Strengthening Workforce Education: Excellence in Programming Securely (SWEEPS)

Deborah Kariuki
Department of Education, University of Maryland, Baltimore County, Baltimore, MD, USA
dkkariuki@gmail.com

Matt Bishop†
Department of Computer Science, University of California, Davis, Davis, CA, USA,
mabishop@ucdavis.edu

Jenny Daugherty
Dark Enterprises, Inc., Lafayette, IN, USA
jenny.daugherty@darkenterprisesinc.com

Phillip Nico
Department of Computer Science and Software Engineering, California Polytechnic State University, San Luis Obispo, San Luis Obispo, CA, USA
pnico@calpoly.edu

Ida Ngambeki†
Department of Information Systems, University of Maryland, Baltimore County, Baltimore, MD, USA
idan1@umbc.edu

Xiaoyan Sun†
Department of Computer Science, Worcester Polytechnic Institute, Worcester, MA, USA
xsun7@wpi.edu

Alex Lowrie
Continuing and Professional Education, University of California, Davis, Davis, CA, USA
awlowrie@ucdavis.edu

Jun Dai†
Department of Computer Science, Worcester Polytechnic Institute, Worcester, MA, USA
jdai@wpi.edu

Melissa Dark
Dark Enterprises, Inc., Lafayette, IN, USA
melissa.dark@darkenterprisesinc.com

Markus Geissler
Computer Information Science, Cosumnes River College, Sacramento, CA, USA
geisslm@CRC.losrios.edu

Arshad Noor
StrongAuth, Inc., Cupertino, CA, USA
arshad.noor@strongkey.com

Abstract

This paper presents and advocates for an initiative to expand access to secure programming education. The Strengthening Workforce Education: Excellence in Programming Securely (SWEEPS) initiative, funded by the National Centers of Academic Excellence in Cybersecurity (NCAE-C) program, seeks to advance secure programming and help achieve security aims. SWEEPS establishes a secure programming curriculum and workforce development coalition of seven institutions across two CAE (Center of Academic Excellence) regions (Northeast and Southwest) and five states (California, Massachusetts, Maryland, Indiana, and North Carolina). This coalition includes industry-based stakeholders collaborating with the US Army and government agencies on various projects. SWEEPS draws on prior work establishing critical concepts in secure programming, assessment tools, learning aids, and system infrastructure. The initiative offers a series of interconnected, stackable learning experiences tailored for early to mid-career professionals looking to enhance their cybersecurity skills. These experiences, which include practical one-day workshops and comprehensive year-long graduate certificates, provide a reassuring path for upskilling in secure programming. This paper recommends the efficacy of stackable training approaches in secure programming by exploring the practices of targeting and training individuals with diverse proficiency levels of programming experience who would benefit from increased knowledge and training.

CCS Concepts

• Security and privacy → Software and application security.

Keywords

Secure Programming; Workforce Development; Education

† Corresponding authors: Drs. Jun Dai, Matt Bishop, Ida Ngambeki, and Xiaoyan Sun.

SIGCSE TS 2025, February 26-March 1, 2025, Pittsburgh, PA, USA.

ACM ISBN 979-8-4007-0531-1/25/2.
https://doi.org/10.1145/3641554.3701897.

ACM Reference format:

Deborah Kariuki, Ida Ngambeki, Jun Dai, Matt Bishop, Xiaoyan Sun, Melissa Dark, Jenny Daugherty, Alex Lowrie, Markus Geissler, Phillip Nico and Arshad Noor. 2025. Strengthening Workforce Education: Excellence in Programming Securely (SWEEPS). In *Proceedings of the 56th ACM Technical Symposium on Computer Science Education V. 1 (SIGCSE 2025), February 26-March 1, 2025, Pittsburgh, PA, USA.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3641554.3701897

1 Introduction

Since 1970, the secure programming landscape has yet to permeate beyond academic research halls. The quality of most software products could be better. Most software needs to react better to unexpected inputs or changing environments. The results have been program and system failures. While such failures may merely frustrate home users, their occurrence in large systems can be devastating, leading to significant compromises and data loss.

