

Toward Standards in Undergraduate Cybersecurity Education in 2018

Rajendra K. Raj, Rochester Institute of Technology
Allen Parrish, United States Naval Academy

There's no consensus on what constitutes a solid undergraduate cybersecurity education. With the upcoming release of CSEC2017 curricular guidelines from the Joint Task Force of the ACM, IEEE Computer Society, AIS, and IFIP, along with the proposed undergraduate cybersecurity accreditation criteria from ABET, now's the perfect time to reexamine the future landscape in this space.

With cybersecurity attacks and data breaches cycling through the news on a near-constant basis, the demand for qualified cybersecurity professionals remains robust.[1] Although training programs and specialized certificates for current practitioners have helped to support growth in this area of the profession, computing professionals and hiring organizations have continued to push for the legitimization of cybersecurity as a more formal academic discipline. Colleges and universities have entered this space by offering cybersecurity Master's programs, and, in recent years they've introduced undergraduate degree programs.

This expansion in undergraduate cybersecurity educational programs has come about without universally accepted expectations for cybersecurity graduates. It's crucial that there be a shared understanding of such expectations, including what are the necessary broad skills and knowledge graduating students must have, based on the overall cybersecurity domain and taught in the context of a well-understood body of knowledge.

0018-9162/18/$33.00 © 2018 IEEE

EDITOR **ANN E.K. SOBEL**
Miami University; sobelae@muohio.edu



As several universities began offering such cybersecurity programs, several challenges have come to light. For instance, at the undergraduate level, there's a lack of consensus on degree name, program objectives, and scope; on a precise disciplinary definition; and on whether to treat cybersecurity as a multidisciplinary program or to develop new academic departments through which to offer these programs.

To help educators in our field move toward consensus, we explored three major efforts to define standards for undergraduate cybersecurity education: National Centers of Academic Excellence,[2,3] CSEC2017 Curricular Guidelines (from the CSEC Joint Task Force),[4] and the ABET Accreditation Criteria for Cybersecurity.[5] Other efforts, such as the NICE Cybersecurity Workforce Framework,[7] aren't covered here, as their impact on the design of undergraduate cybersecurity programs has been limited.

CENTERS OF ACADEMIC EXCELLENCE

In the US, the National Security Agency and Department of Homeland Security (NSA/DHS) were early supporters of cybersecurity education in colleges and universities through the National Centers of Academic Excellence (CAE) in cybersecurity program. This program enabled participating universities to receive different designations denoting their compliance with specific types of requirements in areas such as regional accreditation, program outreach, student development, cybersecurity faculty, and an appropriate curriculum.

The CAE programs has been through several variations over the years, but for undergraduate education, the two that are most relevant are the CAE-CD (cyber defense)[2] and CAE-CO (cyber operations) designations.[3] Both designations have extensive detailed curricular requirements that must be met. Although institutions seeking these CAE designations have some flexibility, many curricular elements are specifically spelled out. CAE-CO, the newer of these programs, is extremely prescriptive, and only a very small number of institutions have achieved this certification. For example, CAE-CO requires coursework in reverse engineering, cellular and mobile technologies, operating systems theory, and low-level language programming, as well as several additional topics.

TABLE 1. CSEC2017 building blocks.

Knowledge areas	Data security, software security, component security, connection security, system security, human security, organizational security, societal security
Crosscutting concepts	Confidentiality, integrity, availability, risk, adversarial thinking, systems thinking
Disciplinary lenses	Computer science, computer engineering, information systems, information technology, software engineering, mixed disciplinary

CSEC2017 CURRICULAR GUIDELINES

Building on earlier efforts, such as the Cyber Education Project (which was created with the purpose of developing undergraduate curriculum guidelines and a case for formal program accreditation),[8] the CSEC2017 curricular guidelines are intended to be "the leading resource of comprehensive cybersecurity curricular content for global academic institutions seeking to develop a broad range of cybersecurity programs at the post-secondary level."[4]

Table 1 presents the CSEC2017 model of cybersecurity, which comprises three parts: knowledge areas ("basic organizing structure for cybersecurity content"), crosscutting concepts ("provide an organizational schema for interrelating knowledge into a coherent view of cybersecurity"), and a set of disciplinary lenses ("representing the underlying computing discipline from which the cybersecurity program was developed").[4]

By design, CSEC2017 wasn't intended to define a program, but instead it explicates content across a broad range of programs. Effectively, CSEC2017 fundamentally describes a broad problem space for cybersecurity as a discipline, rather than required content for a cybersecurity education program. The use of disciplinary lenses tacitly implies that cybersecurity will be taught in the context of existing technical disciplines. That is, although CSEC2017 provides guidance, curriculum language, and concepts for a family of programs, it doesn't define the specific parameters for a cybersecurity degree.

