Bridging the Gap: Empowering Student Veterans for Hardware Security Careers

Hyunju Oh, University of Florida

Hyunju Oh is a Ph.D. student in Educational Technology at UF College of Education. She holds a Bachelor's degree in Education from Kookmin University, South Korea, and a Master's degree in Educational Technology from Korea University, South Korea. She is interested in Online Learning, Learning Analytics, STEM education, and AIED.

Rui Guo, University of Florida

Dr. Rui Guo is an instructional assistant professor of the Department of Engineering Education in the UF Herbert Wertheim College of Engineering. Her research interests include data science & CS education, Fair Artificial Intelligence and Experiential learning.

Wanli Xing, University of Florida

Wanli Xing is the Informatics for Education Associate Professor of Educational Technology at University of Florida. His research interests are artificial intelligence, learning analytics, STEM education and online learning.

Sandip Ray, University of Florida

Dr. Sandip Ray is an Endowed IoT Term Professor at the Department of Electrical and Computer Engineering, University of Florida. His research involves developing correct, dependable, secure, and trustworthy computing through cooperation of specification, synthesis, architecture and validation technologies.

`

Bridging the Gap: Empowering Student Veterans for Hardware Security Careers

1. Introduction

The need for education in hardware security has been growing in recent years. Hardware security encompasses the development, design, and validation of countermeasures intended to detect and prevent compromises in modern electronic components. This field specifically addresses threats such as side-channel attacks, hardware Trojans, and supply chain vulnerabilities, which have become increasingly prominent in recent years. Protecting hardware is critical, as it represents the foundational "root of trust" for all software applications and network operations. Vulnerabilities at this foundational level can compromise the integrity of entire systems [1], potentially causing to catastrophic consequences, especially in critical applications such as military and commercial cyberinfrastructure.

Unlike software and network security, which have been extensively analyzed and deployed, hardware security is a relatively new field. Historically, there has been a flawed assumption that hardware is inherently secure and trustworthy, making it immune to cyber threats [2]. However, experts have increasingly highlighted vulnerabilities in hardware and embedded systems, pointing out significant risks posed by malicious actors exploiting complex and distributed semiconductor supply chains. Consequently, this misconception has led to a critical shortage of trained professionals in hardware security [3]. Training and education in hardware security are critical to building a robust workforce capable of addressing these challenges, especially given the scarcity of skilled experts in this field.

The field of hardware security demands a workforce equipped with both a profound technical understanding of hardware functionality and the analytical skills to assess how vulnerabilities affect microelectronic systems. Traditional educational methods, such as lectures, often fall short in addressing the intricate challenges of this field [4]. Instead, practical, hands-on experience is crucial. Students require direct exposure to semiconductor devices, hack systems, and witness the real-world consequences of their actions within industrial environments [5]. Therefore, training programs led by experienced industry professionals, operating in authentic infrastructure settings, can play a pivotal role in reshaping the microelectronic design ecosystem.

Veterans are uniquely positioned to excel in hardware security, given their specific skillsets and experiences aligning closely with industry demands. Their military training equips them with hands-on expertise in areas like mechanics, electronics, and construction, providing a solid technical foundation for hardware security work. Veterans' ability to thrive in high-stress environments [6], coupled with their precision and attention to detail, makes them particularly suited for hardware security, where mistakes can have critical consequences. However, despite their capabilities, not many veterans are currently working in STEM fields, leaving their talents largely untapped [7]. This highlights the necessity for targeted programs that facilitate veterans' transition into hardware security and STEM careers.

`

In response to the pressing need for skilled hardware security professionals, this project developed an innovative experiential learning program: Veterans SkillBridge through Industry based Hardware Security Training and Education (VETS-HASTE). Grounded in cognitive apprenticeship theory, VETS-HASTE addresses the specific needs of hardware security, emphasizing hands-on engagement, real-world problem-solving, and mentorship from experienced professionals. The program specifically targeted veterans, aiming to bridge the gap between their existing technical skills and the specialized expertise required in hardware security.

