Concept Inventories in Cybersecurity Education: An Example from Secure Programming

Ida Ngambeki
Deparrtment of Computer & Information Technology
Purdue University
West Lafayette, USA
ingambek@purdue.edu

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

Jun Dai
Department of Computer Science
California State Uniersity, Sacramento
Sacramento, USA
jun.dai@csus.edu

Matthew Bishop
Department of Computer SCience
University of California, Davis
Davis, USA
bishop@ucdavis.edu

Abstract— **This Innovative Practice Work in Progress paper makes the case for using concept inventories in cybersecurity education and presents an example of the development of a concept inventory in the field of secure programming. The secure programming concept inventory is being developed by a team of researchers from four universities. We used a Delphi study to define the content area to be covered by the concept inventory. Participants in the Delphi study included ten experts from academia, government, and industry. Based on the results, we constructed a concept map of secure programming concepts. We then compared this concept map to the Joint Task Force on Cybersecurity Education Curriculum 2017 guidelines to ensure complete coverage of secure programming concepts. Our mapping indicates a substantial match between the concept map and those guidelines.**

Keywords—concept inventory, secure programming, cybersecurity

I. Introduction

Estimates suggest that by 2022 demand for cybersecurity workers will exceed supply by 1.8 million positions [1]. As computing-based technologies evolve, so do the number of threats they pose. To make matters worse, tools to exploit software vulnerabilities have become a marketable commodity allowing anybody with the means to purchase everything they need to set up shop as a cybercriminal. Given the hostile environment where the developers of the future will work, it is more important than ever to provide them with the education they need to design systems able to respond to new security needs. This requires them to have a clear understanding of the foundational knowledge that will serve as the basis for building new skills and responding to new challenges. For us to educate practitioners with this knowledge we need to address three questions: 1) What should our students be learning? 2) How should they learn the material? 3) How will we know they have mastered it? The answers will shape our curricula (*figure 1*).

To build a robust cybersecurity workforce we must move beyond a piecemeal approach and build broad consensus as to what the answers to these questions are across the field of cybersecurity. The first question is being addressed by efforts such as the Joint Task Force on Cybersecurity Education Cybersecurity Curricular Guidelines (http://cybered.acm.org/) and the NICE Cybersecurity Workforce Framework (https://www.nist.gov/itl/applied-cybersecurity/national-initiative-cybersecurity-education-nice/nice-cybersecurity) to define the field of cybersecurity, describe cybersecurity work, and develop curricular guidance for cybersecurity education. The second question is being addressed by several private and public educational and training institutions, as well as national efforts such as the National Cybersecurity Curriculum Program, that are working to develop curricula, materials, tools, and pedagogies in cybersecurity. The third question identifies the weakest area in the development of cybersecurity education. While a few certifications exist for professionals, we lack tools to reliably measure students' understanding of foundational concepts. Concept inventories are one tool that can help us address this weakness.

A concept inventory is an assessment tool intended to diagnose students' misconceptions. That is, in addition to identifying what students know, it seeks to identify specific errors in their mental models so they can be addressed directly. It is an assessment meant to measure understanding rather than memorization. A concept inventory typically consists of a short multiple-choice scale. The questions are designed so that meaningful understanding is required to select the most correct answer. The inventory is an extremely useful educational tool that can be used before, during, or after an intervention to establish a learner's level of understanding, determine learning gains, diagnose misconceptions, and highlight areas for improvement. It is therefore useful in informing curricular and course design, evaluating teaching materials and effectiveness, and measuring student proficiency.

