Two Initiatives for Disseminating Software Assurance Knowledge

Dr. Nancy R. Mead
SEI

Dr. Dan Shoemaker
University of Detroit Mercy

Education in software assurance (SwA) is an essential element in the effort to produce secure code. This article describes two efforts that support national cybersecurity education goals: development of SwA learning artifacts that can be integrated into conventional learning environments and establishment of a reference curriculum for a master's degree program, known as the MSwA.

There is general recognition that software engineering practice can best be improved through education. In fact, the establishment of a National Cyberspace Security Awareness and Training Program was among the three highest priorities in [1], which describes the program's purpose as to "improve cybersecurity knowledge, and understanding of the issues" and to produce a "sufficient number of adequately trained ... personnel to create and manage secure systems." The cornerstone of the initiative was the mandate to ensure "adequate training and education to support cybersecurity needs" [1].

The aim of these initiatives was to guarantee that SwA practices would be embedded in the day-to-day actions of the overall workforce [2]. The problem with SwA is that there was no single point of reference to "guide the development and integration of education and training content relevant to software assurance" [3]. That led the DHS to publish a 387-page Common Body of Knowledge (CBK), which specifies a comprehensive set of recommended practices for secure SwA. These range from "heavyweight design methods" to "model contract language for vendors" [3]. The problem is that none of these recommendations have made their way into common use.

The traditional means of disseminating any kind of new knowledge into the society at-large is through formally constituted education, training, and awareness programs [2]. Back in 2003, the National Strategy recognized that fact in Action/Recommendation 3-6, which states that research and development efforts should be conducted in the general area of secure SwA in order to coordinate "the development and dissemination of best practices for cybersecurity." [1].

The obvious question eight years later is, "How close are we to achieving that goal?" The two projects discussed in this article are designed to promote more secure software teaching in higher education. Together, they represent the first attempts to ensure that the principles and practices of secure SwA knowledge are embedded in mainstream higher education processes.

The problem with SwA knowledge is that it is crosscutting rather than disciplinary. In essence, the knowledge base for SwA is located in a range of traditional studies [4]. That includes dissimilar CBK areas such as software engineering, systems engineering, information systems security engineering, safety, security, testing, information assurance, law, and project management [4]. As a result, secure SwA content might appear in many different places and be taught in many different ways in conventional education settings.

"The two projects ... are designed to promote more secure software teaching ... they represent the first attempts to ensure that the principles and practices of secure SWA knowledge are embedded in mainstream higher education processes."

It is clearly unacceptable to approach the teaching and learning process in such a disjointed way. Therefore, the way educators promulgate secure SwA knowledge has to be coordinated. In order to coordinate the teaching and learning process, a formal effort has to be made to integrate "software assurance content ... into the body of knowledge of each contributing discipline" [5]. There are two practical barriers to achieving that outcome:

1. It is not clear what specific knowledge and skills should be taught in each area.
2. There are no validated methods for delivering that knowledge once it has been identified.

Logically, the first step in integrating new knowledge into conventional learning environments is to identify, relate, and catalogue what is presently out there.

Project 1 – Documenting Knowledge

The goal of one project—funded by the DoD and conducted at the University of Detroit Mercy (UDM)—is attempting to identify and document any knowledge, from any source, that could be related to SwA. That knowledge came from all traditional computing disciplines, such as computer science, software engineering, and information systems. Nevertheless (besides the strictly technical areas), the project also incorporated the conventional areas of information security as well as relevant knowledge from the behavioral and social sciences. The knowledge was obtained from all accessible public and private sector sources.

The resulting knowledge base is contained in the DoD's National Software Assurance Repository (NSAR). The NSAR encompasses and relates all commonly accepted practices, principles, methodologies, and tools for SwA. It is managed by an automated online knowledge management system with an underlying knowledge management system roughly based on the CBK; however, to ensure the validity of the CBK framework, the mind map was fine-tuned and validated through conducting a classic Delphi study using a panel of 11 nationally known secure SwA experts.