These major software disruptions are becoming more common and more devastating. A case in point is the latest CrowdStrike incident on July 19, 2024, which Microsoft describes as "one of the worst IT outages impacting over 9 million computers worldwide. Among the most heavily affected industries were hospitals, airlines, banks, and business." Another good example is the Heartbleed vulnerability [1]. In 2014, a vulnerability that allowed someone to read a buffer containing the private information of a previous user was discovered as a failure to validate bounds. The problem was exacerbated by the OpenSSL version of SSL/TLS being widely used commercially. OpenSSL is a free and widely used version of SSL/TLS. It was estimated that about 66% of all web servers used OpenSSL, including several large commercial and financial companies [2]. In fairness to the authors of OpenSSL, this program was maintained by volunteers who had regular jobs, so overlooking such a check is understandable.

Enforcing secure programming practices has become crucial for reducing software vulnerabilities. Various sectors, such as private industries, educational institutions, and governments, strive to ensure their programs are secure in modern software development and to increase the workforce trained in these concepts and practices. SWEEPS addresses this objective through diverse, secure programming education modalities and targeting underserved communities nationwide to upscale their skills.

To strengthen workforce education, the SWEEPS project creates stackable learning modalities that will be offered as workshops, undergraduate certificate programs, or training camps at participating universities. These offerings will cater to the needs of both traditional and non-traditional students, ensuring that diverse groups benefit from this initiative to establish a secure programming workforce. The modalities are designed to meet the different skill levels of project participants. Also, it will give participants a choice of time and geographical locations to participate in these various learning modalities.

Recruitment priority will be given to active, transitioning military personnel, veterans, and first responders. Approximately 700 participants are expected to receive training through this project from the summer of 2024 to the summer of 2026. Significant efforts will be made to recruit from typically underserved areas, including rural and economically depressed regions and communities underrepresented [7] in programming careers, to foster a diverse and well-trained secure programming workforce.

It is well established that adding security after the products are built and deployed offers a different level of protection than building secure infrastructure at the beginning of the process [3]. Many types of malwares (such as Triton, Pipedream, and Blackenergy [4]) are designed to target programmable ladder controllers (PLCs) and industrial control systems (ICS), which are the programs running much of the nation's infrastructure, leaving them vulnerable to attack. Thus, the need and proof of the importance of the SWEEPS solution is evident to address the demand for well-trained, diverse, skilled professionals to upskill in secure programming through behaviorism and constructivism training built in the various modalities of SWEEPS curriculum.

2 Background and Context

SWEEPS initiatives have been designed based on the coalition's previous research and education work in secure programming. The work includes three significant projects, which will be foundations to SWEEPS, fulfilling roles respectively as a modality, an assessment tool, and an evaluation platform. The first project was the "*Secure Programming Clinic*" (SPC) project, which was sponsored by the National Science Foundation (NSF) and ran from August 2014 to July 2019. The project created and tested a secure programming clinic mechanism that helped enhance student learning and expertise in writing robust and secure software, similar to a writing clinic in an English department or law school. The second project was the "*Secure Programming Concept Inventory*" (SPCI) project, sponsored by the NSA Cybersecurity Core Curricula (CCC) Program and ran from Sep 2017 to Sep 2019. The project developed the first concept inventory in the secure programming field, which was an assessment tool designed to measure an individual's understanding of concepts in the knowledge domain of secure or defensive programming. The third project, called "*Secure Programming Intelligent Tutoring System*" (SecTutor), has been sponsored by NSF since October 2019 and will be completed in September 2025. The project develops a dual-purpose adaptive testing and intelligent tutoring system named "SecTutor" to make secure programming training adaptive and intelligent. SPC, SPCI, and SecTutor are elaborated in Section 4.2

This project builds on the coalition's prior work, including the clinic model, concept inventory, and the SecTutor system, to develop secure programming curricula and workforce development activities. The program aims to:

1. Implement clinics at three universities, accessible to both coalition and non-coalition institutions.
2. Host eight one-day workshops.
3. Host two intensive learning summer camps.

4. Develop and offer a 3-credit-hour secure programming introductory course to two cohorts.
5. Provide three types of graduate-level/open-enrollment certificates in secure programming.

These initiatives are tailored for learners with varying programming experience, aiming to train approximately seven hundred participants. By offering diverse activities (explained in detail in Section 3), the program seeks to upskill or transition participants into secure programming careers, broadening their career opportunities and increasing the likelihood they will pursue more education or programs on secure programming.

