Course Development in the Cybersecurity Curriculum

Ingrid A. Buckley, Ph.D., Janusz Zalewski, Ph.D.
Florida Gulf Coast University, USA
ibuckley@fgcu.edu, zalewski@fgcu.edu

***Abstract* – The paper offers a discussion of fundamental concepts of cybersecurity, aimed at use in technical education at the college level. After outlining some of the existing approaches to curriculum design, as presented in guidelines developed by professional organizations, the authors address the issue of teaching basic concepts and principles of cybersecurity, with examples from their own courses in the undergraduate software engineering program at Florida Gulf Coast University.**

***Keywords* – Cybersecurity, cybersecurity curriculum design, cybersecurity education, Cybersecurity Curricula 2017.**

I. Introduction

Cybersecurity has become an overwhelmingly large knowledge area crossing multiple disciplines since with the rapid proliferation of computer technologies, computer security tends to affect every aspect of our lives. Therefore, cybersecurity education is a critical component of preparing society to understand the issues and successfully deal with and prevent various forms of security violations. This paper's primary focus is on technical education at the college level, but the approach to teaching fundamental concepts of cybersecurity discussed here can be applied at any level, from K-12 to the preparation of professional workforce.

The principal question that needs to be addressed in this context is how to structure the curriculum to focus on concepts that are fundamental to this profession, to obtain the most beneficial educational outcomes. It appears like at the college level, the most natural way to approach this problem is by analyzing some of the existing views on curriculum design in cybersecurity, which we perform and apply it to shape the actual courses in the software engineering program.

The rest of the paper is structured as follows. Section II reviews the current approaches to defining cybersecurity curricula proposed by professional organizations. Section III outlines some software engineering concepts on which a cybersecurity education model can be built, and Section IV presents a sample implementation of these concepts in two cybersecurity courses taught by the authors. The paper ends with conclusion.

II. Defining Cybersecurity Curricula

There are a multitude of papers published on cybersecurity education, mostly due to the fact that this discipline, as indicated in [1], crosses multiple boundaries and affects all five computing fields: computer science, computer engineering, software engineering, information systems, and information technology. In this paper, we only review the most important guidelines, which were produced by professional organizations, both in the United States and worldwide.

A. Cybersecurity Curricula 2017 [1]

Probably the most important guideline document for those in post-secondary education who design courses on cybersecurity and implement cybersecurity curricula is CSEC2017 [1]. It was developed jointly by a special Task Force comprising representatives from four major professional computing organizations: ACM, IEEE Computer Society, Association for Information Systems, and International Federation for Information Processing. To quote the Introduction: "The CSEC2017 report provides an overview of the cybersecurity discipline to frame the curricular model. The document then presents the curricular framework and outlines the recommended curricular content." The 120-page report comprises 5 chapters, the most insightful one being Chapter 4 "Content of the Cybersecurity Curricular Framework."

The framework is composed of eight Knowledge Areas (KA's), five of them technical, including Data Security, Software Security, Component Security, Connection Security, and System Security, and three non-technical ones: Human Security, Organizational Security, and Societal Security. Each KA is divided into Knowledge Units (KU's), grouping multiple related topics. For example, Data Security KA encompasses the following KU's: cryptography, digital forensics, data integrity and authentication, access control, secure communication protocols, cryptanalysis, data privacy, and information storage security. Each KA is also characterized by, the term, Essentials, for which Learning Outcomes are defined.

In summary, the CSEC2017 document provides a substantial high-level guideline for curriculum developers in cybersecurity, by defining "a structure for the cybersecurity discipline," as well as its contents. Its weakness, however, is that this structure is given somehow axiomatically, without stating where these KA's are coming from. This issue is partially addressed in Section III of this paper.

