Special Session:
ACM Joint Task Force on Cyber Education

Diana Burley
George Washington University
Graduate School of Education and Human Development
44983 Knoll Square, suite 147
Ashburn, VA 20147
+1 703-553-3761
dburley@gwu.edu

Matt Bishop
University of California, Davis
Department of Computer Science
One Shields Avenue
Davis, CA 95616
+1 530-752-8060
mabishop@ucdavis.edu

Elizabeth Hawthorne
Union County College
STEM Divison-Computer Science
1033 Springfield Avenue
Cranford, NJ 07016
+1 908-497-4232
hawthorne@ucc.edu

Siddharth Kaza
Towson University
Department of Computer and Information Sciences
8000 York Road
Towson, MD 21252
+1 410-704-3868
skaza@towson.edu

Scott Buck
Intel Corporation
2200 Mission College Blvd.
Santa Clara, CA 95054
+1 480-552-2341
scott.buck@intel.com

Lynn Futcher
Nelson Mandela Metropolitan University
School of Information and Communication Technology
Summerstrand Campus (North), R149
+27 41 504 9128
lynn.futcher@nmmu.ac.za

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

1. SUMMARY

In this special session, members of the ACM Joint Task Force on Cyber Education to Develop Undergraduate Curricular Guidance will provide an overview of the task force mission, objectives, and work plan. After the overview, task force members will engage session participants in the curricular development process.

2. BACKGROUND

In the context of computer security and information assurance, cyberscience is a computing-based discipline involving technology, people, and processes aligned in a way to enable "assured operations" in the presence of risks and adversaries. It involves the creation, operation, analysis, and testing of computer systems (including network and communication systems) designed to be secure, as well as the study of how to employ operations, reasonable risk taking, and risk mitigations to further that design goal. It is an interdisciplinary course of study, and includes aspects of law, policy, human factors, ethics, risk management, and other topics directly related to the success of the activities and operations dependent on such systems, often in the context of an adversary.

Recent reports [1, 2] have pointed to the need for developing curricular standards 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 material that spans other knowledge areas. The IAS knowledge area explores aspects of information assurance and security in depth; in other knowledge areas the information assurance and security material is tied to that particular area.

Unfortunately, those curricular guidelines do not treat computer security and information assurance as a cyberscience. The goal of the ACM Joint Task Force on Cyber Education is to develop undergraduate curricular guidance in information assurance and security that teaches computer security and information assurance so students see it as a cyberscience.

3. OBJECTIVE

The objective of this special session is to introduce the work of the ACM Joint Task Force on Cyber Education to Develop Undergraduate Curricular Guidance and to engage the computer science education community in the curricular development process. The session will communicate the objectives and status of the development work, and elicit input from community members. Task force members will engage session participants through general session presentations and small group discussions. In the general session, task force members will highlight the joint task force members and objectives, summarize the work of the Cyber Education Project and how the joint task force will leverage this work, and will provide a roadmap for the development process. This session will provide an opportunity for follow up on the Cyber Education Project's Learning Outcomes Working Group session held at the 2015 SIGCSE Technical

Symposium and will support continued community engagement in the curricular development process.

4. OUTLINE

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

- Session overview, Introduction of the Joint Task Force structure and objectives (10 minutes) – Task Force co-chairs Diana Burley, Matt Bishop
- Background - Cyber Education Project, Cyber Sciences (15 minutes) – Task Force members Beth Hawthorne, Sidd Kaza
- Discussion of stakeholder engagement strategy (10 minutes) – Task Force members Lynn Futcher, Diana Burley
- Audience Engagement (40 minutes) – Task force members will divide the audience into 4 small groups in order to engage in specific discussions on the curricular development process. Small groups will discuss topics for 20 minutes then reconvene as a large group to report out from the small groups (5 minutes per group).

5. EXPECTATIONS

The special session is intended for all participants of the SIGCSE conference who teach or are stakeholders in undergraduate security 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 joint task force activities. In addition, through the facilitated small group discussions, participants will be able to provide direct input to the development process. Session participants will also be encouraged to stay engaged with task force members after the SIGCSE special session.

6. SUITABILITY

This session will provide an opportune time for community engagement in this important curricular development process. The 2016 SIGCSE meeting will be held approximately 6 months after the task force has been launched. As such, task force members will have had sufficient opportunity to develop initial work products upon which community members will be able to offer constructive feedback. 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 following resources prior to the session:

- *The Future of Cybersecurity Education* in IEEE Computer - www.computer.org/csdl/mags/co/2014/08/mco20140800 67-abs.html
- *Usable Cybersecurity: Human Factors in Cybersecurity Education Curricula* in the National Cybersecurity Institute Journal - www.excelsior.edu/static/journals/nci-journal/1-1/offline/download.pdf#page=5
- *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/