The knowledge base contains as many life-cycle methodologies and tools for assuring software as could be identified. It also itemizes all related supporting principles and concepts that are aimed at increasing the assurance and security of internally developed and sustained software. That also includes products and ser-

vices purchased from outside vendors. The knowledge base is evolutionary and inclusive: As the literature of the field expands or new sources are identified, that material will be catalogued and added to the current knowledge base.

Pedagogy Development

The actual purpose of the UDM project was not simply to gather knowledge; it was also to ensure the teaching of secure software topics in all appropriate education, training, and awareness settings. In support of that goal, the project has packaged the contents of its knowledge base into discrete learning modules. These modules are designed to facilitate the efficient SwA knowledge transfer to all relevant teaching and learning settings. As a result, the modules can be incorporated into a wide range of teaching and learning environments. They are appropriate for graduate, undergraduate, community college, and even high school education, as well as in training and awareness applications.

The modules are intended to be separate, standalone learning artifacts capable of conveying all of the requisite know-how for a given topic. At a minimum, each module can be delivered in a conventional classroom. However, the modules embody supporting material that also allows delivery in a range of asynchronous and Web-enabled learning environments. That flexibility facilitates the efficient transfer of new workforce skills and practices to all types of settings.

Each module conveys a logical element of SwA practice. The entire collection of these modules is mapped to the body of knowledge contained in the knowledge base, which is structured on the most commonly accepted model for secure SwA practice (the CBK). This mapping provides precise guidance about the places where the newly developed instructional content fits within the commonly accepted understanding of the correct elements of practical SwA work.

Each of the actual teaching modules incorporates a set of conventional learning artifacts that are easily recognizable to traditional educators. Every module includes:

1. A table of learning specifications.
2. Presentation slides for each concept contained in the module.
3. An evaluation process.
4. Any relevant Web-enabled supporting material.
5. A model delivery system.

There is also an accompanying pedagogical methodology for each individual learning module. In other words, every module incorporates a validated set of teaching tools, with each tool being optimized to ensure the maximum knowledge transfer for all potential teaching settings.

Mapping for Broad-Scale Integration

In order to ensure integration into conventional higher education curricula, the UDM project has formally mapped all of its secure SwA courseware modules to the standard set of computing topics specified for three of the five computer disciplines in the Computing Curricula 2005 standard (CC2005) [6]. This standard is a joint authorization of the Association for Computer Machinery (ACM), IEEE, and Association for Information Systems. Since these are the three associations that are responsible for developing and overseeing computing curricula worldwide, the CC2005 can be considered to be exhaustively authoritative.

The elements of secure SwA practice were mapped from the CBK to the generally accepted curricular recommendations (as itemized in CC2005). The aim of the mapping process was to identify where specifications for secure practice contained in the CBK fit within the recommendations for curricular content in each of the disciplines of computer science, software engineering, and information systems.

The mapping itself was a keyword-based process, utilizing the terms from the curricular requirements contained in Tables 3.1 and 3.2 of CC2005 as the search criterion. Where instances of that term were found in the CBK, anecdotal analysis was employed to determine the intent of the term with respect to the discussion of secure SwA. Those intents were noted, aggregated, and then categorized into highly specific concepts for secure SwA that had to be communicated along with the teaching of each of the conventional CC2005 curricula elements. The detailed mapping of concepts to recommendations was used to tailor the integration of the associated secure SwA teaching module for supporting or facilitating the specific intent of that term.

The project provides a detailed specification of where each learning module best fits within CC2005's curriculum. It also provides a justification for why the module was placed where it was in that particular curriculum. The justification is based on the mapping between the module and the recommended topics for a

standard computer science, software engineering, and information systems curriculum. For instance, the project provides specific recommendations for the precise place in an information systems curriculum where new secure SwA content could be added to current testing topics. The justification is necessary to help individual curriculum designers understand where the learning module should be placed in their curricula. The justification also facilitates the integration and acceptance of that module within the traditional higher education and training communities.