This study seeks to address the following research questions:

1. How can a hardware security program be designed to support veterans' learning based on the cognitive apprenticeship theory?

2. What are the experiences of veteran participants in the VETS-HASTE program?

2. Theoretical Framework

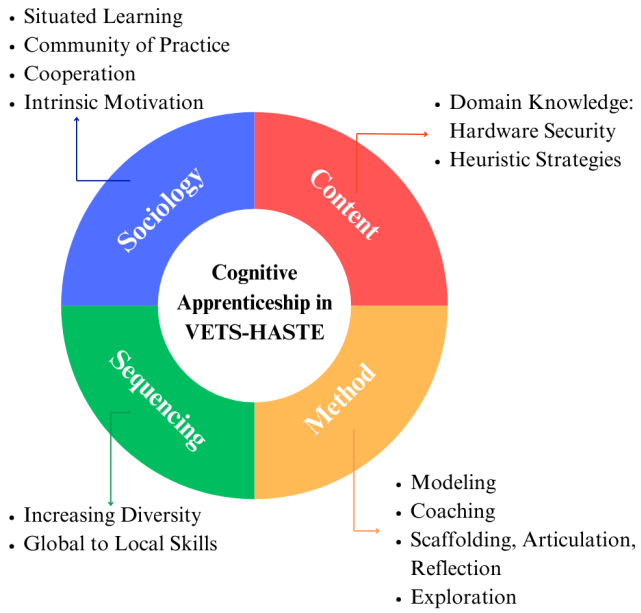

Figure 1. Cognitive Apprenticeship in VETS-HASTE

The Cognitive Apprenticeship Theory supports learners by engaging them in learning processes similar to those of experts. It helps learners develop the cognitive and metacognitive skills necessary to perform learned tasks [8]. [9] proposed four dimensions for designing learning environments based on this model: Content, Method, Sequencing, and Sociology.

First, Content pertains to the types of knowledge learners need to develop expertise, including domain knowledge and heuristic strategies necessary for completing tasks. In this study, students

`

learned hardware security as domain knowledge by solving real-world problems and participating in internships.
Second, Method refers to the various approaches that promote the development of learners' expertise, such as *modeling, coaching, scaffolding, articulation, reflection*, and *exploration* [10]. The VETS-HASTE program utilized these methods throughout its activities. For instance, students could observe experts' performance by following step-by-step *modeling* in industry-driven courses. As part of *coaching*, internship opportunities allowed experts in hardware security to observe and facilitate students' performance. Throughout the program, students were guided, supported in practicing and applying their knowledge, and encouraged to collaborate with peers. This progression represented *scaffolding, articulation, and reflection*, which are crucial components of the cognitive apprenticeship model. Additionally, students were encouraged to *explore* their careers and the domain independently, solving problems on their own.

Third, Sequencing emphasizes the significance of learning order, advocating for conceptual understanding before practice, a progression from simple to complex tasks, and practice in diverse situations. During the program, students tackled various problems related to hardware security in their coursework and later applied this knowledge in real-world settings through internships.

Finally, Sociology highlights the importance of the context in which students engage in learning tasks, emphasizing the role of community and collaboration, as well as the need for intrinsic motivation in learning. In this study, students learned the concept by solving problems driven by industry. They were encouraged to collaborate with veteran colleagues and demonstrated high intrinsic motivation in their learning, as they had prior knowledge or experience in related fields and viewed hardware security as a potential career path.

3. Methodology

1) VETS-HASTE Program

VETS-HASTE is a collaborative program designed to provide veterans with specialized training in hardware security. This initiative is a partnership between the university, a non-profit for veterans' education, and industries with a strong hardware security focus. The program focused on developing a unique, experiential learning curriculum, grounded in cognitive apprenticeship theory, to help veterans gain new skills and create pathways into hardware security careers.

