746th Test Squadron

Best in Test

Civilian GPS Systems and Potential Vulnerabilities

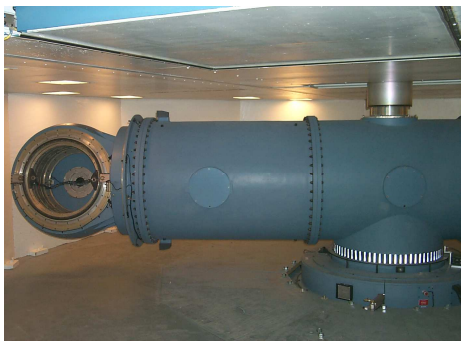
Paul Benshoof
746 TS/CAX
(505) 679-1769
paul.benshoof@46tg.af.mil
www.gpstestcoe.com

Purpose

- Overview of Civil GPS Applications
  - Increasing Reliance
  - Many Aspects of Critical Infrastructure Dependent upon GPS
- GPS Vulnerabilities Discussion
  - DoD GPS test perspective
  - Impacts to Critical Infrastructure
- Recommend Action
  - Mitigate Exploitation of Vulnerabilities
  - Protect Critical Infrastructure

Introduction

- 746 Test Squadron
  - Lead GPS test organization in a multi-service consortium
    - GPS Test Center of Expertise
  - Center of excellence for inertial guidance and navigational systems
  - Civil and military applications
  - Assesses system performance before procurement and deployment
  - Exploits receiver vulnerabilities
  - Recommends corrective action and equipment improvements

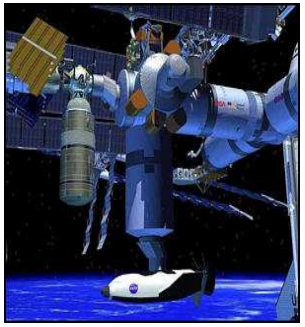


Background

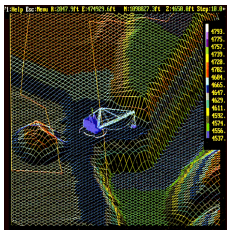
- DOT/Volpe Center's 2001 report
  - Excellent job of examining potential vulnerabilities to civilian systems
  - Transportation, telecommunications, and electronic finance
- Vulnerability stems from what the military has understood for years
  - GPS receivers derive their solutions from extremely low-power satellite signals
  - These signals – like any radio transmission – can be jammed
- Worldwide use of GPS for military applications has driven the development of a 'GPS disruption industry'
  - GPS jamming techniques are no secret
  - Simple plans for building jamming devices are readily available
  - A number of them are available for purchase

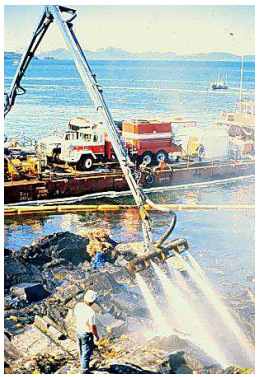
GPS Applications

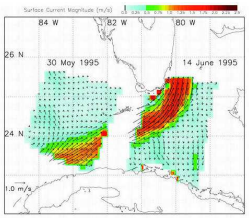
- Military
- Civil
  - Transportation
    - Aviation
    - Automobile
    - Maritime
    - Rail Control
  - Public Services
  - Timing & Frequency
  - Surveying
  - Surveillance
  - Other



