Case Study: Mapping an E-Voting Based Curriculum to CSEC2017

Muwei Zheng
The University of California, Davis
Davis, United States
mzheng@ucdavis.edu

Nathan Swearingen
Indiana University-Purdue University Indianapolis
Indianapolis, United States
nswearin@iupui.edu

Steven Mills
Indiana University-Purdue University Indianapolis
Indianapolis, United States
sdmills@iupui.edu

Croix Gyurek
Indiana University-Purdue University Indianapolis
Indianapolis, United States
crgyurek@iupui.edu

Matt Bishop
The University of California, Davis
Davis, United States
mabishop@ucdavis.edu

Xukai Zou
Indiana University-Purdue University Indianapolis
Indianapolis, United States
xzou@iupui.edu

ABSTRACT

An electronic voting (E-voting) oriented cybersecurity curriculum, proposed by Hostler *et al.* [4] in 2021, leverages the rich security features of E-voting systems and E-voting process to teach essential concepts of cybersecurity. Existing curricular guidelines describe topics in computer security, but do not instantiate them with examples. This is because their goals are different. In this case study, we map the e-voting curriculum into the CSEC2017 curriculum guidelines, to demonstrate how such a mapping is done. Further, this enables teachers to select the parts of the e-voting curriculum most relevant to their classes, by basing the selection on the relevant CSEC2017 learning objectives. We conclude with a brief discussion on generalizing this mapping to other curricular guidelines.
Topics: Graduate studies/undergraduate studies, ACM and IEEE-CS Curricula, Curriculum Issues

CCS CONCEPTS

• **Security and privacy** → *Software and application security*; *Human and societal aspects of security and privacy*.

KEYWORDS

Electronic Voting System, Cybersecurity Education, CSEC2017 Guideline, Cybersecurity curriculum

ACM Reference Format:
Muwei Zheng, Nathan Swearingen, Steven Mills, Croix Gyurek, Matt Bishop, and Xukai Zou. 2023. Case Study: Mapping an E-Voting Based Curriculum to CSEC2017. In *Proceedings of the 54th ACM Technical Symposium on Computer Science Education V. 1 (SIGCSE 2023), March 15–18, 2023, Toronto, ON, Canada.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3545945.3569811

1 INTRODUCTION

Cybersecurity programs use real-world situations and examples to support teaching the principles, concepts, and practice of cybersecurity. By tying cybersecurity studies to current events and well-known problems, students see how what they learn can be applied both to the situations discussed and to new ones. One recurring event that involves everyone, whether they participate or not, is voting in elections. Common to all democracies and republics, the goal of an election is to ensure that the body politic chooses its leaders. Hence elections are critically important.

Hostler *et al.* [4] introduced a cybersecurity program based on an electronic voting (e-voting) system. Such a system must provide the basics of security, but some in an unusual way. For example, an election system must allow people to vote anonymously, and anonymity in security is common. Much less common is the requirement that one *cannot* prove to another how they voted. The particular e-voting system used [9], a mutual restraining e-voting system, allows remote voting, which introduces a plethora of other cybersecurity problems. The civic nature of elections, in particular the laws and regulations controlling them, and the practices that vary from one election jurisdiction to another, also allow the introduction of non-technical material that constrains what techniques of cybersecurity are allowed. Thus, this environment provides for the use of security in typical and non-typical ways.

A key question of any proposed educational proposal is whether it covers sufficient material to meet the goals of the program. This paper maps the cybersecurity program proposed by Hostler *et al.* [4] to the Cybersecurity Curricular Guidelines [2] developed by a joint task force of the ACM, IEEE Computer Society, the AIS special interest Group on Security, and the International Federation of Information Processing Societies' Working Group 11.8, dealing with computer security education. Section 2 reviews related work, section 3 explains the rationale for the curriculum in more detail, and section 4 the learning objectives of the modules. Section 5 presents a mapping of the learning objectives onto the CSEC 2017 guidelines, and section 6 concludes with some remarks about the current and future work.

2 RELATED WORK

Education in cybersecurity has been growing. In 2001, the ACM Curriculum Guidelines for Undergraduate Degree Programs in Computer Science [5] included "security" as part of its operating systems body of knowledge, and as a core component of net-centric computing. In the 2013 revision of the guidelines [1], Information Assurance and Security was its own knowledge area. The Cybersecurity

SIGCSE 2023, March 15–18, 2023, Toronto, ON, Canada

ACM ISBN 978-1-4503-9431-4/23/03.
https://doi.org/10.1145/3545945.3569811

Curriculum Guidelines [2] expanded and revised the information assurance and security parts of those curriculum guidelines.