2) Measurement

We conducted the program with ten veterans in Florida. The industry-driven course ran for 12 weeks, from May 6 to July 28, 2024, and covered topics in hardware security. The first week of the course was conducted on-site, on the university campus, while the remaining eleven weeks were delivered online. Two graduate students majoring in Electrical and Computer Engineering taught and facilitated the course. The internship started after the course and ran for 12 weeks, ending on October 31, 2024. Nine out of ten students participated in internships with one of two local hardware security industries.

`

Participants were asked to answer survey questions during the first week of coursework and again in November, after completing their internships. Eight out of ten participants responded to the post-survey, six participants completed the knowledge test, and five participants took part in interviews to share details about their experiences.

The survey assessed participants' self-efficacy in hardware security using a 5-point Likert scale in both pre- and post-surveys. Four questionnaires, originally developed by [11], were modified to fit the context of our study. Additionally, a post-only survey was conducted to measure participants' engagement in the program, using a 5-point Likert scale and modified questionnaires adapted from [12] and [13], tailored to the context of our study.

Knowledge test questions were designed by the instructors of the industry-driven course. A total of five open-ended questions on hardware security were provided. Two instructors individually graded the test results after the program concluded, and the mean scores were used for the analysis. Each question was worth 10 points, making the total possible score 50 points if all answers were correct.

4. Results

1) VETS-HASTE Program Development

Industry-Driven Course: The program was designed to span 12 weeks and was delivered in a hybrid format. During the first week, participants attended sessions on the university campus to set up their hardware devices and meet their colleagues. The remaining sessions were delivered online. The course featured extensive hands-on activities using the ‘Hardware Hacking board’ (HaHa board, [14]), including detailed step-by-step demonstrations where experts explained their thought processes and provided cognitive mapping for hardware security tasks. Over the 12 weeks, the course covered major hardware security concepts, such as buffer overflow, hardware Trojan attacks, and reverse engineering attacks. Students studied each subject over 1–2 weeks and could join bi-weekly Zoom office hours to ask questions and receive additional support from instructors.

Throughout the course, participants also had the opportunity to attend several webinars hosted by two hardware security companies. A total of seven webinars were provided, covering various aspects of hardware security, such as side-channel attacks.

Internship: Participants had the opportunity to join a three-month full-time internship with one of two local hardware security companies. These internships began in August 2024, following the conclusion of the training sessions in July. The full-time internships aimed to enhance veterans' autonomy and agency, helping them further develop their motivation, interest, and knowledge in hardware security.

`

2) Surveys, Knowledge Tests, and Interviews

The demographics of the study included eight participants, all of whom were male. In terms of education, one participant (12.5%) had a high school diploma or GED, another (12.5%) held an associate or technical degree, five participants (62.5%) had a bachelor's degree, and one participant (12.5%) had a graduate or professional degree. Regarding racial demographics, three participants (37.5%) identified as White or Caucasian, four (50%) as Black or African American, and one participant (12.5%) identified as Other. None of the participants identified as American Indian/Native American or Alaska Native, Asian, or Native Hawaiian or Other Pacific Islander.

Table 1. The Wilcoxon Signed Rank Test on the Self-efficacy Pre-post Surveys (n = 8)

Question	Pre			Post			Statistic Value	
	Mean	Median	SD	Mean	Median	SD	Z	Sig
A. I'm confident I can understand the basic concepts of hardware security.	4.25	4.50	0.89	4.63	5.00	0.52	.879	.380
B. I expect to do well in the hardware security training.	4.75	5.00	0.71	3.88	4.00	1.25	-2.121	.034*
C. I'm certain I can master the skills in hardware security.	4.63	5.00	0.52	3.50	3.50	1.51	-1.807	.071
D. Considering the difficulty of hardware security, the support, and my skills, I think I will do well in learning hardware security.	4.75	5.00	0.71	4.00	4.00	1.07	-2.121	.034*

