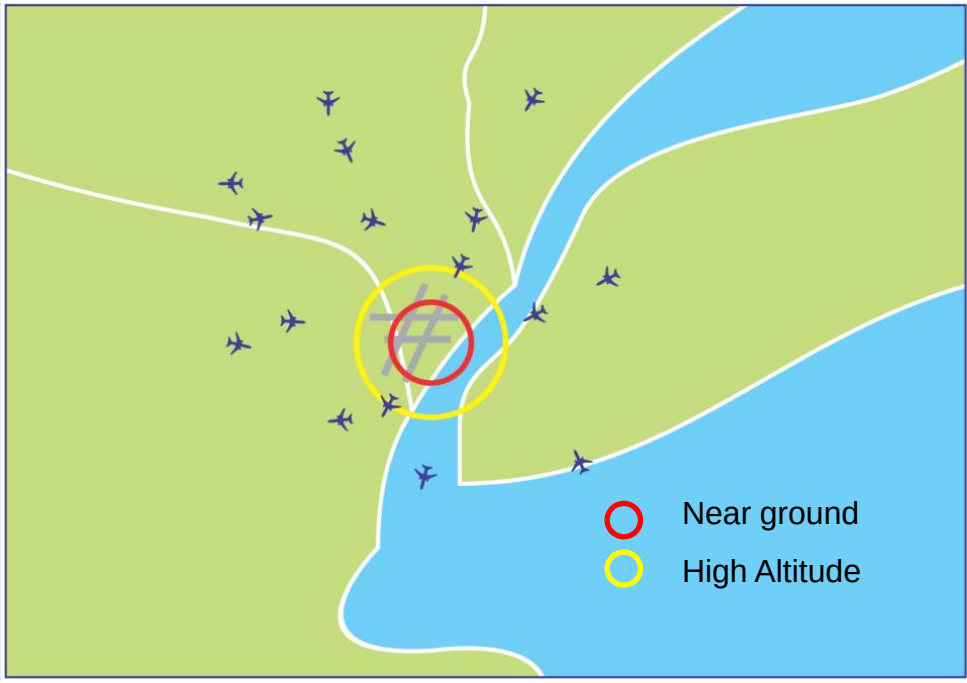
Spoofing Scenarios	GPS/SBAS/GBAS Avionics Impacts
Unintentional Re-radiator	Possible loss of integrity
Pinpoint Spoofing Attack	Possible loss of integrity
Coordinated Spoofing Attack	Possible loss of integrity
Coordinated Interference and Spoofing Attack	Possible loss of integrity

