Contrasting the CSEC 2017 and the CAE Designation Requirements

Wm. Arthur Conklin
College of Technology
University of Houston
waconklin@uh.edu

Matt Bishop
Dept. Of Computer Science
University of California at Davis
mabishop@ucdavis.edu

Abstract

The draft 2017 Cybersecurity Curricula, also called CSEC2017, is being developed to provide guidelines for cybersecurity curricula development. One component, the Knowledge Areas, includes Knowledge Units. This terminology is the same as is used for the U.S. NSA/DHS Centers of Academic Excellence in various disciplines of cybersecurity. The two are different, yet complementary. In order to aid faculty and others in understanding the difference between the two programs, this paper explores both the CSEC2017 and CAE academic designation criteria, and compares and contrasts them.

1. Introduction

Two major academic projects are working on academic curriculum issues associated with cybersecurity curricula. There has been confusion about the objectives of each of these projects and the role they play in assisting educators to create appropriate cybersecurity curricula. The first of these projects is the Cybersecurity Curricula 2017 Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity (CSEC2017), a curricular guidance effort for the broad field of cybersecurity. The second is the Center of Academic Excellence Knowledge Unit program for the CAE CDE program (KU), a community driven effort to create a list of prescriptive educational elements describing a cybersecurity program in an educational setting.

Cybersecurity is a broad set of disciplines, with a body of knowledge that spans multiple distinct educational areas and is intertwined with virtually every aspect of our information age. What began as a computer science and computer engineering discipline has spread into a wide range of disciplines. Today, there is a need for cybersecurity-educated professionals in a wide range of jobs [11]. Educational institutions have responded with cybersecurity education programs in a wide array of disciplines beyond the original computer science and engineering disciplines. Business, information systems, information technology, law, political science, psychology, and interdisciplinary efforts including mathematics and physics have joined into the disciplines that have graduates entering the workforce as cybersecurity workers. This has created a need to define what belongs in a cybersecurity curriculum and how to assess curricular efforts with respect to producing employment ready students.

There is a known shortage of cybersecurity professionals, both in the government and the private sector [3, 6]. The shortage has been raised to national importance by both the current and previous US administrations, each time calling for greater workforce development in cybersecurity [15, 16]. Cybersecurity education has a number of challenges in meeting the workforce needs. [5] Many of these issues have existed for years. Continual efforts by the US government in the form of the NIST-led National Initiative on Cybersecurity Education (NIST NICE) [12, 14] and the NSA/DHS effort with Centers of Academic Excellence in Cyber Defense Education (CAE-CD) [4, 10] have made a dent in the problem, but for academia to fid and shift resources into developing and implementing new curricula takes time and resources. Aligning academia educational output and industry needs in a changing environment has been a challenge for decades and in cybersecurity this has been noted for at least 20 years [1]. A recent academically led effort, CSEC2017, to develop curricular guidance in cybersecurity education has created what may be the missing piece for academics to properly advance academic programs to meet the needs of graduates and industry. [8]

The previously mentioned initiatives from the government, the CAE and NICE programs, initially were targeted to meet specific hiring needs of the federal government. This led to problems with academics adopting them directly for classroom use, as they were far from curricula guidance and targeted specific training as opposed to education [2]. Both of these programs have undergone updates in the past couple of years. This paper examines the knowledge

URI: http://hdl.handle.net/10125/50194
ISBN: 978-0-9981331-1-9

unit development process of the NSA/DHS CAE-CD program, comparing and contrasting it with the CSEC2017 effort.

The ACM, IEEE Computer Society, AIS SIGSEC, and IFIP WG 11.8 started the CSEC2017 Joint Task Force on Cybersecurity Education (JTF) in 2015. Its goal is to "develop comprehensive curricular guidance in cybersecurity education that will support future program development and associated educational efforts at the post-secondary level" ([8], p. 8). The guidance document, called CSEC2017, presents important areas of knowledge in the field of cybersecurity as well as a framework providing structure [8]. The framework provides guidance for curriculum developers to determine which areas of knowledge are most critical for their discipline or professional competence. They can then emphasize those aspects in greater depth than the other knowledge areas while ensuring they cover the knowledge areas applicable to their goals.