Project 2 – MSwA Curriculum

The second education initiative to support the National Strategy focused primarily on development of a reference curriculum for an MSwA. The SEI is leading this ongoing education effort in support of the DHS's National Cyber Security Division. This is a particularly important focus because much of the body of knowledge in secure SwA is based on a foundation of software engineering principles and practices. This project specifies a set of topics and all of the attendant prerequisite knowledge and requirements needed to ensure a properly educated SwA professional. It differs from the prior project in that it identifies just the key knowledge elements required to produce a well-educated practitioner—and structures those elements into a comprehensive curriculum.

The curriculum development team includes technical staff from the SEI and faculty from a number of universities, including international representation. The reference curriculum includes guidelines that were used to develop the curriculum, prerequisites and proposed outcomes, curriculum architecture, a curriculum body of knowledge, implementation guidelines, and a glossary of terms. A number of existing artifacts (including the CBK), the recent graduate software engineering curriculum guidelines [7], and the older SEI reports on graduate software engineering education [8, 9] are inputs to the project. The team also referenced [10] as needed, as software engineering knowledge is fundamental to SwA. The project was inspired in part by the DHS Build Security In (BSI) Web site <https://buildsecurityin.us-cert.gov>, which contains articles providing practical advice on SwA to practitioners. It is this practitioner focus that is central to the curriculum development effort. Another important resource for the team (also inspired by the BSI Web site) is [11], which was used along with the previously noted resources to identify the SwA practices to include in the curriculum.

In order to stay grounded, an invited review team for the curriculum was also involved in the process. In addition, some key industry managers and practitioners generously agreed to be surveyed in order to help validate our understanding of the desired outcomes. The curriculum also includes a detailed list of knowledge units and corresponding Bloom's taxonomy levels [12].

Establishment of a new degree program is a very ambitious undertaking. As a consequence, the team expects that some universities will elect to establish tracks or specializations in SwA within existing graduate disciplines (e.g., Master's-level programs in Software Engineering [MSwE]), rather than establishing a whole new degree. Therefore, guidance is provided on how to implement a track or specialization, and sample course syllabi are also provided. Team members at Monmouth University and Embry-Riddle Aeronautical University developed candidate implementation strategies for incorporating curriculum elements at their universities.

"Our understanding of the knowledge that is needed to ensure capable SwA is beginning to be shaped by these two projects. In that respect—and particularly given the critical importance of secure software to the national interest—they are working together to advance that process."

In addition to the MSwA reference curriculum, this project also produced a set of sample outlines for SwA courses that could be offered at the undergraduate level [13]. These courses might form an area of concentration within a computer science or software engineering undergraduate degree program for any prospective adopter.

Curriculum Transition Plans

There are a number of transition activities that accompany this curriculum work, as a curriculum is only the first step in effecting change in education. The team has started to work with the IEEE Computer Society towards professional recognition, including a seminar at the March 2010 Conference on Software Engineering Education and Training to raise awareness[1]. The curriculum has been presented at the 2010 Curriculum Development in Security and Information Assurance workshop, at a June 2010 DHS Software Assurance Working Group meeting, and also in the Information Assurance Capacity Building Program[2]. Finally, the team will also form a group to work with and provide assistance to universities who wish to offer SwA graduate courses. The team has also started tailoring the curriculum into course offerings that would fit at the community college level.

Looking beyond these near-term activities, the team plans to develop more extensive faculty development workshops, course materials, and course offerings in this area. They also hope to work towards SwA certification along the same lines as IEEE's Computer Software Development Professional. There is an opportunity for distance education in this area, and eventually they may look at high school educational opportunities. The team feels that SwA education is essential at all levels, in order to ensure that software and software-intensive systems are developed with assurance in mind.