In 1997, the US National Security Agency began a program of Centers of Academic Excellence (CAEs) in cybersecurity. Seven institutions were designated initially, each meeting requirements drawn from government needs. The program expanded, and when the US Department of Homeland Security was created, it jointly sponsored the Centers program with the NSA. Recognizing the academic nature of the institutions, the original government-specific requirements evolved into a more academic set of knowledge areas and units, and institutions were required to satisfy foundational core units, technical or non-technical core units and some elective units [8].

3 BENEFITS OF THE E-VOTING CURRICULUM

Using an electronic voting system as the basis for a curriculum has many advantages. E-voting systems have many usual, and unusual, security requirements drawn from the practices used in elections. These requirements range from the technical (for example, the e-voting system must restrict the actions of voters to casting votes) to the legal (for example, a voter-verified paper audit trail must be kept for 22 months). The project-oriented curriculum allows the students to put what they learn into practice, thereby reinforcing the concepts by applying them. The structure of the curriculum is designed in a way that allows different modules to be used as the instructor desires, and these blocks can be expanded. Also, the curriculum speaks to the important topic of elections, which ties the academic work into "real life".

3.1 Rich Security Features

The voting process involves many people in different roles. Each person has their own expectations of how the E-voting system should be used. Voters want it to be convenient, accurate, reliable, and protect ballot secrecy. System administrators want it to be secure, resilient, and easy to administer and maintain. Election officials, auditors, and other parties all have different requirements. Many of the requirements are contradictory. For example, how does one audit a system (election) where particular actions (how voters vote) or artifacts (ballots) must be disassociated from the user (voter)? The combination makes the E-voting system have a rich feature in security mechanisms. Therefore, it is a curriculum that is valuable for students to learn from.

3.2 Interactive Teaching and Learning

Studies show that interactive learning has positive impacts on student learning outcomes [6, 7]. The E-voting cybersecurity curriculum also adopts interactive teaching and learning approach. As mentioned above, different parties are involved in voting. Students can play the roles of these parties and interact with each other as the parties would interact with one another. Attacker-versus-defender is a classic pair. Another example could be that legitimate voters verify their votes, while system administrators prove that voters' identities cannot be associated with particular ballots. The role playing makes students better understand the security mechanisms introduced in the curriculum.

3.3 Composable Modules

The curriculum consists of composable educational units that can be combined in various ways. Each unit, or set of units, covers a particular topic in such a way that the units build upon one another. Thus, they can be used in non-security courses to teach (for example) network or software security, or to build a computer security course. Such a course may be general, covering many aspects of security using the first few units from each module, or a specialized course using units from one particular module such as software security. The interactive projects within the blocks entice and enable students to fully engage in the entire learning process and more efficiently learn to master cybersecurity knowledge and skills.

3.4 Extensibility

The modular curriculum structure enables new techniques and research findings to be added to the curriculum. It also covers the spectrum of cybersecurity issues. For example, the E-voting system involves both highly secure computation systems (at the servers) and lowly secure computation systems (at the voting area), so cybersecurity practices for either or both types of systems can be included. These factors contribute to the extensibility of the curriculum, allowing it to change with new advances in cybersecurity.

3.5 Civic Education about Elections

Elections are the cornerstone of democratic societies, and key to their success is that citizens vote. This means voters need access to however they cast their vote, and that they trust their votes, and those of others, will be counted accurately, that the final count decides the election, and that those as well as all of the required protections are in place. This is easy to achieve with paper ballots the voters fill in, as the entire process can be observed from the setting up of the voting stations to the canvass.[1] But with E-voting, the part of the election process in the computer system cannot be directly observed. Hence voters must understand why they should trust the E-voting system(s). The modules can be taught at many levels, ranging from the non-technical focusing on civic matters to the technical such as secure computation. In the process of studying, perhaps more young scholars can be attracted to study in the E-voting field to make it more robust and reliable.

4 LEARNING OBJECTIVES OF E-VOTING CURRICULAR MODULES

The E-voting curriculum can fit into, or use, topics from other established cybersecurity curricula due to its composable structure, instructors may choose any topics they are familiar with. To attain a measure of consistency, the following learning objectives are associated with each module.