2. CSEC2017

The term "cybersecurity professional" is ambiguous [9]. While it designates a worker in the field of cybersecurity, the skills and knowledge that such a professional is expected to have varies wildly among jobs. One who sets security policy need not understand precisely how the technology works, or the Harrison-Ruzzo-Ullman theorem of the undecidability of security, but that person should know the limits of what the technology can do and what is feasible to require of both people and systems. A security administrator need not understand the laws and regulations that underlie the security policies the system is to enforce, but she must understand how the technology works and how to install and configure it to enforce those policies (or say what cannot be enforced). A cybersecurity professor needs to know the Harrison-Ruzzo-Ullman theorem as well as the principles underlying cybersecurity and their application in technology. Thus, the term "cybersecurity profession" is generic and not specific – really, it should be "cybersecurity professions".

A cybersecurity professional typically completes a curriculum to obtain a degree or certification, and then practices her work for some period of time. This raises the issue of what an appropriate cybersecurity curriculum should cover. Given the wide range of jobs that cybersecurity professionals undertake, no single curriculum can serve all needs. Yet there are certain underlying themes common to all cybersecurity professions that any cybersecurity curriculum must cover. The depth, time spent, and knowledge, skills, and abilities in these themes depend upon the goals of the particular curriculum.

The CSEC2017's goals speak to this need. It is to provide curricular guidance that is comprehensive enough to support a wide range of disciplines and competencies. This guidance is to be grounded in the basic principles of cybersecurity, yet be flexible enough to accommodate educational programs with differing needs, and enable them to evolve as the field of cybersecurity, and the needs of the workforce, also evolve.

In order to achieve this goal, the JTF is composed of cybersecurity experts from academia, industry, and government. They work in both technical and non-technical disciplines. In addition to international representation on the JTF, a Global Advisory Board provides input to make the guidelines useful to non-United States institutions and programs. Working groups include educators and practitioners from all over the world who have experience in the particular knowledge areas on which they are working.

The structure of the CSEC2017 model consists of four parts:

- Knowledge areas;
- Crosscutting concepts;
- Disciplinary lenses; and
- Application areas.

2.1. Knowledge Areas

Knowledge areas (KAs) organize the knowledge of cybersecurity. Figure 1 shows their structure.

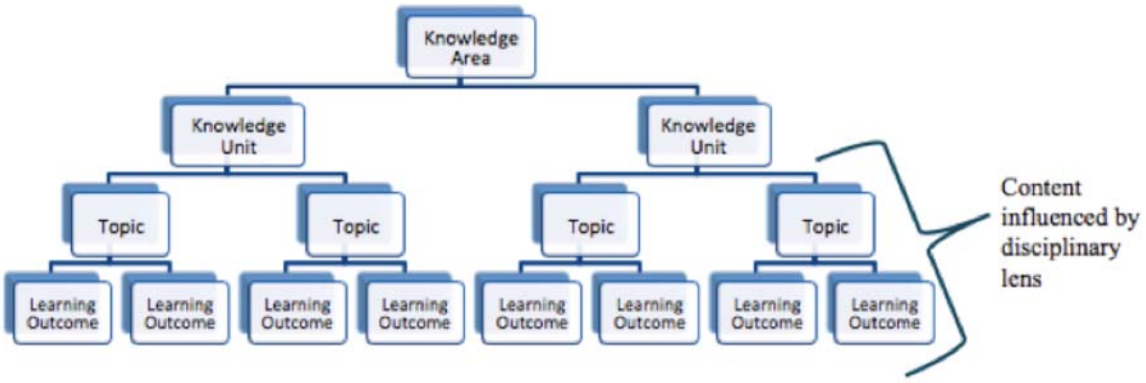

Figure 1. The structure of the knowledge areas. The same topic may appear under different knowledge units; this simply gives a different emphasis for the topic.