B. BCS Endorsed Cybersecurity Learning Outcomes

The British Computer Society published recently its "Guidelines on Course Accreditation" [2], where it mentions the criteria for cybersecurity education, with respect to accreditation. The guideline states the following: "For a given computer technology development or information system – such as an individual service, application, server, network device, laptop, smartphone or network or combinations thereof – students will be expected to show knowledge and understanding of the core concepts and principles within the following themes where this is relevant to the Programme Learning Outcomes under consideration." The five themes

This material is based in part upon work supported by CyberFlorida 2017 Capacity Building Award.

Digital Object Identifier (DOI):
http://dx.doi.org/10.18687/LACCEI2019.1.1.238
ISBN: 978-0-9993443-6-1 ISSN: 2414-6390

explicitly listed and described in more details in another document [3] include:

1) Information and risk.
2) Threats and attacks.
3) Cybersecurity architecture and operations.
4) Secure systems and products.
5) Cybersecurity management.

In [3], each theme is outlined in terms of: (a) core concepts; (b) example terms, techniques, and technologies; (c) learning outcomes; (d) advanced concepts; and (e) further learning outcomes. Learning outcomes are viewed as "the understanding and knowledge of the core concepts", while further learning outcomes are defined as "more advanced understanding and knowledge."

C. *Comparison of CSEC2017 and (ISC)^2/CPHC Guidelines*

Since both documents, CSEC2017 [1] and (ISC)^2/CPHC [3], have been created for accreditation of academic programs, it would be interesting to compare them. One most obvious observation is that they both include lists of fundamentals, called *essentials* in [1] and *core concepts* in [3]. Both documents are also very specific in listing learning outcomes.

Then, the similarities end, however, because Knowledge Units in [1] are much more specific than Example Terms, Techniques, and Technologies in [3]. Although they both cover the topical contents of respective Knowledge Areas in [1] and Themes in [3], they appear to address these topics from slightly different perspectives and on different levels: CSEC2017 from a curricular angle and (ISC)^2/CPHC document from the technology viewpoint.

Since cybersecurity is the common field targeted in both documents, mutual mapping between Knowledge Areas and Themes should be possible and an initial attempt is shown in Table I. Nevertheless, even such simple mapping shows some obvious mismatch, as the (ISC)^2/CPHC does not cover Cybersecurity Management in detail as CSEC2017 does, for example.

CSEC2017 guidelines split the architectural and system knowledge into four knowledge areas, KA2-KA5, while (ISC)^2/CPHC document defines it in two Themes. At any rate, a more detailed mapping between the two documents would be useful.

TABLE I
INITIAL MAPPING BETWEEN [1] AND [3]

Knowledge Area in CSEC2017 [1]	Theme in [3]				
Security Type	Info. & Risk	Threats & Attacks	Cyber Archit.	Secure System	Cyber Mgmt
KA1 Data	X				
KA2 Software					
KA3 Component			X		
KA4 Connection			X		
KA5 System		X		X	
KA6 Human					X
KA7 Organization					X
KA8 Societal					X

III. TWO CYBERSECURITY COURSES AT FGCU

Florida Gulf Coast University (FGCU) does not have a formal cybersecurity degree. At the time of this writing, the only two related courses offered in the undergraduate Software Engineering program are CEN 3078 Software Security and elective CEN 4930 Introduction to Cyber Security. Contents of both courses are described below, taking into account several curriculum recommendations discussed in the previous section.

A. *CEN 3078 Software Security*

There were a couple of initial assumptions when designing a syllabus for this course. First, it had to fit into the Software Engineering bachelor's degree program, as one of the required courses. Therefore, it should precede all senior level courses to allow the students an understanding of software security issues in software development. In particular, this includes senior level courses on Software Requirements Specification, Software Architecture and Design, Software Testing, and a sequence of two senior level software project courses.

The second assumption to develop the syllabus and course contents was to maintain consistency with professional guidelines, although not just with the CSEC2017 guidelines [1], but also with two other documents, which are important from the professional standpoint:

- SWECOM [4], and
- ITU-T X.800 [5].

