Special Session: Joint Task Force on Cybersecurity Education

Diana Burley
George Washington University
Graduate School of Education and
Human Development
+1 202-994-5829
dburley@gwu.edu

Matt Bishop
University of California, Davis
Department of Computer Science
+1 530-752-8060
mabishop@ucdavis.edu

Siddharth Kaza
Towson University
Department of Computer and
Information Sciences
+1 410-704-3868
skaza@towson.edu

David S. Gibson
United States Air Force
Academy
Department of Computer
Science
+1 719-333-3590
david.gibson@usafa.edu

Scott Buck
Intel Corporation
+1 480-552-2341
scott.buck@intel.com

Allen Parrish
United States Naval
Academy
Department of Cyber Science
Annapolis
aparrish@usna.edu

Herb Mattord
Kennesaw State University
Information Systems
+1 470-578-4741
hmattord@kennesaw.edu

CCS Concepts

- **Social and professional topics** ~ Computing education
- **Social and professional topics** ~ Model curricula
- **Social and professional topics** ~ Computing education programs
- **Social and professional topics** ~ Accreditation

Keywords

Curriculum; Cybersecurity education; security education; cyber sciences

ACM Reference format:

Diana Burley, Matt Bishop, Siddharth Kaza, David S. Gibson, Scott Buck, Allen Parrish, and Herb Mattord. 2018. Special Session: Joint Task Force on Cybersecurity Education. In *SIGCSE '18: 49th ACM Technical Symposium on Computer Science Education*, Feb. 21–24, 2018, Baltimore, MD, USA. ACM, NY, NY, USA, 6 pages.
<https://doi.org/10.1145/3159450.3159635>

1. SUMMARY

In this special session, members of the Joint Task Force (JTF) on Cybersecurity Education will provide an overview of the CSEC2017 curricular guidelines (finalized in December 2017) and engage session participants in a discussion of the curricular framework and body of knowledge. The session will conclude with an interactive panel discussion on implementing the curricular guidance.

2. BACKGROUND

The Joint Task Force on Cybersecurity Education (JTF) was

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the Owner/Author(s). Copyright is held by the owner/author(s).

SIGCSE'18, February 21–24, 2018, Baltimore, MD, USA.

ACM ISBN: 978-1-4503-5103-4/18/02.

DOI: <https://doi.org/10.1145/3159450.3159635>

chartered by the ACM Education Board in September 2015 to develop comprehensive, post-secondary curricular guidance in cybersecurity education to support future program development and associated educational efforts. The JTF is a collaboration among major international computing societies: the Association for Computing Machinery (ACM), the IEEE Computer Society (IEEE-CS), the Association for Information Systems Special Interest Group on Security (AIS SIGSEC), and the International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8). The JTF grew out of the foundational efforts of the Cyber Education Project (CEP) and its members continue to collaborate with the JTF.

Recent reports [1, 2] have pointed to the need for developing curricular guidelines for cybersecurity education. Currently the 2013 ACM Curricular Guidelines for Undergraduate Degree Programs in Computer Science (CS2013) [3] treats information assurance and security (IAS) as a specific knowledge area as well as an area that spans other knowledge areas. Appearing for the first time in ACM computer science curricular guidance, the IAS knowledge area explores aspects of information assurance and security in depth; in other knowledge areas, the information assurance and security material may be tied to a particular knowledge unit. The CSEC2017 curricular guidance structures the cybersecurity discipline and provides guidance to institutions seeking to develop or modify a broad range of programs, concentrations.

3. OBJECTIVE

The objective of this special session is to provide an overview of the CSEC2017 curricular volume (December 2017). Throughout the development process, the JTF held several activities (including special sessions at SIGCSE 2016 and 2017) to ensure broad community engagement. The resulting CSEC2017 curricular thought model is based on this input; as well as a rigorous review of existing curricular frameworks in science education, computing education, and cybersecurity education.