The JTF has identified eight such areas:

1. The *data security* KA covers the protection of data both when stationary and during transmission.
2. The *software security* KA covers the development, deployment, operation, maintenance, and decommissioning of software in such a way that desired security and robustness properties are maintained throughout the software life cycle.
3. The *component security* KA deals with the security of components and their manufacture and fabrication, including the supply chain and interfaces.
4. The *connection security* KA deals with the connection of components; this includes the physical media used in transmission, network services, and network security.
5. The *system security* KA deals with the security of the system as a whole, such as the composition of components, authentication, system architectures, and the security of specialized systems such as embedded and autonomous systems and the Internet of Things.
6. The *human security* KA looks at protecting the data, and through that the privacy, of people.
7. The *organizational security* KA focuses on the protection of organizations from threats that impede their accomplishing their mission.
8. The *societal security* KA treats cybersecurity aspects that affect society at large, such as cyberlaw and cybercrime, ethics, professional and social responsibility, and intellectual property.

These knowledge areas are not mutually exclusive. A knowledge unit may sit in more than one KA, in which case the KA it is in drives the way one looks at the unit. For example, a knowledge unit on cryptography certainly falls into the data security KA because it is central to the protection of data. It also falls into the system security KA because cryptography is used to authenticate components of a system (for example, by using and validating digital signatures). Finally, the use of cryptography has societal implications—witness the debate about whether "back doors" should be embedded in products—and for this aspect would fall under the societal security KA.

Each knowledge unit groups topics of a single theme together. These knowledge units in turn are made up of topics, each of which has an associated set of learning outcomes. Topics may fall under multiple knowledge units, and learning objectives may also fall under multiple topics.

2.2. Cross-Cutting Concepts

The cross-cutting concepts connect the knowledge areas. They emphasize key concepts common to all aspects of cybersecurity. The model has five such concepts.

1. *Confidentiality* rules limit access to data and resources.
2. *Integrity* rules aim to provide assurance that data and resources are trustworthy.
3. *Availability* rules ensure that access to data or resources meet quality of service requirements.
4. *Risk* deals with threats from the environment and from adversaries.
5. *Adversarial thinking* considers how an adversary might hinder or thwart obtaining the desired result.

For example, consider confidentiality. It is clearly a key component of the data security, connection security, system security, and organizational security

KAs. It is a component of the human security KA in the guise of privacy, among other things. And it affects societal security through a combination of the above, so would also be in the societal security KA. Finally, its importance to the software security KA lies in the protection of sensitive data such as passwords, and indeed the use of obfuscation to protect the software itself.

2.3. Disciplinary Lenses

The disciplinary lenses provide the approach, depth, and learning outcomes for each knowledge unit that are appropriate for a particular discipline. For example, consider an enterprise architecture. A non-technical discipline (such as pre-law) would examine the effect and consequences of legislation involving computer technology. That discipline would require an understanding of what technology can, and cannot, do to inform how the laws should be written and what the effects of the laws would be (or are). It would not require a detailed knowledge of how the components making up the technology in question work. An information systems student would emphasize how the security policies derived from (among other things) legislation and regulations affects the protection of data. Thus, she would need to know details of the configuration and management of the technology, but not the effects or consequences of specific legislation. Finally, a computer science major would need to know how the components of the system work, with management and legal issues being weighted much less heavily than in the pre-law program.

The disciplines in the model are based on those identified by the ACM:

1. The *computer science* discipline covers the development of software, ways to use computers to solve problems, and new ways to use computers.
2. The *computer engineering* discipline looks at designing and implementing computing devices.
3. The *information systems* discipline explores the uses of information processing technology in enterprises, with an emphasis on the use of information on those systems.
4. The *information technology* discipline is similar to that of information systems, but focuses on the technology rather than the use of information on that technology.
5. The *software engineering* discipline deals with defining, developing, implementing, testing, maintaining software
6. Finally, the *other disciplinary* majors includes other disciplines, with elements chosen from the above disciplines as appropriate.

2.4. Application Areas

Application areas link cybersecurity curricular elements to professional practice. They filter the knowledge, skills, and abilities gleaned through appropriate disciplinary lenses to frameworks used in professional societies and the workforce. Specifically, they define the breadth and depth of coverage expected for each core idea in the particular profession or job.

