Software Assurance (SwA) Information Session:
Enhancing Software Trustworthiness

OMG Technical Meeting, Tampa, FL - Wednesday, February 15, 2006

To register, see: http://www.omg.org/registration/registration.htm

As complications to assessing the trustworthiness of software continue to evolve, formalized and standardized mechanisms and approaches must be developed that increase software assurance. The OMG is hosting a Software Assurance Information Session on February 15. During this session, attendees will hear about ways to architect and develop more secure and reliable software and the role that standards play in those efforts. The event will feature perspectives from members of Government, Industry and Academic organizations.

Agenda

14:00 – 14:10 *Introduction and Welcome - The Role of SwA in OMG*
Dr. Richard Soley, Chairman & CEO, Object Management Group

14:10 – 14:20 *SwA Special Interest Group: Focus and Directions*
SwA SIG Organizing Chairs:
Djenana Campara, CTO, klocwork, Inc.
J.D. Baker, Systems and Software Engineering, BAE Systems

14:20 – 15:30 *Government Perspective*

14:20-14:45 **DoD Software Assurance Strategy**
Mitchell Komaroff, DoD/OASD(NII)

Mitch will briefly discuss the DoD Software Assurance Strategy: engineering-in-depth, S&T for vulnerability prevention, detection and mitigation and industry outreach. The focus of his discussion will be the industry outreach. Here the discussion will center on DoD efforts to establish communication channels between government stakeholders, the systems integration and engineering community and commercial industry. The goal is to establish an effective standards based approach for designing, developing and testing assured systems from commercial products.

14:45-15:10 **Technology, Tools and Product Evaluation**
Dr. Larry Wagoner, NSA

It is increasingly difficult to establish or verify whether or not software is sufficiently trustworthy due to variety of factors such as the ever increasing size and complexity of the software systems/components, rapid evolvement of software where new technologies continue to introduce an ever greater level of complexity, accelerating dependency on COTS and Open Source driven by economic factors, etc. It is for these reasons we need tools and technologies that will support our efforts in building secure software products. This presentation will elaborate on the status and gaps of such tools and technologies and their adoption.

15:10-15:30 **The SAMATE Project and How it Helps Enhance Software Trustworthiness**
Dr. Vadim Okun, NIST

NIST Software Assurance Measurement and Tool Evaluation (SAMATE) project is specifying software assurance tool functions and developing a standard reference dataset of programs with known security vulnerabilities. This requires a taxonomy of software assurance tool functions and a common taxonomy of security vulnerabilities. We will discuss how our work will contribute to the development of a software assurance framework.

15:30 – 15:45 Afternoon Refreshments

15:45 – 16:00 *Academia Perspective*

Professional Society and Educational Efforts in Secure Software
Dr. Samuel T. Redwine, Jr., Associate Professor, James Madison University

Software security is of rising interest within higher education and professional societies and associations. This interest has been reflected in a number of new events, publications, committees, and working groups as well as efforts to establish relevant courses. Existing and planned activities in the areas of software security and assurance will be highlighted along with the difficulties faced both intellectual and institutional. Progress, prospects for the future, and related opportunities will be discussed.

16:00 – 17:40 *Industry Perspective*

16:00-16:25   **Enabling Software Assurance for DoD NCW Environments**
Robert Stow, Vice President, Engineering and Technology, BAE Systems

DoD NCW environments require industry to leverage a mixture of COTS software with custom developed software to meet the capability needs, affordability costs, and development schedules of new and evolving systems for DoD and Intelligence applications. The challenges of this environment for industry will be highlighted. Enabling software assurance in this complex environment will be discussed with recommendations of best practices that enhance software assurance.

16:25-16:50   **Implementing a Software Assurance Program at a Security Product Company**
Mark Kardich, Senior Principal Software Engineer, Symantec

This presentation deals with trials and tribulations encountered while implementing a software assurance program at a company that produces a security product. This talk covers the history, the process of developing the plan, tool selection, tool integration, and what really enabled us to move forward with the project.

16:50-17:15   **COTS, MIL-SPEC and MILS, A Necessary Harmony for Affordable Multilevel Secure Architectures**
Dr. Ben A. Calloni, P.E., Research Program Manager, Lockheed Martin -

The DoD customer base perceives that COTS Standards-based products are a way to reduce cost of ownership and better synergize with commercial technology advancements. In the aftermath of 9/11 it is imperative that a collaborative effort between DoD, Gov't, and Business be leveraged. Such effort would borrow the best from DoD in the area of safety and security while maintaining the cost / benefit ratio of commercial enterprise technology that would result in the development of safe and secure, standards-based, commercial software that will enhance the national computer infrastructure.

17:15-17:40   **Systems Development Governance to Manage Business Challenges: The IBM Rational Approach**
Sridhar Iyengar, Distinguished Engineer, IBM Rational Software

The software & systems industry in general and IBM's customers in the DOD and Systems Engineering communities in particular are grappling with challenges in developing and integrating COTS applications with custom developed software in a global environment. These challenges include organizational, geographic and architectural resulting in a shift to unify key concepts in Service Oriented & Model Driven Architectures. This talk will summarize IBM's efforts in addressing the challenges of designing, developing, integrating, testing, securing and deploying SOA applications using an open standards based model driven platform. The talk will reinforce the assertion that managing this inherent complexity is both a Business & IT challenge and needs a focus on Governance of the software and systems development and deployment process.

17:40 – 17:50 *Summary, Close and Next Steps*
SwA SIG Organizing Chairs

18:00 – 20:00 *Technical Meeting Reception* hosted by