Open Access License Notice

What Constitutes Core in a Cyber Security Curriculum?

William Arthur Conklin
waconklin@uh.edu

College of Technology
University of Houston
Houston, TX

Abstract - Cyber security is an expansive domain that has components from many different disciplines. From the obvious computer science and information technology areas, to business, psychology, political science, law, law enforcement, and more, the list goes on. With the rise of programs such as the Centers of Academic Excellence in Cyber Defense Education, one of the key questions is "what constitutes an appropriate curriculum." A subset of this question is: what constitutes the core knowledge that is essential regardless of program specialty. This paper addresses this very question.

Categories and Subject Descriptors

K.3.2 [Computers and Education]: *Computer and Information Science Education - Curriculum*

Keywords

Cyber security curriculum, Knowledge Unit (KU)

1 INTRODUCTION

Cyber security is not a single discipline, but rather a component of many domains. From the obvious computer science and information technology areas, to business, psychology, political science, law, law enforcement, and more, the list goes on, cyber security is a part of many aspects of our lives. With the increase in need for cybersecurity professionals, the education establishment responded with programs. Then came the need for recognition and accreditation, including the U.S. Government's Centers of Academic Excellence (CAE-CDE) program. These programs attempt to address the issue of what elements are necessary for a proper curriculum in the programs being examined. A subset of this question is: what constitutes the core knowledge that is essential regardless of program specialty.

The initial critical mass of cyber security programs came from computer science and information technology based programs. The foundational element behind these curricula efforts was technically focused on programming and tools. The natural expansion of cybersecurity into engineering ensued, a further expansion of the technical side of the discipline. The operationalization of cybersecurity led to expansion into the disciplines of business, law, political science, psychology, and a whole host of additional supporting disciplines. In these disciplines, foundational principles and theories were mapped into the realm of cybersecurity to explain observed phenomena.

When examining a curriculum used to educate students in cybersecurity, there is an underlying central question – what materials constitute a proper curriculum? With a wide variety of curricula, there is naturally a wide range of appropriate content components. To address the diversity, one method is have a core curriculum which covers the common cybersecurity fundamentals, with additional elements covering the specialization aspects. This is the methodology employed in the Knowledge Unit basis for the CAE-CDE program. This paper will examine the issue of a core knowledge base that spans all of the potential curricula used to educate cybersecurity enabled professionals across a wide range of disciplines. Data has been collected from various military and government agencies as well as

employers as to what is needed in graduates. Information from CAE academic colleagues as to proper curriculum composition has been collected from a series of CAE meetings over the past 18 months. These data sources point to a clear set of requirements which will be described in the paper.

2 HISTORY

There are other sources of information that can be used to define the elements required in a cybersecurity program, including curriculum standards, industry certification programs, and other sources [1-7]. Each of these sources examines the workforce requirements issue from a different lens, and positions the importance of content with respect to the views of their stakeholders. This results in significant overlap, and differentiation, partly due to the lens of the drafter, partly due to the specificity of scope of the standard. Each of these has specific value for the shareholder that they serve, yet for a national standard to be used in broad-base education across a variety of disciplines and programs, a more general, and designed for education approach was needed.

The DHS / NSA Center of Academic Excellence program has a charge to define the requirements associated with cyber security education. The CAE-CDE program has undergone several revisions in its history. Originally based on a series of training standards, the CNSS series, the educational component has shifted to a set of requirements known as knowledge units (KUs). The CNSS training standards were a challenging fit for many education programs, because rather than being a definition of education requirements, they were a series of training documents and thus lacked much of the academic rigor used to define academic requirements. The knowledge units were designed to specifically address this problem, while providing a broader base of cyber security background requirements. The knowledge units describe a set of information for a series of security related topics, including a set of topics and outcomes to be covered in the subject area. The development of the KU's was largely done by the academic community in a multi-year crowd-sourcing methodology. The information that forms the basis of the KU's will always be a work in progress as the field continues to evolve.

