Multidisciplinary Experiential Learning for Holistic Cybersecurity Education, Research and Evaluation

Aunshul Rege, *Temple University*

Abstract

Experiential learning is defined as learning through action, experience, and discovery and exploration. Capture the Flags (CTFs) events have been offering experiential learning to computer science/engineering students for over 20 years. However, existing pedagogical technical research recognizes the need to address certain shortcomings of CTFs, such as novice encouragement, skewed experiences of CTF type (attack-defend vs. attack only vs. defend only), the difficulty and clarity of CTF challenges, and temporal constraints. This paper argues that CTFs can offer valuable experiential learning experiences for criminology/criminal justice students as well, by improving their hands-on research skills as well as their understanding of cyberattacks/defense. The paper also argues that multidisciplinary experiential learning is critical in improving CTFs for both technical and criminological domains. Specifically, it offers four benefits: breakdown of disciplinary silos in cybersecurity education; innovative research; enhanced learning experiences; and greater transparency in the evaluation of CTFs. The paper also offers some challenges of multidisciplinary experiential learning and offers possible implementation suggestions.

1. Introduction to Experiential Learning Theory

Experiential Learning Theory (ELT) is defined as "the process whereby knowledge is created through the … combination of grasping and transforming experience" [7: 41]. Experiential learning is also referred to as learning through action, learning by doing, learning through experience, and learning through discovery and exploration [10]. ELT is built on six principles [1, 8]:

1. Learning is a process that must include feedback on the effectiveness of students' learning efforts. Students take initiative, make decisions and are accountable for results.

2. Learning is a process that that draws out students' beliefs and ideas about a topic so that these can be examined, tested, and integrated with newer and/or more refined ideas. Experiences are supported by reflection, critical analysis and synthesis. The student is thus actively and continually engaged in a dynamic learning process that involves posing questions, investigating, being curious, solving problems, and being creative.

3. The learning process is driven by conflict, differences, and disagreement; moving between opposing modes of reflection and action are critical. Students cooperate and learn from each other in a semi-structured approach.

4. Learning is a holistic process of adaptation and involves the integrated functioning of thinking, feeling, perceiving and behaving. Students are not only engaged intellectually, but also emotionally and socially, which makes learning more authentic.

5. Learning results from the synergistic transactions between students and their environments. Students may thus experience success, failure and uncertainty as the environment and experience cannot always be fully predicted.

6. Learning is the process of creating knowledge; unlike transmission models where preexisting fixed ideas are transmitted to the learner, knowledge is (re)created by the learner. The results of learning are thus personal and form the basis for future experience and learning.

Thus, the main aspects of experiential learning are the students, and learning occurs when they are personally involved (and invested) in the production of their knowledge. The *focus of EL is placed on the process of learning and not the product of learning* [16].

2. The Experiential Learning Process

Experiential learning has several stages through which students gain a hands-on, collaborative and reflective learning experience [10]. Each of the following five stages allows students to engage with stage-specific content, self-reflect and learn [10]:

1. Experience/Explore "Doing": In this stage, students are engaged in hands-on experiences.

2. Sharing/Reflecting "What Happened?": Here students share the results, reactions and observations with each other, and discuss feelings generated by the experience.

3. Processing/Analyzing "What's Important?": Students discuss how their respective experiences were carried

out, how problems emerged, how these were addressed, and how these experiences might relate to future experiences.

4. Generalizing "So What?": Students connect the experience with real world examples.

5. Application "Now What?": Students apply what they learned in this (and past) experience(s) to similar/different situations. Specifically, students discuss how and what they learned can be applied to future situations.

3. CTFs, Experiential Learning for Computer Science/Engineering Students and Challenges

Capture the Flags (CTFs) are essentially computer security competitions of technical skills where teams participate in real-time for prizes [4]. CTFs have been in existence for almost 20 years with more than 70 yearly competitions, and are structured around three main themes: attack-defend, attack-only, and defend-only [3, 4]. CTFs offer participants a fun environment where they can learn about practical computer security [4]. Moreover, CTFs offer a safe place where participants can test various modes of attacks and learn how attacks work; an otherwise risky venture that could result in arrest and prosecution [4]. CTFs provide students a desirable venue to progress through each of the five experiential learning stages.

