Implementing Cyber Defense at JPL

Bob Vargo
Assistant Director For
Engineering and Science Directorate
Recent Past

• “Blissful ignorance” within the mission community despite successful cyber attacks on Landsat, Terra and other spacecraft
• All responsibilities for cyber defense allocated to IT security department
• Mission cyber defense R&D group formed in 2010
• Significant intrusion in November 2011, just weeks before the launch of Curiosity Rover to Mars

Chinese hackers took over NASA's Jet Propulsion Lab, Inspector General reveals
Very Recent Past

• Concern is increasing in the engineering community, but apathy still dominates

• JPL Director takes action in 2013, forming the Cyber Security Council:
  • The Cybersecurity Council (CSC) is a subcommittee of the Executive Council (EC), appointed by the Laboratory Deputy Director. The CSC will be a decision making body that provides executive management for the Lab’s cybersecurity, which includes, cyber research, Space Asset Protection (SAP) and malicious threats or incidents at JPL. The CSC develops JPL cyber strategies, plans, policies, and provides guidance for investment and operations funding, and coordinates internal cyber incident notification and response. The CSC is chaired by the JPL Deputy Director and has a supporting CSC Working Group that responds to CSC tasking.
Key Challenge #1: Harmonizing IT Security with Cyber Defense Research

- Installing an authentication infrastructure, e.g., PKI, username and passwords, etc.
- Executing anti-viral software
- Implementing access control policies
- Configuring firewalls for perimeter defense
- Encrypting data in transit, implementing Transport Layer Security
- Restricting remote access to authorized users
- Implementing logging capabilities to capture password changes and failed login attempts

- Automated diagnosis and remediation (counter-response)
- Survivability – operational resilience through attacks
- Design of security metrics – measuring assurance in a proposed defensive posture
- Situational awareness encompassing complex systems that span large networks, vast amounts of data and several levels of operation
- Analysis of new malware and detector design
- Testing – evaluating the effectiveness of defenses that are subject to
  - changing operational environments
  - environments that expand rapidly in number of components and speed of data flow
  - new attacks/faults
Key Challenge #2: Managing our environment’s large risk envelope

• Legacy systems
  • ~ 40M SLOC in our mission systems

• Contractors
  • Heavily used for development and operations

• Academia
  • Principal and Co-investigators operate remotely

• International partners
  • ESA, Canada, India, Russia, Japan, Australia, Spain, and many more
Key Challenge #3: Indifference, Ignorance, Overconfidence and Lack of Guidance

“Hackers aren’t interested in space systems”

“We know how to land rovers on Mars, so we’re able to solve the cyber defense problem ourselves”

“We share everything we do with the world”

“Investing in cyber defense is a wasteful distraction”

“Nobody would possibly want to build a 111 foot dish and position it just to hack a spacecraft”

“No show me the requirements or I’m not lifting a finger”
Native Assets to Build On

• Delay-Tolerant Networking
  • A useful remediation strategy for distributed space assets and to address adversarial-induced delays on terrestrial networks

• LaRS (Laboratory for Reliable Software)
  • All cyber-security properties are variants of safety and liveness properties for a formal specification of the system
  • This is more than static analysis of software; it’s static analysis of models of systems & their operational environment

• Critical experience in testing strategies
  • To address arguably the most prominent and difficult problem in cyber security - determining the effectiveness of cyber-security measures.

• Expertise in detection and diagnosis
  • Applied to attacks/malicious faults – patented model-based reasoning and rule-based techniques/algorithms.
Top Level Approach

• Imagine very bad days

• Identify “Crown Jewels”

• Prioritize

• Invest

• Act
Specific Investments

- Creation of a JPL Cyber Security Strategy
- Creation of Cyber Defense Test, Verification, and Validation regimes
- Creation of a cyber defense research laboratory facility
- Creation of a modeling infrastructure that enables integrated reasoning about the physical system, computing infrastructure, files, software, and mission functions
Going Forward

External Community (NASA, DHS, Law Enforcement, Counter-intelligence, Academia)

Cyber Security Council

Cyber Security Improvement Project

Cyber Security Management Advisory Group (CSCWG-enhanced)

Risk Assessments and Improvement Planning
i) Threat assessments
ii) Vulnerability assessments
iii) Architecture reviews and recommendations
iv) Forensics
v) Improvement activity prioritization

Development and Acquisition [of new institutional assets]
i) Requirements
ii) Design and Operations Principles
iii) Processes and Procedures
iv) Standards
v) Policies
vi) Acquisition Guidelines
vii) Novel cyber defense technologies
viii) Sensor mesh

Training, Coaching and Communication
i) Awareness
ii) Classes
iii) Certifications
iv) Experts for consultation
v) Infusion/Compliance advice
vi) Distribution of actionable information
vii) Informationsharing
viii) Exercises

Monitoring, Metrics, and Effectiveness Assessment
i) Evaluations and V&V in the CDRL
ii) Metrics specification, gathering, and analysis
iii) Active monitoring
iv) Incident analysis
v) ROI analysis
vi) Operational efficiency analysis
vii) Assurance

9/1/2015 AIAA Space 2015