The seven application areas are:

1. *Public policy* covers managers such as executive management, legislators, regulators, and other public and private personnel who develop or affect cybersecurity policy.
2. *Procurement* covers those who purchase or otherwise acquire information technology, and hire the people who will work with it. They must understand the cybersecurity considerations involved in such procurement and hiring, including risk management and assurance with respect to the mission of the systems and people.
3. *Management* refers to those who administer the systems and the environment necessary to support the systems, users, and administrators. Cybersecurity considerations include business continuity matters, managing identity and authorization, and incident handling.
4. *Software development* involves ensuring the software meets requirements, including those aimed at compliance with policy, laws, and regulations, and that it is robust. This includes testing the software as well as maintaining it and developing patches and updates as needed.
5. *IT security operations* focuses on the operation of the systems in such a way that they meet cybersecurity requirements. Practitioners must be able to translate policy into operational procedures, and be able to configure systems and networks to this end.
6. *Enterprise architecture* refers to the aggregation of all technology in the enterprise, as well as their operation and management. It covers elements from the above five application areas.
7. Finally, *research* in cybersecurity requires an understanding of access control and the three general properties, namely confidentiality, integrity, and availability. Beyond these, the

specific topic(s) of research dictate what else a researcher should know, and in what depth. A researcher in network security needs to know how networks are used in practice to determine how best to design an intrusion detection system to gather data for analysis, but does not need to know the proof of the Harrison-Ruzzo-Ullman theorem. However, a researcher in the foundations of computer security needs to know both the theorem and its proof, but not how networks are used in practice.

These application areas are preliminary, and may change as the CSEC2017 undergoes refinement.

2.5. Summary

It is *critical* to understand that CSEC2017 is not a curriculum. For example, in the topic "cryptography", the CSEC2017 does not say which algorithms should be taught. This is because the state of the art changes. In the 1970s, the Data Encryption Standard was considered state of the art; in the 2000s, it clearly is not. So it is left to the curriculum designers to instantiate the topics that they believe should be covered, and determine what exactly should be taught to satisfy the needs of their specific curriculum.

The contents of the CSEC2017 are being validated through comparison with existing bodies of knowledge and curricula. For example, the Fundamental Principles knowledge unit in the Software Security KA has been compared to numerous software vulnerabilities lists, including the *OWASP Top Ten Most Critical Web Application Security Risks* and the IEEE Cyber Security document *Avoiding the Top 10 Software Security Design Flaws* [7, 13]. As the practice and documentation knowledge units are fleshed out, they will again be compared to these (and other) documents, as well as various course syllabi involving secure software development. Other KAs will proceed similarly.

The CSEC2017 is a work in progress. Undoubtedly it will change before being finalized. For example, the systems security KA is likely to be split into two or more knowledge areas because its scope is so large, or the scope may be narrowed. The JTF is actively discussing both possibilities.[1]

Even when finalized, the CSEC2017 will need to be updated as cybersecurity education, and cybersecurity professions, evolve. This is expected, and the intent is to provide a sound basis both for curricular development and the evolution of the guidelines.

3. CAE KU Project

In 1997, the U.S. National Security Agency designated 7 schools in the United States as Centers of Academic Excellence in Information Assurance Education (CAE-IAE). Other schools were designated in successive years, and soon the criteria for such designation was that the academic program had to meet criteria defined by U.S. national training standards CNSS 4011 and at least additional such standard.

Academic institutions pushed back against this criteria, pointing out the difference between training and academic education — both are appropriate, but the four-year institutions focus on the latter rather than the former [2]. In part because of this, the National Security Agency and the Department of Homeland Security (which had joined to co-lead the CAE program) began to focus on what should be in a curriculum in order to educate a cybersecurity worker.

In 2014, the criteria for designation was revised radically, around the educational elements associated with cybersecurity. These curricular components, the Knowledge Units, covered specific topics to be taught by institutions using the KUs. Being designated a CAE-CD (the new name for what was a CAE-IAE) now required the institution to cover the material in a set of basic KUs and selected optional KUs that described their academic program content. In addition, two-year academic institutions such as Community Colleges could now also be designated CAE-2Y, indicating they also satisfied a set of KUs. How the institution taught the specific topics was up to the institution — but all the material in a KU had to be covered.