Research supported by NSA Grant no. H98230-17-1-0417 and NSF Grant nos. DGE-1303048 and DGE-1303211

978-1-5386-1174-6/18/$31.00 ©2018 IEEE

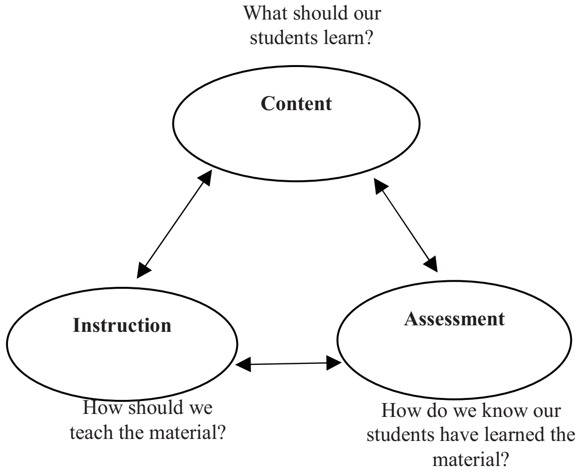

What should our students learn?
Content
Instruction
Assessment
How should we teach the material?
How do we know our students have learned the material?

Fig 1: Linking content, assessment, and instruction

II. CONCEPT INVENTORIES

Concept inventories are standardized tests, designed so that the questions, administration, scoring procedures, and interpretations are consistent and adhere to a predetermined standard/protocol. Since their purpose is diagnostic rather than evaluative, they are not intended to be used as a replacement for other methods of assessing student learning. They are instead meant to uncover a students' existing conceptual framework by determining to what extent a student recognizes and understands core concepts, whether the student is making correct connections among these concepts, and how able the student is to harness this knowledge in novel situations.

The first concept inventory was developed in the field of physics education in the early 1980s [2]. Based on years of trying to teach students basic Newtonian concepts, Hallhoun and Hestenes, realized that while students were able to recite the laws and apply them to rote tasks, they were struggling with anything more complex. They determined that students were coming into the class with sometimes incorrect or incomplete ideas about motion and force gleaned from prior experiences and that their teaching was failing to connect with, correct, or replace these ideas [3]. To address this they developed an instrument, the Force Concept Inventory (FCI), to determine what ideas the students held about force and how those ideas compared to Newtonian concepts. As a result, they were able to uncover misconceptions and target them specifically using appropriate pedagogical approaches. Other researchers [4] using the FCI proved the effectiveness of these methods leading to a revolution in physics education. Active learning methods such as interactive engagement, peer instruction, and inquiry-based pedagogy became widely used to encourage the development of understanding. These changes in instruction led to the development of new textbooks and learning aides, a massive increase in research into disciplinary learning, and extensive reforms in the education of physics teachers. These highly impactful advances in physics education spurred the development of concept inventories in other fields of science and engineering including astronomy, biology, chemistry, circuits, design graphics, electromagnetism, heat transfer, genetics, nursing, statics, and statistics. Studies of concept inventories across several disciplines have proven their effectiveness in diagnosing misconceptions, and in discriminating between memorization and understanding [5] [6] [7]. The positive impact of concept inventories on disciplinary education cannot be denied.

Concept inventories are based on the idea of identifying existing mental structures or conceptual frameworks and correcting any misconceptions. This idea draws from the group of learning theories known as conceptual change theories. These theories posit that a lot of learning is the process of constructing a mental map that identifies and categorizes concepts, linking old concepts to new ones [8]. This map is then accessed to make predictions or decisions [9]. One such theory is Ausubel's assimilation theory that contrasts rote learning (temporary acquisition of disorganized or poorly understood isolated or arbitrarily related concepts, for example memorization) with meaningful learning (long-term acquisition of organized, interrelated concepts into existing cognitive structures) [10]. In order for learning to be effective, sometimes prior identification and categorization of ideas must be corrected or eliminated in order to make correct links to new knowledge. Incorrect information must be uncovered and replaced with valid and reliable instruments. This can often be difficult since often the student's current mental model has persisted because it has worked up to that point. Correcting that model requires a good understanding of what the misunderstanding is and where it originated.

A. The Power of Concept Inventories

In computer science, we mostly use assessment methods that target procedural knowledge, focusing on whether students can produce a functional program; they do not consider students' understanding of the underlying processes [11]. Concept inventories on the other hand, are educational assessment tools that we can use to measure the level of a student's understanding of certain content. Concept inventories have several advantages over most standard tests:

- They probe beyond recognition or memorization to examine a student's *understanding* of a concept [12]. They are designed to target concepts identified as being foundational to the understanding of the discipline. Therefore, we can use the instrument to go beyond measuring proficiency and determine which concepts an individual student, or group of students is struggling with.

