CEP SIGCSE Workshop: Validating the Draft “Cybersecurity” Accreditation Criteria

March 4, 2016
Memphis, TN

CEP Steering Committee

Andy Phillips - United States Naval Academy, Jean Blair - United States Military Academy,
Allen Parrish - The University of Alabama, Chris Inglis - United States Naval Academy,
Sue Fitzgerald - Metropolitan State University, Diana Burley - George Washington University,
David Gibson – United States Air Force Academy, Elizabeth Hawthorne - Union County College,
Scott Buck – Intel Corporation, Raymond Greenlaw - United States Naval Academy,
C. Steven Lingafelt - IEEE CEAA & IBM

Version 13
Andy
Agenda

Introduction & Background:
08:00-09:00 - Introduction - Andy
09:00-09:30 - Introduction to draft CS Criteria - Jean/Allen

Section by Section Discussion: Steven
9:30 - 10:00 - Program Application & 6. Faculty
15 minutes - Break
10:15 - 11:15 - 3. Student Outcomes
11:15 - 12:30 - 5. Curriculum

Wrap-up: Andy
12:30 - 1:00 - Go Forward Next Steps, "parked" questions not addressed in prior discussion
Goals for Today’s Workshop

1. Provide progress report on the Cyber Education Project (CEP) efforts since Summer 2014

2. Describe on-going transition of the CEP efforts
   • Shift CEP Learning Outcomes work to ACM-IEEE/CS Joint Task Force (JTF)
   • Shift CEP Accreditation Criteria work to CSAB and ABET/CAC

3. Finalize the current (“Alpha”) draft of Cybersecurity Criteria in support of its transition to CSAB and ABET/CAC as a foundation for their further work
The Cyber Education Project (CEP)

• What are the goals of the CEP?
  • **Goal 1**: To develop *curriculum guidelines* for the “cyber sciences”
  • **Goal 2**: To develop *ABET program criteria* for one or more programs among those within the “cyber sciences”

• Who are we?
  • Academia, Industry, Government, Professional Societies

• How is the CEP organized?
  • 5 Subcommittees:
    • Steering
    • Learning Outcomes; Accreditation
    • Stakeholder; Industry Advisory Board
Professional Society Engagement

• ACM, IEEE-CS, and IEEE are **formally** engaged with CEP
  • ACM and IEEE-CS are co-sponsoring a delegation to produce a **curricular volume (similar to CS2013)**
    • Leaders are Diana Burley (GWU) and Matt Bishop (UC-Davis)

• ACM “official” representatives to CEP:
  • Sue Fitzgerald (Metro State), Beth Hawthorne (Union County)

• IEEE-CS “official” representatives to CEP:
  • Allen Parrish (Alabama), J. Ekstrom (BYU)

• IEEE “official” representative to CEP:
  • Steven Lingafelt (IBM)

• SIGSEC of AIS also is significantly involved although AIS has not formally “signed on”
  • David Biros (Oklahoma State), Yair Levy (Nova Southeastern U)

• CSAB has officially endorsed the project
Cyber Science (n.)
Defining the “Cyber Sciences”

The **Cyber Sciences** are computing-based disciplines involving technology, people, and processes aligned in a way to enable “assured operations” in the presence of risks and adversaries. They involve the creation, operation, analysis, and testing of secure computer systems (including network and communication systems) as well as the study of how to employ operations, reasonable risk taking, and risk mitigations. The Cyber Sciences are interdisciplinary courses of study, and include 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.
CEP Learning Outcomes Goal #1

**Goal**: Develop learning outcomes and curricular guidance which characterize the knowledge, skills, and abilities to be gained by students in undergraduate “cyber sciences” programs

- Results of the work ...
  - Final report is available at CEP website
  - There are MANY learning outcomes that define SEVERAL different kinds of programs that fall under “Cyber Sciences”
  - Hence ... the Cyber Sciences is/are a “Big Tent” consisting of a variety of related but different Cyber fields

- The CEP has now transitioned this work to others ...
ACM Joint Task Force (JTF) on Cybersecurity Education

• Purpose

To develop comprehensive curricular guidance in cybersecurity education that will support future program development and associated educational efforts.

• ...where cybersecurity is defined 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 often in the context of adversaries.” (JTF working definition established December 7, 2015)
What does this mean?

