Workshop: How to Get Started in Software Assurance Education

Nancy R. Mead
Software Engineering Institute
nrm@sei.cmu.edu

Dan Shoemaker
University of Detroit Mercy
shoemadp@udmercy.edu

Abstract

Interest in software assurance and software assurance education has been growing over the past few years. As more investigation into software assurance education takes place, it has become clear that it is a natural fit for institutions that are offering software engineering, information systems, and computer science degree programs. In this workshop, software assurance education will be introduced to faculty members who are interested in incorporating software assurance concepts into existing and new degree programs. At the completion of the workshop, the faculty members will have developed an initial strategy for software assurance education at their institutions and outlined the software assurance content to be included in their offerings.

1. Topic, theme, goals

Cyber security education is a hot topic these days. We see frequent references to it in the news, such as a recent article in the New York Times that discusses the need for more practitioners with cyber security expertise [1]. This article also discusses the shortage of graduates at various educational levels with the needed background. Many of the news articles address the problems of defending existing systems from attack. However, as educators we know that systems need to be developed with good software engineering practices and with security in mind in the first place. This line of thinking leads us in the direction of software assurance. In our work, we use the following definition of software assurance: "Software assurance (SwA) is the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its life cycle, and that the software functions in the intended manner" [2]. The topic of this workshop is the development of strategies for software assurance courses, tracks, and degree programs and the associated outlines for implementation at the participants' institutions.

In order to accomplish this, we will introduce the participants to some of the current projects and artifacts in software assurance education [3, 4, 5]. These include sample course outlines, the draft curriculum for a master's degree in software assurance, a discussion of software assurance tracks, and a repository of software assurance instructional materials. The goal of the workshop is to teach participants about software assurance education, the resources that are available to them, how to contact others with similar interests, and possible implementation strategies and plans.

2. Audience

The intended audience is faculty members who wish to include undergraduate and graduate software assurance courses, tracks, and master's degree programs among their offerings.

Although most of our work is targeted at academic audiences, this workshop could also be used to develop continuing education offerings. The typical CSEET attendees who are looking to extend their elective offerings in the software assurance area or to establish new degree programs are the ideal audience.

3. Activities and format

The workshop will start with an overview of the existing resources. These resources include the draft Master of Software Assurance curriculum, being developed under the leadership of Nancy Mead at the Carnegie Mellon Software Engineering Institute (SEI) in support of the Department of Homeland Security National Cyber Security Division (NCSD). This reference curriculum will describe a structure that calls for a core of five or six courses that cover the software assurance body of knowledge. The curriculum will provide for students entering the program with a variety of backgrounds. It will allow for several elective courses so that students or a university can specialize in particular security domains and, perhaps, a capstone that could consist of a master's thesis or a two-semester group project in the specialty domain. The curriculum architecture will not specify how materials and topics should be packaged into individual courses, although the project may provide examples of course packaging for such a curriculum. In the end, the decision on how to structure courses will be determined by the faculty of each institution's program.

The workshop will also include an overview and demo of the contents of the National Software Assurance Repository, developed under the leadership of Dan Shoemaker at the University of Detroit Mercy, and its heuristic, online knowledge management system, which is mind-mapped to the concepts in the previously published DHS Software Assurance Common Body of Knowledge (CBK) [5]. Using the structure of the CBK, the contents of the repository, and a Delphi process involving a panel of 11 nationally recognized experts (which produced 150 pages of annotated comments), the University of Detroit Mercy has produced a validated model of the discipline that incorporates, refines, and adds to the findings of the CBK. From this model, the researchers have produced targeted courseware that can be inserted into currently existing curricula in computer science, software engineering, and information systems. The courseware incorporates multimedia approaches for both synchronous and asynchronous delivery. The documentation of where this courseware fits is based on a detailed mapping to the Computing Curricula 2005 recommendations [6]. Additional resources include the DHS Build Security In website [7] and the recently published book titled *Software Security Engineering: A Guide for Project Managers* [8].

Once this presentation of resources is complete, participants will focus on using them to do one of the following: (1) develop software assurance course outlines for their institution, (2) develop a software assurance track in conjunction with an existing undergraduate or master's program, or (3) develop a master of software assurance degree program. They will work on these assignments individually or in teams and report their results back to the group.

4. References

[1] C. Drew, "Wanted: 'Cyber Ninjas,'" New York Times, December 29, 2009, http://www.nytimes.com/2010/01/03/education/edlife/03cybersecurity.html?emc=eta1

[2] Department of Homeland Security National Cyber Security Division, Software Assurance, https://buildsecurityin.us-cert.gov/swa/, 2010

[3] N. Mead, D. Shoemaker, and J. Ingalsbe, “Integrating Software Assurance Knowledge into Conventional Curricula”, Crosstalk, January, 2008

[4] K.M. Goertzel (ed.), Software Security Assurance State-of-the-Art Report (SOAR), Information Assurance Technology Analysis Center (IATAC), Data and Analysis Center for Software (DACS), July 31, 2007

[5] S. Redwine (ed.), Software Assurance, A Curriculum Guide to the Common Body of Knowledge to Produce, Acquire and Sustain Secure Software, Department of Homeland Security, October, 2007. https://buildsecurityin.us-cert.gov/daisy/bsi/dhs/927-BSI.html

[6] Association for Computing Machinery, Association for Information Systems (AIS), and Computer Society (IEEE-CS), Computing Curricula 2005: The Overview Report, http://www.acm.org/education/curricula-recommendations, 2006

[7] Department of Homeland Security National Cyber Security Division, Build Security In Home, https://buildsecurityin.us-cert.gov/daisy/bsi/home.html, 2010

[8] J.H. Allen, S. Barnum, R.J. Ellison, G. McGraw, and N.R. Mead Software Security Engineering: A Guide for Project Managers, Addison-Wesley, Boston, MA: 2008 (ISBN 032150917X)