Journal of Cybersecurity Education, Research and Practice

Volume 2023 | Number 2 Article 6

October 2023

Exploring Network Security Educator Knowledge

Jennifer B. Chauvot
University of Houston, jchauvot@uh.edu

Deniz Gurkan
University of Houston, dgurkan@central.uh.edu

Cathy Horn
University of Houston, chorn@Central.UH.EDU

Follow this and additional works at: https://digitalcommons.kennesaw.edu/jcerp

 Part of the Adult and Continuing Education and Teaching Commons, Higher Education Commons, and the Information Security Commons

Recommended Citation

Chauvot, Jennifer B.; Gurkan, Deniz; and Horn, Cathy (2023) "Exploring Network Security Educator Knowledge," *Journal of Cybersecurity Education, Research and Practice*: Vol. 2023: No. 2, Article 6.
Available at: https://digitalcommons.kennesaw.edu/jcerp/vol2023/iss2/6

This Article is brought to you for free and open access by the Active Journals at DigitalCommons@Kennesaw State University. It has been accepted for inclusion in Journal of Cybersecurity Education, Research and Practice by an authorized editor of DigitalCommons@Kennesaw State University. For more information, please contact digitalcommons@kennesaw.edu.

Exploring Network Security Educator Knowledge

Abstract

It is critical for nations to have trained professionals in network security who can safeguard hardware, information systems, and electronic data. Network security education is a key knowledge unit of the National Centers of Academic Excellence in Cybersecurity and various information systems security curricula at the master's and bachelor's levels in higher education. Network security units are components of computer science curricula in high school contexts as well. Educators who teach these concepts play a significant role in developing a skilled workforce of network security experts for both governmental and non-governmental organizations. Understanding the necessary knowledge and skills of network security educators serve to better inform institutes of higher education, educator preparation programs, and others who support educators in the field. This study describes knowledge constructs of a higher education faculty member who teaches networking and network security and was developing, and piloting innovative network security curriculum embedded in both undergraduate and graduate courses. Data were transcripts of recorded monthly meetings with the educator, fieldnotes taken during the meetings, and course artifacts. Existing teacher knowledge frameworks that have been applied in both K-12 and higher education contexts were used to deductively code the data. Examples of curricular knowledge and pedagogical content knowledge specific to the teaching of network security are provided. The affordances of using engagement within curriculum development to understand educator knowledge constructs and the existing teacher knowledge frameworks as tools for analyses are highlighted.

Keywords

Teacher knowledge, cybersecurity education

Cover Page Footnote

This work was supported by the National Science Foundation, Award #1907537

This article is available in Journal of Cybersecurity Education, Research and Practice: https://digitalcommons.kennesaw.edu/jcerp/vol2023/iss2/6

Exploring Network Security Educator Knowledge

Jennifer B Chauvot, Associate Professor
Department of Curriculum and Instruction
University of Houston
Houston, Texas, USA
jchauvot@uh.edu
https://orcid.org/0000-0002-2374-3734

Deniz Gurkan, Professor
College of Aeronautics and Engineering
Kent State University
Kent, Ohio, USA
dgurkan@kent.edu
https://orcid.org/0000-0002-3574-5040

Cathy Horn, Professor and Dean
College of Education
University of Houston
Houston, Texas, USA
chorn@Central.UH.EDU
https://orcid.org/0000-0003-4959-5810

***Abstract*— It is critical for nations to have trained professionals in network security who can safeguard hardware, information systems, and electronic data. Network security education is a key knowledge unit of the National Centers of Academic Excellence in Cybersecurity and various information systems security curricula at the master's and bachelor's levels in higher education. Network security units are components of computer science curricula in high school contexts as well. Educators who teach these concepts play a significant role in developing a skilled workforce of network security experts for both governmental and non-governmental organizations. Understanding the necessary knowledge and skills of network security educators serve to better inform institutes of higher education, educator preparation programs, and others who support educators in the field. This study describes knowledge constructs of a higher education faculty member who teaches networking and network security and was developing, and piloting innovative network security curriculum embedded in both undergraduate and graduate courses. Data were transcripts of recorded monthly meetings with the educator, fieldnotes taken during the meetings, and course artifacts. Existing teacher knowledge frameworks that have been applied in both K-12 and higher education contexts were used to deductively code the data. Examples of curricular knowledge and pedagogical content knowledge specific to the teaching of network security are provided. The affordances of using engagement within curriculum development to understand educator knowledge constructs and the existing teacher knowledge frameworks as tools for analyses are highlighted.**

Keywords—teacher knowledge, cybersecurity education

I. Introduction

It is critical for nations to have trained professionals in network security who can safeguard hardware, information systems, and electronic data. Network security education is a key knowledge unit of the National Centers of Academic Excellence in Cybersecurity [1] and various information systems security curricula at the master's and bachelor's levels in higher education. Network security concepts are a component of computer science curricula in K-12 education as well (e.g., K12 Computer Science (https://k12cs.org/a-vision-for-k-12-computer-science/)), endorsed by many organizations. The push to introduce computer science in K-12 schools has motivated a desire to understand better how to prepare and support educators of computer science [2, 3, 4] including how to measure the effectiveness of interventions that do so [5, 6]. This work parallels what others have done in K-12 disciplines such as mathematics, physics, and statistics [7, 8, 9, 10, 11].