Table 1 summarizes the Wilcoxon Signed Rank Test results comparing participants' self-efficacy before and after the training (n = 8). This non-parametric test was chosen due to deviations from normal distribution observed in survey responses. Although onfidence in understanding hardware security was slightly increased after the program, this change was not statistically significant (A. $Z = .879$, $p = .380$). Conversely, participants' certainty in mastering skills slightly decreased, but this was also not significant (C. $Z = -1.807$, $p = .071$). However, significant decreases were observed in expectations to perform well (B. $Z = -2.121$, $p = .034$) and confidence in succeeding in the hardware security field (D. $Z = -2.121$, $p = .034$).

Participants' engagement with the VETS-HASTE course was assessed through a post-only survey focusing on behavioral, cognitive, and emotional engagement (See Table 2, n = 8). In terns of behavioral engagement, participants reported moderate attention during the online portion (E. $M = 3.88$, $SD = 1.55$) and notably high attention during face-to-face sessions with all agreeing (F. $M = 4.63$, $SD = 0.52$). Additionally, punctuality in completing hands-on experiments had a mean score of 3.88 (G. $SD = 0.84$), with seven out of eight participants agreeing. Regarding cognitive engagement, results showed high levels of involvement, with all participants agreeing they read extra materials (H. $M = 4.38$, $SD = 0.52$) and found ways to learn

`

unclear concepts (I. M = 4.5, SD = 0.54). Emotional engagement was also positive, as participants showed general satisfaction with the hybrid format (J. M = 4.25, SD = 1.04) and expressed excitement about coursework (K. M = 4.13, SD = 0.99). Overall, participants exhibited high engagement across all evaluated domains, with minimal negative feedback.

Table 2. Post-only survey on Engagement (n = 8)

	Question	Mean	Median	SD	Disagreement	Agreement
Behavioral Engagement	E. I can pay attention well in the online part of the hybrid course.	3.88	4.50	1.55	2	6
	F. I can pay attention well in the face-to-face part of the hybrid course.	4.63	5.00	0.52	0	8
	G. I complete hands-on experiments on time in the hybrid course.	3.88	4.00	0.84	1	7
Cognitive Engagement	H. I read extra materials to learn more about topics covered online.	4.38	4.00	0.52	0	8
	I. If I don't understand something in the online class, I find a way to learn it.	4.5	4.50	0.54	0	8
Emotional Engagement	J. I like taking the combination of online and face-to-face courses.	4.25	4.50	1.04	1	7
	K. I feel excited about my work in the hybrid course.	4.13	4.00	0.99	1	7

Participants' knowledge acquisition was evaluated using a paired t-test comparing pre- and post-test scores (See Table 3). A paired t-test was appropriate since the knowledge scores were normally distributed. Results indicated a significant improvement, with mean scores rising from 16.92 (SD = 4.61) on the pre-test to 38.00 (SD = 6.77) on the post-test. The t-value was 8.687, and the p-value indicated a statistically significant difference ($p < .001$). Additionally, a large effect size (Cohen's d = 5.94) was noted, indicating a strong positive impact of the intervention on participants' knowledge levels. However, due to the small sample size, caution is advised when generalizing these results broadly.

`

Table 3. The t-test on the Pre-Post Knowledge Test (n = 6)

	Mean	Median	SD	t	df	Cohen's d	P-value
Pre Knowledge Test	16.92	17.25	4.61	8.687	5	5.94	< .001***
Post Knowledge Test	38	40.75	6.77				

Participants provided diverse feedback regarding the the VETS-HASTE program though the interview:

1. The VETS-HASTE program was structured as a hybrid course with one week of face-to-face instruction and the remaining weeks online. How satisfied or not satisfied are you with the balance between face-to-face and online components?

   "Since we had our board with us at home, we could have followed along with the experiment as well."