Module 0: Introduction to E-Voting.

0.1 Understand different types of E-Voting systems.
0.2 Understand different parties involved in an E-Voting process.
0.3 Understand law and policy requirements for E-Voting systems.

[1] Except, of course, for watching a voter vote.

0.4 Understand different threats to elections using E-Voting systems.
0.5 Describe different components of an E-Voting system.
0.6 Explain the main security concerns of E-Voting systems and appropriate defenses.

Module 1: Authentication.

1.1 Explain the similarities and differences of common authentication methods.
1.2 Describe how voters authenticate themselves.
1.3 Describe common security concerns of authentication systems, and their defenses.
1.4 Understand software security principles and practices of robust, secure coding.
1.5 Explain challenges to authenticate users on untrusted or compromised systems.

Module 2: Confidentiality.

2.1 Understand basic cryptography concepts.
2.2 Describe public key cryptography and algorithms.
2.3 Describe how public key cryptography is used in end-to-end encryption protocols, and how this protection might be countered.
2.4 Describe ways to store sensitive information and best practices to do so.
2.5 Explain the importance of organizational security and human security, and why social engineering is often used to compromise well protected systems.
2.6 Describe laws and regulations regarding security breaches.
2.7 Describe the proper procedure to delete sensitive data or to dispose of systems with sensitive data.

Module 3: Data integrity and message (sender) authentication.

3.1 Understand different ways to generate and use hash functions.
3.2 Describe techniques used to store protected data and to verify or compute them without revealing sensitive information.
3.3 Describe certification criteria for E-voting systems.
3.4 Describe the challenges of maintaining a secure system life cycle.
3.5 Describe how monitoring and access controls are used to protect a system.

Module 4: Cryptographic Key Management.

4.1 Describe common key exchange protocols.
4.2 Describe common random number generation algorithms and their weaknesses.
4.3 Explain how secret keys are used in proofs of identity, integrity protection mechanisms, and challenges in doing so.
4.4 Explain attacks targeting key exchange protocols or key management.

Module 5: Privacy and anonymity.

5.1 Describe privacy and anonymity concerns in voting. Explain how these are different from concerns in other industries like the health industry and banking.
5.2 Describe the procedures taken in elections to protect voter privacy.
5.3 Understand common techniques used to preserve anonymity in a network.
5.4 Explain techniques used to help voters verify their votes being recorded correctly without being able to reveal those votes.
5.5 Explain how data mapping is used to compromise privacy and anonymity.
5.6 Explain the trade-off between security techniques and legal considerations.

Module 6: Access Control.

6.1 Describe common access control methods such as discretionary access control(DAC), mandatory access control (MAC), role-based access control (RBAC), and originator-based access control (ORCON).
6.2 Explain the access control mechanisms used in the E-voting system.
6.3 Explain how different devices access each other in the E-voting system.
6.4 Explain access rights of various parties involved in the E-voting system.
6.5 Describe how monitoring and logging can be used to enforce access control.
6.6 Describe challenges for access control if online voting is allowed.

Module 7: Secure Group/Multi-Party Interaction and Secret Sharing.

7.1 Describe schemes for multi-party secret sharing.
7.2 Describe how these schemes handle insider threats.
7.3 Explain how these schemes protect transmissions of shares.
7.4 Explain security challenges to widely deploying these techniques in online voting.
7.5 Explain non-technical challenges in using multi-party secret sharing in online voting.

Module 8: Secure Multi-Party Computation and Homomorphic Encryption.

8.1 Describe different schemes for secure multi-party computation.
8.2 Describe how to ensure the correctness of the result when there is a small percentage of adversarial participants in a secure multi-party computation.
8.3 Explain how voters can verify the correctness of the results of the election.
8.4 Explain security challenges to widely deploy these techniques in online voting.

Module 9: Attacks and defenses.

9.1 Understand the laws and ethics involving red team tests.
9.2 Understand how monitoring and documentation is used in red team tests.
9.3 Understand how to construct a framework to exploit a vulnerability in a system.
9.4 Simulate different attacks targeting E-Voting systems.

9.5 Explain different metrics to analyze cyber-risks; understand how to do risk management.
9.6 Understand how to do strategy and planning.
9.7 Understand different techniques to detect an attack.
9.8 Understand basic digital forensics to analyze an attack.
9.9 Understand system recovery from an attack.
9.10 Understand laws and regulations about revealing an attack after it happens.