Network security is a topic that is dynamic and developing [12] and has received less attention in terms of understanding effective ways to teach this content, and the kinds of knowledge and skills network security educators need and use in their teaching. In addition, the instruction of networking and network security concepts in post-secondary education plays a significant role in developing a skilled workforce of cybersecurity experts for both governmental and non-governmental organizations and in undergraduate and graduate degree programs in areas such as electrical and computer engineering, computer science, and information systems. Curricular components continue to be developed and released by thought leaders in federal institutions such as the National Institute of Standards and Technology (NIST) [13], the National Security Agency (NSA), and the United States Department of Homeland Security (DHS) (e.g., National Centers of Academic Excellence in Cybersecurity [1]) as well as industry [14].

Empirical studies have reported relationships between educator knowledge and positive learning outcomes such as interest in the discipline and achievement [7, 8, 9, 10, 11]. Thus, it behooves the field to better understand educator knowledge within the realm of network security education. A way to attend to understanding and describing network security educator knowledge is to capitalize on existing frameworks of teacher knowledge [2,15]. This study uses such frameworks as tools to describe salient knowledge constructs of post-secondary education faculty for the instruction of concepts related to networking and network security. It illustrates these knowledge constructs through discussions with an expert higher education faculty member as she developed and taught innovative curricula about networking and network security concepts for undergraduate and graduate education courses. The research

question for this study was what kinds of educator knowledge are evident in designing and delivering curricula about networking and network security?

II. Relevant literature

The building blocks of this work come from the ideas presented in [15]. This seminal piece prompted a reframing of how the disciplines in education and educational research conceive of teacher content knowledge. He described content knowledge in three categories: subject matter content knowledge, pedagogical content knowledge, and curricular knowledge. *Subject matter content knowledge* was described as ''the amount and organization of knowledge per se in the mind of the teacher'' (p. 9). It includes knowledge of the facts and concepts of the domain as well as knowledge of the ''rules for determining what is legitimate'' (p. 9). Subject matter content knowledge also includes how the domain relates to other disciplines, in theory and practice.

Pedagogical content knowledge goes beyond the subject matter knowledge to "the dimension of subject matter knowledge *for teaching*" that which embodies ''aspects of content most germane to its teachability'' (p. 9). Given ideas and concepts within a subject area, pedagogical content knowledge is knowledge of

> [t]he most useful forms of representation of those ideas, the most powerful analogies, illustrations, examples, explanations, and demonstrations—in a word, the ways of representing and formulating the subject that makes it comprehensible to others. … Pedagogical content knowledge also includes an understanding of what makes the learning specific topics easy or difficult; the conceptions and preconceptions that students of different ages and backgrounds bring with them to the learning of those most frequently taught topics and lessons. (p.9)

Finally, *curricular knowledge* is knowledge of available and appropriate materials for the instruction of the content knowledge. It includes knowledge of different programs and corresponding ''characteristics that serve as both the indications and contraindications for the use of particular curriculum or program materials in particular circumstances'' (p. 10). Curricular knowledge also includes what [15] described as ''lateral curriculum knowledge'': knowledge of curriculum materials for content areas relevant to the learner at that time and "vertical curriculum knowledge," which entails knowledge of materials related to topics and issues that have been and will be taught in the same content area before and then after the given timeframe.

The work in [15] has been extended and applied in a variety of areas, primarily in K-12 contexts but also in higher education contexts. Examples include science teacher knowledge [16], mathematics teacher knowledge [17], English teacher knowledge [18], teacher knowledge of use of technology in teaching [19] and the conceptualization of teacher knowledge around the role of social justice in classroom practices and teacher preparation [20]. Extending further, researchers have utilized aspects of the descriptors of [15] when the teachers are teacher educators. In other words, what kinds of knowledge do teachers of teachers have? Examples include [21] and [22] who brought together studies specific to mathematics teacher educators and generated a framework for mathematics teacher educator pedagogical content knowledge. Another example is [23], who used teacher knowledge frameworks such as the one in [15] to reveal the complexity of the knowledge content and structure of a mathematics teacher educator in the beginning years of a tenure-track position at a research institution. Closer to this study, work related to educator knowledge has emerged in the field of computer science. We next describe this work.

Reference [2], building from previous work [24,25,26,27] applied constructs of teacher knowledge from [15] in their conceptualization of a competency model for the kinds of knowledge one might need to teach computer science. Their intent was to inform program development for the preparation of K-12 computer science teachers. The framework was developed theoretically, and then further refined through interview data of 23 computer science experts in Germany. Thirteen of the participants were secondary school computer science teachers, and ten were in higher education in computer science teacher education. All had a university degree in computer science. Here, experts responded to problem-based teaching scenarios as opportunities to elaborate more specifically about their teaching practices. From this, competencies of computer science teachers were generated. For example, two resulting competencies were "The teachers are able to represent computer science tasks and learning content in different ways and to concretize abstract concepts by various examples," and "The teachers are able to interpret and apply relevant curricula and standards for planning computer science lessons" [2, p. 527]. Like the conceptualization of teacher knowledge presented in [15], the model is somewhat general and nonspecific in that the subject matter knowledge, in this case computer science, serves as a placeholder; any content area could be named in the framework.