   "I think we needed more face to face interaction…It was very challenging because our knowledge was so limited in it requires a lot of preparation to do some of this."

2. The VETS-HASTE program contained 3 months of internship opportunities. How satisfied or not satisfied are you with the internship program?

   "Yes, employee A went out of his way to give me a better understanding of what he was trying to do, as far as dealing with machine learning and artificial intelligence, because that's a whole new concepts within hardware security."

3. In your opinion, did the VETS-HASTE program have an impact on your future aspirations and life choices in hardware security?

   "It actually put me on the path of hardware security. It's actually something I'm seeking and learning. ... And being around other veterans ... they're encouraging me. So it was very beneficial to me… because it allowed me to gain that confidence that I felt like I lacked."

   "No, I don't think I have an interest in hardware security…it was just difficult for me to catch on… because I didn't have a solid foundation"

4. Overall, how would you rate your experience with the VET-HASTE training program? What were the most positive aspects of the program? What areas do you think could be improved?

   "I give it a nine because it was really eye opening, and it helped me get a better understanding in information technology and specifically hardware security. ... And the other thing is, all the veterans always kept on sharing information. If they found something, they were sharing information…. everybody has been extremely professional and in that so I thank everybody for their time and effort and helping our veterans get a better understanding hardware security…. Why don't give it a 10? With the terms a book,

`

the different concepts, maybe we would read about it the night before and then go into it."

"Looking at other programs of the hardware packet programs, it's not as robust as the one that I experienced with this course…. you gotta outstand the program already. Just expound on that make it more simplified, so that way the student don't have to call on an instructor or email anything like that for help."

5. Discussion

The findings of this study provide valuable insights into the design, implementation, and impact of the VETS-HASTE program, which aimed to equip veterans with specialized hardware security skills through experiential learning grounded in cognitive apprenticeship theory. While the program demonstrated notable successes, it also revealed areas for improvement to enhance the learning experience and outcomes for future participants.

The VETS-HASTE program successfully incorporated core elements of the cognitive apprenticeship framework, such as modeling, coaching, scaffolding, and reflection. The significant knowledge gains underscore the effectiveness of the program in enhancing participants' technical expertise. It demonstrates that the curriculum effectively built upon participants' foundational knowledge and advanced their understanding of hardware security. However, the lack of significant improvement in self-efficacy metrics highlights a potential gap between knowledge acquisition and learners' confidence in their abilities. The decline in self-efficacy measures, particularly in expectations to perform well and confidence in mastering skills, suggests that participants may have faced challenges in fully internalizing the complex concepts presented. This may reflect the steep learning curve of hardware security and points to the need for enhanced support mechanisms, such as more frequent face-to-face interactions or structured preparatory resources, to bolster confidence alongside competence.

Overall engagement in the program was high across behavioral, cognitive, and emotional dimensions, indicating that the participants were invested in their learning experiences. The hybrid format, which blended in-person and online components, was generally well-received. However, interview feedback indicated a desire for more interactions to better support the comprehension of challenging topics. The participants' ability to share information and support one another contributed to a positive learning environment and community, aligning with the sociological dimension of the cognitive apprenticeship model.

While the program demonstrated significant strengths, several areas for improvement were identified: First, expanding in-person sessions or bi-weekly meetings could address the challenges participants faced in mastering complex topics, as highlighted in interview feedback. Second, participants suggested that simplifying course content or providing more detailed preparatory readings could reduce reliance on instructor intervention and promote greater independence. Third, some participants showed less improvement when their initial scores were already high, highlighting areas where the training could be further refined to benefit those who already had a stronger baseline understanding before the program.