Learning objectives may be met at levels appropriate for students in different majors. For example, students will learn how to store confidential information in Module 2. Those with majors other than Computer Science only need to know intellectually what the best practice is and why it is used. Students in a Computer Science major but not specializing cybersecurity may need to know how to implement those practices and why they are better than other alternatives. Finally, students specializing in cybersecurity need to further understand that system-wide deployment of access controls are necessary for such best practices to work properly. The E-voting curriculum emphasizes equally promoting education of elections using E-voting systems and teaching cybersecurity. Learning objectives with non-technical students may focus more on the former, while the goals with technical students may focus more on the latter.

The topic mapping itself can be considered an interaction between students and a real world application. Students are introduced to voting technology and analyze the properties of such an application and the security requirements of E-voting. Then they bring their understanding of the topics by mapping different concepts and activities into E-voting systems. This will help students understand the overall picture of cybersecurity and its related topics at the very beginning, and accelerate students' learning these topics throughout the class.

5 MAPPING TO CSEC-2017 CYBERSECURITY CURRICULUM

The E-voting curriculum covers all the fundamental, and many advanced, topics of cybersecurity. Demonstrating this requires mapping the curriculum into existing guidelines and ensuring the key learning objectives of those guidelines are satisfied. CSEC2017 [2] is such a standard set of cybersecurity curriculum guidelines. It defines eight Knowledge Areas (KAs), each composed of different Knowledge Units (KUs) broken into topics. The CSEC2017 guidelines list the topics in the KAs in detail, so it is unlikely that any single cybersecurity curricula could cover everything, but each KA has a set of "essential learning objectives" that any cybersecurity course or program should address. These capture the cybersecurity proficiency that every student needs to achieve regardless of program focus. Thus, when we integrate the E-voting curriculum with CSEC2017, the resulting curriculum has to cover the essentials from CSEC2017. Below is a mapping between the CSEC2017 guideline and the E-voting curriculum learning objectives. The mapping goes in two directions. In one direction, instructors could use the relevant topics in the CSEC2017 guidelines to expand course materials in the E-voting modules. In particular, they could present security concerns of different computing systems like health-care systems, banking systems, and so forth, related to the module being studied. In the opposite direction, instructors could use the E-voting system and election process as examples to demonstrate ideas in the CSEC2017 guidelines. Thus, the CSEC2017 guidelines provide fundamentals, basics, and advanced topics that can be combined with real world examples of E-voting. This approach helps students to correlate their knowledge to real world applications and to more easily understand the materials.

For reasons of space, we explain only one mapping for each direction. The full mapping with comments is available on the web.[2] In the table, essentials for each CSEC2017 knowledge area are mapped to E-voting curriculum module learning objectives.

CSEC2017 Knowledge Area (KA)	CSEC2017 KA's Essentials	E-voting Curriculum Module Learning Objectives
Data Security	Cryptography concepts	2.1, 2.2, 2.3, 3.1, 4.1, 4.3, 7.1, 7.3, 8.1, 8.3
	Digital forensics	2.7, 4.4, 9.8
	Data integrity and authentication	1.1, 1.3, 3.1, 3.2, 3.5, 4.4, 6.6, 9.4, 9.7
	Information storage security	2.7, 3.2, 3.5, 5.1, 5.5, 5.6, 9.1, 9.4, 9.8
Software Security	Fundamental design principles	1.4
	Security requirements and their role in design	0.3, 0.4, 0.6, 1.3, 5.1, 5.6, 9.3, 9.6
	Implementation issues	1.4, 3.4, 5.5, 9.3, 9.4
	Static and dynamic testing	2.3, 3.3, 6.5, 9.1
	Configuring and patching	1.1, 3.3, 3.4, 6.3, 6.4, 6.6, 9.6, 9.7
	Ethics, especially in development, testing and vulnerability disclosure	0.3, 5.6, 6.4, 9.1, 9.10
Component Security	Vulnerabilities of system components	0.5, 1.5, 2.3, 2.4
	Component lifecycle	0.5, 3.4
	Secure component design principles	0.4, 6.3
	Supply chain management security	2.3, 3.3, 3.4, 4.1, 6.3
	Security testing	1.4, 2.4, 3.2, 3.3, 6.2, 9.2, 9.3
	Reverse engineering	3.4, 9.4
Connection Security	Systems, architecture, models, and standards	0.1, 0.5
	Physical component interfaces	0.5, 1.5, 9.4
	Software component interfaces	1.4, 2.4, 3.3, 3.4, 9.4
	Connection attacks	1.5, 2.3, 4.3, 4.4, 7.3, 8.2, 9.4