• Goal 1 is now handed off from CEP to the ACM JTF
  • The CEP is mostly “out of business” (a good thing) regarding Goal 1

• The JTF has elected to use the term Cybersecurity for its curriculum development work

• The JTF has adopted a definition of Cybersecurity nearly identical to the CEP Cyber Sciences definition
ACM JTF Collaborators

• Collaborating Associations
  • ACM, IEEE-CS, AIS SIGSEC, IFIP WG 11.8, CEP

• Co-chairs
  Diana Burley, George Washington University
  Matt Bishop, University of California, Davis

• Members
  Scott Buck, Intel Corporation
  J. Ekstrom, Brigham Young University
  Lynn Futer, Nelson Mandela Metropolitan University
  David Gibson, US Air Force Academy
  Elizabeth Hawthorne, Union County College
  Siddharth Kaza, Towson University
  Yair Levy, Nova Southeastern University
  Herb Mattord, Kennesaw State University
  Allen Parrish, University of Alabama
## ACM JTF Timeline

<table>
<thead>
<tr>
<th>Date</th>
<th>Milestone</th>
</tr>
</thead>
<tbody>
<tr>
<td>September 2015</td>
<td>JTF formally launched by ACM Ed Council and Ed Board</td>
</tr>
<tr>
<td>October 2015</td>
<td>Delegations from all collaborators seated</td>
</tr>
<tr>
<td>December 2015</td>
<td>JTF develops working definition of cybersecurity to guide and bound development efforts</td>
</tr>
<tr>
<td>March 2016</td>
<td>Special session - SIGCSE, Memphis, TN <em>JTF will launch public face incl. website during this time period</em></td>
</tr>
<tr>
<td>June 2016</td>
<td>Special session - CISSE, Philadelphia PA</td>
</tr>
<tr>
<td>August 2016</td>
<td>Special session - International Security Education Workshop (ISEW), Washington, DC</td>
</tr>
<tr>
<td>August – May 2017</td>
<td><em>Continued development and community engagement</em></td>
</tr>
<tr>
<td>May 2017</td>
<td>Special session - WISE, Rome Italy</td>
</tr>
<tr>
<td>June - August 2017</td>
<td>Draft guidelines published for review, comment and revision</td>
</tr>
<tr>
<td>Sept – Dec 2017</td>
<td>Revision, review and approval process</td>
</tr>
<tr>
<td>December 2017</td>
<td>Publish final curricular guidelines</td>
</tr>
</tbody>
</table>
CEP Accreditation Goal #2

• **Goal:**
  • Develop and submit to ABET proposed undergraduate accreditation criteria for one or more selected disciplines under the “Cyber Sciences” Big Tent

• **Sources of Information to inform that criteria:**
  • CEP Learning Outcomes Committee results
  • Existing ABET Criteria
  • Existing curricula and other bodies of knowledge
  • Existing programs
  • Stakeholders and/or Subject Matter Experts
Today’s Work ....

• To facilitate Goal #2!

• The CEP has narrowed its focus to ONE of the many possible focused curriculum areas in the Cyber Sciences:
  • Cybersecurity ← CEP has chosen this as the name

• Goal for today: Develop an “alpha” draft of an ABET style undergraduate accreditation criteria, framed by the CEP definition of Cyber Sciences, for Cybersecurity
After Today’s Work ...

• Today’s work product will be “handed off” to CSAB next week

• CSAB and the ABET/CAC will then begin to formally refine/develop the criteria for eventual consideration as a new CAC program criteria in Cybersecurity

• The CEP will then be mostly “out of business” (another good thing) regarding Goal 2
  • There will certainly be MANY more opportunities to provide feedback on the criteria – CSAB and CAC routinely gather input from interested constituents
Where Have We Been So Far?

- July 2014 – ABET Commission meeting, Arlington VA
- November 2014 – NICE/NSF CAE Meeting, Columbia MD
- March 2015 – SIGCSE 2015, Kansas City MO
- June 2015 – 8th Annual Southeastern Cyber Security Summit, Huntsville AL
- June 2015 – 19th CISSE Colloquium, Las Vegas NV
- June 2015 – Community College Cyber Security Summit, Las Vegas NV
- July 2015 – ABET Commission meeting, Baltimore MD
- August 18-20, 2015 – Academy of Science and Engineering (ASE) International Conference on Cyber Security, Stanford University
- November 5-6, 2015 – NICE, San Diego CA
- December 13-16, 2015 – ICIS, Fort Worth TX
CEP Funding

• Travel funding for CEP leaders and key participants (you!) has been provided by the National Science Foundation.
  • We gratefully acknowledge that funding for this work was provided in part by the National Science Foundation under grant number DGE-1539715