The resulting framework presented by [2] is a reorganization of the constructs in [15]. It identifies three domains of competencies: pedagogical content knowledge, teacher beliefs, and motivational orientations. Pedagogical content knowledge was divided into five dimensions: (a) subject- and curriculum-related issues, (b) teaching methods and use of media, (c) learner-related issues, (d) teacher-related issues, and (e) issues of the educational system. The five dimensions in fact envelope ideas around subject matter content knowledge and curricular knowledge of [15], while highlighting pedagogical content knowledge as a significant construct.

The other two domains of the model in [2] were teacher beliefs and teacher motivational orientations. Teacher beliefs included epistemological beliefs about computer science subject matter knowledge, beliefs about teaching and learning computer science, and beliefs about data security and privacy. Epistemological beliefs refer to beliefs about the nature and justification of knowledge in a subject area, in this case, computer science. Epistemological beliefs are linked to beliefs

about teaching and learning processes of the subject area; for example, if a subject area is epistemologically viewed as certain and free of context and human values, then one assumes that the teaching and learning of the content is straightforward, transmitted from the teacher to the learner with little misinterpretation. If a subject area is epistemologically viewed as uncertain or relative, based in context, and subject to the values of those involved, then beliefs about teaching and learning processes tend to center on multiplicity and sense-making in different ways.

Beliefs about data security and privacy were described as "aspects of dealing with intellectual property, privacy and civil liberties, security policies, laws, and computer crimes" [2, p. 521]. Reference [24] described these beliefs as containing "a sensitive understanding of community values and the laws by which we live, maintaining awareness of consequences of ethical dissent and whistle blowing with regard to information systems" (p. 1961). This set of beliefs within the framework provide specificity in that data security and privacy is specific to computer science. Finally, teacher motivational orientations of the competency model in [2] referred to enthusiasm for teaching the content and teacher self-efficacy for teaching computer science.

While [2] provides general descriptors of knowledge and competencies of computer science teachers, [27] provided specificity of teacher pedagogical content knowledge for computer science by describing topic-specific misconceptions of learners of computer science. They achieved this by interviewing 60 secondary school students enrolled in the first computer science course in their program. This work brought forward common misconceptions of beginning programmers, specifically about iterations and runtime. In the process, they unearthed two new misconceptions not previously reported in the literature, thus further informing computer science teachers and the discipline of computer science of additional understandings of "what makes the learning specific topics easy or difficult" [15, p. 9]. Similarly, others have reported on learners' thinking related to algorithms and data structures [28,29] and object-oriented programming misconceptions [30,31].

Research specific to learners' common misconceptions of concepts within computer science along with the frameworks from [15] and [2] allow for a balance of generalized knowledge constructs of describing computer science teacher knowledge with specific knowledge constructs unique to a given topic in a discipline, in this case, the topic of programming in the discipline of computer science. A point is that while frameworks provide generalized understandings of teacher knowledge for a given knowledge domain, research around conceptions of learners provide the also necessary specificity for that knowledge domain.

Other studies within computer science start with the known misconceptions of learners to work with teachers to better understand pedagogical content knowledge around teaching programming concepts. Reference [6] used teaching vignettes that illustrated learner misconceptions to explore ways to describe and capture programming pedagogical content knowledge of teachers; this work led to the development of an instrument designed to measure the knowledge needed to teach this topic of computer science [5]. In other words, practically and methodologically, when common learner misconceptions are known, vignettes illustrating the misconceptions are useful for both teaching about and measuring of pedagogical content knowledge of educators in a subject area. To date, research about conceptions of learners and research about educators' pedagogical content knowledge related to the teaching and learning of network security concepts has not been explored. As an additional example, the review of pedagogical content knowledge in computing education in [32] did not reveal empirical studies specific to network security.

Self-report data is another venue for understanding teacher knowledge. Reference [33] used semi-structured interviews that asked teachers of grade 10-12 students in the Netherlands to self-report their knowledge of goals, instructional strategies, students' understanding, and assessment to describe computer science teacher pedagogical content knowledge for teaching algorithms and algorithmic thinking, arguing that the topic of algorithms remains as a centralizing topic for computer science despite the fast-changing world of computer technology. While their sample size was small (seven), their work captures the intricate complexity of components of pedagogical content knowledge for teaching algorithms and connections between them.

Network security is a topic within computer science. To date educator knowledge specific to teaching network security has not been investigated. Our work attends to this gap. We used a 2-year NSF-funded curriculum development and implementation project specific to teaching network security concepts in undergraduate and graduate higher education courses as an opportunity to describe network security educator knowledge constructs. The frameworks previously described served as tools for describing these knowledge constructs. For example, curricular knowledge, as defined by [15], was evident in our context in that the educator sought out funding to develop a new curriculum because of dissatisfaction of other curricula available for teaching these concepts.