3 Target Learners

3.1 Target Participants

The Cybersecurity and Infrastructure Security Agency (CISA), through the National Initiative for Cybersecurity Careers and Studies (NICCS), describes "the underserved communities as those sharing a particular character or geographic communities that have been systematically denied a full opportunity to participate in aspects of economic, social and civil life." Those in the military on active duty, transitioning to civilian, and veterans are considered underserved populations in the cybersecurity workforce.

Based on the aforementioned reasons for promoting robust/secure programming, the coalition has identified the following categories as being eligible for and benefiting from transitioning or upskilling opportunities through the proposed project. Military/veteran or first responder background will be prioritized, and only US Citizens or permanent residents will be considered.

1. Junior software engineers who are able to transition to secure programming roles early in their careers.
2. IT professionals working in government, schools, healthcare, and other sectors who could benefit from additional training in secure programming.
3. Educators and students in all types of colleges and universities, including two-year and four-year institutions, who would benefit from increased knowledge and training in secure programming.
4. Mid- to senior-level cybersecurity professionals who could benefit from developing their skills in secure programming.

3.2 Recruiting and Selection

The coalition will recruit by reaching out to both national and regional targeted participants via social media, email campaigns, listing in the university and university continuing and professional education catalogs, a central SWEEPS website listing all study options (locations and formats), and through campaigns with professional associations. All coalition members will work as a committee on recruitment, exploiting regional resources and seeking cross-institution coordination. The University involved particularly acknowledges the acute need to remove barriers to the recruitment, retention, and advancement of talented students, faculty, and staff from historically excluded populations who are currently underrepresented [7].

4 The Proposed Program

4.1 A Collaborative Project

This proposed program is a collaboration of seven institutions across at least 2 CAE regions (Northeast and Southwest) and five states (California, Massachusetts, Maryland, Indiana, North Carolina), including the University of California, Davis (UC Davis), Worcester Polytechnic Institute (WPI), the University of Maryland, Baltimore County (UMBC), Dark Enterprises, Inc. (a non-profit organization in cybersecurity education), and StrongAuth, Inc. (a technology company that has collaborated with the US Army, the State of California, and the NIST National Cybersecurity Center of Excellence (NCCoE) on various projects).

SWEEPS workforce development initiatives are built on the coalition's extensive background in research and education related to secure programming. These efforts include three major projects:

- The "Secure Programming Clinic" (SPC) project, funded by the National Science Foundation (NSF), ran from August 2014 to July 2019. This project established and evaluated a secure programming clinic model, aimed at improving students' skills in developing robust and secure software, akin to a writing clinic in an English department or law school.
- The "Secure Programming Concept Inventory" (SPCI) project, funded by NSA CCC program, spanned from Sep 2017 to Sep 2019. It introduced the first concept inventory in the secure programming domain, serving as an assessment tool to gauge an individual's grasp of secure programming concepts.
- The "Secure Programming Intelligent Tutoring System" (SecTutor) project, sponsored by the NSF since October 2019, is ongoing and expected to conclude in September 2025. This project focuses on creating an adaptive testing and intelligent tutoring system named "SecTutor," designed to enhance secure programming training through adaptive and intelligent methodologies.

This program will draw on outcomes from such prior work, including the clinic model, the concept map, the concept inventory, and the SecTutor system, to build secure programming curricula, shape the workforce development activities, and facilitate the participants in learning about secure programming (e.g., the SecTutor system will be used as an infrastructure for participants to work on secure programming practice and assessments). Specifically, the program proposes to implement *3 clinics* in UC Davis, WPI and UMBC, and make them available to institutions both inside and outside of the coalition. The program will host *8 one-day workshops*, offer *2 introductory-learning summer camps*, develop *a 3-credit-hour secure programming foundational course* and offer it for *2 cohorts*, and provide *3 flavors of graduate-level/open-enrollment certificates*, all about secure programming. These activities at different levels are designed for targeted learners with varying levels of programming experience, and in total,

approximately *700 participants* will get secure programming training at appropriate levels. By offering activities catering to various skill levels, this program aims to upskill or transition participants for career opportunities in the secure programming workforce that may have previously been inaccessible. Overall, the program's initiatives will provide secure programming training to diverse learners, enabling them to pursue career opportunities in the secure programming field.

