ABET CYBERSECURITY ACCREDITATION

Two Distinct Efforts

CAC

Cybersecurity

EAC

Cybersecurity Engineering

Undergraduate, B.S. programs

General Versus Program Criteria

- CAC and EAC have “General Criteria” that apply to all programs:
  - CAC – In computing
  - EAC – In engineering
- Cybersecurity and Cybersecurity Engineering criteria are considered to be “Program Criteria”
  - Cybersecurity – Proposed as one option under CAC
  - Cybersecurity Engineering – Proposed as one option under EAC

Cybersecurity Criteria

- Assumes new changes to the ABET General Computing Criteria:
  - Criterion 3 (Student Outcomes)
  - Criterion 5 (Curriculum)
  - Both are currently under review
- Cybersecurity Program Criteria:
  - Inserts additional required Student Outcomes for Cybersecurity (extends Criterion 3)
  - Inserts additional Curriculum requirements for Cybersecurity (extends Criterion 5)

DRAFT Criterion 3 General Student Outcomes

The program must have documented and publicly stated student outcomes that include (1) through (5) below and any additional outcomes required by applicable Program Criteria. The program may define additional student outcomes at its discretion.

1. An ability to analyze a problem, and to identify and define the computing requirements appropriate to its solution.
2. An ability to design, implement, and evaluate a computer-based solution to meet a given set of computing requirements in the context of the discipline.
3. An ability to communicate effectively with a range of audiences about technical information.
4. An ability to make informed judgments in computing practice based on legal and ethical principles.
5. An ability to function effectively on teams to establish goals, plan tasks, meet deadlines, manage risk, and produce deliverables.

DRAFT Criterion 5 General Curriculum

The program's requirements must be consistent with its program educational objectives and designed in such a way that each of the student outcomes can be attained.

The curriculum requirements specify subject areas, but do not prescribe specific courses. The program must include each of the following in a manner appropriate to its discipline:

1. At least **one academic year of up-to-date coverage of fundamental and advanced computing topics** that provides both breadth and depth.
2. College-level mathematics.
3. Current techniques, skills, and tools necessary for computing practice.
4. **Information assurance and security principles and practices.**
5. Concepts involving the local and global impact of computing solutions on individuals, organizations, and society.

DRAFT Cybersecurity Student Outcomes

3. Student Outcomes

The student outcomes for cybersecurity programs must include outcomes (6) and (7).

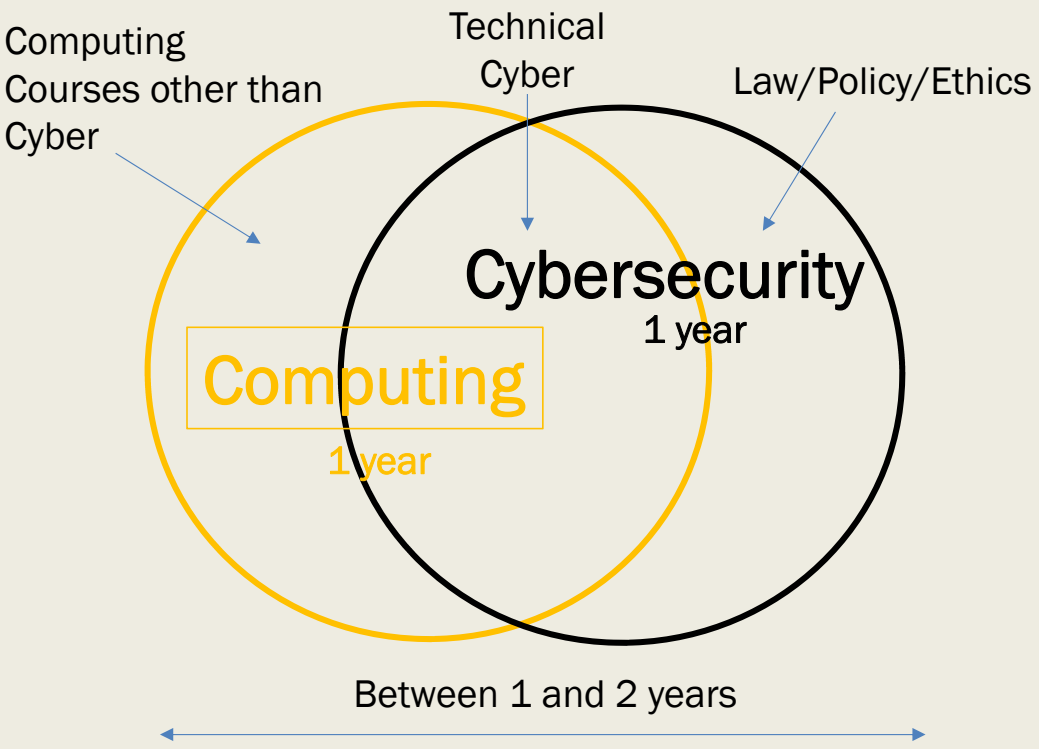
6) An ability to apply security principles and practices to the environmental, hardware, software, and human components of a system.
7) An ability to analyze and evaluate systems with respect to maintaining operations in the presence of risks and threats.

