Teaching Secure Coding- Report from Summit on Education in Secure Software

Blair Taylor (moderator)
Towson University
btaylor@towson.edu

Matt Bishop
University of California Davis
bishop@cs.ucdavis.edu

Diana Burley
George Washington University
dburley@gwu.edu

Steve Cooper
Stanford University
coopers@cs.stanford.edu

Ron Dodge
United States Military Academy
Ron.Dodge@usma.edu

Robert Seacord
Carnegie Mellon University/SEI
rcs@cert.org

Categories and Subject Descriptors

D.2.4 [**Software**]: Software/Program Verification - *reliability*

K.3.2 [**Computers and Education**]: Computer and Information Science Education – *computer science education*

General Terms

Reliability, Security

Keywords

Secure Coding

1. SUMMARY

Software is critical to life in the 21st century. It drives financial, medical, and government computer systems as well as systems that provide critical infrastructures in areas such as transportation, energy, networking, and telecommunications. As the number and severity of attacks that exploit software vulnerabilities increase, writing reliable, robust, and secure programs will substantially improve the ability of systems and infrastructure to resist such attacks. Education plays a critical role in addressing cybersecurity challenges of the future, such as designing curricula that integrate principles and practices of secure programming into educational programs.

To help guide this process, the National Science Foundation Directorates of Computer and Information Science and Engineering (CISE) and Education and Human Resources (EHR) jointly sponsored the Summit on Education in Secure Software (SESS), held in Washington, DC in October, 2010. The goal of the summit was to develop roadmaps showing how best to educate students and current professionals on robust, secure programming concepts and practices, and to identify both the resources required and the problems that had to be overcome.

Copyright is held by the author/owner(s).
SIGCSE'12, February 29–March 3, 2012, Raleigh, North Carolina, USA.
ACM 978-1-4503-1098-7/12/02.

The Summit made 10 specific recommendations, developed from the roadmaps:

1. Increase the number of faculty who understand the importance of secure programming principles, and will require students to practice them.
2. Provide faculty support for the inclusion of security content through clinics, labs, and other curricular resources.
3. Establish professional development opportunities for college faculty, non-computer science professionals, and K-12 educators to heighten their awareness and understanding of secure programming principles.
4. Integrate computer security content into existing technical (e.g. programming) and non-technical (e.g. English) courses to reach students across disciplines.
5. Require at least one computer security course for all college students:
   a. For CS students focus on technical topics such as how to apply the principles of secure design to a variety of applications.
   b. For non-CS students focus on raising awareness of basic ideas of computer security.
6. Encourage partnerships and collaborative curriculum development that leverages industry and government needs, resources, and tools.
7. Promote collaborative problem solving and solution sharing across organizational (e.g. corporate) boundaries.
8. Use innovative teaching methods to strengthen the foundation of computer security knowledge across a variety of student constituencies.
9. Develop metrics to assess progress toward meeting the educational goals specified in the roadmaps presented in this document.
10. Highlight the role that computer security professionals should play in key business decision-making processes.

The goal of this session is to share some of the key findings and challenges identified by the summit and to actively engage the community in the discussions. Each of the speakers participated in the summit and brings a unique viewpoint to the session.

2. MATT BISHOP

Matt Bishop is on the faculty of the Department of Computer Science at the University of California at Davis. His main research area is the analysis of vulnerabilities in computer

systems, including modeling them, building tools to detect vulnerabilities, and ameliorating or eliminating them. He has participated in numerous studies of computer systems, including as one of the co-PIs of the California Top-to-Bottom Review of electronic voting systems certified for use in that state. He helped organize, and chaired the first two USENIX UNIX Security workshops. He is active in information assurance education, and has presented tutorials at SANS, USENIX, and other conferences. His textbook, *Computer Security: Art and Science*, was published in December 2002 by Addison-Wesley Professional. **As co-organizer of the Summit and a co-author of the Summit report, he will present the foundation for the session discussion by describing the importance of robust coding.**