As in all human data collection efforts, there is the chance of bias. Bias can color results and in this case the bias is related to the subset of all academics that contributed to the KU work. The vast majority were from technical computer science and engineering based programs of study. This would result in a bias associated with the selection KU elements. This is understandable given the CAE program, its focus on technical computer science cyber security programs, and the available community of academic practitioners. With the expansion of cyber security programs into a wider range of academic programs, including business, political science, law, law enforcement, psychology and others, this initial cut KU definitions needs to be broadened and expanded. The wiki based collaboration project was created with support from NSF grant 1465260 SaTC-EDU:EAGER:A Wiki Space for Information Security Education Exchange to assist in this effort.

3 PROGRAM DIFFERENTIATION

The history of cyber security programs has been built upon technical programs in computer science and engineering. The future of these programs is much broader than just the technical programs. To define the proper curriculum, one needs to examine the broader case of cyber security, not just the technical side of the domain. In addition to differentiation between technical and non-technical programs, there are other differentiation factors as well. Academic levels, from 2 year community colleges, to 4 year undergraduate programs, to graduate programs, these all have differing requirements. There is also an issue of programmatic focus – whether the program is a CAE-CDE, CAE-R or CAE-O basis, or even depending upon what focus areas a program chooses, there are different curricula needs.

The differences of all of these programs is in the focus of the program, the devil is in the details so to speak. The foundational elements of cyber security is the same for all programs, it is in the detailed programs that build upon the foundations that the different programs are defined. This paper is not about the curricula that provides the elements for these differences, but rather it is about defining the common core curriculum that is shared by all programs.

3.1 Current KU Core

The current set of core KU's are specified in two sets. The current set of core KU's per the 2014 CAE-CD program is: [8]

2Y core requirements	4Y core requirements
▪ Basic Data Analysis ▪ Basic Scripting ▪ Cyber Defense ▪ Cyber Threats ▪ Fundamental Security Design Principles ▪ IA Fundamentals ▪ Introduction to Cryptography ▪ IT Systems Components ▪ Networking Concepts ▪ Policy, Legal, Ethics, and Compliance ▪ System Administration	▪ Databases ▪ Network Defense ▪ Network Technology and Protocols ▪ Operating Systems Concepts ▪ Probability and Statistics ▪ Programming

As one can see from the current core listing, it is hard to tell all of the content from the KU name alone. Some of the KU's, such as Basic Scripting, are fairly obvious as to type of content, whereas others, such as Cyber Defense and Cyber Threats, are less so. This has led many to inflate the core, as when asked "Does X belong in a program", the answer is "yes" and this led to the inclusion in the core.

The core defined above suffers from a couple of deficiencies. First is the bias from the group of academics that created it, and second is the phenomenon of scope creep. Scope creep is common in many projects, and it is when the requirements expand beyond original parameters. An examination of the list above shows some obvious candidates of scope creep – such as Basic Data Analysis.

3.2 Purpose of Core

Defining the core elements of a cyber security curriculum is an exercise in minimalism. Rather than examine all of the things that might belong in a cyber security program, and label them core, a minimalist method is to apply a sharp focus to the problem. The term core relates to essential elements, not all the elements. A great example of this focus is found in the paper "What the Graduate Needs to Know About Cryptography." [9] This paper does not espouse to be the total compendium on cryptography, but rather focuses on essential elements for graduates of programs that go forth and "do" security. Are there other elements of cryptography that belong in a curriculum? Sure, but not for all graduates. And this is the lens that needs to be applied when building a core curriculum.

3.3 Proposed Core

Using the focus of "what does every program need to know", and applying it with rigor is the first step in building a core. The second, and equally valuable step is in examining the size of the resulting core. When you look at the length of the current core curriculum, and compare it to the total set of required KU's, the percentage of core (77%) is way too high.

When we look at the elements that are needed, the first rule is: What does every graduate need to know? The first part of that answer is: cyber security foundations. If one is going to apply advanced elements from any discipline into the cyber security realm, they need to understand what cyber security is, and the principles behind it. They also need to understand the vocabulary used in cyber security, for mixing terms such as threat, risk, vulnerability, hack, etc. only leads to difficulty in

communicating and results in errors. There is also a need for some fundamental knowledge of the basic building blocks behind some of the elements, such as cryptography, networks, threats and software issues. There is a need for a KU to cover the components of information systems, what are all the parts that constitute a system. This KU, IT System Components, is needed to ensure that everyone understands the key elements of the systems associated with cyber security.