4.2 The Coalition's Prior Foundation Work for Secure Programming Workforce Development

4.2.1 Secure Programming Clinic (SPC). The SPC is a method of supplementing or providing secure programming training among college students using a practical training experience method modeled on clinical education. In this model, students can consult with a more experienced "clinician," who is usually a graduate student or instructor. The clinician has greater expertise in secure programming and provides feedback on the security and robustness aspects of the student's program. Much like a writing lab where feedback is provided on writing quality, structure, and grammar regardless of content, students can receive feedback on the security and robustness of any program regardless of purpose or functionality. Over the past four years, the SPC has been deployed at UC Davis, California State University-Sacramento, Purdue University, and Cal Poly-San Luis Obispo.

An investigation was conducted to understand how students learn secure programming to improve the SPC. The first step of this process was to map the domains in secure programming. To identify and map the foundational topics in secure programming, the researchers conducted a Delphi study. This study gathered input from ten secure programming experts in academia, industry, and government. This Delphi study was conducted over four rounds. In the first round, the researchers created a questionnaire listing initial characteristics related to secure programming. The respondents rated each characteristic on a five-point scale from very important to unimportant and indicated whether they agreed that the principle should be included. The respondents also added any core characteristics they felt were missing. This resulted in thirty-one characteristics, which were reviewed during the second round. In the third round the experts were asked to visually map the characteristics to each other. These mappings were reviewed and consolidated over the fourth round. The result was a secure programming concept map outlining the foundational principles, concepts, and techniques in secure programming [10]. The term "concept map" is used to refer to a collection of concepts and the relationships among those concepts.

Coalition members have published research studies on SPC in reputable conference proceedings, including [10-14], demonstrating its effectiveness in secure programming education.

4.2.2 Secure Programming Concept Inventory (SPCI). To assess how well students were learning secure programming, a concept inventory for secure programming was further developed with the support of a grant from the National Security Agency's National Cybersecurity Core Curriculum (CCC) Project funded in 2017 (H98230-17-1-0417). A concept inventory is an assessment tool designed to measure an individual's understanding of concepts in a specific knowledge domain. Concept inventories have two advantages over most standard tests: they are easy to administer and score, and they probe beyond recognition or memorization to examine a student's *understanding* of a concept [18]. To develop the concept inventory, interviews were conducted with instructors and students to determine what concepts students found difficult and what misconceptions students commonly hold about secure programming concepts. The misconceptions were classified into a Taxonomy of Misconceptions in Secure Programming. An item bank was then developed comprising 230 multiple-choice items. These items were tested by administering them to computer science students at four institutions and analyzing the results using item response theory. The best items were compiled into SPCI [15, 16].

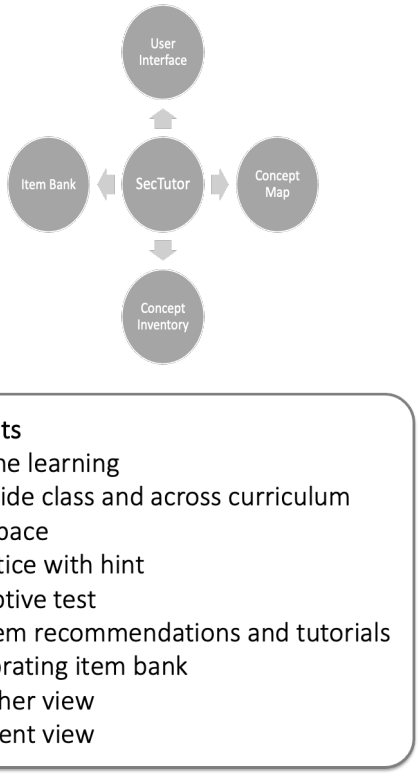

Figure 1. The Overview and Benefits of the SecTutor System

4.2.3 Secure Programming Intelligent Tutoring System (SecTutor). The two previous projects mentioned have produced valuable outcomes, including 1) a Concept Map of Secure Programming that will inform the expert knowledge model in secure programming, 2) a Taxonomy of Misconceptions in Secure Programming that will inform the student knowledge model in secure programming, and 3) a Secure Programming Concept Inventory, an item bank, and a calibration of those items that can be integrated into an adaptive tutoring and test system named SecTutor. The purpose of developing SecTutor was to combat one of the most significant

cybersecurity challenges we have today: individuals' failure to practice defensive, secure, and robust programming.