DRAFT Cybersecurity Curriculum

5. Curriculum. Students have at least one year of course work or equivalent educational experiences in cybersecurity that *must* cover fundamental and advanced topics from the following:

1. **Information Security** topics such as information confidentiality, data integrity, availability, cryptography, and cryptanalysis.
2. **Software Security** topics such as secure software development, software reverse engineering, and/or malware analysis.
3. **System Security** topics such as availability, authentication, access controls, secure systems design, computer network defense, computer network attack/penetration testing, reverse engineering (hardware), cyber physical systems, digital forensics, and supply chain management.
4. **Usable Security** topics such as identity management, social engineering, social networks, and human-computer interaction.
5. **Organizational Security** topics such as risk management, incident response, mission assurance, disaster recovery, business continuity, security evaluations/compliance, organizational behavior, intelligence, and economics.
6. **Societal Security** topics such as cybercrime, cyber law, ethics, policy, privacy, intellectual property, professional responsibility, and global societal impacts.

Computing - Cybersecurity



Cybersecurity Engineering Program Criteria

IEEE PROGRAM CRITERIA FOR SECURITY, CYBERSECURITY, INFORMATION ASSURANCE AND SIMILARLY NAMED ENGINEERING PROGRAMS
DRAFT, NOT FOR USE OR DISTRIBUTION, NOT APPROVED BY EAC
Lead Society: Institute of Electrical and Electronics Engineers
Cooperating Society CSAB

These program criteria apply to engineering programs that include "security", "cybersecurity", "information assurance" or similar modifiers in their titles.

1. Curriculum
The structure of the curriculum must provide both breadth and depth across the range of engineering topics implied by the title of the program.

The curriculum must
- Include probability, statistics, and cryptographic topics including applications appropriate to the program.
- Include discrete math and specialized math appropriate to the program, such as, abstract algebra, information theory, number theory, complexity theory, finite fields.
- Include engineering topics necessary to analyze and design complex devices, software, and systems containing hardware, software and human components.
- Provide both breadth and depth across the range of engineering and computer science topics necessary for the:
  1) application of security principles and practices to the design, implementation, and operations of the physical, software, and human components of the system as appropriate to the program
  2) application of protective technologies and forensic techniques
  3) analyzing and evaluation of components and systems with respect to security and to maintaining operations in the presence of risks and threats
  4) consideration of legal, regulatory, privacy, ethics, and human behavior topics as appropriate to the program

2. Faculty
The program must demonstrate that faculty members teaching core engineering topics understand engineering problem solving methods and engineering practice with specific relevance to security.

black is text drawn from existing IEEE criteria, blue text is addition

Next Steps

- Approval of first draft criteria (by Fall 2017)
- Some possible pilot visits in Fall 2017
- Final approval of criteria in Fall 2018
- Visits in Fall 2019?
- Need volunteers to help us pilot and refine the criteria