ABET ACCREDITATION CRITERIA FOR CYBERSECURITY

ABET, the internationally recognized accreditation body for engineering, computing, technology, and natural and applied sciences, has proposed accreditation criteria for cybersecurity.[5] As cybersecurity is generally viewed as a computing discipline, these accreditation criteria for cybersecurity

programs are administered by ABET's Computing Accreditation Commission (CAC), and are an addition to existing program criteria for computer science, information systems, and information technology. The ABET accreditation criteria for cybersecurity were developed to provide a flexible approach for accrediting academic programs in cybersecurity. They are currently available for public review and comment at the ABET website.[5] (Note that ABET's Engineering Accreditation Commission has also released a draft of cybersecurity engineering criteria.[6])

By the time they graduate, students satisfying the ABET CAC cybersecurity criteria are expected to have knowledge, skills, and behaviors relating to five core *outcomes* that refer to all aspects of computing (items 1–5 below), and two additional outcomes that are specific to cybersecurity program graduates (items 6 and 7 below):

1. Analyze a problem, and to identify and define the computing requirements appropriate to its solution.
2. Design, implement, and evaluate a computer-based solution to meet a given set of computing requirements in the context of the discipline.
3. Communicate effectively with a range of audiences about technical information.
4. Make informed judgments in computing practice based on legal and ethical principles.
5. Function effectively in teams to establish goals, plan tasks, meet deadlines, manage risks, and produce deliverables.
6. Apply security principles and practices to the environment, hardware, software, and human aspects of a system.
7. Analyze and evaluate systems with respect to maintaining operations in the presence of risks and threats.

In addition, the ABET CAC criteria state that the *curriculum* for the computing and cybersecurity coursework should cover crosscutting concepts, fundamental and advanced topics in each knowledge area, and mathematics coursework that includes discrete mathematics and statistics.

The outcomes and curriculum as defined above are likely to undergo minor revisions before the final version of the cybersecurity criteria are adopted following the ABET approval processes in 2018.

The curriculum requirements described in the ABET CAC cybersecurity criteria are consistent with CSEC2017, though they set additional boundaries, offering some breadth-based coverage of all CSEC2017 knowledge areas, combined with in-depth coverage of at least one of the knowledge areas.[4] Thus, although it isn't presented in this fashion, CSEC2017 defines a universal body of knowledge, whereas the ABET CAC criteria define what constitutes a cybersecurity degree.

> To become a mainstream major, a cybersecurity program needs to be built on a disciplinary foundation of education, not training.

These three efforts can be reconciled as a spectrum of approaches from the general to the specific.

CSEC2017: Describes a body of knowledge for cybersecurity that's appropriate at the undergraduate level, without committing to specific requirements for an undergraduate cybersecurity program.

ABET cybersecurity criteria for bachelor's programs: Provides parameters for bachelor's degree programs in cybersecurity writ large, by placing boundaries on the level of coverage of CSEC2017 that's sufficient for an undergraduate cybersecurity degree.

CAE-CD and CAE-CO: Provides more specific requirements for programs in "cyber defense" and "offensive cyber operations." Programs meeting these requirements are likely to be both accreditable by ABET and consistent with the broad context of CSEC2017.

These approaches have a role in improving the state of the practice in undergraduate cybersecurity education. Until now, only the CAE existed; with the advent of CSEC2017 and ABET's cybersecurity criteria, the potential exists for increased impact on the shape of available undergraduate experiences in cybersecurity.

To become a mainstream major, a cybersecurity program needs to be built on a disciplinary foundation of education, not training. That is, students must be encouraged to think and learn, with the understanding that specific content isn't as important as it would be in training scenarios. However, there's still a need for commonality across institutions, with peer review and academic norms. These three approaches thus represent a trifecta in establishing such norms.

ACKNOWLEDGMENTS

This paper resulted from collaborations with several people, including Edward Sobiesk, Joseph J. Ekstrom, Jean R.S. Blair, John Impagliazzo, David Gibson, Harry Reif, and Steven Lingafelt. We also thank other members of the Cyber Education Project and the CSEC2017 Joint Task Force. This article is also based upon work partly supported by NSF under award No. DGE-1433736.

REFERENCES

1. "Occupational Outlook Handbook: Information Security Analysts," Bureau of Labor Statistics, US Department of Labor, 2016–2017 Edition; www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm.
2. "CAE Requirements and Resources," National Centers of Academic Excellence in Cyber Defense (CAE-CD); www.iad.gov/nietp/CAERequirements.cfm.
3. "National Centers of Academic Excellence in Cyber Operations," National Security Agency, Central Security Services; www.nsa.gov/resources/educators/centers-academic-excellence/cyber-operations.
4. The CSEC2017 Joint Task Force, "Cybersecurity Curricula 2017," version 0.95 report, 13 November 2017, [Association for Computing Machinery (ACM), IEEE Computer Society (IEEE-CS), Association for Information Systems Special Interest Group on Security (AIS SIGSEC), and International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8)]; www.csec2017.org.
5. "Proposed Accreditation Criteria for Cybersecurity Academic Programs," ABET, Inc., 13 Nov. 2017; www.abet.org/blog/news/abet-seeks-feedback-on-proposed-accreditation-criteria-for-cybersecurity-academic-programs.
6. "Proposed Accreditation Criteria for Cybersecurity Academic Programs," ABET, Inc., 14 Dec. 2017; www.abet.org/blog/news/abet-seeks-feedback-on-proposed-accreditation-criteria-for-cybersecurity-engineering-academic-programs.
7. W. Newhouse et al., "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework," NIST Special Publication 800-181; http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf.
8. Cyber Education Project, website; www.cybereducationproject.org.

RAJENDRA K. RAJ is a professor of computer science at the Rochester Institute of Technology. Contact him at rajendra.k.raj@rit.edu.

ALLEN PARRISH is a professor of cyber science at the United States Naval Academy. Contact him at aparrish@usna.edu.