The current set of KU's cover most of these elements between the Fundamental Security Design Principles (renamed Cyber Security Principles) and IA Fundamentals (renamed Cyber Security Fundamental Concepts). The final core KU, IT System Components, covers the fundamental knowledge associated with the systems cyber security protects.

A new element to the KUs, to cover what is missing is a vocabulary element – a listing of core terms needed to be understood by all. Rather than make this a separate KU, the three core KU's already identified can be modified with the addition of a vocabulary element. A note on the vocabulary elements listed below – these are for example only and need additional terms.

3.3.1 Cyber Security Principles Knowledge Unit (Proposed)

Description

The intent of this Knowledge Unit is to provide students with basic security design fundamentals that help create systems that are worthy of being trusted.

Outcomes

1. Students will be able to define the principles of security.
2. Students will be able to describe why each principle is important to security and how it enables the development of security mechanisms that can implement desired security policies.
3. Students will be able to analyze common security failures and identify specific design principles that have been violated.

4. Given a specific scenario, students will be able to identify the needed design principle.
5. Students will understand the interaction between security and system usability and the importance for minimizing the effects of security mechanisms.
6. Students should be able to properly use the vocabulary associated with cyber security

Topics

- Separation (of domains / duties)
- Isolation
- Encapsulation
- Modularity
- Simplicity of design (Economy of Mechanism)
- Minimization of implementation (Least Common Mechanism)
- Open Design
- Complete Mediation
- Layering (Defense in depth)
- Least Privilege
- Fail Safe Defaults / Fail Secure
- Least Astonishment (Psychological Acceptability)
- Minimize Trust Surface (Reluctance to trust)
- Usability

Vocabulary

Packet, risk, secure system, trust, trusted system, trustworthy, vulnerability

3.3.2 Cyber Security Fundamental Concepts Knowledge Unit (Proposed)

Description

The intent of this Knowledge Unit is to provide students with basic concepts of cyber security fundamentals.

Outcomes

1. Students shall be able to describe the fundamental concepts of the cyber security discipline.
2. Students will be able to describe the use of fundamental concepts of cyber security to provide system security.
3. Students should be able to properly use the vocabulary associated with cyber security.

Topics

- Threats and Adversaries (threat actors, malware, natural phenomena)
- Vulnerabilities and Risk management (include backups and recovery)
- Common Attacks
- Basic Risk Assessment
- Security Life-Cycle
- Cryptography and PKI
- Data Security (in transmission, at rest, in processing)
- Security Models (Bell-La Padula, Biba, Clark Wilson, Brewer Nash, Multi-level security)
- Access Control Models (MAC, DAC, RBAC, Lattice)
- Confidentiality, Integrity, Availability, Access, Authentication, Authorization, Non-Repudiation, Privacy
- Session Management

- Exception Management
- Security Mechanisms (e.g., Identification / Authentication, Audit)
- Legal issues

Vocabulary

Advanced persistent threat (APT), attacker, Block ciphers, DoS, DDoS, malware, mitigations, residual risk, risk, stream ciphers, vulnerability

3.3.3 IT System Components Knowledge Unit (Proposed)

Description

The intent of this Knowledge Unit is to provide students with a basic understanding of the components in an information technology system and their roles in system operation. This is a high level introduction or familiarization of the topics, not a deep dive into specifics.

Outcomes

1. Students will be able to describe the hardware components of modern computing environments and their individual functions.
2. Students will be able to describe the basic security implications of modern computing environments.
3. Students should be able to properly use the vocabulary associated with cyber security.

Topics

- Workstations
- Servers
- Mobile Devices
- Peripheral Devices (Printers, scanners, external storage)

- System Architectures
- Alternative environments (SCADA, real time systems, critical infrastructures)
- Networks (Internet, LANs, wireless)
- Storage Devices
- Network Components (Routers / Switches)
- Network Security Components (Data Loss Prevention, VPNs / Firewalls)
- Intrusion Detection and Prevention Systems, Incident Response
- Cloud
- Managed Services
- Software Security (secure coding principles, software issues by type)
- Configuration Management
- People and security (social engineering)
- Physical and environmental security concerns

Vocabulary

BYOD, IaaS, PaaS, SaaS, SAN, USB

These three proposed core KUs have been modified from the current set of KUs. These modifications include expansion, de-confliction, and the addition of vocabulary elements. These changes are to support a common body of cyber security knowledge that applies across the entire discipline, not just in the technical aspects of it.