Our philosophy, shaped in part by the U.S. National Research Council Next Generation Science Standards¹, views cybersecurity as a body of knowledge grounded in enduring principles and continuously extended, refined, and revised through evidence-based practice.

The JTF defines cybersecurity as a “computing-based discipline involving technology, people, information, and processes to enable assured operations. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management in the context of adversaries.”

The CSEC2017 thought model has four dimensions: knowledge areas, crosscutting concepts, disciplinary lens, and application areas. Knowledge areas serve as the basic organizing structure for cybersecurity content and collectively represent the full body of knowledge within the field of cybersecurity. Crosscutting concepts help students explore connections among the knowledge areas and are fundamental to an individual’s ability to understand them. The disciplinary lens represents the underlying computing discipline that forms the foundation of the cybersecurity program and drives the approach, depth of content, and learning outcomes. The application areas provide an organizing structure to combine curricular content, professional development and training opportunities, and professional certifications.

4. OUTLINE

The 75-minute session will be organized to allow ample time for audience participation. The tentative session outline is:

- Session overview – Remind participants of the Joint Task Force structure, objectives and development process (10 minutes) – Task Force co-chairs Diana Burley, Matt Bishop
- Presentation of Curricular Guidelines (25 minutes) – Sidd Kaza, David Gibson, J Eckstrom
- Implementation (25 min) – Discussion of how to use the guidelines through program, course, and job role exemplars. – Beth Hawthorne, Allen Parrish, Scott Buck
- Open Discussion (15 minutes) – Task force members will engage the audience in an open discussion on how to position the guidelines as a “living” document.

5. EXPECTATIONS

The special session is intended for all participants of the SIGCSE conference who teach or are stakeholders in undergraduate cybersecurity curricula. Since cybersecurity is interdisciplinary by nature, we expect participants from all areas in the computing sciences, including computer science, information systems and information technology. The session will provide participants with the background and current status of the guideline document. In addition, through the facilitated small group discussions, participants will be able to provide direct input to the development process. We will encourage session participants to stay engaged with task force members after the SIGCSE special session.

6. SUITABILITY

This session will provide an opportunity for community members to receive an in depth overview on the content and application of the first set of global cybersecurity curricular guidelines. The 2018 SIGCSE Technical Symposium will be held approximately 2 months after the publication of the final version of the guidelines. As such, community members will have had an opportunity to review the document prior to the session and then engage in a rich discussion with JTF members on its implementation. As an ACM-sponsored task force, the SIGCSE community represents a primary set of potential adopters of the guidance being developed. Participants are encouraged to review the task force website for background documents (csec2017.org) and the following resources prior to the session:

- *The Future of Cybersecurity Education* in IEEE Computer - www.computer.org/csdl/mags/co/2014/08/mco2014080067-abs.html
- *Final Report: Workshop on Cybersecurity Education - NSF*, https://research.gwu.edu/sites/research.gwu.edu/files/downloads/CEW_FinalReport_040714.pdf
- *Toward Curricula Guidelines for Cybersecurity: Report of a Workshop on Cybersecurity Education and Training*, ACM - www.acm.org/education/TowardCurricularGuidelinesCybersec.pdf
- *Blueprint for a Science of Cybersecurity in The Next Wave*, Cornell University - www.cs.cornell.edu/fbs/publications/SoS.blueprint.pdf

7. REFERENCES

- [1] McGettrick, A. 2013. Toward Curricular Guidelines for Cybersecurity. ACM.
- [2] Hogan, M., & Newton, E. 2015. Report on Strategic U.S. Government Engagement in International Standardization to Achieve U.S. Objectives for Cybersecurity (draft). National Institute of Standards and Technology
- [3] ACM Computer Science Curriculum 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science (Dec. 2013); doi: 10.1145/2534860
- [4] Cyber Education Project. <http://cybereducationproject.org/about/>
- [5] U.S. National Research Council, Next Generation Science Standards. <http://nextgenscience.org/>. Accessed 2016 August 12

¹ US National Research Council Next Generation Science Standards website: <http://nextgenscience.org>