Enabling GPS Information Sharing with Improved GPS OCX Security

Michael Worden
GPS OCX Overview

OCX Transforms GPS From Signals to Service-Based Capabilities

... Provides Enhanced Capabilities
- Plan and execute NAVWAR mission
- Additional signals: L5, L1C, L2C, M-Code
- C2 and Navigation for GPS II and GPS III
- Robust IA counters emerging cyber-threats
- Multi-level security and data distribution
- Improved accuracy inherent in design

... Supports Future Capabilities
- Flexible architecture to accommodate new functional capabilities and evolving CONOPS
- Net Ready/GIG compliant
- Re-programmable monitor station receiver
- Infrastructure supports future FAA integrity requirements
GPS OCX IA Challenges

- Global Network of Monitor Stations and Ground Antennas
- NIPRNET, SIPRNET and Internet Connectivity
- GPS supports Mission Critical Military and Civil functions
- Escalating Cyber Threat

OCX is a Global Network Controlling a Critical National Asset
2007 - Landsat-7 and Terra AM-1 Satellite Systems Attacked

September 2012 – White House confirms breaching Military Office for nuclear commands

March 2011
RSA Hacked; data used to attack Lockheed-Martin, Northrop, and L-3 Communications.
# GPS OCX IA Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Approach</th>
<th>Benefit</th>
</tr>
</thead>
</table>
| “De-Militarized Zone” for all external Connections | Multiple IA Controls (including Encryption, Firewall, IDS, and Application Security) | • Separation between Communications network and constellation C2 systems  
• Scalable Net-Centric Interfaces maximizes interoperability |
| Hardened COTS Architecture   | Segmented Network with multiple Policy Enforcement Points  
OS/Database/Apps hardened to DoD guidelines                          | • Capability to operate in a through attack  
• “Crumple Zones” between critical subsystems  
• Reduced attack surface |
| Hardened Software            | Refactoring ~ 2 million LOC (lines of code) of the reuse baseline to remove any vulnerabilities | • Significant improvement in application security |
| Multi-Level Security         | UCDMO certified Cross-Domain Guard (Raytheon High Speed Guard)         | • SOA architecture that provides products to multiple security levels |
GPS OCX IA Architecture Features

- Encrypted, Authenticated Links for all customers
- DMZ buffers outside communications from C2 Systems
- All applications run on a tested, hardened COTS architecture
- All Custom Applications designed securely
- Active IA monitoring throughout the system
Significant IA utility can be gained with inexpensive fixes:

- Firewalls at WAN links
- Proactive patching of COTS
- Minimize admin privileges
- Application Whitelisting (Configuration Control)
- Hardened Operating Systems

Older Application Code is largely insecure

- C++ is particularly problematic
- Java is better, but not perfect

“Trust No One”

- Look to protect yourself from your neighbors security problems
- Monitor your system to guard against insider threat
- Look to constantly improve