- They are a multiple-choice instrument that we can easily and quickly administer in paper or electronic form. We can therefore easily use them to measure individual proficiency with foundational concepts.
- They can be used in a pre/post format that allows for measuring understanding before and after an intervention. The results of initial testing can be used to determine areas of weakness and therefore guide the development of an intervention to challenge these specific areas. The results of post testing can then be used to measure the effects of the intervention.
- The answer options for each question represent common misconceptions around the concept. This enables the instrument to diagnose not just whether an individual understands a concept or not but what the misconceptions they hold might be.

Concept inventories therefore have the ability to measure proficiency, determine learning gains, guide instruction, and inform curriculum design.

B. Developing a Concept Inventory

The core task of a concept inventory is to demonstrate a student's understanding by uncovering conceptual frameworks and highlighting any flaws in that conceptual framework. The construction of a concept inventory is therefore more complex than the construction of a simple multiple-choice test. The test items must have sufficient coverage of the core items. The distractors for the multiple-choice items must represent misconceptions commonly seen with the concept. There are three broad steps in developing a concept inventory: defining the content, obtaining information about students' misconceptions, and developing the diagnostic test.

There are several methods to define the content area in a domain. In well-established fields one would simply consult the standard textbooks or course syllabi. In less well-established fields, such as cybersecurity, where there is still debate about what constitutes the discipline, the content area can be defined by creating consensus among experts representative of the field in question. Interviews, focus groups, or Delphi studies (consensus from a panel of experts through iterative communications) can be used to achieve this. In addition to determining the concepts that represent the field, any domain description must also include some ranking of the criticality, complexity, and relationships among the concepts. This is essential since concept inventories typically target foundational knowledge rather than more advanced, specialized, or obscure topics. The resulting domain information can then be communicated as a taxonomy, an ontology, or a concept map.

Once the domain has been sufficiently described and the topics to be targeted have been selected, the next step is to explore difficulties and misconceptions. A good concept inventory will uncover the misconceptions that students hold in the difficult topics. Interviews with students, instructors, and other experts in the field will uncover patterns and trends in what concepts students find difficult, how students get things wrong, and why students get these things wrong. These patterns and trends are then used to inform the creation of the test questions and distractors.

The final step is the creation of a pool of items which represent a reasonable coverage of foundational concepts in the field. The item distractors are constructed to represent misconceptions. Iterative testing is performed with this item pool to determine item clarity, item difficulty, and item discrimination (the ability of the question to separate those who understand the content from those who do not). Questions which are too simple, too difficult, or unclear are discarded. Questions that do a poor job at differentiating between those who know the content and those who do not are also be discarded. Questions that perform moderately are revised to increase their efficacy. Testing is also used to determine the validity and reliability of the inventory. This includes measures of consistency (the test's ability to measure understanding of a concept consistently across items, across populations, and across time); internal consistency (that items intended to measure the same concept produce the same scores); content validity (that the test measure the breadth of content required); construct validity (that the items measure what they are intended to measure); and criterion validity (that the items map to knowledge of the concept). The results of this testing are used to eliminate or refine items to create the final inventory.

III. Concept Inventories in Computing

In computer science, concept inventory development is still in its infancy [13]. Herman, Loui and Zilles [14] developed a concept inventory in Digital Logic and efforts are underway for concept inventories in discrete mathematics, computer architecture, cybersecurity and operating systems [15] [16] [17] [18]. We are developing a Secure Programming Concept Inventory (SPCI).

