Developing ABET Criteria for Undergraduate Cybersecurity Programs

Allen Parrish
Department of Cyber Science
The United States Naval Academy
Annapolis, MD 21402
aparrish@usna.edu

Edward Sobiesk
Army Cyber Institute
West Point, NY 10996
edward.sobiesk@usma.edu

***Abstract*—This special session will introduce current work on program criteria currently being developed for use by ABET in accrediting undergraduate cybersecurity programs. It will provide a status report on current efforts in this area, along with expectations for future development and deployment of these criteria.**

Keywords—Cybersecurity, accreditation, program assessment

I. PANEL PARTICIPANTS

This special session will be conducted by a panel consisting individuals representing current ABET cybersecurity accreditation criteria work, from the following:

- Allen Parrish, United States Naval Academy
- Edward Sobiesk, Army Cyber Institute
- Jean Blair, United States Military Academy
- J.J. Ekstrom, Brigham Young University
- Steven Lingafelt, IBM
- Mark Stockman, The University of Cincinnati

II. BACKGROUND

The Cyber Education Project (http://www.cybereducationproject.org) (CEP) was formed in 2014 as a consortium of educational institutions with interests in improving cybersecurity education. The objective of the CEP was to develop both a Model Curriculum for the discipline and a set of accreditation criteria to be proposed to ABET for use in conducting cybersecurity program accreditation evaluations.

Based on the work of the CEP, ACM has mobilized a Task Force for Cybersecurity Education that is utilizing CEP participants and work products for development of a Model Curriculum to be published in late 2017. Similarly, CSAB (as a member society of ABET, representing ACM and the IEEE Computer Society) is utilizing CEP participants and work products for development of program accreditation criteria. The intent is to deploy these criteria for use in ABET accreditation evaluations at least by the 2019-20 academic year; draft versions may be used for selected pilot evaluations prior to 2019.

This Special Session will be divided into two parts. Part I will be a report on the results of the work so far. Part II will involve dividing the participants into small groups and facilitating a session to obtain feedback on draft cybersecurity accreditation criteria.

III. MODEL CURRICULUM

The work on the Cybersecurity Body of Knowledge is currently under the auspices of the ACM Joint Task Force on Cybersecurity Education (JTF). The JTF is currently developing a Model Curriculum document, which will be known as CSEC 2017. CSEC 2017 will be based on work to be developed by the JTF, and informed by preliminary documents produced by the CEP. In the CEP Preliminary BOK (October 2015, http://cep-public.caps.ua.edu/wp-content/uploads/2016/03/Draft-Cyber-Sciences-Knowledge-Areas-Oct-2015.pdf), there were 15 draft knowledge areas identified:

1. Cryptography
2. Cyber Attack
3. Cyber Defense
4. Cyber Ethics
5. Cyber Intelligence
6. Cyber Physical Systems
7. Cyber Policy, Governance and Law
8. Cyber Risk Management
9. Digital Forensics
10. Human Computer Interaction
11. Network Security
12. Privacy
13. Reverse Engineering
14. Secure Software Engineering
15. Secure Systems Design

The CEP work developed hundreds of learning outcomes, which were then discussed, analyzed and reduced based on opinions of relative importance. This work has then informed the startup of the JTF, which will create, finalize and promulgate a professional society sanctioned document for use as a reference model in defining a cybersecurity program and curriculum.

IV. ACCREDITATION CRITERIA

The CEP also developed proposed accreditation criteria for cybersecurity. These criteria have informed the work of two separate groups:

- CSAB – Now developing accreditation criteria for cybersecurity and similarly named programs (including information assurance).
- IEEE – Now developing accreditation criteria for cybersecurity-related engineering programs.

Drafts of both sets of program criteria currently exist. We will present the current status of the work from both of these groups, and seek feedback on enhancements and improvements.