[2] *http://cs.iupui.edu/~xzou/NSF-EVoting-Project/CSEC2017Mapping.pdf*

	Transmission Attacks	1.5, 2.3, 4.3, 4.4, 7.3, 8.2, 9.4
System Security	Holistic approach	0.1, 0.6, 2.4, 3.2, 5.1, 5.4, 6.2
	Security policy	0.1, 0.6, 1.1, 1.3, 3.2, 5.1, 6.1, 6.2
	Authentication	1.1, 1.2, 1.3, 1.5, 2.3, 2.4, 3.5, 4.3, 7.1, 8.1
	Access control	0.2, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6
	Monitoring	0.6, 2.4, 3.5, 6.5, 9.2
	Recovery	0.5, 0.6, 2.4, 3.2, 9.9
	Testing	1.4, 3.3, 6.2, 6.3, 9.1, 9.2, 9.3
	Documentation	0.1, 1.4, 9.1, 9.2
Human Security	Identity Management	0.2, 0.5, 1.2, 6.3, 6.4, 6.5, 6.6
	Social engineering	1.3, 2.5, 9.6, 9.9
	Awareness and understanding	2.5, 9.5, 9.6, 9.9
	Social behavioral privacy and security	5.1, 5.4, 5.5, 5.6
	Personal data privacy and security	2.6, 5.1, 5.5, 5.6
Organizational Security	Risk management	0.1, 0.4, 0.6, 1.5, 7.2, 8.2, 9.5
	Governance policy	0.1, 0.4, 2.4, 3.2, 3.3, 5.2, 5.4, 6.2
	Laws, ethics, and compliance	0.3, 2.6, 5.1, 5.6, 9.1, 9.10
	Strategy and planning	0.2, 3.4, 9.6
Societal Security	Cybercrime	0.4, 0.6, 1.5, 2.5, 3.4, 7.2, 8.2, 9.4, 9.8
	Cyber law	0.3, 2.6, 5.1, 5.6, 9.1, 9.10
	Cyber ethics	9.1, 9.10
	Cyber policy	2.6, 5.6
	Privacy	5.1, 5.2, 5.3, 5.5, 5.6

The philosophy behind the E-voting curriculum is very different from the one behind the CSEC2017 guidelines. In the E-voting curriculum, there is a specific system, the E-voting system, that serves as the motivator. So each module starts with one aspect of this particular system, and then explores broader and deeper topics. However, the CSEC2017 guidelines are not based on any particular system, so each topic can be dealt with on its own. As a result, there is not a one-to-one relationship between the E-voting curriculum learning objectives and the CSEC2017 guidelines essential topics, even though some share the same naming. For example, Module 6, which shares name with a KU in the Data Security KA, should also relate to topics in Connection Security, System Security, Organizational Security, and Human Security. In a real system, especially a system with so many different parties involved like the E-voting system, access control can be very complicated. Beyond the overall access control model (MAC, DAC, RBAC, ORCON, and so forth), many other considerations arise, such as connections among devices, remote user access, staff security training, irregular access monitoring, and privacy concerns.

The difference of the philosophy brings the difference in the focus. The E-voting curriculum emphasizes interactive learning, while the CSEC2017 guidelines are more general and not intended to be a curriculum (hence the term "guidelines" in its title). The E-voting curriculum has a designated system from the beginning, so all hands-on projects can be done on a single type of system. Students will observe how different parts of the system interfere with each other to complicate the security problems. It is a more holistic approach to learn cybersecurity. The CSEC2017 guidelines suggest security practices about the same problem from different systems can be compared in a curriculum based on those guidelines.

5.1 Example Mapping From E-voting Curriculum: Module 3

Module 3 in the E-voting curriculum focuses on the protection of integrity of the system. Among other topics, it covers the integrity of data stored in the system, the integrity of data transmitted into or out from the system, the integrity of the software of the system, and the integrity of the access to the system itself. It has the following 5 learning objectives:

(1) Understand different ways to generate and use hash functions.
(2) Describe techniques used to store protected data and to verify or compute them without revealing sensitive information.
(3) Describe how an E-voting system is certified for use.
(4) Describe the challenges of maintaining a secure system life cycle.
(5) Describe how monitoring and access controls are used to protect a system.