The educator designed the curriculum with the assumption that network protocol behavior observations and trust points are centralizing topics for teaching networking and network security concepts, and instruction of the content should center on "designing for security," [34]. The instructional modules and hands-on laboratory experiments supported students in developing networking and network security concepts through network protocol behavior observations and learning elements on implied trust boundaries. The educator took the stance that this was in contrast to other curricula that focus on the mindset of adversaries, for example "capture the flag" scenarios that are designed to develop skills such as exploiting websites, cracking passwords, and breaching unsecured networks [35]. While such activities develop technical knowledge of network security, they are lacking in developing best practices of design mindset

with security policy and in developing understanding and skills to combat emerging and non-encountered advanced cyberthreats. Alternatively, this new curriculum centralizes on developing an understanding of how systems work in preparation of emerging threats that have not yet happened.

Pedagogical content knowledge of the educator was also evident in that the curriculum was intentionally designed to address misconceptions of learners. We wondered what an in-depth analysis of the educator's rationale for the curriculum and the initial implementations of the curriculum would further reveal about network security educator knowledge. We asked what kinds of educator knowledge are evident in designing and delivering curriculum about networking and network security?

III. Methodology

A. Setting

This is a descriptive study that uses frameworks of teacher knowledge [2,15] to describe network security educator knowledge. The work took place at a large urban research university located in a southcentral region of the United States. This university has Centers of Academic Excellence in Cyber designation. The educator is an Associate Professor in a Department of Engineering Technology and has been at the university since 2010. The other two authors are faculty in a College of Education since 2004 and have expertise in teaching and learning processes in K-12 mathematics and teacher education, and the impact of systemic influences of assessment and related policies on the learning trajectory of students. Opportunities to engage with the network security educator as she developed and piloted materials occurred about monthly, led by the first author, in the context of teaching different courses over two years. Courses were on undergraduate and graduate degree plans of majors such as computer engineering technology, computer information systems, cybersecurity, and network communications.

One course is a required undergraduate course in the undergraduate Computer Engineering Technology degree program that provides foundational knowledge of computer networking. Every computer system is connected in a network setting with data exchange requirements. Therefore, graduates of this degree are expected to understand how their computer-based systems will network and provide data flow capabilities in various application settings. This course also serves as a required prerequisite for other courses in other programs.

A second course, an elective, is an advanced undergraduate course for which the foundational course serves as a prerequisite. A third course is at the graduate level and focuses on cybersecurity concepts and is required in the Cybersecurity master's degree program. The graduate course requires no specific prerequisite coursework.

The curriculum specific to network security is sequenced so that learners gain the requisite knowledge on how networks are designed and operated while made aware of how the implied and explicit trust is placed for the data flows that are exchanged and stored using the network protocols. The protocol behavior observation scenarios walk students through trusted network packet fields and endpoint data stores, and how these trust points can become vulnerable.

The delivery platform utilizes a web-based note-taking environment, Jupyter notebooks (https://jupyter.org/), that has become popular for data science applications. The Jupyter notebooks provide code execution and note-taking in students' lab notebooks. Students only need a computer or tablet with an internet connection and a browser. The lab notebooks are possible to save into the course lab system for future use. The course exercises, practice problems, lab tasks, and exams are conducted in these notebooks. In addition, the course has online documentation that is web-based and dynamically updated. More details about the curriculum can be found at the UH-Netlab (http://info.uh-netlab.org/info/instruction.html).

The admitted student body to the graduate program come from different backgrounds and careers. The students in the course are sometimes existing cybersecurity professionals who are interested in fortifying their resume with a Master of Science degree. There are also students who have had no prior exposure to the field other than having completed a technical degree in majors such as Computer Science or Electrical Engineering. The assortment of careers reported from students in this course are security guard, armed forces, and engineering fields such as biomedical, chemical, and mechanical and social sciences. The work experience level of the students in their existing careers range from entry level to more than 10 years.

B. Data and Data Analyses

An intent of data collection and data analysis was to gather and then describe evidence of network security educator knowledge within a post-secondary setting. The primary data source was transcriptions of the recorded monthly meetings with the educator as she discussed her experiences as she piloted the materials. Oftentimes, the meeting would start with the educator sharing highlights regarding strengths and challenges of the most recently taught class. Teaching and learning topics discussed included how well she felt a lecture was delivered, student engagement during the lecture, how well students performed on the assigned homework, how students performed on assessments, and how the curriculum and the platform facilitated or hindered student learning. Additionally, they engaged in discussions about different learning theories. For example, the educator reviewed the Universal Design for Learning Framework (UDL, https://udlguidelines.cast.org/) and discussed ways in which chosen instructional strategies and the curriculum design aligned with this framework. Fieldnotes were also taken during these meetings. Additional and secondary data sources included the submitted proposal that was awarded as well as instructional artifacts such as PowerPoint slides, assigned exercises, and tests. Selected recorded class sessions were also viewed. The instructional artifacts were primarily used as prompts for the educator to further share her thinking as she reflected on her delivery of the curriculum.