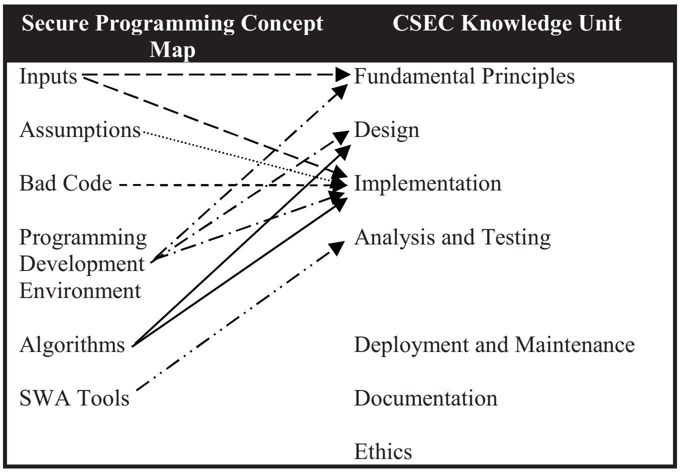
A. The Secure Programming Concept Inventory (SPCI)

The team developing the SPCI is made up of researchers at Purdue University, University of California Davis, California State University Sacramento, and California Polytechnic State University San Luis Obispo.

B. Defining the Secure Programming Concept Area

We used a Delphi study conducted with experts from government and academia to define the content area for the SPCI. The Delphi study gathered information from ten experts over four rounds. In each round, the experts weighed in on a proposed set of concepts related to secure programming, commenting on the importance of each concept; adding, combining, and eliminating concepts, and finally commenting on the connections among concepts. The result was a graphical representation, or concept map that categorized principles, concepts, and techniques in secure programming [19].

TABLE 1: COMPARING THE SECURE PROGRAMMING CONCEPT MAP AND THE JOINT TASK FORCE CYBERSECURITY CURRICULUM GUIDELINES 2017



We compared this concept map to the Cybersecurity Curriculum Guidelines proposed by the Joint Task Force on Cybersecurity Education (https://www.csec2017.org/). The secure programming concept map compares most closely to the Software Security Knowledge Area in the Curriculum Guidelines (*Table 1)*. Although the two approaches use some different terminology, the knowledge units proposed under this knowledge area (specifically: fundamental principles, design, implementation, and analysis and testing), map well onto the overarching concept areas proposed by the Secure Programming concept map (inputs, assumptions, bad code, programming development environment, tools, and algorithms). The other knowledge units, deployment and maintenance, documentation, and ethics are not currently part of the secure programming concept map and therefore not represented in the current version of the concept inventory. However, the instrument is still under construction and discussions of whether to expand the concept map continue.

C. Developing the Pool of Secure Programming Concepts

Our next step in developing the SPCI is developing the item pool. The item pool is a pool of potential questions that we will test for possible addition to the final concept inventory. Our concept pool for the SPCI currently stands at ninety questions covering the six main concept areas identified by the concept map (most questions address more than one topic). Many of the questions cover inputs, assumptions and bad code. The reliability (Cronbach's alpha α) of the current items is displayed in Table 2. As the item pool is further expanded and refined, we expect the number of questions for each concept to increase and the reliability to also increase.

IV. Future Work

The development of the Secure Programming Concept Inventory is ongoing. We are currently in the process of interviewing students and instructors in computer science, information technology, and related fields to develop a taxonomy of misconceptions in secure programming. This taxonomy will be used to refine the item pool that will be used to construct the secure programming instrument. The item pool will then be reviewed by a set of experts and rigorously tested with a diverse population of students in security related courses at several institutions.

TABLE 2: NUMBER OF QUESTIONS AND RELIABILITY FOR SPCI CONCEPTS

SPCI Concepts	No. of Questions	α
Inputs	43	.52
Assumptions	18	.46
Bad code	21	.47
Programming development environment	4	.71
SWA tools	10	.47
Algorithms	3	.39

V. Conclusion

We need to educate cybersecurity practitioners in sufficient numbers to fulfill workforce requirements and with the knowledge and skills required to deal with evolving security threats. Our efforts to meet this need are being hampered by the lack of tools to reliably assess foundational knowledge in cybersecurity. Concept inventories are one reliable tool that could be used to support assessment. They are especially useful to help uncover where and how students are misunderstanding the material. The field of cybersecurity needs to support the development of concept inventories and other assessment tools.

Ackowledgement

This research is supported by grant number H98230-17-1-0417 from the National Cybersecurity Curriculum Program.

References

[1] Frost and Sullivan, "2017 Global Information Security Workforce Study," Internatioal Information System Security Certification Consortium , Florida, 2017.