The basic course concept follows the three-pillar OSI Security Architecture from [5]: (1) addressing potential security attacks, (2) providing security services to counteract them, and (3) implementing respective protection mechanisms. This coverage follows another idea of the X.800 document to distinguish in the attacks between their prevention, detection, and recovery, from which we selected only the first two: Prevention and Detection.

Based on this initial consideration, the following categories of topics have been included in coverage:

- regarding prevention: Cryptography, Network Security Protocols (for transport and network layers)
- regarding detection: Penetration Testing and Threat Modeling.

Then, the protection mechanisms for implementing security services are covered by discussing cybersecurity in the software development cycle: addressing Security in Software Requirements, Design for Security, and security in software construction (Security in Programming Languages, and Security in Operating Systems).

To prepare the students to understand all of these topics, of course, significant attention has to be paid to fundamental concepts of cybersecurity, definitions of respective terms and the overall context. The first lecture module is devoted to these topics and includes the following items clarifying the terminology:

- definition of “security” and a distinction between security as a system property and security as a state
- principle of a CIA triad: confidentiality, integrity and, availability
- definitions of other basic terms, including “threat” and “vulnerability.”

Another important issue to clarify at the beginning of the course is to emphasize the difference and mutual relationship between computer security and safety [4]. Basic security terms: threat, vulnerability, and breach, are compared to fundamental terms in safety: hazard, fault, and failure, with definitions taken from professional dictionaries developed by respective communities [6]-[7]. Additional clarification of these parallels can be found in [8].

Finally, a critical consideration in any college course focusing on software is the proper selection of programming exercises. At the junior level, where this course is offered, FGCU students have experience in developing small programs in Java and C/C++, but lack skills in team software development. Therefore, only individual tasks or assignments can be given, covering topics such as coding cryptographic algorithms or use of transport layer protocols.

B. CEN 4930 Introduction to Cyber Security

While CEN 3078 course was considered to focus narrowly on software security, specifically in the Software Engineering degree program, CEN 4930 was initially offered as an elective and meant to have a broader scope, to make it ultimately into the curriculum as a mandatory introductory course. In this view, its objectives are broader, and thus aligns well with the CSEC2017 guidelines.

CEN 4930 focuses primarily on cybersecurity fundamentals, and tools: terminology, risks, threats, vulnerabilities and standards associated with the transformation to a digital world and the Internet of Things (IoT). Given the seven domains of a typical IT infrastructure, bring your own device (BYOD) and the respective roles, responsibilities, and practices of users, students are taught how to assess a variety of systems by identifying risks, vulnerabilities, threats, and selecting the appropriate security controls to reduce or mitigate potential attacks.

In addition to learning the fundamental cybersecurity principles, practices and security controls, this course is augmented with a cybersecurity laboratory that reinforces the topics covered with hands-on activities. To accomplish this, students are given access to a security sandbox where they use industry adopted security tools, and are given step-by-step instructions of how to actively perform assessments, and apply a variety of security controls (reconnaissance and probing, packet capture and traffic analysis, cryptography, applying role-based access controls, etc.).

Additionally, students are given access to supporting cybersecurity materials on SEP-CyLE [9]. SEP-CyLE is a cyberlearning environment which employs a variety of Learning and Engagement Strategies (LESs) which include: gamification, problem-based learning, social interaction, and collaborative learning, to help enhance students’ understanding and encourage them to learn cybersecurity topics. On SEP-CyLE, students are assigned cybersecurity Learning Objects (LOs) and tutorials on a variety of cybersecurity principles and tools discussed in the lectures. They are required to complete this work outside of class time. Each Learning Object has a quiz which evaluates their understanding and assimilation of cybersecurity principles.

Out of several textbooks on the market, [10] was selected as its contents appear to best match the guidelines, which is reflected in Table II. The table shows the correspondence of topics in [10] with the Knowledge Areas in [1].