Conclusions

Our understanding of the knowledge that is needed to ensure capable SwA is beginning to be shaped by these two projects. In that respect—and particularly given the critical importance of secure software to the national interest—they are working together to advance that process. Both projects are beginning to establish the foundation for moving into the mainstream of education, training, and awareness a field that has historically not been either well understood nor well recognized.

The maturity of SwA education will have advanced when:

- MSwA programs—and SwA specializations within MSwE programs—are widely available.
- The SwA materials database is commonly used in course development.
- SwA offerings are standard elements

of undergraduate computer science and software engineering degree programs.

- The SwA body of knowledge has been codified.

In the case of the MSwA curriculum project, these master's programs and tracks provide an explicit curriculum of knowledge and skills necessary to produce a well-educated SwA professional. Ultimately, the curriculum will be supported by the needed course materials and course offerings. In the case of the UDM project, every instructor in a computer-related discipline now has access to validated content and instructional materials that can be easily incorporated into existing courses.

In both projects, the boundaries and elements of the teaching and learning process for SwA education are clarified. They are initial steps in the long road to being able to assure the correctness and integrity of the nation's software with total confidence. Together, they create a direction and foundation on which the future of the profession can be built.

References

1. Clark, Richard A., and Howard A. Schmidt. *A National Strategy to Secure Cyberspace*. Washington: The President's Critical Infrastructure Protection Board. Feb. 2003 <www.us-cert.gov/reading_room/cyberspace_strategy.pdf>.
2. Cogburn, Derrick L. *Globalization, Knowledge, Education and Training in the Information Age, United Nations Educational, Scientific and Cultural Organization.* Director, Centre for Information Society Development in Africa and Africa Regional Director, Global Information Infrastructure Commission. 1 Dec. 2009 <www.unesco.org/webworld/infoethics_2/eng/papers/paper_23.htm>.
3. Redwine, Samuel T., Ed. *Software Assurance: A Guide to the Common Body of Knowledge to Produce, Acquire and Sustain Secure Software, Version 1.1*. Washington D.C.: DHS, 2006.
4. Mead, Nancy R., Dan Shoemaker, and Jeffrey Ingalsbe. "Integrating Software Assurance Knowledge into Conventional Curricula." CrossTalk Jan. 2008 <www.stsc.hill.af.mil/crosstalk/2008/01/0801MeadShoemakerIngalsbe.html>.
5. Shoemaker, Dan, et al. *A Comparison of the Software Assurance Common Body of Knowledge to Common Curricular Standards*. Proc. of the 20th Conference on Software Engineering Education and Training. Dublin, Ireland. 3-5 July, 2007.
6. The Association for Computing Machinery, The Association for Information Systems, and The Computer Society. *Computing Curricula 2005: The Overview Report, Computing Curricula Series*. 30 Sept. 2005 <www.acm.org/education/curric_vols/CC2005-March06Final.pdf>.
7. Integrated Software & Systems Engineering Curriculum Project – Stevens Institute of Technology. *Graduate Software Engineering 2009 (GSWe2009) Curriculum Guidelines for Graduate Degree Programs in Software Engineering*. 30 Sept. 2009 <www. gswe2009.org/>.
8. Ford, Gary. *1991 SEI Report on Graduate Software Engineering Education*. SEI, Carnegie Mellon University. Technical Report CMU/SEI-91-TR-002. Apr. 1991 <www.sei.cmu.edu/reports/91tr002.pdf>.
9. Ardis, Mark, and Gary Ford. *SEI Report on Graduate Software Engineering Education*. SEI, Carnegie Mellon University. Technical Report CMU/SEI-89-TR-21. June 1989 <www.sei.cmu.edu/reports/89tr021.pdf>.
10. IEEE Computer Society. *Guide to the*

Software Defense Application

Cybersecurity has been an area of national interest for almost a decade. Education has been noted for years—all the way up to the White House—as one of the most important elements in securing cyberspace. Yet, the DHS's Common Weakness Enumeration [14] documents 797 common defects—and the list is still growing. That is due to current software engineering practice, which has generated software defects at a relatively constant rate for the past 40 years. Those defects—according to a 2008 International Data Corporation survey (see <www.coverity.com/html/press_story65_08_04_08.html>)—now cost the average U.S. corporation $22 million dollars annually. Worse, they leave DoD systems, as well those of all government and industry, susceptible to attack. This article shows successful educational experiences in developing concepts and passing along the principles and practices of secure SwA knowledge.