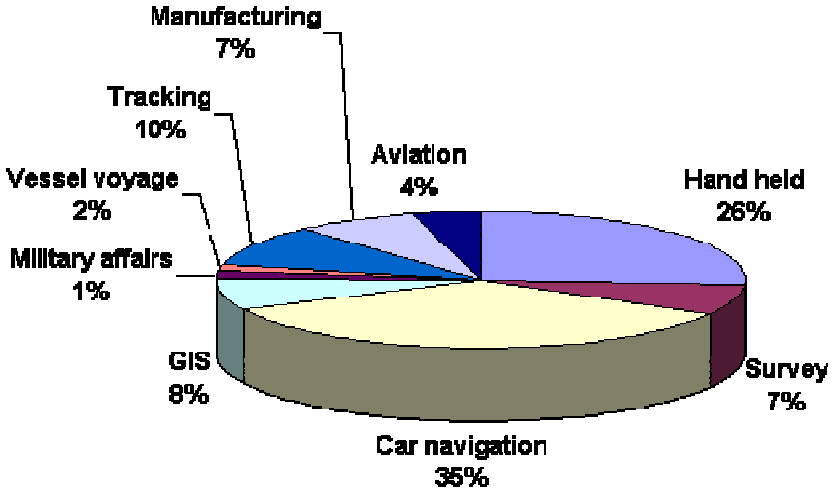



Military GPS Reliance

- Military
  - GPS as effective force enhancer to the US military and allies
  - GPS now required on all US systems
  - Recognized NATO standard
  - Forefront of developing anti-jam technology
  - Produced solutions making military navigation systems much more robust than their civilian counterparts
  - Minority user



Civil GPS Reliance

- Commercial applications of GPS far exceed those of the military
  - GPS satellites broadcast a signal freely available to the public
  - Openly published GPS specifications allow anyone to build receivers (no licensing fees)
- Innovative applications
  - Using GPS in ways that the original developers could have never imagined
  - Profoundly affected the way we live, communicate, and travel
- Potential applications of GPS are vast and nowhere near maturity

GPS Usage

- Despite Volpe Report, commercial use continues to increase
  - We encourage it!
  - US policy is to promote acceptance and use of GPS
  - Its low-cost and worldwide availability make it extremely attractive for all of its applications
- Users beware…
  - Civilian infrastructure is not invulnerable to enemy attack
  - Must proactively identify potential weaknesses
  - Implement appropriate mitigation strategies

Message to Civil GPS Community

GPS provides many benefits to civilian users. It is vulnerable, however, to interference and other disruptions that can have harmful consequences. GPS users must ensure that adequate independent backup systems or procedures can be used when needed.

SOURCE: Interagency GPS Executive Board. GPS policy, applications, modernization, international cooperation. February 01

GPS System Vulnerabilities

- Unintentional Interference
  - Radio Frequency Interference (RFI)
  - Ionospheric; Solar Max
  - Spectrum Congestion
- Intentional Interference
  - Jamming
  - Spoofing – Counterfeit Signals
- Human Factors
  - User Equipment & GPS SV Design Errors
  - Lack of Knowledge/Training
  - Over-Reliance

1 Watt Jammer

Factors Impacting GPS Vulnerability

- Very Low Signal Power
  - Jamming Power Required at GPS Antenna on order of a Picowatt (10^{-12} watt)
- Single Civil Frequency
  - Known Signal Structure
- Many Jammer Models Exist
  - KWatt to MWatt Output – Worldwide Militaries
  - Lower Power (<100 watts)
  - Easy to Make
- Jamming Signal Types
  - Narrowband
  - Broadband
  - Spread Spectrum - PRN Modulation