Learning goal 1 (LG1) focuses on the cryptography background of the checking and ensuring the integrity of the data. Unlike writing documents, digital data is easy to copy and modify, so it is necessary for students to understand the usage of encryption, message authentication codes, and digital signatures to protect the integrity. Thus, it is related to the *Cryptography Concepts* and the *Data Integrity and Authentication* essentials in the *Data Security* KA in CSEC2017.

LG2 focuses on storing ballots in the system. It involves many security domains. How to store sensitive information and verify its integrity in general is related to the *Data Integrity and Authentication* and *Information Storage Security* essentials in *Data Security*. After that, the specific requirements of storing ballots, which requires they not be revealed before a certain time, and can be verified by a voter without revealing its contents, relate it to *Governance and Policy* in the*Organizational Security* KA and is a good example to discuss in the *Security Policy* topic in the *System Security* KA. Accessing the ballots can be done by voters, election officials, or even local judges. The timing of access to the ballots is also relevant, so *Security Testing* in the *Component Security* KA and *Holistic approach* in the *System Security* KA also have to be mentioned. Finally, the recovery plan from an accident binds it to *Recovery* in the *System Security* KA.

LG3 focuses on ensuring the security of the system. All US states require that voting systems are certified before they can be used, and any changes require recertification. The details vary among states. This is a case of *Governance and Policy* in the *Organizational Security* KA. To be certified, a voting system must demonstrate that its software and hardware and associated procedures, meet specific criteria. This leads to a discussion of practices in *Supply Chain Management Security* in the *Component Security* KA, *Configuring and Patching* in the *Software Security* KA, and *Software Component Interfaces* in the *Connection Security* KA. Different ways to test the system, which is part of the certification process, include *Static and Dynamic Testing* in the *Software Security* KA, *Testing* in the *System Security* KA, and *Security Testing* in the *Component Security* KA.

LG4 focuses on keeping a working E-voting system working. This is perhaps the most challenging part. Configuring the system and the software to minimize the attack surface would be covered in *Configuring and Patching* in the *Software Security* KA and *Software Component Interfaces* in the *Connection Security* KA. Similarly, how to handle updating the system securely is covered by *Configuring and Patching* as above, and *Supply Chain Management Security* in the *Component Security* KA. *Component Lifecycle* in the *Component Security* KA covers retiring a system used in elections. Differences between secure, robust coding initially and adding security through patching is covered in *Implementation Issues* in the *Software Security* KA. At the managerial level, *Strategy and Planning* in the *Organizational Security* KA and *Cybercrime* in the *Societal Security* KA are all relevant.

LG5 focuses on the use of monitoring and access control. As discussed before, the access control of the E-voting system is more complicated than normal systems due to many different parties using it, and the type of access required by each. Thus, *Data Integrity and Authentication* and *Information Storage Security* in the *Data Security* KA, and *Authentication* and *Monitoring* in the *System Security* KA can cover this topic.

5.2 Example Mapping From CSEC2017: Data Security

This example uses materials in CSEC2017 to map into the E-voting curriculum. The *Data Security* Knowledge Area is focused on the protection of data at rest, during processing, and in transit [2]. It has the following essential topics:

(1) Cryptography Concepts
(2) Digital Forensics
(3) Data Integrity and Authentication
(4) Information Storage Security

Essential 1 (E1) covers cryptography concepts and algorithms and their usage. Many topics in the E-voting curriculum are directly related to cryptography, including the Confidentiality Module (LG 2.1, 2.2, 2.3), Integrity Module (LG 3.1), Key Management Module (LG 4.1, 4.3), Secure Multi-party Communication Module (LG 7.1, 7.3), and Secure Multi-party Computation Module (LG 8.1, 8.3). Topics from these modules not only cover algorithm and their implementation, but also a wide variety of real world applications of cryptography. This provides examples to fulfill the educational purpose of this essential topic.

