# Changing the Game in Software Assurance

No developer or application manager likes to learn that their code was hacked and their applications exploited. Therefore, CrossTalk readers who manage and write code are often the strongest advocates of "doing the right thing," especially when it comes to software assurance (SwA). That is why the DHS is proud to sponsor this issue, primarily focused on SwA *Game-Changing Tools and Practices*.

CrossTalk would like to thank the Department of Homeland Security for sponsoring this issue.

Many SwA tools focus on automatic bug-finding, the first stage in a two-phase process where the tool finds bugs and the human then corrects them; Dr. Yannick Moy's article, *Static Analysis Is Not Just for Finding Bugs*, argues for a larger view of SwA by looking at the computing properties of software.

With today's global IT software supply chain, project management and software/systems engineering processes must explicitly address security risks posed by exploitable software. In *Considering Software Supply Chain Risks*, Dr. Robert J. Ellison and Dr. Carol Woody point out that a software supply chain can involve a combination of internal development, outsourced development, multiple commercial suppliers, and the use of legacy systems. The composite system inherits the risk of SwA failure at any point in such a supply chain. The authors recommend three practices: 1) mitigation of items on a CWE/SANS Institute Top 25 list linked to detailed design or coding practices, 2) mitigations associated with risk analysis, requirements, architecture, and testing, and 3) employment of a full life-cycle context for security improvement.

Two articles build on the SwA Automation Protocols from MITRE's DHS-sponsored Making Security Measurable program. *Studying Software Vulnerabilities* by Dr. Robin A. Gandhi, Dr. Harvey Siy, and Yan Wu points to the potential for using these automation protocols to build tools for developers. Sean Barnum's *The Balance of Secure Development and Secure Operations in the Software Security Equation* shows how these protocols enable development and operations staffs to better communicate and cooperate to secure applications.

Education is another essential arena for addressing the security risks posed by exploitable software. Lt. Col. Thomas A. Augustine (Ret.) and Dr. Lori L. DeLooze examine *Information Assurance Applications in Software Engineering Projects* from U.S. Naval Academy student capstone projects. Dr. Nancy R. Mead and Dr. Dan Shoemaker detail *Two Initiatives for Disseminating Software Assurance Knowledge*: Carnegie Mellon's SwA Master's program, providing an explicit curriculum of knowledge and skills necessary to produce a well-educated SwA professional; and the University of Detroit Mercy's efforts to give every instructor in a computer-related discipline access to validated content and instructional materials that can be easily incorporated into existing courses.

Online readers of CrossTalk get a bonus article: Patti Spicer's *Gaining Software Assurance Through the Common Criteria* gives both a background of the Common Criteria and explains how its certification process provides software product assurance.

As the new Director of the National Cyber Security Division, part of my responsibility is to advance efforts like those described in this issue. I look forward to working with talented professionals like readers of CrossTalk, who make our nation's software and applications resilient and secure.

Bobbie Stempfley
Director, National Cyber Security Division