TABLE II
MAPPING OF KNOWLEDGE AREAS [1] TO BOOK CHAPTERS [10]

Knowledge Area in CSEC2017 [1]	Chapters in [10]												
	1	2	3	4	5	6	7	8	9	10	11	12	15
KA1 Data	x	x	x	x					x				
KA2 Software											x		
KA3 Component			x				x						
KA4 Connection										x			
KA5 System					x	x	x						
KA6 Human													x
KA7 Organization						x		x					
KA8 Societal												x	x

One other observation made during the mapping process is about terminology. Even though the general understanding of basic terms in cybersecurity is essentially consistent across the professional domains, it is not always realized that textbooks and other materials used in an academic course should quote definitions primarily from major professional sources, such as [6]-[7].

C. Mapping CSEC2017 to Course Learning Outcomes

The assumptions made in approaching the course design, in both cases outlined in subsections III-A and III-B, are only of general nature and require further specialization regarding respective mapping to Learning Outcomes that translate further into the course contents. Tables III and IV presented in this section give a more detailed view of such outcomes, showing how the CSEC2017 material has been translated into developing the specific courses at FGCU.

Table III shows the translation of CSEC2017 Learning Outcomes to those adopted in the CEN 3078 Software Security course. What is worth emphasizing is that due to the technical nature of this course, CSEC2017 Knowledge Areas, KA-6 Human Security, KA-7 Organization Security, and KA-8

Societal Security have been left out since it has very little bearing on the software profession.

TABLE III
MAPPING OF COURSE LEARNING OUTCOMES IN CEN 3078 SOFTWARE SECURITY

CSEC2017 Curriculum Essentials embracing respective Learning Outcomes	**Mapping to Course Learning Outcomes**	**Course Topics CEN 3078**
KA-5: System Security Holistic approach	Explain the challenges and scope of software security	Introduction to Software Security
	Explain basic security concepts: confidentiality, integrity, and availability	Introduction to Software Security
KA-1: Data Security Basic cryptography concepts	Understand the basics of cryptographic algorithms	Introduction to Cryptography Programming with Cryptographic Algorithms
KA-2: Software Security Security requirements and their role in design	Explain malicious software issues such as those introduced by software-based viruses	Security at the Software Requirements Stage
KA-2: Software Security Fundamental design principles	Describe the basic process of risk assessment in software development	Design for Security
KA-2: Software Security Implementation issues	Apply prevention and mitigation techniques	Security in Programming Languages Security in Operating Systems
KA-4: Connection security Software component interfaces Transmission attacks		Transport Layer Security Network (IP) Layer Security
KA-5: System Security Threat model (expressed as a Topic rather than Essential)	Use threat modeling to build software security in the design	Threat Modeling
KA-5: System Security Testing	Apply penetration techniques to study system vulnerabilities	Penetration Techniques

Table IV is meant to contain the same information for CEN 4930 Introduction to Cyber Security, as Table III does for CEN 3078, but the perspective is different. Because the textbook is used in this course, it has fixed contents, listing preselected topics without linking them to the Learning Outcomes, no direct association with CSEC2017 Essentials is possible. Instead, mapping from the specific Knowledge Areas in CSEC2017 is shown to the Learning Outcomes adopted for the course. Then, the mapping is extended to the specific topics from the textbook, listed as book chapters.

TABLE IV
MAPPING OF COURSE LEARNING OUTCOMES IN CEN 4930 INTRODUCTION TO CYBER SECURITY

CSEC2017 Curriculum Knowledge Areas embracing respective Learning Outcomes	**Mapping to Course Learning Outcomes**	**Book Chapters [10] in CEN 4930**
KA-1: Data Security KA-3: Component	Understand the fundamental cybersecurity principles, protocols, and standards	1. Information Systems Security
		2. Internet of Things
	Understand some of the common problems and solutions in the cybersecurity domain	3. Malicious Attacks, Threats, Vulnerabilities
		4. The Need for Information Security
KA-1: Data Security	Use selected cybersecurity tools and operations to implement cybersecurity principles and protocols	9. Cryptography, Testing, and Monitoring
KA-4: Connection Security		10. Networks and Communication
KA-5: System Security		5. Access Control
KA-2: Software Security	Evaluate cybersecurity breaches and provide appropriate solutions	11. Malicious Code and Activity
KA-3: Component KA-5: System Security KA-7: Organization Security KA-8: Societal Security	Understand cybersecurity hygiene, ethics, auditing, testing and management of software systems	6. Security Operations and Administration
		7. Auditing, Testing, and Monitoring
		8. Risk, Response and Recovery
		12. Information Security Standards