The coalition members implemented SecTutor to aid learners in understanding the foundational concepts behind secure programming. Based on incorporating all of the previous secure programming work, SecTutor is a tutoring system that uses adaptive testing to select instructional modules that allow users to pursue secure programming knowledge at their own pace and depth. Specifically, the system presents users with questions chosen to identify common misconceptions. If the users demonstrate those misconceptions, it guides them to resources to help educate them on the topics involved. This allows for scalable self-paced study, efficiently focusing on areas with deficits and skipping those where the learner already understands the subject matter. Figure 1 illustrates the overview and benefits of SecTutor. The SecTutor design and rationales were elaborated in [17].

4.3 Proposed Learning Activities

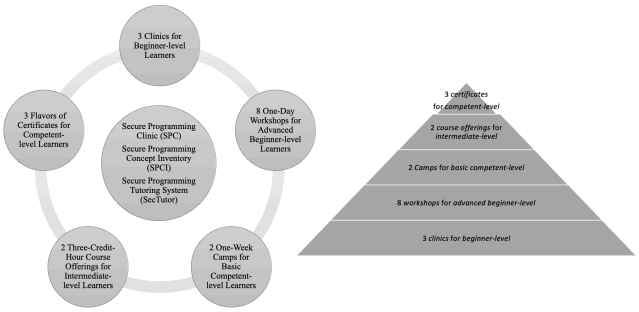

Figure 2. The Overview of Proposed Learning Activities

To ensure that the underserved populations are successfully served. This SWEEPS project has proposed activities that will meet the participants where they are and upskill or introduce new skills to them. There are 3 clinics for beginner-level, 8 workshops for advanced beginning-level, 2 camps for basic competent-level, 2 course offerings for intermediate-level, and 3 certificates for competent-level. These activities are described in the numbered paragraph following Figure 2 diagram of the overview of proposed learning activities. Activity modules will be adapted from existing community resources or newly created by recruited experts. The curriculum will progressively expand in breadth and depth, transitioning from workshops to camps, then to courses, and ultimately to certificate programs. Each module will feature pre-tests and post-tests to evaluate learners' knowledge gains.

This program offers a range of activities tailored to the specific needs of our target audience, taking into account their differing proficiency levels of programming experience, including *beginner, advanced beginner, basic competence, intermediate, and advanced competence*. The objective is to cater to the diverse demands of participants with varying levels of programming knowledge and provide them with the most suitable secure programming content and pace of learning to enhance their competency. Figure 2 illustrates the designed activities that revolve around content development and instructional infrastructure built upon the achievements of the coalition's previous endeavors.

1) The program caters to participants with beginner-level programming experience, such as college students, by following the previously well-established "Secure Programming Clinic" model. The clinic is analogous to a writing center for secure programming that can be implemented at high-education institutions as an extracurricular mechanism to allow students to learn about secure programming and receive feedback on the security and robustness of their programming without further burdening the curriculum. The mechanism targets students in non-security classes like Computer Networking and Operating Systems, where programming for security and robustness is not covered. Students in the participating courses will be required to program not just for functionality, but also for security and robustness. To assist these students in learning secure programming approaches and rectifying security errors in their code, three institutions in the coalition (i.e., UC Davis, WPI, and UMBC) will train graduate students as "*Clinicians*" to provide regular office hours in both physical and virtual formats. This is to give students maximum flexibility for participation and also enable virtual support to students external to the clinician's home institution. The team will proactively outreach to colleges and universities, including two-year and four-year institutions, and expand clinician support to them.

   The learning offered through the clinic is expected to benefit a minimum of 300 participants, potentially leading them to pursue careers in the secure programming workforce that may have otherwise been inaccessible.

2) The program is designed to cater to individuals who possess advanced beginner-level programming experience, including college educators and IT professionals, and offers a one-day virtual workshop (9am-5pm) providing them with introductory-level training on secure programming. The program has tailored a one-day curriculum specifically for this level of learning, focusing on the most important and representative secure programming topics. Each topic will be allocated a 50-minute time slot, covering basic concepts, examples, misconceptions, and small practices. The workshop will include approximately seven topics, and the team aims to host eight workshops in 2025. Each workshop is designed to accommodate 25 participants, ensuring an optimal learning experience for all attendees. The workshops are all virtual for maximum flexibility for participants, offered through WPI and UMBC.