The transcriptions and other artifacts were imported into a qualitative analysis software called Dedoose. A deductive

This work was supported by the National Science Foundation, Award #1907537.

coding process was used with five initial parent codes defined from [2] and [15]. The five initial codes were subject matter content knowledge (CK), pedagogical content knowledge (PCK), and curricular knowledge (CuK), from [15], and teacher beliefs (TB) and teacher motivational orientations (MO) from [2]. Transcripts and other artifacts were divided into excerpts in which the coder identified evidence of teacher knowledge. Additional parent codes were generated if the coder inferred that the excerpt was not captured by the five initial codes. A sixth parent code, general pedagogical knowledge (PK) emerged early in the initial coding process. After this first phase of coding, child codes were generated within each parent code using an inductive open-coding process to categorize the ideas within each parent code.

IV. FINDINGS

The goal of this work was to use frameworks of teacher knowledge to describe network security educator knowledge in the provided context. Fig. 1 illustrates the kinds of knowledge that emerged from the data, as well as the relationships between them, as perceived by the researchers. The dotted lines in Fig. 1 illustrate the blurred boundaries across the kinds of knowledge; Fig. 1 also illustrates the overlap of kinds of knowledge that exist when considering educator knowledge from a holistic perspective. Finally, the text inside Fig. 1 were the child codes generated within the indicated parent code.

A. Curricular Knowledge

Curricular knowledge is illustrated as an oval in Fig 1. One form of curricular knowledge, identified as *other curricula*, was knowledge of available materials for instruction of networking and network security concepts. As was stated earlier, the motivation to seek funding to develop a new curriculum was in response to an analysis of other curricula available for teaching these concepts. The proposal for the funding outlined the deficiencies of existing curriculum for the purposes of teaching networking and network security concepts, thus illustrating the educator's knowledge of available and appropriate materials.

The data also revealed the educator's established understandings of the trainings and certifications required by different careers and professions that use network security concepts in their respective domains. These instances were coded as evidence of educator *industry knowledge*. While identified as a component of curricular knowledge, discussions about these certifications led to identification as pedagogical content knowledge because it emerged primarily in discussions about learners who had misconceptions related to networking and network security concepts as a consequence of these industry-valued certifications.

As explained by the educator, the certification trainings were rooted in simulation environments where protocol behavior is preloaded into components, and operators used drag and drop mechanisms to experiment and observe behaviors. The educator expressed that these training opportunities led by major vendors in networking and cybersecurity interfered with the development of a deep understanding of networks from a design perspective. Application and implementation of design templates offered by the major vendors facilitated the

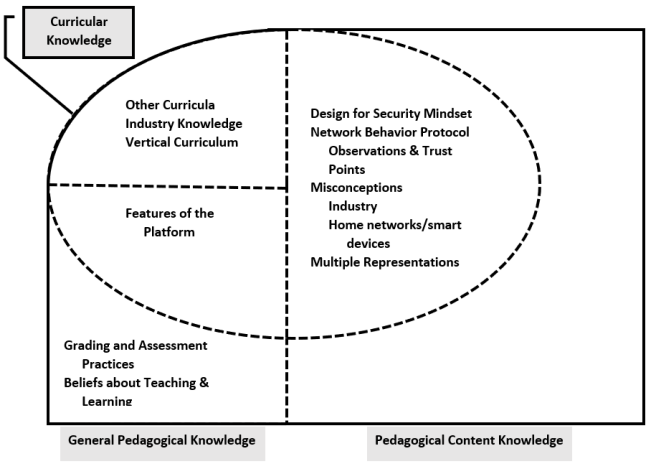

Figure 1. Kinds and Examples of Network Security Educator Knowledge

misconception that these templates could be applied in a successful manner, without taking into account the vulnerability of trust boundaries. The expectations from employers on such certifications made it more challenging to convince learners in the graduate course, in particular, that a design for security mindset is a generative approach to securing networks.

The educator explained that these experiences and other trainings oftentimes led to fragile conceptual understandings about network security that limited learners' capacities to initially make sense of the educator's innovative curricular approach of designing for security. In this sense pedagogical content knowledge and curricular knowledge are seen as overlapping constructs. The educator was aware of the misconceptions of the learners brought on by these different platforms, and accordingly considered ways to adapt the course curriculum and instructional practices to account for said misconceptions. One way to do this was to provide practice items within the homework assignments that would lead the learner with the misconception to the wrong answer. The feedback loop embedded in the platform then allowed the learner to reflect on their error.

A second form of curricular knowledge was that of vertical curricular knowledge which emerged when the educator had opportunity to discuss where a given course was situated within different majors of the department, and any perceived impact the course content might have for students' progress in their respective programs. This form of curricular knowledge was less prevalent than other forms of curricular knowledge because at the time of the study, the focus was on the initial implementation of the new curriculum.

B. Pedagogical Content Knowledge

Pedagogical content knowledge is illustrated by the rectangular right portion of Fig 1. Additional illustrations of pedagogical content knowledge were evident in the original design of the innovative curriculum. As was described earlier, the curriculum centered around the assumption that network protocol behavior observations and trust points were centralizing topics for delivery of network security concepts. Accordingly, the curriculum was specifically designed to bring forward anticipated misconceptions of learners while instilling

the mindset of "designing networks for security". For example, components of the curriculum such as session notes, the practice exercises and the hands-on experiments were designed to provide learners opportunity to observe and respond to the protocol trust points that showed how route definitions may cause packets to be looped in a network, even when there is no layer 1 or 2 loop in the network graph. Other designs provided opportunity to investigate how unintended recipients of packets can cause unauthorized access to potentially sensitive data while the protocol is operating as intended, or to notice where the destination interface for its corresponding IP address was due to a spoofed address in another protocol.