Although this initial set of KUs was developed as a result of a series of information gathering meetings where academics provided input into the content of the KUs, many academic institutions felt the KUs were inadequate. In 2016 the U.S. National Science Foundation funded a project to create a social community and wiki to update the KUs.

The result of this KU refinement has been a broadening of the information describing a knowledge unit. What began as a name, a description, and a list of topics and outcomes, has been expanded to include many additional elements such as a vocabulary, a connection to the NIST NICE Job Tasks, and connection to industry certifications. On the current schedule, the next set of KUs will be submitted to the program office at NSA in the fall of 2017 for use in

[1] Indeed, the original system security KA has been split into the component security, connection security, and system security KAs shown above between the writing of the submitted version and final version of this paper.

2018, although the program will continue to refine and develop the KUs for future releases.

The objective of the KU project is simple: to provide a set of prescriptive elements that can be used to assess a program with respect to academic content elements. The way this works begins with each institution defining what their educational outcome objectives are with respect to their cybersecurity program. With the field being so broad, programs need to specialize in some aspect of the discipline, and from there define the curriculum that will produce graduates aligned with these objectives. The Centers of Academic Excellence program allows programs to define their academic program in the form of a series of core (mandatory) knowledge units, supported by a larger set of elective KUs to shape the curriculum objectives to the school's objectives. Assessors can then assess the mapping of the school's academic work to the chosen set of KUs to determine whether a program is satisfactorily comprehensive on the academic side. There are additional programmatic elements, and the program office will consider the package as a whole to determine whether the institution's cybersecurity program meets the standards of a Center of Academic Excellence.

The key to the assessment of the academic program comes from the comprehensiveness of the KUs, and this content is in the hands of academics. As academics improve the comprehensive nature of the KUs through the refinement project, they will more closely represent the actual needs of an organization with respect to content that has both an education component and a workforce development and training component, making program assessment easier, and more meaningful.

4. Contrasting the CSEC2017 and CAE KU Projects

Both CSEC2017 and the CAE KU project have knowledge units, and this has caused many in the academic community to question how these projects differ and ask which they should back.

Indeed, both projects have Knowledge Units, and over time, these two knowledge bases are expected to converge. They are being developed by different groups at the present time, and while the groups, and the goals of the groups, are different, both efforts are open to public input and cross pollination is and will continue to occur. But this is really a minor aspect and ignores the bigger question. How are they different and what does that mean to a faculty member?

CSEC2017 is an effort to develop comprehensive curricular guidance in cybersecurity education that will support future program development. Again, it is not a curriculum document, but the basis for developing curriculum documents. Those documents will draw upon the contents of CSEC2017, the specific requirements of the academic institution or group developing the curriculum, and sources within the industries and organizations that hire current graduates of the program. As the curricular guidance contains the necessary information for any and all curricula in the cybersecurity disciplines, it is up to the curriculum developers to select the topics, decide upon an instantiation of those topics, the way those topics are to be covered, and in what depth they should be covered, for a specific program. In this way, the curriculum developer can create a curriculum that is both academically sound and that gives graduates the practical aspects they need to succeed.

The CAE KU project has an entirely different focus. Its goal is to provide a basis for recommending programs as meeting the needs of educating cybersecurity workers. Like CSEC2017, it recognizes the need for flexibility, in that no single program meets the needs of all cybersecurity professionals. So it provides a set of KUs, topics, and outcomes that schools can map their programs into (and, if necessary, add material from) to demonstrate they are meeting the criteria for a CAE. No program would use all of the KU's, or even more than a small fraction for that matter. In other words, what has to happen is that the program pick from the set of KUs the appropriate ones to describe their program.

The first step is to decide what your cybersecurity program attempts to accomplish. From there, the CSEC2017 effort will help you develop a sound comprehensive curriculum, and the CAE KU effort provides a means to describe the program to the CAE office. What is most important in the near term is that both the CSEC2017 and CAE KU efforts will be ongoing and need academic input to properly refine them towards their objectives.