3. DIANA BURLEY

Diana Burley is an Associate Professor in the Graduate School of Education and Human Development at the George Washington University. She is also a board member of the GW Cyber Security Policy and Research Institute (CSPRI). Prior to joining GW, Dr. Burley served as a Program Director in the Directorate for Education and Human Resources at The National Science Foundation (NSF). While at NSF, she served as the lead Program Director for the Federal Cyber Service: Scholarship for Service (SFS) program. **As a co-organizer of the Summit and co-author of the report, Diana will describe the goals and outcomes of the summit.**

4. STEVE COOPER

Steve Cooper is an Associate Professor in the Computer Science Department at Stanford University. He formerly taught at Purdue University and Saint Joseph's University. Steve worked in NSF's Division of Undergraduate Education, within its Education and Human Resources Directorate as a program manager, and worked on the CCLI, ATE, NSDL, SFS, and S-STEM programs. Steve also serves as Chairman of the Board of Directors for the Computer Science Teachers Association. In addition to his extensive work with Alice, his current research includes the creation of a serious game to teach secure coding practices to novice programmers. (This work is supported in part by NSF – 1022557.) **For the past three years, Steve has led a series of Working Groups at ITICSE towards creating a series of curricular guidelines for IA programs [2, 3] and will link these results to the summit.**

5. RON DODGE

Ron Dodge has served for over 23 years in the United States Army. Currently he is an Associate Professor permanently stationed at the United States Military Academy and the Associate Dean for Information and Education Technology. Ron is the vice-chair for the Colloquium for Information Systems Security Education (CISSE), Secretary for the IFIP TC 11.8 working group on Information Security Education, and on the executive committee for the Institute for Information Infrastructure Protection. Ron has spent the last 10 years developing innovative methods to teach and train Cyber Security and Assurance. **In addition to offering a viewpoint from a military institution, Ron will address the role that security in general and secure software development in particular will play in Computing Curriculum 2013.**

6. ROBERT SEACORD

Robert Seacord manages the Secure Coding Initiative at CERT, located in Carnegie Mellon's Software Engineering Institute (SEI). CERT, among other security related activities, regularly analyzes software vulnerability reports and assesses the risk to the Internet and other critical infrastructure. Robert is an adjunct professor in the Carnegie Mellon University School of Computer Science and in the Information Networking Institute. His principal areas of expertise include software security, C, C++, and Java-programming languages, component-based development, graphical interface design, and human factors. His books include: Secure Coding in C and C++, The CERT C Secure Coding Standard, The CERT Oracle Secure Coding Standard for Java (SEI Series in Software Engineering). **Robert will discuss the ongoing work and resources available at CERT in the area of secure software education.**

7. BLAIR TAYLOR (moderator)

Blair Taylor is a Clinical Assistant Professor in the Department of Computer and Information Sciences at Towson University and is the PI for the NSF-funded Security Injections @ Towson project. *Security injections* are strategically-placed security-related modules for existing undergraduate classes. (This work is supported by NSF – 0817267.) Blair has experience in information assurance education and two and four-year computer science articulation. **Blair will serve as moderator of the session.**

8. REFERENCES

[1] Burley, D and Bishop, M. 2011. Summit on Education in Secure Software Final Report. http://nob.cs.ucdavis.edu/bishop/notes/2010-sess/2010-sess.pdf

[2] Cooper, S., Nickell, C., Piotrowski, V., Oldfield, B., Abdallah, A., Bishop, M., Caelli, B., Dark, M., Hawthorne, E., Hoffman, L., Pérez, L., Pfleeger, C., Raines, R., Schou, C., and Brynielsson, J. 2010. An exploration of the current state of information assurance education. SIGCSE Bull. 41, 4 (January 2010), 109-125. DOI=10.1145/1709424.1709457

[3] Cooper, S., Nickell, C., Pérez, L., Oldfield, B., Brynielsson, J., Gökce, A., Hawthorne, E., Klee, K., Lawrence, A., and Wetzel, S. 2010. Towards information assurance (IA) curricular guidelines. In Proceedings of the 2010 ITiCSE working group reports on Working group reports (ITiCSE-WGR '10), Alison Clear and Lori Russell Dag (Eds.). ACM, New York, NY, USA, 49-64. DOI=10.1145/1971681.1971686