`

6. Conclusion and Future Directions

The VETS-HASTE program demonstrated the potential of experiential learning, grounded in cognitive apprenticeship theory, to address the growing demand for skilled hardware security professionals while providing veterans with a pathway into STEM careers. Despite the challenges highlighted, the program's successes underscore the importance of hands-on training, mentorship, and community-driven learning in fostering technical expertise and engagement. By addressing identified areas for improvement, future iterations of the program can further enhance its impact, ensuring that it meets the diverse needs of its participants and contributes to building a robust hardware security workforce.

Acknowledgements

This work was supported by the National Science Foundation under Grant No. #2322465. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

References

[1] W. Hu, H. C. Chang, A. Sengupta, S. Bhunia, R. Kastner, and H. Li, "An overview of hardware security and trust: Threats, countermeasures, and design tools," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 40, no. 6, pp. 1010–1038, Jun. 2021. doi:10.1109/tcad.2020.3047976

[2] Y. Narges, A. Malhi, and K. Främling. "Security in product lifecycle of IoT devices: A survey." *Journal of Network and Computer Applications.* Vol. 171, pp. 102779, 2020.

[3] J. A. Lewis and W. Crumpler, "The Cybersecurity Workforce Gap," CSIS, https://www.csis.org/analysis/cybersecurity-workforce-gap (accessed May 2, 2025).

[4] C. Konstantinou, "Cyber-physical systems security education through hands-on lab exercises," *IEEE Design & Test*, vol. 37, no. 6, pp. 47–55, Dec. 2020. doi:10.1109/mdat.2020.3005365

[5] S. Bhunia and M. M. Tehranipoor. *Hardware security: a hands-on learning approach*. Morgan Kaufmann, 2018.

[6] V. A. DeCoster, "The needs of military veterans returning to college after service," International Journal of Arts & Sciences, vol. 11. no. 1, pp. 11-19, 2018.

[7] Intergragency Working Group on Veterans and Military Spouses in STEM Federal Coornidation in STEM Education Subcommittee Committee on STEM Education of the National Science and Technology Council, "STRATEGIC PLAN TO IMPROVE REPRESENTATION OF VETERANS AND MILITARY SPOUSES IN STEM CAREERS," https://www.energy.gov/sites/default/files/2024-03/12-21_CoSTEM-STEM-Vets-Plan.pdf (accessed May 2, 2025).

`

[8] A. Collins, J. S. Brown, and S. E. Newman, “Cognitive apprenticeship: Teaching the crafts of reading, writing, and Mathematics,” *Knowing, Learning, and Instruction*, pp. 453–494, Dec. 2018. doi:10.4324/9781315044408-14
[9] A. Collins and M. Kapur, “Cognitive apprenticeship,” *The Cambridge Handbook of the Learning Sciences*, pp. 109–127, Sep. 2014. doi:10.1017/cbo9781139519526.008
[10] A. Collins, “Cognitive apprenticeship,” *The Cambridge Handbook of the Learning Sciences*, pp. 47–60, Apr. 2005. doi:10.1017/cbo9780511816833.005
[11] P. Pintrich, D. Smith, T. Duncan, and W. Mckeachie, “A Manual for the Use of the Motivated Strategies for Learning Questionnaire (MSLQ),” National Center for Research to Improve Postsecondary Teaching and Learning, Ann Arbor. Michigan, 1991.
[12] J. C. Sun and R. Rueda, “Situational Interest, computer self-efficacy and self-regulation: Their impact on student engagement in distance education,” *British Journal of Educational Technology*, vol. 43, no. 2, pp. 191–204, Jan. 2011. doi:10.1111/j.1467-8535.2010.01157.x
[13] J. A. Fredricks, P. Blumenfeld, J. Friedel, and A. Paris, “School engagement,” *The Search Institute Series on Developmentally Attentive Community and Society*, pp. 305–321. doi:10.1007/0-387-23823-9_19
[14] S. Yang, S. D. Paul, and S. Bhunia, “Hands-on learning of hardware and systems security.,” Advances in Engineering Education, https://eric.ed.gov/?id=EJ1309224 (accessed May 2, 2025).