Software Security Assessment Instrument: Reducing Security Risks

Dr. David Gilliam & John Powell

Wednesday, July 17, 2002
12:00 - 1:00 PM
Conference Room 167

The Software Security Assessment Instrument (SSAI) is an instrument for assessing and reducing the security risks throughout the software development and maintenance life-cycle. Vulnerabilities in operating systems and software applications render an otherwise secure environment insecure. Any operating system or application added to a secure environment that has exploitable security vulnerabilities affects the security of the whole environment. An otherwise secure system can be compromised easily if the system or application software on it, or on a linked system, has vulnerabilities. Therefore, it is critical that software on networked computer systems be free from security vulnerabilities. Security vulnerabilities in software arise from a number of development factors; but these vulnerabilities can generally be traced to poor software development practices, new modes of attacks, mis-configurations, and unsecured links between systems.

The SSAI can aid in providing a greater level of assurance that software is not exposed to vulnerabilities as a result of defective software requirements, designs, code or exposures due to code complexity and integration with other applications that are network aware. The instrument makes use of an integrated approach utilizing previously known security vulnerabilities, systematic testing at the code level, modeling and simulation techniques during requirements and design phases, as well as checklists, both before and during the deployment and distribution phases.

The SSAI is the product of joint work by JPL and the University of California at Davis (UC Davis), and is sponsored by NASA's Goddard Independent Verification and Validation (IV&V) Facility.

Dr. David Gilliam is a Principal Investigator (PI) for the research task "Reducing Software Security Risk Through an Integrated Approach" (RSSR), and is in the Network and Computer Security Group of the Engineering and Communications Infrastructure Section (366) at JPL. He also developed the JPL Security Problem Log (SPL) to help in tracking and reducing vulnerabilities in JPL's systems. Gilliam is Co-Chair of the IEEE Wet Ice Workshop on Enterprise Security, as well as an invited speaker. He has authored several publications for NASA, JPL and other refereed organizations. He is also a member of the NASA Trust Working Group Windows Working Group, working to ensure the security of NASA's IT environment. Gilliam is currently working towards a M.S. in Software Engineering at the University of Maryland, and he already holds a Ph.D. in Theology from Fuller Seminary.

John D. Powell is a researcher in the Software Quality Assurance Group of the Quality Assurance Office (512) at JPL. Currently he performs research in the areas of quality and cost estimation and prediction, as well as formal methods. In addition to his work with JPL, he collaborates with Dr. Barry Boehm and the Center for Software Engineering at the University of Southern California, in research pertaining to cost and delivered defect prediction. Prior to his work at JPL and USC, Powell worked as a System Software IV&V Analyst for NASA's prime IV&V contractor performing IV&V analysis on the Redundancy Management and Control systems for the Space Shuttle's Checkout Launch and Control System. Prior to that, Powell performed research at the NASA Goddard IV&V Facility under the Intelligent Systems Initiative exploring alternatives to traditional model checking, in conjunction with West Virginia University's Software Research Laboratory. Powell holds a M.S. in Computer Science from West Virginia University.

CSMISS
Center for Space Mission Information and Software Systems

CSMISS IT Spotlight Series: Putting a "spotlight" on Information Technology that is or could be significant to JPL missions.