Reducing Software Security Risk through an Integrated Approach

David P. Gilliam, John D. Powell
Jet Propulsion Laboratory, California Institute of Technology

Matt Bishop
University of California, Davis
Acknowledgement

**NOTE:**

- This research was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.
- The work was sponsored by the NASA Office of Safety and Mission Assurance under the Software Assurance Research Program lead by the NASA Software IV&V Facility.
- This activity is managed locally at JPL through the Assurance and Technology Program Office.
Current Collaborators

- David Gilliam – Principle Investigator, JPL
- John Powell – JPL Software Engineer
- Matt Bishop – Professor of Computer Science, University of California at Davis

http://rssr.jpl.nasa.gov
Agenda

- Goal
- Problem
- Approach
- Importance/benefits
- Relevance to NASA
  Accomplishments
- Next steps
Goal

- Reduce security risk to the computing environment by mitigating vulnerabilities in the software development and maintenance life cycles

- Provide an instrument and tools to help avoid vulnerabilities and exposures in software

- To aid in complying with security requirements and appropriate best practices
Problem

- Cost of Fixing Security Weaknesses in Software and Systems Is Expensive
- Security Weaknesses Can Lead to Loss / Corruption / Disclosure / Availability of DATA and Systems Impacting Missions
  - Poor Security Requirements
  - Poor System Engineering
    - Leads to poor design, coding, and testing
  - Cycle of Penetrate and Patch
  - Piecemeal Approach to Security Assurance
Approach

- Develop a Software Security Assessment Instrument for the Life Cycle
  - Several Foci
    - Training/Education
    - Security Checklist for the Life Cycle
    - Application of Lightweight Formal Verification Techniques for Security Weaknesses in Code and Systems
Reducing Software Security Risk Through an Integrated Approach

- **Software Vulnerabilities Expose IT Systems and Infrastructure to Security Risks**

- **Goal:** Reduce Security Risk in Software and Protect IT Systems, Data, and Infrastructure

  - Security Training for System Engineers and Developers
  - Software Security Checklist for end-to-end life cycle
  - Software Security Assessment Instrument (SSAI)

**Security Instrument Includes:**
- Model-Based Verification
- Property-Based Testing
- Security Checklist
- Vulnerability Matrix
- Collection of security tools
Inception-to-Retirement Process

- Coincides with Organizational Policies and Requirements
- Security Risk Mitigation Process in the Software Lifecycle
- Software Lifecycle Integration
  - Training
  - Software Security Checklist
    - Phase 1
      - Provide instrument to integrate security as a formal approach to the software life cycle
      - Requirements Driven
    - Phase 2:
      - External Release of Software
      - Release Process
  - Vulnerability Matrix – NASA Top 20
  - Security Assurance Instruments
    - Early Development – Model Checking / FMF
    - Implementation – Property Based Testing
  - Security Assessment Tools (SATs)
    - Description of available SATs
    - Pros and Cons of each and related tools with web sites
- Notification Process when Software or Systems are Decommissioned / Retired
Importance/Benefits

- Enhances a Secure Trusted Network Environment
- Reduces Cost of Maintenance
- Reduces Loss or Destruction of DATA and Systems
- Improves NASA’s Overall Security Posture
  - Fewer Intrusions and Audit Findings
  - Leads to a Better Image (OMB & Public)
Relevance to NASA Accomplishments

- Increases NASA’s Security Reliability of Systems and Software
- Helps to Prevent Negative Public Exposure Due to Security Breach
- Prototyped the SSAI Instrument on PatchLink Agents
  - Used large scale across NASA on its systems
  - Findings leading to improved vendor product
Next steps

- Integrate the Overall Process in the Project Life Cycle at NASA Centers
FOR MORE INFO...
Web Site: http://rssr.jpl.nasa.gov/

David Gilliam, JPL
400 Oak Grove Dr., MS 144-210
Pasadena, CA 91109
Phone: (818) 354-0900
Email: david.p.gilliam@jpl.nasa.gov

John Powell, JPL
MS 125-233
Phone: (818) 393-1377
Email: john.d.powell@jpl.nasa.gov

Matt Bishop, UC Davis
Department of Computer Science
Kemper Hall
phone: +1 (530) 752-8060
fax: +1 (530) 752-4767
email: bishop@cs.ucdavis.edu
QUESTIONS?