5. Future Efforts

Both the CSEC2017 and CAE KU effort will be ongoing as future revisions of both projects will further clarify and refine the outputs of the two efforts. And over time, the KU portion of both projects may in fact become aligned, but that is several revisions in the future. And all of this effort is occurring in the rapidly changing environment of cybersecurity. The US government has produced the National Initiative for Cybersecurity Education National Cybersecurity Workforce Framework (NCWF), a third generation attempt at documenting the workforce needs in

cybersecurity in a notional framework. Over time, this effort too, will have to shift and move as the field of cybersecurity advances. In the interim, there is a need for all three elements, the Center of Academic Excellence program, the CSEC2017 initiative and the NCWF, for each comes at different problems, from different angles and provides crucial information to further define and develop the needed academic programs to address a workforce shortage.

Acknowledgements. Development of the CSEC2017 is supported by the U.S. National Science Foundation with grant DGE-1623104 to the George Washington University, an award from the U.S. National Security Agency's CNAP Curriculum Development Effort (RFI-2017-0002) to the George Washington University, and additional support from the ACM Education Board and Intel® Corporation. We thank them for their support.

Development of the community led KU refinement effort was supported by the U.S. National Science Foundation with grant 1465260 SaTC-EDU: EAGER: *A Wiki Space for Information Security Education Exchange,* and an award from the U.S. National Security Agency's *CAE-CD National and Regional Resource Centers (CNRCs/CRRCs) and FY17 CNAP Initiatives,* S-001-2017. We thank them for their support.

10. References

[1] K. Beckman, N. Coulter, S. Khajenoori, and N. R. Mead, "Collaborations: closing the industry-academia gap," *IEEE Software,* vol. 14, pp. 49-57, 1997.

[2] M. Bishop and C. Taylor, "A Critical Analysis of the Centers of Academic Excellence Program," in *Proceedings of the 13th Colloquium for Information Systems Security Education, Seattle, WA June*, 2009, pp. 1-3.

[3] Burning Glass Technologies, "Job Market Intelligence: Cybersecurity Jobs, 2015," BostonJuly 2015 2015.

[4] CAE Office - NSA, "NSA / DHS National Centers of Academic Excellence in Cyber Defense (CD) Knowledge Units," NSA, Ed., ed. Baltimore, MD: NSA CAE Office, 2013, p. 73.

[5] W. A. Conklin, ;Cline, Raymond E.;Roosa, Tiffany, "Re-engineering Cybersecurity Education in the US: An Analysis of the Critical Factors," in *47th Hawaiian International Conference on Systems Sciences*, Waikoloa, HI, 2014.

[6] DHS Task Force on CyberSkills, "CyberSkills Taks Force Report," D. o. H. Security, Ed., ed. Washington, DC, 2012, pp. 1-41.

[7] IEEE Computer Society, "Avoiding the Top 10 Software Security Design Flaws," IEEE Computer Society Center for Secure DesignNovember 2015 2015.

[8] Joint Task Force on Cybersecurity Education, "Cybersecurity Curricula 2017 Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity," 12 June 2017 2017.

[9] National Research Council, *Professionalizing the Nation's Cybersecurity Workforce? Criteria for Decision-Making*. Washington, DC: The National Academies Press, 2013.

[10] National Security Agency. (2017, 6/15/2017). *National Centers of Academic Excellence in Cyber Defense*. Available: https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-defense/

[11] B. Newhouse, S. Keith, B. Scribner, and G. Witte, "NICE Cybersecurity Workforce Framework (NCWF)," National Institute of Standards and Technology (NIST), Ed., ed. Gaithersburg, MD, 2016.

[12] NIST, "National Initiative for Cybersecurity Education Strategic Plan," National Institute of Standards and Technology (NIST), Ed., ed. Washington, DC: NIST, 2012, p. 26.

[13] Open Web Application Security Project (OWASP), "OWASP Top 10 Application Security Risks," OWASP Foundation2017.

[14] C. Paulsen, E. McDuffie, W. Newhouse, and P. Toth, "NICE: Creating a Cybersecurity Workforce and Aware Public," *IEEE Security & Privacy,* vol. 10, pp. 76-79, 2012.

[15] White House, "Cybersecurity National Action Plan," W. House, Ed., ed. Washington, DC: White House,, 2016.

[16] White House, "EO 13800 Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," White House, Ed., ed. Washington, DC: White House,, 2017.