Raytheon

Testing GPS/OCX

Mark Bradbury
Chief Engineer, CODE Center
Mark_A_Bradbury@Raytheon.com

Raytheon CODE Center
CYBER OPERATIONS
DEVELOPMENT & EVALUATION

Outline

- What is GPS OCX?
- Why the interest?
- What is being done?
- Conclusion

GPS-OCX

- Global Positioning System Next Generation Operational Control System
  - Key planned benefits
    - Dramatic Performance Improvements
    - **Unparalleled Cyber Protection**
    - Enabling Secure Information Sharing
    - Effective Use of the Most Modern Civil and Military Signals
    - A Flexible, Open Architecture Built for the Future

Unparalleled Cyber Protection

With cyberthreats to U.S. military, civilian, corporate and financial infrastructure growing exponentially, as well as becoming much more sophisticated, it is critical that the GPS system be fully secure and protected from hacking, interruption or signal and information compromise. The GPS OCX system is at the forefront of implementing DODI 8500.2 Information Assurance Standards that provide multilayered Defense in Depth security controls to protect the GPS mission from a spectrum of threats. OCX will raise the level of protection using a suite of technologies and techniques compliant with the best practices and standards of the U.S. military and government cybersecurity experts. Most importantly, the system is being designed with robust security and information assurance built in, enabling integration with every single aspect of the system. As one of the first large acquisition programs to embrace the new Risk Management Framework (RMF) approach, GPS OCX has been under additional scrutiny by the Acquisition community.

Testing GPS OCX

- Software static analysis
  - One of the first testing initiatives was checking legacy Ada source code
    - Used CodePeer to scan Ada code and map findings to CWEs
    - Security requirements required mapping to STIGs
    - Used Fortify's vulnerability catalog, Vulncat, to map CWEs to STIGs
  - Next was standing up automated source code static analysis of source code as part of the build process
    - New code scanned before each check in and findings remediated before check in allowed
  - Used Grammatech CodeSonar and Fortify to scan FOSS libraries

GRAMMATECH

FORTIFY An HP Company

Testing GPS OCX

- ARCH review
  - An **A**rchitectural **R**eview for **C**yber **H**ardening (ARCH) review was done as the result of a Government change order to an OCX portal
    - Performed independent review of the security impact of change
    - Provided report detailing impact to design and overall security stance
      - Primary recommendations
        - Review and revise security assertions
        - Established a mission performance monitoring capability
        - Developed “playbook” allowing operational staff to respond to mission performance degradation
        - Reconstitute portal on an ongoing basis
        - Full Red Team of GPS portal

Testing GPS OCX

- STIG review
  - Customer requested review of Security Technical Implementation Guidelines (STIG) of GPS OCX Storage solution
    - Vendor stated full STIG application would affect storage solution operation
    - Reviewed hardening profile against STIG compliance
    - Recommended further hardening and follow-on testing to create accreditation strategy for storage solution
    - Customer approved follow-on testing
    - Accreditation strategy approved

Testing GPS OCX

- STIG hardening
  - STIG hardening of multiple pieces of hardware being delivered to OCX
    - Implemented STIG hardening on various hardware
    - Security testing accomplished to ensure STIGS appropriately implemented

Image subject to copyright Top Gear

Testing GPS OCX

- PenTest
  - OCX Security team requested penetration test
    - Using same tools and techniques that Government testers will use
    - 300+ IP addresses to be tested
    - Risk reduction task to be performed two months prior to Government testing to allow for remediation or mitigation of findings

Conclusion

- Many types of cybersecurity testing has been done on GPS OCX at many levels
- More testing is still to be done
- Goal
  - Make GPX OCX the most secure system among new acquisitions


Questions?