CTFs and Experiential Learning

First, it is obvious that students "explore doing", as CTFs by their very nature require students to engage in hands-on security challenges. One of PicoCTF's goals, for instance, has three goals: to encourage highschool students to pursue computer science/engineering (CSE) degrees, to introduce critical computer security topics before students enter college, and is to complement and supplement classroom exercises with hands-on experiences [2]. Similarly, CTF competitions such as CSAW CTF, Plaid CTF, UCSB iCTF, and RuCTF all offer learning platforms and have been about education [3]. CTF education works as a "group self-guided project-based instruction", where participants teach themselves how to apply core security concepts under time constraints [4]. Novice participants can collaborate to learn and develop their skill sets [12].

The second and third stages are about reflecting and sharing results, and how any problems were managed. Individuals not only learn, but also develop reasoning and problem solving skills and connect pieces of information thereby improving their cognitive capacities [12]. They can discuss their individual and collective positive and negative experiences and moments of victory and frustration. During 2014 CSAW CTF, for instance, the author observed one participating team's members. When students finished a particular challenge, they quickly discussed what challenge they solved and the how they tackled it. Also, when students were stuck on a particular challenge, they approached their teammates for ideas and alternatives. This one case alone clearly illustrates how the second and third stages of reflecting and analyzing occurred in a dynamic, real-time CTF environment.

In the fourth and fifth stages, students generalize their CTF-generated experiences to real world examples and discuss how they might apply their CTF experiences to future situations. Participants can analyze what was relevant to the learning exercise as well as specific problems that arose and techniques that were used to mitigate or bypass them. Furthermore, students can connect the CTF experience not only with real-world cyberattack/security but can also take these lessons and knowledge back to the classroom environments, to future CTF exercises. Given the tight timelines and rigorous nature of CTFs, it is unlikely that these stages occur during the course of the actual CTF. The team members observed at the 2014 CSAW CTF certainly did not have the time to have discussions of broader generalizations and possible applications to future scenarios. It is unknown, however, whether students have these conversations at a later time.

Challenges

While many have asserted the effectiveness of the CTFs, they have also recognized that CTFs still experience four main shortcomings. First, newcomers are faced with the daunting task of playing and becoming immediately immersed in the competition [3]. As such, there is a high likelihood that novices will be stuck, quickly discouraged and stop playing [3, 12]. If one has a strong knowledge base of technology, that individual is more likely to be successful at not only solving the problem, but also immediately becoming embedded in the CTF environment [3]. This is problematic as only the learning and engagement of those *without* need for instructional guidance will be enhanced [12]. It may therefore be more appropriate to match the competition with the existing skill and knowledge levels of participants, which will effectively contribute to growth in engagement and learning overall [12].

Second, the nature of the CTF (attack-defend vs. attack-only) has also been recognized as causing difficulties. In attack-only CTFs, participants do not have to concern themselves with administrative tasks, and can instead focus on learning by pure problem-solving. These CTFs, however, depart from realistic scenarios precisely because of the absence of defense [3]. While the attack-defend is more representative of reality, there is a power imbalance between the red and blue teams as the former tends to enjoy more notoriety and is seen as more desirable [3]. However, both defenders and attackers need to understand what they are defending against and why attacks fail (respectively) [4]. Thus, regularly rotating participants between defensive and attack roles is crucial so that they can understand and appreciate the challenges faced by each side [4].

The third issue concerns the difficulty of the CTF challenges. If challenges are harder because they are too convoluted so as to intentionally frustrate participants, the CTF may be detrimental to its purpose and also to the experiential learning process [3]. If a challenge is ambiguous and has too many possible paths that participants pursue, it may simply become just too hard to be solved [3]. Alternatively, challenges that are too easy may not be detrimental to the CTF, but may not be challenging enough to participants and hinder their learning experience [3].

Fourth, the element of time was critical in learning effectiveness. One temporal aspect that directly impacted the experiential learning process was that over time, all activity declined as the CTF progresses and teams are unable to solve the more difficult challenges or just lose interest. Related, PicoCTF found that teams were more active on the weekdays than weekends, which may be indicative of after-school gathering convenience [2]. Of course, time pressures force students to apply textbook lessons and theoretical knowledge [4]. Another temporal issue is that CTFs occur over compressed time frames (typically one to two days most likely over a weekend), which may not capture certain aspects of attacks. Those attacks that require slow stealthy techniques or social engineering strategies may not always be employed [4].

Despite these issues, CTFs have several benefits that mesh nicely with the experiential learning process. They (i) support problem solving in authentic situations, (ii) develop greater interest and enthusiasm, (iii) allow for the application of knowledge from courses to real-world problems, (iv) promote individual learning via the application of knowledge gained throughout the competition, which results in continuous development and learning, and (v) encourage the development of teamwork and communication skills [3, 12]. Even if competencies vary from novice to experts, CTFs provide diverse opportunities for practicing skills, techniques and knowledge to help the progression from beginner to expert, which will collectively be useful for students' individual careers in the future [12].

