Software Assurance (SwA) Information Session:
Open Standard Based Enabling Technologies to Achieve Higher Software Security

OMG Technical Meeting, Washington, DC
Thursday, December 7, 2006

[TM Homepage] [Registration]

08:30 – 8:40 **The Role of SwA in OMG, Introduction and Welcome**
Dr. Richard Soley, Chairman & CEO, Object Management Group

08:40 - 09:40 **Keynote: US Government's Software Assurance Strategy**
Joe Jarzombek, Director for Software Assurance, DHS

DHS's Software Assurance Strategy and DoD's engineering-in-depth are two major activities intended to transform how government and industry deal with Software Assurance. Areas of research and technology creation for vulnerability prevention, detection and mitigation are being identified as a product of these efforts. The focus of Mr. Jarzombek's discussion will be industry outreach, engagement, and opportunities, with a focus on DHS efforts to establish communication channels between government stakeholders, the systems integration and engineering community and the commercial industry. The goal is to establish an effective standards-based approach for designing, developing and testing assured systems from commercial products.

09:40 – 10:40 **Software Assurance Programs Overview**
Robert Martin, Principal Engineer, MITRE Corporation

There are a wide variety of activities aimed at developing and implementing an overall strategy for the adoption of software assurance technology, standards, and practices by commercial industry and government. These efforts include the creation and modification of international standards, the establishment of education and training activities, and the adoption of standard approaches and knowledge within the tools and services industries used to develop and maintain software. Details of these activities, challenges, and progress will be provided throughout this presentation.

10:40- 11:00 ***Break***

11:00 -12:00 **Technology, Tools and Product Evaluation**
Konrad Vesey, NSA Center For Assured Software (CAS)

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.

12:00 – 13:00 Lunch

13:00 – 13:50 **Systems Assurance**
Mitchell Komaroff, OCIO/I&NA, Information Assurance Policy, DoD

Mr. Komaroff will provide an overview of the role of engineering-in-depth within the Department of Defense Software and Systems Assurance Concept of Operations. The status update on the DoD/NDIA Systems Assurance Guidebook will be provided, followed by discussion of Systems Assurance as developed in the Guidebook.

13:50 - 14:40 **Lessons Learned in Static Analysis Tool Evaluation**
James Butler, Knowledge Solutions Manager, Concurrent Technologies Corporation

Mr. Butler will talk about best practices and lessons learned from a study that compared a set of five state-of-the-art, commercially available, static analysis solutions for third party security analysis. He will demonstrate how seemingly simple tasks such as establishing a platform for analysis, determining veracity of a reported flaw and even counting the lines of code in a target contain numerous pitfalls. He will also describe strategies for creating the level playing field necessary for a fair comparison among tools including standardization/formalization of vulnerabilities and approaches for generating evaluation criteria, test cases and meaningful measurements of detection accuracy.

14:40 – 15:00 Break

15:00 – 15:50 **COTS, MIL-SPEC and MILS, A Necessary Harmony for Affordable Multilevel Secure Architectures**
Dr. Ben A. Calloni, P.E., 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.

15:50 - 16:40 **Software Assurance Challenges for System Integrators**
Dr. Sumeet Malhotra, Global Director of Advanced Research, Unisys

In order to do a comprehensive job of information assurance analysis in any operational environment, it is important to look at the complete environment in which information resides - from the software in which content is available down through the various layers of APIs of frameworks that the original writers of the corresponding software leveraged, down to the OS and then to the BIOS, firmware and actual hardware of the systems where information exists. Also, during initial software development, vulnerabilities can become inherent at any stage of the complete software development lifecycle (SDLC). Vulnerabilities can appear during the inception and requirements gathering stage of the SDLC or during the architectural design and analysis stage or during the actual development stage or during the testing or debugging stage. In this presentation, Dr. Sumeet Malhotra will explain what kinds of vulnerabilities can crop up at what stages during the development of software and during actual runtime of that software. He will

give an industry overview of the leading edge solutions that are available to combat those vulnerabilities. Dr. Malhotra has been involved in cutting-edge research (basic and applied) with many partner organizations of Unisys and will present some of the resulting frameworks that have been generated as a result of his extensive advanced research work in his labs and in various standards organizations.

16:40 – 17:10 **OMG SwA AB Special Interest Group: Focus, Directions and Next Steps**

Djenana Campara, CEO, KDM Analytics
J.D. Baker, Systems and Software Engineering, BAE
OMG SwA ABSIG Co-chairs