Another important feature of the materials that illustrated pedagogical content knowledge was the use of multiple representations to illustrate the content. Text, tables, and flow charts were used, with flow charts highlighted by the educator as "a concise language for representing networking and network security concepts," particularly in illustrating conditional statements. Multiple representations were useful in allowing learners to make sense of the content in multiple ways that may support their learning styles; the educator noted that some textbooks relied too heavily on text, which in turn hindered student learning.

These representations were important as the educator acknowledged and built from conceptions that everyday users of the internet and home networks bring to the classroom. For example, smart switches that can be managed remotely, smart phones, smart appliances and the like are bundled and integrated and ready for use. However, a consumer who can network one's home does not necessarily have the knowledge set needed for understanding networking and network security. In fact, the educator argued that the manufactured simplicity of using such devices had potential for fostering misconceptions related to designing for security as well as hindering the thinking processes of how networks behave, and the security risks that arise. While simplicity was ideal for the everyday user, it was not ideal for learning networking and network security concepts. The educator was aware of misconceptions that arise from everyday technology use and designed and implemented the curriculum around these known experiences. Again, similar to attending to misconceptions that arose from *industry knowledge*, the educator provided opportunities for learners to reassess their answers, without penalty to the course grade. The goal was to foster skills and tools to combat problems that did not have pre-made, manufactured solutions.

C. Generalized Pedagogical Knowledge

General pedagogical knowledge is illustrated by the rectangular left corner of Fig. 1. Discussions about the platform's design features brought forward this generalized pedagogical knowledge and indicated how educator beliefs interact with the design and implementation of curricular materials. For example, within the practice feature of the platform, learners received immediate feedback to the correctness of their responses to the exercises. The intent was to provide a reflective space for the learner to discern what was incorrect and why, presumably from the previously provided course content, and to refine their understandings and try again. Two main ideas emerged in discussions about this feature. First, in initial implementations, the platform did not provide specificity to why the learner's response was incorrect; the manner of the feedback to the learner did not provide enough information to initiate the intended reflective activity. As the educator explained, "they could not make sense of why." Comments such as these indicated epistemological beliefs and the expectation that learners are active and sense-making in learning processes.

Second, grading and assessment practices, a component of generalized pedagogical knowledge, were evaluated and re-evaluated by the educator as a way to message to the students that a grade in a course was not as important as the learning the content. That is, the educator wanted learners to be willing to take risks and to learn from mistakes and move forward. At the same time, the educator was cognizant of student expectations that there needed to be graded components of the course that would result in a course grade for college credit. This proved to be a challenging goal, as one would expect in higher education.

V. DISCUSSION

Our findings contribute in the following ways. First, it speaks to the utilization of teacher knowledge frameworks. Second, this work contributes to methodological strategies for studying teacher knowledge. Finally, insights provided are specific to educator knowledge within computer science education where the topics are networking and network security. These ideas are further elaborated upon.

The teacher knowledge frameworks from [15] and [2] were useful tools for describing network security educator knowledge. On the one hand, the three seemingly discrete categories in [15], namely subject matter content knowledge, pedagogical content knowledge, and curricular knowledge, had descriptive power. On the other hand, the competencies in [2] embedded subject matter knowledge and curricular knowledge as components of pedagogical knowledge, and their other two domains of teacher beliefs and teacher motivational orientations provided a means for considering educator dispositions. Allowing for framing teacher knowledge in both ways highlights an appreciation of acknowledging discrete constructs while also acknowledging the paradox that in fact these constructs are intrinsically intertwined. This was particularly evident for us since our process led us to infer pedagogical content knowledge from discussions around curriculum development and initial implementation. Of particular interest is the emergence of evidence of pedagogical content knowledge to specific topics, in our case, topics about networking and network security.

Consideration of this paradox is necessary within training programs for higher education faculty as well as teacher education programs preparing computer science educators. Within higher education and within discipline-based colleges in particular, subject matter content knowledge of higher education faculty is assumed, and training programs focus on pedagogical practices. To what extent do training programs highlight curricular knowledge that can be in part, characterized by assumptions about pedagogy? Explicit trainings, comparing and contrasting curricula specific to an evolving discipline such as cybersecurity could be a useful venue for supporting growth in educator knowledge and practices by focusing on implicit

assumptions about pedagogy embedded in the curricula. Additionally, we recommend training programs that invest time in making these frameworks explicit to educators; this allows them to reflect on what they perceive to be successes and failures while teaching the content. For novice educators, the frameworks provide a language for which to describe their work; in our case, the experienced educator was able to align and describe her practices in terms of the frameworks provided by the education experts on the team.