• ABET and CSAB also have been most generous with their support
Jean/Allen
Criteria

General Criteria
1. Students
2. Program Educational Objectives
3. Student Outcomes
4. Continuous Improvement
5. Curriculum
6. Faculty
7. Facilities
8. Institutional Support

Program Criteria
3. Student Outcomes (CAC)
5. Curriculum
6. Faculty

Existing Cyber Related Program Criteria
- Information Systems
- Computer Science
- Information Technology
- Software Engineering
Proposed Changes

In the General Criteria:

• Criterion 3 – Student Outcomes
• Criterion 5 – Curriculum
• Cleans up some structural ambiguities and lays out specific outcome requirements that should ultimately make it easier for programs

In the Program Criteria:

• CS* Criteria – Consistency with CS 2013 (latest curriculum model revision for CS)
• IS and IT Criteria – Structural adjustments to be consistent with other changes
• IS and IT Criteria have been changed in recent years

*CS = Computer Science
Proposed Changes

Criterion 3 (Student Outcomes)
would now specify outcomes that graduating students must meet:

1. An ability to analyze a problem, and to identify 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.
Criterion 5 (Curriculum) would be restructured and add a security requirement:

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 must combine technical, professional, and general education components to prepare students for a career, further study, and lifelong professional development in the computing discipline associated with the program.

The curriculum requirements specify subject areas, but do not prescribe specific courses. The following requirements are to be satisfied in the context of the discipline associated with the program:

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. Consideration of the impact of computing solutions in global, economic, environmental, and societal contexts.
Proposed Changes

Program Criteria

• Computer Science:
  – Reworked for better consistency with ACM’s “CS 2013”.
  – General structural improvements

• Information Systems and Information Technology:
  – General structural improvements

• CyberSecurity would be an additional set of computing focused program criteria to be added to this mix
Proposed Computer Science Program Criteria

Three criteria would have additional requirements:

• Criterion 3 (Student Outcomes)
  – 2 additional outcomes unique to Computer Science

• Criterion 5 (Curriculum)
  – Several additional curriculum requirements

• Criterion 6 (Faculty)
  – Additional requirement for Computer Science faculty
CS Example – Criterion 3

In addition to outcomes (1) through (5), the following outcomes are required:

6. An ability to apply theory in the design and implementation of computer-based solutions. [CS]

7. An ability to reason about and explain computer-based solutions at multiple levels of abstraction. [CS]
The curriculum requirements specify subject areas, but do not prescribe specific courses. These requirements are:

a) Computer science: At least one and one-third academic years that must include:
   1. Computer science fundamentals including algorithms and complexity, computer science theory, concepts of programming languages, and software development.
   2. Some coverage of computer architecture and organization, information management, networking and communication, operating systems, and parallel and distributed computing.
   4. In-depth coverage of at least one high-level language.
   5. A substantial project requiring application of knowledge and skills acquired in earlier course work.

b) Mathematics: At least one-half academic year of college-level mathematics that must include discrete mathematics. The additional mathematics might consist of course work in areas such as calculus, linear algebra, numerical methods, probability, statistics, number theory, or geometry.

c) Science: Natural science course work that develops an understanding of the scientific method, provides exposure to laboratory work, and provides students with an opportunity to experience this mode of inquiry in courses appropriate for science or engineering majors.
At least one full time faculty member must have a Ph.D. in computer science.
Cybersecurity Criteria

• Criterion 3 (Student Outcomes)
  – Needs one or more outcomes unique to cybersecurity

• Criterion 5 (Curriculum)
  – Needs fundamental characteristics of what should be in the curriculum

• Criterion 6 (Faculty)
  – Needs special requirements for faculty, if desired
Steven
Next Few Hours:

• CEP Accreditation Committee Approach
• Cybersecurity Knowledge Areas
• Discuss each section for fixed time
  – Now to 10:00 - 0. Program Application & 6. Faculty
  – Break - 15 minutes
  – 10:15-11:15 - 3. Student Outcomes
  – 11:15-12:30 - 5. Curriculum
Illustration of Accreditation Committee Approach

1. Prepare
- Solicit Participation
- Setup collaboration tools and method
- Training

2. Deliberate

3. Submit

Into the ABET Criteria Proposal Process
CEP SIGCSE Workshop - 3/4/15

Cybersecurity Programs

3. Student Outcomes
   “S-1”
   “S-2”

5. Curriculum
   “C-1”

7. Faculty
   “F-1”

LO Knowledge Areas:
- “A”
- “B”
- “D”
- “T”