Software Engineering Body of Knowledge (SWEBOK). 2004 <www.computer.org/portal/web/swebok/html format>.

11. Allen, Julia, et al. *Software Security Engineering: A Guide for Project Managers*. Upper Saddle River, NJ: Addison-Wesley, 2008.
12. Bloom, Benjamin S., ed. *Taxonomy of Educational Objectives: The Classification of Educational Goals: Handbook I: Cognitive Domain*. New York: Longman, 1956.
13. Mead, Nancy R., Thomas J. Hilburn, and Richard C. Linger. *Software Assurance Curriculum Project Volume II: Undergraduate Course Outlines*. SEI, Carnegie Mellon University. Technical Report CMU/SEI-2010-TR-019. Jan. 2010.
14. The MITRE Corporation. *Common Weakness Enumeration*. 17 May 2010 <http://cwe.mitre.org>.

Notes

1. The seminar will be distributed at a later time in the Virtual Training Environment format.
2. This is a faculty development program that was held this July at Carnegie Mellon University.

About the Authors

Nancy R. Mead, Ph.D., is a senior technical staff member for the CERT Program at the SEI. She is also a faculty member in the Master of Software Engineering and Master of Information Systems Management programs at Carnegie Mellon. Her research interests are information security, software requirements engineering, and software architectures. Mead has more than 150 publications and invited presentations. She is an IEEE fellow and a Distinguished Member of the ACM. Mead received her doctorate in mathematics from the Polytechnic Institute of New York and has bachelor's and master's degrees in mathematics from New York University.

SEI
4500 Fifth AVE
Pittsburgh, PA 15213-3890
E-mail: nrm@sei.cmu.edu

Dan Shoemaker, Ph.D., is the Director of the Institute for Cyber Security Studies, a National Security Agency Center of Academic Excellence, at the UDM. He has been professor and chair of computer and information systems at the UDM for 25 years, and co-authored the textbook, "Information Assurance for the Enterprise." His research interests are in the areas of secure SwA, information assurance and enterprise security architectures, and information technology governance and control. Shoemaker has both a bachelor's and doctorate degree from the University of Michigan, and master's degrees from Eastern Michigan University.

Computer and Information Systems
College of Business Administration
University of Detroit Mercy
Detroit, MI 48221
Phone: (313) 993-1202
E-mail: shoemadp@udmercy.edu

Coming Events

September 27-October 1
13th Semi-Annual DHS Software Assurance Forum
Gaithersburg, MD
https://buildsecurityin.us-cert.gov/bsi/events/1133-BSI.html

October 31-November 3
Milcom 2010
San Jose, CA
www.milcom.org

November 7-11
18th International Symposium on the Foundations of Software Engineering
Santa Fe, NM
http://fse18.cse.wustl.edu

December 4-8
MICRO-43
Atlanta, GA
www.microarch.org/micro43

December 14-16
DHS Software Assurance Working Group Sessions
McLean, VA
https://buildsecurityin.us-cert.gov/bsi/events/1135-BSI.html

January 4-7, 2011
Hawaii International Conference on System Sciences
Koloa, Kauai, HI
www.hicss.hawaii.edu

February 28-March 4, 2011
14th Semi-Annual DHS Software Assurance Forum
McLean, VA
https://buildsecurityin.us-cert.gov/bsi/events/1136-BSI.html

Coming Events: **Please submit coming events that are of interest to our readers at least 90 days before registration. E-mail announcements to: <kasey.thompson@hill.af.mil>.**