[2] I. Halloun and D. Hestenes, "The initial knowledge state of college physics students," *American Journal of Physics,* vol. 53, p. 1043, 1985.

[3] D. Hestenes, M. Wells and G. Swackhamer, "Force concept inventory," *The Physics Teacher,* vol. 30, no. 3, pp. 159-166, 1992.

[4] R. Hake, "Interactive engagement versus traditional methods: A six thousand student survey of mechanics test data for introductory physics courses," *American Journal of Physics,* vol. 66, no. 1, pp. 64-74, 1998.

[5] K. Garvin-Doxas, M. Klymkowsky and S. Elrod, "Building, Using, and Maximizing the Impact of Concept Inventories in the Biological Sciences: Report on a National Science Foundation-sponsored Conference on the Construction of Concept Inventories," 2007.

[6] C. D'Avonzo, "Biology concept inventories: Overview, status, and next steps," *BioScience,* vol. 58, pp. 1079-1085, 2008.

[7] P. Laws, D. Sokoloff and R. Thornton, "Promoting active learning using the results of physics education results," *UniServe Science News,* vol. 13, pp. 14-19, 1999.

[8] M. Chi, "Three types of conceptual change: Belief revision, mental model transformation, an categorical shift.," in *Handbook of research on conceptual change*, New York, Routledge, 2008, pp. 61-82.

[9] J. Bransford, A.L. Brown and R. Cocking, How people learn: Brain, mind, experience, and school, Washington D.C.: National Academy Press, 1999.

[10] D. Ausubel, J. Novak and H. Hanesian, Education psychology: A cognitive view, New York, NY: Holt, Rinehart & Winston, 1978.

[11] J. Davis and M.J. Dark, "Teaching students to design secure systems," *IEEE Security and Privacy,* vol. 1, no. 2, pp. 56-58, 2003.

[12] R. ufresne, W. Leonard and W. Gerace, "Making sense of students' answers to multiple-choice questions," *The Physics Teacher,* vol. 40, pp. 174-180, 2002.

[13] C. Taylor, D. Zingaro, L. Porter, K. Webb, C. Lee and M. Clancy, "Computer Science Concept Inventories: Past and Future," *Computer Science Education,* vol. 24, no. 4, pp. 253-276, 2014.

[14] G. Herman, M. Loui and C. Zilles, "Students' Misconceptions about Medium-scale Integrated Circuits," *IEEE Transactions on Education,* vol. 54, pp. 637-645, 2011.

[15] V. Almstrum, P. Henderson, V. Hrvey, C. Heeren, W. Marion, C. Riedesel and A. Tew, "Almstrum, V.L., Henderson, P.B., Hrvey, V., Heeren, C., Marion, W., Riedesel,Concept Inventories in Computer Science for the Topic Discrete Mathematics," *ACM SIGCSE Bulletin,* vol. 38, pp. 132-145, 2006.

[16] L. Porter, S. Garcia, H. Tseng and D. and Zingaro, "Porter,Evaluating Student Understanding of Core Concepts in Computer Architecture," in *Porter, L., Garcia, S. Tseng, H.W., and Zingaro, D. (2013). Evaluating Student Understanding of Core Concepts iProceedings of the 19th Annual Conference on Innovation and Technology in Computer Science Education (ITiCSE)*, Uppsala, Sweden, 2013.

[17] K. Webb and C. Taylor, "Developing a Pre- and Post-Course Concept Inventory to Gauge Operating Systems Learning," in *Webb, K, and Taylor, C. (2014) Developing a Pre- and Post-Course Concept Inventory to Gauge OperaProceedings of the 45th ACM Technical Symposium on Computer Science Education (SIGCSE)*, Atlanta, GA, 2014.

[18] A. Sherman, Creating Concept and Curriculum Assessment Tools for Cybersecurity, Available from: http://www.cisa.umbc.edu/cats/documents.html..

[19] M. Dark, S. Belcher, I. Ngambeki and M. Bishop, "Practice, practice, practice... Secure Programer!," in *Colloquium for Information Systems Security Education*, La Vegas, 2015.