Existing CAC Accreditation Criteria
Proposed CAC Accreditation Criteria
Other Materials, Stakeholders SMEs, etc.
Draft “Cyber Sciences” Knowledge Areas

Source:
Cyber Education Project - Learning Outcomes Committee
David Gibson and Beth Hawthorne, Co-chairs
October 2015

Knowledge Areas:
1. Cyber Defense
2. Cyber Operations
3. Digital Forensics
4. Cyber Physical Systems
5. Secure Software Engineering
6. Cyber Ethics
7. Cyber Policy, Governance, and Law
8. Cyber Risk Management
9. Behavioral Science
Alpha Draft – “CyberSecurity” Program Criteria
PROGRAM CRITERIA FOR CYBERSECURITY
AND SIMILARLY NAMED COMPUTING PROGRAMS

Lead Society: CSAB

These program criteria apply to computing programs using cybersecurity, computer security, cyber operations, information assurance, information security, or similar terms in their titles.

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 design and implement computing systems with consideration of the physical, software, and human aspects of the computing system.

(7) An ability to analyze and evaluate cyber systems with respect to security and maintaining operations.

5. Curriculum
Students must have course work or an equivalent educational experience as specified below:

a. Cybersecurity: One and one-third years that includes fundamentals and application of:
   1. Cyber defense and digital forensics.
   2. A variety of computing systems and tools appropriate to cybersecurity.
   3. Cyber ethics, policy, governance, law, and risk management.

b. Behavioral Science: Material that develops an understanding of human behavior relating to cyber systems and operations, including social engineering, social networks, user experience, and organizational behavior.

6. Faculty
Some full-time faculty members, including those responsible for the cyber security curriculum development, must hold a terminal degree with a program of study in cyber security or a closely related field.
Alpha Draft – “Cyber Security” Program Criteria
PROGRAM CRITERIA FOR CYBERSECURITY
AND SIMILARLY NAMED COMPUTING PROGRAMS

Lead Society: CSAB

These program criteria apply to computing programs using cybersecurity, computer security, cyber operations, information assurance, information security, or similar terms in their titles.

LAMBDA - General Criteria:
Program: Computer Science and Similarly Named ...

At least one full-time faculty member must have a Ph.D. in computer science.

Program: Information Systems and Similarly Named..

At least one full-time faculty member must hold a terminal degree with a program of study in information systems.

Program: ALPHA CEP Draft

Some full-time faculty members, including those responsible for the cybersecurity curriculum development, must hold a terminal degree with a program of study in cybersecurity or a closely related field.
LAMBDA - General Criteria:

The program must have documented student outcomes that include (1) through (5) below and any additional outcomes required by applicable Program Criteria. A program for which none of the Program Criteria are applicable must define at least one additional student outcome that characterizes the distinctive nature of its discipline. 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.
3. Student Outcomes – Program Specific

LAMBDA - General Criteria:

In addition to outcomes (1) through (5), the following outcomes are required:

Program: Computer Science and Similarly Named ..

(6) An ability to apply theory in the design and implementation of computer-based solutions. [CS]
(7) An ability to reason about and explain computer-based solutions at multiple levels of abstraction. [CS]

Program: Information Systems and Similarly Named ..

(6) An understanding of and an ability to support the use, delivery, and management of information systems within an information systems environment. [IS]

Program: Information Technology and Similarly Named ..

(6) An ability to identify and analyze user needs and take them into account in the selection, integration, evaluation, and administration of computer-based systems. [IT]

Program: ALPHA CEP Draft

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

(6) An ability to apply security principles and practices to design and implement computing systems with consideration of the physical, software, and human aspects of the computing system.

(7) An ability to analyze and evaluate cyber systems with respect to security and maintaining operations.

Knowledge Areas:

1. Cyber Defense
2. Cyber Operations
3. Digital Forensics
4. Cyber Physical Systems
5. Secure Software Engineering
6. Cyber Ethics
7. Cyber Policy, Governance, and Law
8. Cyber Risk Management
9. Behavioral Science
BREAK

Meeting resumes at 10:10
LAMBDA - General Criteria:

General:

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 must combine technical, professional, and general education components to prepare students for a career, further study and lifelong professional development in the computing discipline associated with the program.