4. CTFs, Experiential Learning for Criminology/Criminal Justice Students and Challenges

Criminology/Criminal Justice (CCJ) students typically are exposed to research methods courses where they are taught the basics of various research methods, such as surveys, interviews, observations, and so on. They also examine the pros and cons of these methods, and do so often through a standard class project. While students get experience on the foundations of research methods, they are unable to progress effectively beyond this classroom knowledge and how to apply of their knowledge to real-world settings with confidence.

CCJ students interested in cybercrime and cybersecurity learn the standard topics of hacker taxonomies and motivations, attack typologies, various types of cybercrimes, and the policing, forensics and legal aspects of managing cybercrimes. While these are undoubtedly important topics and build the basic knowledge base, students are often limited in their ability to apply these principles outside the classroom.

CTFs and Experiential Learning

CTFs offer CCJ students two main benefits: (i) hands-on experiences with interview/observational methods and (ii) exposure to understanding the dynamics and complexities of cyberattacks and cybersecurity. Each of these two experiential learning processes is discussed next.

Research-based Experiential Learning

First, CCJ students experience/explore doing as they are actively involved in the design, implementation and analysis stages of research. Students can be involved in the *design* process of interview and observation guides. They can work closely with their faculty mentors to understand who to interview, what to ask and how to ask. They are actively involved in discussion of sampling techniques, what the right sample size might be, where to sample from and sampling limitations. Through this process, students experience hands-on learning (and appreciate) the difficulties of the implementation and design process.

Students can also be involved in the implementation stage, where they can actually engage in *conducting* interviews and observations in live settings. This gives them the ability to learn essential skills of how to interview individuals with a variety of backgrounds, how to use prompts and probes during the actual interview, and how to manage interview contexts (sensitive topics, unanticipated and/or new topics, participant reluctance, and so on). With observations, students see for themselves what is occurring in the environment. They become active collectors of data and they are engaged through their eyes and ears in real-time. Students thus learn the art of thinking on their feet and developing a critical eye in an actual research environment in a professional manner.

Finally, students can benefit from analyzing interview and observational data. Typically, undergraduate students who do work on research projects are relegated to the rather mundane task of interview transcriptions. However, students can work more closely with their faculty mentors to analyze interviews; they can engage in a multitude of coding approaches (grounded, narratives, conversation analysis, discourse analysis, and semiotics to name a few). Not only does this expose the student to a variety of coding strategies, but they can also learn validity issues via inter-rater reliability. Students and faculty can code *separately* and then reconvene to share their the coding themes they generated; this approach helps improve the validity of qualitative research by checking for overlapping codes and having a constructive discussion about other codes. Undergraduate students rarely get to experience this validation side of data analysis, which is a critical component of qualitative research.

In the second and third stages, students share what happened and analyze what is important. In the research context, CCJ students can discuss what they thought of the research experience itself: how did they feel *doing* the research? Students can share their respective experiences and learn from each other. Students can discuss what challenges they faced while interviewing and observing, and how they managed these. Furthermore, faculty mentors should actively listen when students discuss their thoughts and struggles.

In the last two stages of experiential learning, Students can discuss how interview and observational techniques might apply to other cyberattack/defense studies. CCJ students can apply what they have learned in both the research and cybersecurity contexts to future similar/different situations. For instance, the first interview/observational experience will make them stronger interviewers/observers for the second CTF they are a part of; each subsequent event will allow students to build on prior experiences and improve their methodological skills.

Not only can CTFs offer CCJ students the opportunity to delve deep into the concepts learned in research methods courses, but it allows them to understand the art of conducting qualitative research, limitations and how best to manage them.

Cybersecurity-based Experiential Learning

CCJ students can benefit from CTFs in several ways when studying cyberattacks and cybersecurity. First, they can explore what real cyberattacks look like through real-time CTFs, even though the latter are not entirely representative of reality. Real cyberattacks vary with regards to their intensity, frequency, durations, and objectives, which CTFs simply cannot capture; CTFs offer a skewed and distorted representation of what 'really' happens. Yet, students get a snapshot of attackers and defenders in action, an experience that simply cannot be obtained by reading about cyberattacks in courses or hearing about them from guest speakers. Students can then share and process (stages two and three) what they found via observations and interviews about adversaries and defenders, and how this built on (or nor) classroom concepts of attack techniques and organizational dynamics; it allows them to be critical thinkers and evaluators about existing CCJ literature.