4 PROGRAMMATIC ALIGNMENT

While there might be an immediate reaction that some of the other KU's need to be involved, it is important to focus on the role of the core. Does a student studying the psychology associated with cyber security operators or attackers need to understand networking or programming or defense? Does a law student, or a

political scientist looking at cyber security from a treaty perspective? Each of these specialties will have a different subset of supporting elements. And this is the role of the supporting (or optional) KUs. Calling the additional KU's supporting more closely defines them to a program – they are not optional – a program needs them, but they may differ from program to program.

Determining what KUs are needed to support a program is at first a challenge, yet it is one that has already been done by every program. The vast majority of education programs have developed their curriculum to meet an external driver, such as a job market skill set, alignment with an external certification (network+, security+, CE|H, CISSP, or others), or the NICE workforce framework. Allowing programs more flexibility to align their programs with these workforce elements is needed and provides the diversity of programs to support regional as well as national needs.

Aligning the number of needed supporting KUs to determine sufficient coverage in a program was defined in the current system as 11 KUs (all core currently) for CAE-2Y, and 22 KUs (17 core + 5 optional) for CAE-CDE (4Y) schools. There are no specific counts for graduate or specialty programs. Determining the correct number is outside the scope of this paper, but there is nothing in the analysis that says the number of total KUs should change.

The argument for this paper is; what is the correct number of core KUs? The proposed set of KUs, numbering 3, would represent 27% of a set of 11 KUs for 2Y schools, and 14% of the 22 KUs for 4Y schools. This number seems much more in alignment with a reasonable level of common expectations across all related cyber security engaged disciplines.

5 CONCLUSION

This paper recommends changing the number of core KUs for all programs to the two KUs detailed earlier. This allows more flexibility for programs to build programs that align to their programmatic needs and still have the necessary quantity of cyber security materials. There needs to be an examination of the correct number

of KUs for each program type, and we as a community need to define this for ancillary programs such as political science, law, etc. We also will need to re-examine the number of KUs required every time the KUs undergo major revisions, for as their granularity changes, the total number required may go up and down. If the flexibility of too many non-core elements worries the CAE program office, there can be a place in the application for a school to explain how and why they chose the supporting set of KUs – how the set aligns to their programmatic objective. This information would also be useful in improving communication as to what is in each program for prospective students and future employers.

REFERENCES

[1] A. Association for Computing Machinery, "Computer Science Curricula 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science," ed: Association for Computing Machinery (ACM), 2013, p. 518.

[2] A. Association for Computing Machinery, 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), "Cybersecurity Curricula 2017: Curriculum Guidelines for Undergraduate Degree Programs in Cybersecurity," ed, 2017.

[3] ABET. (2013). *Criteria for Accrediting Computing Programs, 2013 - 2014*. Available: http://www.abet.org/DisplayTemplates/DocsHandbook.aspx?id=3148

[4] ACM and IEEE Computer Society, "CS 2008: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science," ed: IEEE/ACM Joint Task Force on Computing Curricula, 2008.

[5] CompTIA, "CompTIA Network+ Certification Exam Objectives," ed: CompTIA, 2016, p. 22.

[6] CompTIA, "CompTIA Security+ Certification Exam Objectives," p. 28, 2016.

[7] B. Newhouse, S. Keith, B. Scribner, and G. Witte, "SP 800-181: NICE Cybersecurity Workforce Framework (NCWF) National Initiative for Cybersecurity Education (NICE) (Draft)," National Institute of Standards and Technology, Ed., ed: Department of Commerce, 2016.

[8] C. O.-. 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.

[9] W. H. Murray, "What the Graduate Needs to Know about Cryptography," in *12th Colloquium for Information Systems Security Education (CISSE)*, Dallas, TX, 2008, pp. 153-157.