The curriculum requirements specify subject areas, but do not prescribe specific courses. The following requirements are in the context of the discipline associated with the program:

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. Consideration of the impact of computing solutions in global, economic, environmental, and societal contexts.
5. Information assurance and security principles and practices.
“Alpha” CEP Draft – 5. Curriculum – Program Specific

LAMBDA - General Criteria:
The curriculum requirements specify subject areas, but do not prescribe specific courses. These requirements are:

Program: Computer Science and Similarly Named …
a. Computer science: At least one and one-third academic years that must include:
   1. Computer science fundamentals including algorithms and complexity, computer science theory, concepts of programming languages, and software development.
   2. Some coverage of computer architecture and organization, information management, networking and communication, operating systems, and parallel and distributed computing.
   4. In-depth coverage of at least one high-level language.
   5. A substantial project requiring application of knowledge and skills acquired in earlier course work.

b. Mathematics: At least one-half academic year of college-level mathematics that must include discrete mathematics. The additional mathematics might consist of course work in areas such as calculus, linear algebra, numerical methods, probability, statistics, number theory, or geometry.

c. Science: Natural science course work that develops an understanding of the scientific method, provides exposure to laboratory work, and provides students with an opportunity to experience this mode of inquiry in courses appropriate for science or engineering majors.

Program: Information Systems and Similarly Named ..
a. Information systems: At least one academic year that includes coverage of fundamentals and applied practice in application development; data and information management; IT infrastructure; systems analysis, design and acquisition; project management; and the role of information systems in organizations.

b. Information systems environment: At least one-half academic year of course work that includes a cohesive set of topics that provide an understanding of an environment in which the information systems are applied professionally.

c. Quantitative analysis or methods, including statistics.

Program: Information Technology and Similarly Named ..
a. The core information technologies of human-computer interaction, information management, programming, web systems and technologies, and networking.

b. System administration and system maintenance.

c. System integration and system architecture.

Program: ALPHA CEP Draft

Students must have course work or an equivalent educational experience as specified below:

a. Cybersecurity: One and one-third years that includes fundamentals and application of:
   1. Cyber defense and digital forensics.
   2. A variety of computing systems and tools appropriate to cybersecurity.
   3. Cyber ethics, policy, governance, law, and risk management.

b. Behavioral Science: Material that develops an understanding of human behavior relating to cyber systems and operations, including social engineering, social networks, user experience, and organizational behavior.

Knowledge Areas:
1. Cyber Defense
2. Cyber Operations
3. Digital Forensics
4. Cyber Physical Systems
5. Secure Software Engineering
6. Cyber Ethics
7. Cyber Policy, Governance, and Law
8. Cyber Risk Management
9. Behavioral Science
Lead Society: CSAB

These program criteria apply to computing programs using cybersecurity, computer security, cyber operations, information assurance, information security, or similar terms in their titles.

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 design and implementation of the physical, software, and human component of the system.

(7) An ability to analyze and evaluate cyber systems with respect to security and maintaining operations in the presence of risks and threats.

5. Curriculum
Students have course work or an equivalent educational experience that includes the fundamentals of Cybersecurity:

1. **Cyber Defense**, such as cryptography, data security, network security, information assurance.
2. **Cyber Operations**, such as cyber attack, penetration testing, cyber intelligence, reverse engineering, cryptanalysis.
3. **Digital Forensics**, such as hardware and software forensics, incident response, cybercrime, cyber law enforcement.
4. **Cyber Physical Systems**, such as Supervisory Control and Data Acquisition (SCADA) systems, internet-of-things (IOT), industrial control systems.
5. **Secure Software Development**, such as secure systems design, secure coding, deployability, maintainability, usability of secure information system.
6. **Cyber Ethics**, such as ethical use of information systems, privacy and anonymity, intellectual property rights, professional responsibility, global societal impact of information systems.
7. **Cyber Policy, Governance, and Law**, such as government and institutional cyber policy and practices, regulatory authorities for cyber systems and operations, cyber law.
8. **Cyber Risk Management**, such as cyber resilience, mission assurance, disaster recover, business continuity, security evaluation, cyber economics.
9. **Human Behavioral Relating to Cyber Systems and Operations**, such as social engineering, social networks, user experience, and organizational behavior.

6. Faculty
At least some full-time faculty members, including those responsible for the cybersecurity curriculum development, must hold a terminal degree with a program of study in cybersecurity or a closely related field.
Andy
Wrap-up

• Items not attended to yet today?

• Next steps

• How to stay involved
Thank you for your participation !!
End