Spoofing and Interference Impacted Areas

Intentional Med/High Power

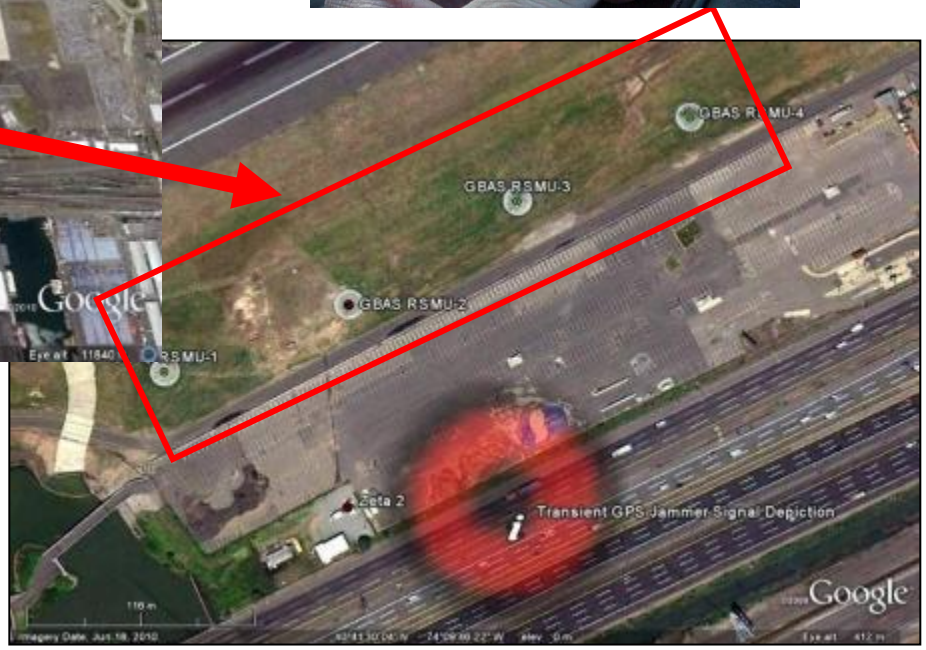


Personal Privacy Device



Low Power Mobile/Stationary Interference

GBAS Facility at Newark



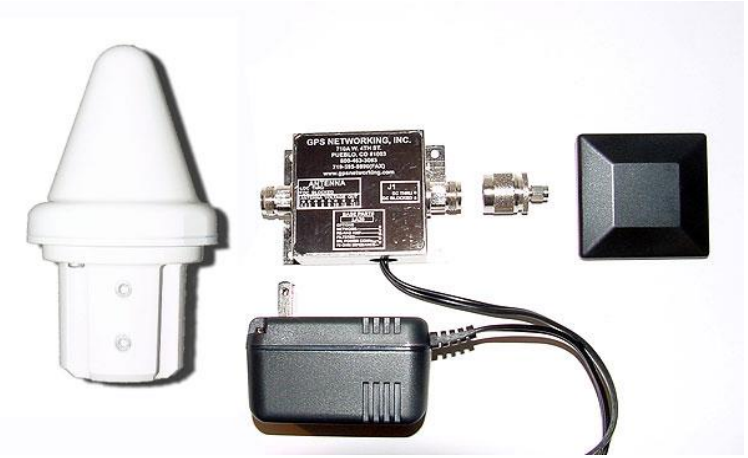
High Power Interference

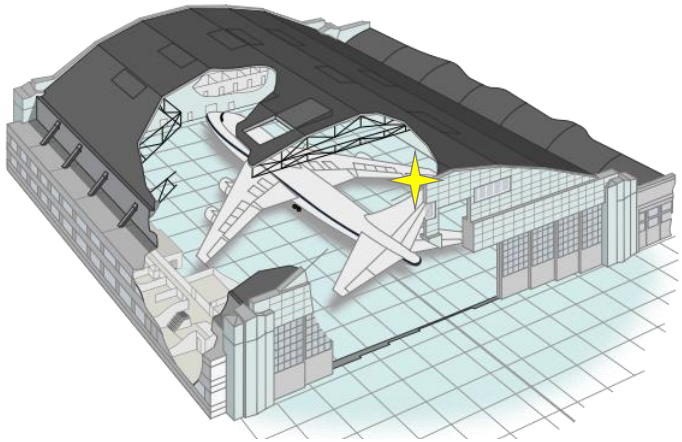
- **Examples of misuse or unplanned use of military equipment in the United States**
  - 1994 – 1995 - St. Louis “wormhole” due to military contractor performing outdoor antenna testing
  - January 2007 – USN ship in San Diego
  - May 2013 – USN amphibious ship near Norfolk
- **North Korean jamming resulted in FAA issuing NOTAMs in 2013, 2014 and 2015**

  “EXERCISE CAUTION DURING FLIGHT OPERATIONS AS THERE HAVE BEEN PRIOR REPORTS OF CIVIL AIRCRAFT EXPERIENCING GPS NAVIGATION SYSTEMS INTERFERENCE AND DISRUPTION”

Illegal or Malfunctioning/Modified Re-radiator

- GPS re-radiators may be used, with authorization, in the United States and many other countries
- Inappropriately installed/modified systems have resulted in unintentional spoofing or disruption of aviation GNSS receivers





Typical Installation

Examples of Aviation Impacts:

- Mar ‘07 - Loss of STARS, DVRS at Des Moines, IA
- May ‘10 - Spoofing caused erroneous Ground Proximity Warning System alerts in Germany
- July ‘10 - Loss of WAAS vertical guidance during approaches into Sanford, FL airport
- Sep ‘14 - Suspected re-rad spoofed avionics on approach into Northwest Florida Beaches Airport
- Oct ‘14 - Loss of GPS on ramp, on departure and additional ATC impacts at Nashville Int’l, TN

Aircraft System Impacts

- **Intentional Interference**
  - Primary impact is loss of GPS or GPS/SBAS/GBAS continuity/availability, and reversion to other means of navigation
  - Not anticipated to impact integrity for certified equipment
  - Operator may not be aware of all GPS dependencies
    - For example, TAWS, simulated ADF and DME, degradation in low-cost attitude information
- **Spoofing**
  - Potential for unflagged, erroneous position to be output to primary flight displays/indicators and other aircraft and ATC systems
  - RAIM only partially effective against GPS spoofing

Operational Mitigations

- **Loss of GPS**
  - Reversion to backup navigation (IRU, DME/DME, VOR)
  - ATC intervention
- **Spoofing**
  - Use of other airborne systems mitigates hazards (e.g., GPWS, TCAS, etc.)
  - Pilot may detect error through cross-check and other information (heading, altitude, situational awareness through map display)
  - ATC provides separation and will detect grossly erroneous navigation for IFR

Findings

- **Civil aviation use of GNSS is vulnerable to intentional interference/spoofing**
- **Backup systems and mitigations allow continued safe operation at reduced levels of efficiency and capacity**
- **Current avionics not required to detect spoofing**
- **Threat of interference and spoofing likely to increase**
- **Additional mitigations available and necessary**
  - Focus on detection/awareness to transition to use of other means of navigation (vs. fly-through)
  - Many spoofing detection methods identified; testing/evaluation required for civil aviation environment

Findings – Mitigations

- **Dual-frequency can reduce vulnerability to unintentional interference**
- **Some low-complexity receiver techniques could reduce vulnerability to spoofing, including:**
  - AGC/SNR valid range
  - PVT ‘reasonableness’ checks
  - Additional channels to detect presence of duplicate PRNs
  - Navigation data ‘reasonableness’
  - Cross checks of GPS to other navigation systems (e.g., IRU, DME/DME)
- **Antenna technologies can reduce vulnerability to spoofing/ interference**
  - Adaptive antennas (higher complexity and ITAR* limitations)
  - Two-state antenna (lower complexity, potentially non-ITAR)

*International Traffic in Arms Regulations

Recommendations - Guidance

- **Address aircraft vulnerabilities to GPS interference or spoofing in aircraft integration**
  - Example: March 2014 release of AC20-138D regarding potential for misleading information from GNSS re-radiators:
    - "manufacturers should consider measures to mitigate"
    - "… cross-checks… against independent position sources and/or other detection monitors using GNSS signal…"
  - Consider GNSS-aided inertial systems (SC-159 WG-2C)
  - Ensure holistic review at aircraft level (all functions)
- **Update pilot and controller training materials to address interference and spoofing**

Recommendations - Technology

- **Develop MOPS spoofing detection requirements**
  - Require future aircraft equipment to cease GNSS use when continued operation is unsafe
  - Assess effectiveness of “low-cost” techniques
- **Promote development and availability of higher performance spoofing mitigations**
- **Implement digital signatures within future satellite-based augmentation system (SBAS) messages**
  - Encourage the inclusion of digital signatures within the GPS L5 navigation data

Summary

- **GNSS is vulnerable to intentional interference and spoofing**
- **Per new SC-159 TOR, “new MOPS should address, to the extent practicable, the threats of intentional interference and spoofing”**
- **FAA is pursuing mitigations to these vulnerabilities, including:**
  - Proof-of-concept techniques to support MOPS development
  - Operational and system mitigations