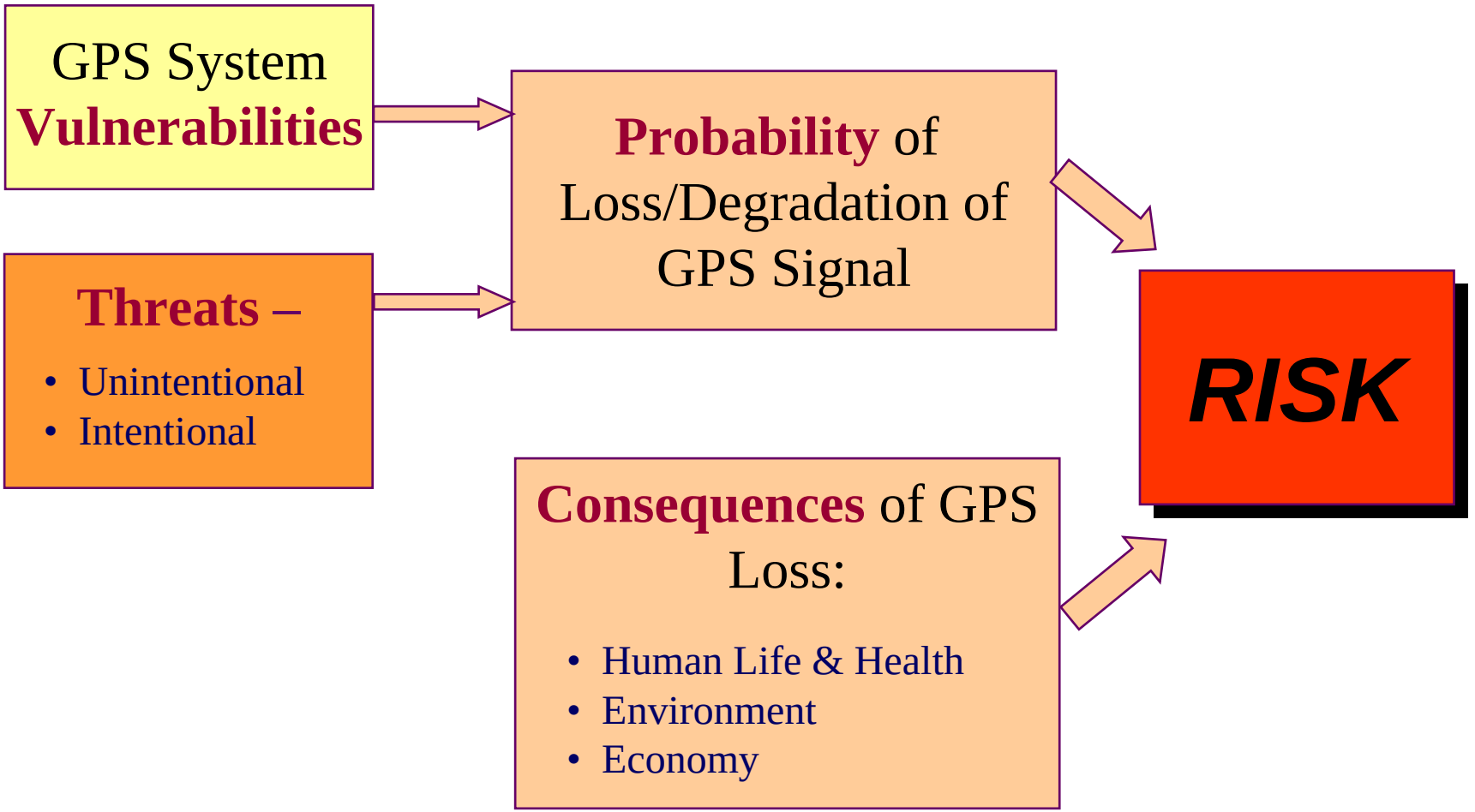
A 100 Watt bulb is 10^{18} times more powerful than a GPS satellite signal at the receiver's antenna!

Disruption Mechanisms - Spoofing/Meaconing

- Spoofing – Counterfeit GPS Signal
  - C/A Code Short and Well Known
  - Widely Available Signal Generators
- Meaconing – Delay & Rebroadcast
  - Emerging Threat
  - German Patent
- Possible Effects
  - Long Range Jamming
  - Injection of Misleading GPS Information
- No "Off-the-Shelf" Mitigation

Russian Jammer

Risk Considerations



Source: John A. Volpe National Transportation Systems Center. Vulnerability Assessment of the Transportation Infrastructure Relying on the Global Positioning System. 29 Aug 01

Consequences of GPS Loss/Degradation

- Depending on …
  - Application Mode Involved
  - Duration of GPS Loss/Degradation
- Impact Can Be
  - Minimal - Quick Recovery
  - Operational - Reduced Effectiveness & Efficiency
  - Safety - Potential Loss of Life, Environmental, Economic Damage
- Timing & Synchronization
  - GPS Outage Can Disrupt Communications/Networks

Real-world GPS Disruptions

- Jamming in Mesa, AZ
  - 13 – 18 Dec 01, GPS jammer caused GPS failures within 180nm of Mesa, AZ
  - Boeing was preparing for upcoming test
    - Accidentally left Jammer on L1 frequency radiating at .8mW
    - Jammer operated continuously for 4.5 days
  - Impact to ATC operations
    - A/C lost GPS 45nm from PHX, performed 35° turn toward traffic
    - NOTAM was not issued until 2nd day
    - Numerous pilots reported loss of GPS NavAid
    - Reports of hand-held GPS receivers not working