The use of a curriculum development project to study educator knowledge is a second contribution of this work. Educators are both consumers and creators of curriculum. Therefore, use of such projects can serve as fruitful contexts for studying the nature and organization of educator knowledge. Furthermore, networking and network security are evolving knowledge domains; it makes sense that curriculum will need to evolve as the topics do, providing plentiful opportunities to capture and understand educator knowledge.

Finally, our work provides insights into educator knowledge within computer science education where the topics are networking and network security. To date, these areas are rarely explored. As one example, our findings identify *industry knowledge* as a form of curricular knowledge which speaks to the evolving nature of network security because as technological advances are made, network security educators' knowledge about advances will need to follow. A second example is the topic-specific misconceptions about networking and network security that stem from everyday technology use. Awareness of these misconceptions and how to address them led to illustrations of pedagogical content knowledge through instructional practices structured to bring the misconceptions forward rather than being surprised by them. These examples help balance what we gain from generalized educator knowledge frameworks by including topic-specific knowledge constructs in computer science education in general, and cybersecurity more specifically.

REFERENCES

[1] National Centers of Academic Excellence in Cybersecurity (NCAE-C) (2022). *CAE Documents Library*. https://public.cyber.mil/ncae-c/documents-library/

[2] Bender, E., Hubwieser, P., Schaper, N., Margaritis, M., Berges, M., Ohrndorf, L., Magenheim, J. & Schubert, S. (2015) Towards a competency model for teaching computer science, *Peabody Journal of Education*, *90*(4), 519-532, https://doi.org/10.1080/0161956X.2015.1068082

[3] Ni, L., Tian, Y., McKlin, T., & Baskin, J. (2023). Who is teaching computer science? understanding professional identity of American computer science teachers through a national survey. *Computer Science Education*, 1-25, https://doi.org/10.1080/08993408.2023.2195758

[4] Sadik, O & Ottenbreit-Leftwich, A. T. (2023) Understanding U.S. secondary computer science teachers' challenges and needs, *Computer Science Education*, https://doi.org/10.1080/08993408.2023.2209474

[5] Yadav, A. & Berges, M. (2019). Computer Science Pedagogical Content Knowledge: Characterizing Teacher Performance, *ACM Transactions on Computing Education*, *19*(3), Article 29, Publication date: May 2019. DOI: https://doi.org/10.1145/3303770

[6] Yadav, A. Berges, M., Sands, P. & Good, J. (2016). Measuring computer science pedagogical content knowledge: An exploratory analysis of teaching vignettes to measure teacher knowledge, WiPSCE '16: *Proceedings of the 11th Workshop in Primary and Secondary Computing Education* October 2016, 92-95, https://doi.org/10.1145/2978249.2978264

[7] Baumert, J., Kunter, M., Blum, W., Brunner, M., Voss, T., Jordan, A., Klusmann, U., et al. (2010). Teachers' mathematical knowledge, cognitive activation in the classroom, and student progress. *American Education Research Journal*, *47*(1), 133-180, https://doi.org/10.3102/0002831209345157

[8] Callingham, R., Carmichael, C. & Watson, J.M. (2016). Explaining student achievement: the influence of teachers' pedagogical content knowledge in Statistics. *International Journal of Scencei and Mathematics Education*, *14*, 1339–1357, https://doi.org/10.1007/s10763-015-9653-2

[9] Hill, H.C., Rowan, B., & Ball, D.L. (2005). Effects of teachers' mathematical knowledge for teaching on student achievement. *American Educational Research Journal*, *42*(2), 371-406. https://doi.org/10.3102/00028312042002371

[10] Keller, M. M., Neumann, K., & Fischer, H. E. (2017). The impact of physics teachers' pedagogical content knowledge and motivation on students' achievement and interest. *Journal of Research in Science Teaching*, *54*(5), 586-614, https://doi.org/10.1002/tea.21378

[11] Voss, T., Kunter, M., & Baumert, J. (2011). Assessing teacher candidates' general pedagogical/psychological knowledge: Test construction and validation. *Journal of Educational Psychology*, *103*(4), 952–969. https://doi.org/10.1037/a0025125

[12] Cabaj, K., Domingos, D., Kotulski, Z., & Respicio, A. (2018). Cybersecurity education: Evolution of the discipline and analysis of master programs, *Computers & Security*, *75*, 24-35, https://doi.org/10.1016/j.cose.2018.01.015

[13] Peterson, R., Santos, D., Smith, M. C., Wetzel, K.A. & Witte, G. (2020). *Workforce framework for cybersecurity (NICE Framework)*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

[14] Paloalto Networks (2022). *Cybersecurity Curriculum*. https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/cybersecurity-academy-curriculum

[15] Shulman, L. S. (1986). Those who understand: knowledge growth in teaching. *Educational Researcher*, *15*(2), 4–14, https://doi.org/10.2307/1175860

[16] Carlson J. et al. (2019). The refined consensus model of pedagogical content knowledge in science education, In A. Hume, R. Cooper, A. Borowski (eds). *Repositioning Pedagogical Content Knowledge in Teachers' Knowledge for Teaching Science,* Springer: Singapore. https://doi.org/10.1007/978-981-13-5898-2_2