E2 introduces the application of digital forensics in data security. Digital forensics is directly related to the Attacks and Defenses Module (LG 9.8), and is also related to other modules such as the Confidential Module and the Key Management Module. Forensics techniques can be used to retrieve deleted data in the disk or system running information in the memory; therefore knowing how to avoid a data breach from an attacker employing these techniques is essential in the E-voting system (LG 2.7). Another widespread usage of forensics tools is the cracking of passwords or encryption protection. This makes digital forensics also an important issue to consider in key compromise attacks (LG 4.4)

E3 covers data integrity and authentication. This is covered in depth in the Authentication Module (LG 1.1, 1.3) and the Integrity Module (LG 3.1, 3.2, 3.5). Access control also plays a role here, including how people and devices authenticate to a device (LG 6.6). Besides concepts and implementations, attacks are covered in the Key Management Module (LG 4.4) and the in the Attacks and Defenses Module (LG 9.4, 9.7).

E4 also discusses information storage security but from a systems view. It includes disk and file encryption, data erasure, data masking, database security, and data security law. Disk and file encryption can be found in the Integrity Module (LG 3.2). Data erasure is covered in the Confidentiality Module (LG 2.7). Data masking and its privacy concerns are discussed in the Privacy Module (LG 5.1, 5.5). Database security including attacks and defense are covered in LG 3.5, 9.4, and 9.8. Finally, LG 5.6, 9.1 cover issues of law and regulations.

From these two mappings, we see that the E-voting curriculum covers the essential learning objectives identified in the Data Security KA of CSEC2017, and CSEC2017 identifies key learning objectives in the E-voting curriculum. Although born from different philosophies, the two mesh well together.

6 CONCLUSION

This paper has presented a mapping of the E-voting curriculum to the CSEC2017 guidelines. As mentioned above, the CAE knowledge units [8] are also widely used, and their organization and structure are fundamentally different than those of CSEC2017 [3]. So the next step is to map the E-voting curriculum onto those knowledge units. That will make the E-voting curriculum useful to academic institutions that wish to be certified or recertified as Centers of Academic Excellence in cybersecurity.

The more students learn about cybersecurity, the better they will understand how this interconnected, computerized society works. And the more they understand the security of elections in general and E-voting systems in particular, the more they will understand the need to, and ways to, protect the security of elections, and thereby the security of their country and society.

ACKNOWLEDGMENTS

This material is based upon work supported by the National Science Foundation under Grant Nos. DGE-2011117 and DGE-2011175. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

REFERENCES

[1] ACM/IEEE-CS Joint Task Force on Computing Curricula. 2013. *Computer Science Curricula 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science.* Technical Report. ACM, New York, NY, USA. https://www.acm.org/binaries/content/assets/education/cs2013_web_final.pdf

[2] ACM/IEEE-CS/AIS SIGSEC/IFIP WG 11.8 Joint Task Force. 2017. *Cybersecurity Curricula 2017: Curriculum Guidelines for Undergraduate Degree Programs in Cybersecurity.* Technical Report Version 1.0. ACM, New York, NY, USA. https://doi.org/10.1145/3184594

[3] Wm. Arthur. Conklin and Matt Bishop. 2018. Contrasting the CSEC 2017 and the CAE Designation Requirements. In *Proceedngs of the 51st Hawaii International Conference on System Sciences*. 2435–2441.

[4] Ryan Hosler, Xukai Zou, and Matt Bishop. 2021. Electronic Voting Technology Inspired Interactive Teaching and Learning Pedagogy and Curriculum Development for Cybersecurity Education. In *IFIP World Conference on Information Security Education*. Springer, 27–43.

[5] IEEE-CS/ACM Jpint Task Force on Computing Curricula. 2001. *Computing Curricula 2001 Computer Science.* Final Report. ACM, New York, NY, USA. https://www.acm.org/binaries/content/assets/education/curricula-recommendations/cc2001.pdf

[6] D. A. Kolb. 1984. Experiential Learning: Experience as the source of learning and development. *Englewood Cliffs, NJ, Prentice Hall* (1984).

[7] D. Laurillard. 2002. Rethinking university teaching: a conversational framework for the effective use of learning technology, 2nd Edition. *London, RoutledgeFarmer* (2002).

[8] U.S. National Security Agency and U.S. Department of Homeland Security. 2019. 2019 Knowledge Units.

[9] Xukai Zou, Huian Li, Yan Sui, Wei Peng, and Feng Li. 2014. Assurable, Transparent, and Mutual Restraining E-Voting Involving Multiple Conflicting Parties. In *Proceedings of the 2014 IEEE Conference on Computer Communications (IEEE INFOCOM 2014)*. IEEE, Piscataway, NJ, USA, 136–144.