What is characteristic in this mapping is that non-technical Knowledge Areas KA-7 and KA-8 appear and have their counterparts both in the Course Learning Outcomes and in the book topics. So does the KA-6 Human Security, which appears in the required textbook chapter (see Table II) but is not currently covered in CEN 3078 or CEN 4930. Overall, conducting both mappings (Table III and IV) turned out to be very instructive as they reveal several opportunities for improvement in each of the Knowledge Areas being mapped:

- Learning Objectives for each course should be more tightly related to the CSEC2017 Essentials and individual Learning Objectives specified there.
- Future textbooks on Introduction to Cybersecurity should have their contents more clearly tied with the specific CSEC2017 Learning Objectives.

IV. Conclusion

The paper discussed basic course development for a new curriculum in cybersecurity. Two main curriculum guidelines, created for accreditation purposes, CSEC2007 and (ISC)^2/CPHC were discussed, including the course development process for two cybersecurity courses in a software engineering program at FGCU.

The first experience with course development is positive and both courses were successfully offered, but it points to several issues in the process. Due to a very broad scope of the cybersecurity discipline, different curricular guidelines are not necessarily consistent and curriculum developers and instructors face a challenge in selecting topics the most appropriate for their program. It also appears that the guidelines may need more time to mature. The paper does not cover the teaching support aspects of courses developed, such as exercises, labs, and assessment, because there are not enough data, yet, to analyze. This is left for future work after the courses are offered more than once.

References

[1] *Cybersecurity Curricula 2017. Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. Version 1.0*. Joint Task Force on Cybersecurity Education: ACM, IEEE-CS, AIS SIGSEC, IFIP WG 11.8. December 31, 2017.

[2] *Guidelines on Course Accreditation. Information for Universities and Colleges*. British Computer Society, The Chartered Institute for IT, May 2018.

[3] *Cybersecurity Principles and Learning Outcomes for Computer Science an IT-related Degrees: A Resource for Course Designers and Accreditors*. (ISC)^2 and The Council of Professors and Heads of Computing. Version 1.1, July 2015.

[4] *SWECOM: Software Engineering Competency Model. Version 1.0*. IEEE Computer Society, 2014.

[5] ITU-T CCITT, *Data Communication Networks: Open System Interconnection (OSI); Security Structure and Applications*. Recommendation X.800. International Telecommunication Union, Geneva, 1991.

[6] IEEE Computer Society, *Software and Systems Engineering Vocabulary*. URL: http://www.computer.org/sevocab

[7] C. Paulsen, “Glossary of Key Information Security Terms,” Draft Report NISTIR 7298 Rev. 3. National Institute of Standards and Technology. URL: https://csrc.nist.gov/publications/detail/nistir/7298/rev-3/draft

[8] J. Zalewski, “IoT Safety: State of the Art,” *IT Professional*, vol. 21, no. 1, January/February 2019, in press.

[9] I. A. Buckley and P. J. Clarke. “An Approach to Teaching Software Testing Supported by two Different Online Content Delivery Methods”, Proceedings of the 16th LACCEI International Multi-Conference for Engineering, Education and Technology. July 18-20, 2018. URL: http://www.laccei.org/LACCEI2018-Lima/meta/FP377.html

[10] D. Kim, M.G. Solomon, *Fundamentals of Information Systems Security. 3rd ed*. Burlington, Mass.: Jones and Bartlett, 2016.