Real-world GPS Disruptions

- Jamming in Moss Landing Harbor, CA
  - 15 Apr 01 – 22 May 01, VHF/UHF television antenna with pre-amplifier caused GPS failures to all of Moss Landing Harbor
    - Boat owner purchased TV antenna, which was equipped with pre-amp
    - From interior location Amp's emitter jammed all of Moss Harbor and 1km out to sea
    - No GPS in entire area = 37 days
  - Impact to Moss Harbor
    - Research vessels relied heavily on timing from GPS
    - Extreme difficulty going through harbor in foggy conditions
    - Notification to all vessels in area that GPS was down
    - Switched back to radar control for harbor entrances

Reducing Vulnerabilities

- Military is leading the way in reducing vulnerabilities to their applications
  - The COE has tested many of these technologies
  - Measured significant anti-jam protection
  - Little of it has transitioned into commercial applications
- Military anti-jam solutions
  - Encrypted GPS signal that offers increased anti-jam protection
  - Specialized antenna electronics and hardware to reduce the effects of jammers
  - Size and cost of these systems generally are not considered practical for most commercial applications

Reducing Vulnerabilities (cont)

- US government pursuing alternative solutions
  - Further improvements to anti-jam performance
  - Benefiting both military and civilian GPS user
- Modifying GPS architecture to offer civilian users free access to three satellite signals
  - This will take some time to implement
  - 2nd signal not available before 2008
  - 3rd signal is not expected before 2012
- Micro-electromechanical systems (MEMS)
  - Embedding small inertial navigation sensors inside GPS antenna would help improve a system's anti-jam performance
  - Not adequate to support this yet, continue to improve significantly
  - 746 TS is very active in evaluating MEMS technology

JAMFEST

- Conducted by 746 Test Squadron on White Sands Missile Range, NM: 16-20 May 2005
- Low cost realistic GPS jamming environment
  - Test vulnerability of GPS-based systems
  - Train personnel in unique operational environments
- Both the military and civilian sectors can benefit
  - Targets potential weaknesses in all GPS receivers
  - Gives anyone in need of GPS vulnerability awareness an outlet to test GPS assets in realistic jamming environments
- Arms GPS users with realistic vulnerability data
  - Better understand their system limitations
  - Work to mitigate these effects
  - Apply backup systems or procedures as appropriate

Conclusion

- Civilian systems rely heavily on GPS
  - Potential applications of GPS are vast and nowhere near maturity
  - Potential serious economic and potentially fatal consequences if signals are disrupted
- GPS is a tempting target for adversaries
  - Continues to penetrate civil infrastructure
  - GPS Users are Vulnerable to Signal Loss or Degradation
  - The Vulnerability Will Not Be Fully Eliminated
  - Awareness & Planning Can Mitigate the Worst Vulnerabilities

Recommendations

- Study Vulnerabilities to Determine Tolerable Levels of Risk and Cost for Critical Infrastructure Applications
  - Determine Costs of Lowering Risks to an Acceptable Level
  - Implement Appropriate Mitigation Strategies
  - JAMFEST is an opportunity to get started
- For Each Application, Choose or Maintain Appropriate Backup System or Procedure
  - Reflect Interference Impact in Application Designs
  - Implement Systems to Monitor/Report/Locate Interference
  - Assess Applicability of Military Anti-Jam Technology
  - Be Cognizant of Timing Applications
- Encourage User Training and Use of Backup Systems

Contacts

Paul H. Benshoof, COE Director
746th Test Squadron
1644 Vandergrift Rd
Holloman AFB, NM 88330-7850
(505) 679-1769
paul.benshoof@46tg.af.mil

Capt Brett Casey, Vulnerabilities Element Chief
746th Test Squadron
1644 Vandergrift Rd
Holloman AFB, NM 88330-7850
(505) 679-1358
brett.casey@46tg.af.mil

Questions