   The workshops aim to provide introductory-level secure programming learning to a minimum of 200 participants, potentially upskilling them or facilitating their transition into careers in the secure programming workforce that may have been previously inaccessible.

3) The program proposes to host one-week virtual summer camps for individuals with programming experience up to basic competent-level, including cyber professionals, software engineers, graduate students, college educators, and IT professionals, who expect an in-depth understanding of secure programming. The camps are structured to offer a more comprehensive introduction, providing tutorials and covering topics beyond the basics, in contrast to one-day workshops. The camps will run weekly, with 2.5-hour morning and afternoon sessions. The team plans to host two summer camps in 2025, accommodating approximately 25 participants in each camp to ensure optimal engagement and learning experience. All the camps are virtual to give individuals maximum flexibility for participation, with one camp offered through UC Davis and one offered through WPI.

   The objective of the camps is to provide at least 50 participants with more extensive and in-depth education on secure programming, enabling them to upskill or transition into careers in the secure programming workforce that were previously unattainable.

4) The program is designed to provide a more intensive and advanced-level curriculum to secure programming via a three-credit-hour course for participants with essential competent-level programming experience, including early career software engineers, IT professionals, graduate students, and college educators. The course will more thoroughly introduce participants to the critical modules of secure programming, with all relevant topics, outcomes, knowledge units, hands-on practices, and assessments logically delivered via the Canvas LMS (Learning Management System). The course will be administered asynchronously online, with the support of instructors and graduate teaching assistants from UC Davis and UMBC. A synchronous option may be available. The team plans to have four cohorts, each consisting of 25 participants.

   The objective of the three-credit hour course is to provide a comprehensive introduction to secure programming for a minimum of 100 participants. The program aims to upskill the participants and enable them to transition into careers in the secure programming workforce, which may have previously been inaccessible to them.

5) The program is also designed to offer graduate-level/ open-enrollment certificate studies in secure programming for participants with competent-level programming experience, including mid-senior level software engineers, cyber professionals, IT professionals, and graduate students. The certificate study consists of 12 credit hours (i.e., four graduate-level courses) and is available at three universities: UC Davis, WPI, and UMBC to meet different participants' needs, schedules, and preferences. Although the options are offered in various flavors and formats, as summarized in Figure 2, the shared objective is to provide an in-depth and systematic education on secure programming in cybersecurity and/or programming contexts. The certificates cover all relevant modules, topics, and outcomes necessary for participants to become experts in the field. The program aims to enhance participants' career prospects and enable them to take on challenging roles in cybersecurity workforce.

   The certificate, as a credential, aims to greatly facilitate the transition of 50-75 participants into careers in the secure programming workforce, which may have previously been inaccessible to them. By upskilling the participants, the certificate opens up opportunities for them to pursue fulfilling careers in the field of secure programming.

5 Challenges

There are several challenges to the successful completion of this project. The target audience for the offerings are underserved populations, including active duty military, transitioning service members, and veterans, which presents several challenges. Recruiting participants from these diverse groups can be difficult due to varying accessibility to information and differing levels of awareness about available programs. For instance, underserved populations may lack reliable internet or networks that disseminate information about workshops, certificate courses, or camps. Additionally, the unique schedules and commitments of active-duty military personnel can make it challenging for them to participate in scheduled training activities. Transitioning service members and veterans may face obstacles such as adjusting to civilian life or dealing with mental health issues, which can impact their ability to engage in upskilling activities.

Furthermore, logistical challenges such as securing appropriate venues, providing transportation, and offering childcare or other support services can also hinder participation. Overcoming these challenges requires targeted outreach, flexible scheduling, and comprehensive support services to ensure these valuable programs are accessible and effective for all intended participants. Another challenge is staffing instructors knowledgeable enough to teach secure programming in the various SWEEPS modalities.

6 Conclusion

The high frequency of cyber attacks and breaches indicates that too many insecure applications are rushed to market. SWEEPS aims to address this issue by enhancing the secure programming skills of early and mid-career professionals, thereby reducing the reliance on costly and ineffective post-release patches that fail to address the root causes of cybersecurity breaches. Through a combination of clinics, workshops, camps, courses, and graduate certificate programs, SWEEPS provides diverse educational opportunities catering to various levels of expertise. This project underscores the importance of integrating secure programming principles from the very beginning of software development rather than as an afterthought.