[17] Hill, H.C., Ball, D. L., & Schilling, S. G. (2008). Unpacking pedagogical content knowledge: Conceptualizing and measuring teachers' topic-specific knowledge of students, *Journal for Research in Mathematics Education*, *39*(4), 372-400, https://doi.org/10.5951/jresematheduc.39.4.0372

[18] Freeman, D., Katz, A., Gomez, P. G., & Burns, A. (2015). English-for-teaching: rethinking teacher proficiency in the classroom, *English Language Teaching Journal*, *69*(2), 129-139, https://doi.org/10.1093/elt/ccu074

[19] Mishra, P. & Koehler, M. J. (2006). Technological pedagogical content knowledge: A framework for teacher knowledge, *Teachers College Record*, *108*(6), 1017-1054, https://doi.org/10.1111/j.1467-9620.2006.00684.x

[20] Dyches, J. & Boyd, A. (2017). Foregrounding equity in teacher education: Toward a model of social justice pedagogical and content knowledge, *Journal of Teacher Education*, 68(5), 476-490, https://doi.org/10.1177/0022487117705097

[21] Chick, H. & Beswick, K. (2018). Teaching teachers to teach Boris: a framework for mathematics teacher educator pedagogical content knowledge, Journal of Mathematics Teacher Education, 21, 475-499, https://doi.org/10.1007/s10857-016-9362-y

[22] Beswick, K. & Goos, M. (2018). Mathematics teacher educator knowledge: What do we know, and where to from here? *Journal of*

Mathematics Teacher Education, 21, 417-427, https://doi.org/10.1007/s10857-018-9416-4

[23] Chauvot, J. (2009). Grounding practice in scholarship, grounding scholarship in practice: Knowledge of a mathematics teacher educator-researcher. *Teaching and Teacher Education, 25*(2), 357-370, https://doi.org/10.1016/j.tate.2008.09.006

[24] Bender, E., Schaper, N., Caspersen, M. E., Margaritis, M., & Hubwieser, P. (2016). Identifying and formulating teachers' beliefs and motivational orientations for computer science teacher education. *Studies in Higher Education*. https://doi.org/10.1080/03075079.2015.1004233

[25] Hubwieser, P., Berges, M., Magenheim, J., Schaper, N., Br¨oker, K., Margaritis, M.,. .. Ohrndorf, L. (2013). Pedagogical content knowledge for computer science in German teacher education curricula. In M. Caspersen, M. Knobelsdorf, & R. Romeike (Eds.), *WiPSCE '13, Proceedings of the 8th Workshop in Primary and Secondary Computing Education* (pp. 95–103). https://doi:10.1145/2532748.2532753

[26] Hubwieser, P., Mühling, A., Magenheim, J., & Ruf, A. (2013). Towards a Conceptualization of Pedagogical Content Knowledge for Computer Science, *ICER '13: Proceedings of the ninth annual international ACM conference on International computing education research*, pp. 1–8, https://doi:10.1145/2493394.2493395

[27] Shah, P., Capovilla, D., Hubwieser, P. (2015). Searching for barriers to learning iteration and runtime in computer science Association for Computing Machinery's, 2015 annual conference, Workshop in Primary and Secondary Computing Education (WiPSCE '15), *Proceedings of the 10th Workshop in Primary and Secondary Computing Education* (pp. 73-75). http://dx.doi.org/10.1145/2818314.2818326

[28] Danielsiek, H., Paul, W., Vahrenhold, J. (2012). Detecting and understanding students' misconceptions related to algorithms and data structures. In *Proc. 43rd SIGSCE Comp. Sci. Ed.*, pp. 21-26, https://doi.org/10.1145/2157136.2157148

[29] Gal-Ezer, J., Zur, E. 2003. The efficiency of algorithms– misconceptions. *Computers & Education, 42*(3), 215-226, https://doi.org/10.1016/j.compedu.2003.07.004

[30] Holland, S., Griffiths, R., Woodman, M. (1997). Avoiding Object Misconceptions. *SIGCSE Bulletin, 29*(1), 131-134. https://doi.org/10.1145/268084.268132

[31] Ragonis, N., Ben-Ari, M., 2005. A long-term investigation of the comprehension of OOP concepts by novices. *Computer Science Education, 15*(3), 203-221, http://dx.doi.org/10.1080/08993400500224310

[32] Hubbard, A. (2018) Pedagogical content knowledge in computing education: a review of the research literature, *Computer Science Education, 28*(2), 117-135, https://doi.org/10.1080/08993408.2018.1509580

[33] Nijenhuis-Voogt, J., Bayram-Jacobs, D., Meijer, P. C., & Barendsen, E. (2021). Teaching algorithms in upper secondary education: a study of teachers' pedagogical content knowledge. *Computer Science Education*, 1-33, https://doi.org/10.1080/08993408.2021.1935554

[34] Shostak, A. (2014). *Threat modeling: Designing for security*. John Wiley & Sons.

[35] Švábenský, V., Čeleda, P., Vykopal, J., & Brišáková, S. (2021). Cybersecurity knowledge and skills taught in capture the flag challenges. *Computers & Security, 102*, 1-14, https://doi.org/10.1016/j.cose.2020.102154