ACKNOWLEDGMENTS

SWEEPS is supported by NCAE-C Grant #H98230-23-1-0090, with SecTutor development also funded by NSF Awards #1934269, #1934279, #1934285, and #2403603.

REFERENCES

[1] CVE-2014-0160, National Vulnerability Database. https://nvd.nist.gov/vuln/detail/cve2014-0160. Accessed in Nov, 2024.

[2] "The Heartbleed Bug", Synopsys, Inc. https://heartbleed.com/. Accessed in Nov, 2024.

[3] Matt Bishop, 2002. Computer Security: Art and Science, Section 20.1.2.2.

[4] "Cyber Attacks on the Power Grid", IronNet Threat Research. https://www.ironnet.com/blog/cyber-attacks-on-the-power-grid. Accessed in Nov, 2024.

[5] Ralph Langer, "Stuxnet: Dissecting a Cyberwarfare Weapon," IEEE Security and Privacy, 9(3) pp. 49–52 (May 2011); DOI 10.1109/MSP.2011.67.

[6] Matt Bishop, 2002. Computer Security: Art and Science, Section 1.3.

[7] O'Donnell, T. UC statement on diversity. Diversity, Equity & Inclusion. https://diversity.ucdavis.edu/uc-statement-diversity. August 9, 2019.

[8] Robert J. Mislevy and Geneva D. Haertel. 2006. Implications of evidence-centered design for educational testing. Educational measurement: issues and practice, 25(4), pp.6-20.

[9] Muwei Zheng, Nathan Swearingen, Steven Mills, Croix Gyurek, Matt Bishop, and Xukai Zou. 2023, March. Case Study: Mapping an E-Voting Based Curriculum to CSEC2017. In Proceedings of the 54th ACM Technical Symposium on Computer Science Education (ACM SIGCSE) V. 1 (pp. 514-520).

[10] Melissa Dark, Steven Belcher, Matt Bishop, and Ida Ngambeki, "Practice, Practice, Practice … Secure Programmer," Proceedings of the 19th Colloquium on Information Systems Security Education (June 2015).

[11] Melissa Dark, Ida Ngambeki, Matt Bishop, and Steven Belcher., "Teach the Hands, Train the Mind … A Secure Programming Clinic," Proceedings of the 19th Colloquium on Information Systems Security Education (June 2015).

[12] Melissa Dark, Lauren Stuart, Ida Ngambeki, and Matt Bishop, "Effect of the Secure Programming Clinic on Learners' Secure Programming Practices," Proceedings of the 20th Colloquium on Information Systems Security Education (June 2016)

[13] Matt Bishop, Jun Dai, Melissa Dark, Ida Ngambeki, Phillip Nico, and Ming Zhu, "Evaluating Secure Programming Knowledge," Proceedings of the 10th World Conference on Information Security Education pp. 51–62 (May 2017).

[14] Matt Bishop, Ida Ngambeki, Shivan Mian, Jun Dai and Phillip Nico, "Measuring SelfEfficacy in Secure Programming: The Context of a Secure Programming Clinic". Proceedings of the 14th World Conference on Information Security Education (WISE 14), Oslo, Norway, June 22-24, 2021.

[15] Ida Ngambeki, Phillip Nico, Jun Dai, Matt Bishop, "Concept Inventories in Cybersecurity Education: An Example from Secure Programming". 48th Annual Frontiers in Education (FIE 2018) Conference, San Jose, California USA.

[16] Ida Ngambeki, Matt Bishop, Jun Dai, Phillip Nico, "Validation of a Secure Programming Concept Inventory". ACM Special Interest Group on Computer Science Education (SIGCSE) Technical Symposium (TS) 2023.

[17] Ida Ngambeki, Matt Bishop, Jun Dai, Phillip Nico, Shiven Mian, Ong Thao, Tran Ngoc Bao Huynh, Zed Chance, Isslam Alhasan, and Motunrola Afolabi, "SecTutor: An Intelligent Tutoring System For Secure Programming". Proceedings of the 15th World Conference on Information Security Education (WISE 15), Copenhagen, Denmark, June 13-15, 2022.

[18] RJ Dufresne, WJ Leonard, WJ Gerace, "Making sense of students' answers to multiple choice questions," The Physics Teacher, vol. 40, pp. 174-180, 2002.