CCJ students also experience the fourth and fifth stages of experiential learning (generalizing and application). Here students can witness the back-and-forth 'game' in CTFs, which gives them an appreciation of the complex nature of cyberattacks and the challenges of real-time defense. CCJ students can watch how the red team adapts and evolves in response to defender actions, which can make students realize that cyberattacks and defense are not static but rather dynamic phenomena that play off of each other. This can help CCJ students develop possible attack/defender attack trajectories. CCJ students can also learn about possible group dynamics in cyberattacks through CTFs: (how) does division of labor occur? How do groups make decisions? How do they plan attacks? How do power dynamics pan out? (How) are conflicts and tensions resolved? The area of group dynamics in the context of cyberattacks/defense is under-researched in the open literature, especially in the CCJ discipline. Understanding these aspects are vital to not only identify how adversaries attack, adapt and evolve, but also how the role of group dynamics impacts each of these elements. Furthermore, the different characteristics of CTFs (attack-defend; attack-only; defend-only) would offer interesting insights into different types of group dynamics. Students can generalize and frame real cyberattack cases in the context of their observations and interviews, better understanding behind-the-scenes group operations and attack trajectories. In the context of cyberattacks/defense, CCJ students will be more attuned to group traits and dynamics, and can identify patterns and trends in organizational dynamics and attack paths.

Challenges

CCJ experiential learning, like CSE, faces several hurdles at implementation stages. The first difficulty is gaining access to CTFs; these cybersecurity exercises are (by their very nature) intended for CSE students. CCJ students cannot partake in technical challenges and as such, by eligibility restrictions, cannot be a part of CTFs. However, the author was granted permission to attend, observe and interview the members of one team participating in the 2014 CSAW CTF exercise; such access to future CTFs for both faculty and students might alleviate this hurdle.

Second, like CSE students, CCJ students might also be newcomers to the qualitative research arena and may not know how to observe or interview in a live setting. This challenge can be addressed by doing 'mock' observations and interviews in trial settings to provide students with confidence and training before attending an actual CTF.

Finally, as with CSE experiences, CCJ students may also face the element of temporal exhaustion. CTFs occur over compressed time periods. Conducting continuous observations not only exhausts students, but also lowers their ability to focus and conduct effective observation/interviews. One possible means to manage this problem is to have two teams of student observers/interviewers who alternate shifts and use similar data collection instruments. This not only ensures an alert researcher, but also offers a standardized interview/observation guide to collect data.

Regardless of these challenges, CTFs offer pros than cons in educating CCJ students about cyberattacks and improving their research skills.

5. Multidisciplinary Experiential Learning: Benefits, Challenges and Possible Solutions

The preceding sections make the case that CTFs can offer valuable experiential learning experiences to both CSE and CCJ students *separately*. However, there is the possibility to move beyond disciplinary-specific experiential learning to multidisciplinary experiential learning (MEL).

MEL is already being practiced effectively in other disciplines and countries [11; 14; 15]. It has been used for civil engineering and architectural students [11], engineering and science [14], and nursing, consumer science and hospitality [15]. However, there is a paucity of data on MEL that incorporates the hard and soft sciences. In this context, MEL offers four benefits:

1. Breaking down disciplinary barriers: Cybersecurity is currently being studied in disciplinary silos. Incorporating both CCJ and CSE disciplines would provide the space for undergraduates (and professionals) to discuss the phenomena of cyberattacks and cybersecurity. This will not only offer a richer and holistic approach to the study, but students/professionals will also realize the importance of multidisciplinary dialog that can be achieved and fostered in undergraduate curriculums as well as in the professional workforce.

2. MELs and Innovation: Given the multidisciplinary nature of MELs, researchers and professionals can find innovative means to study cybersecurity. For instance, criminologists, computer scientists, and electrical and computer engineers can apply their respective theoretical knowledge to study adversary dynamics in smart grid security [13]. Criminology, for instance offers an assortment of complementary approaches, such as rationality and decision-making attackers (rational choice perspective), crime scripts (attack trajectories) and situational crime prevention principles to protect targets. Each of these has something to offer the CSE fields as it gives the human element a voice in the cyberattack/security equation.

3. Enhancing learning experiences: Both CCJ students and CSE students would greatly benefit from MEL experiences. For instance, CSE students could help validate observations and interviews conducted by CCJ students. For instance, CCJ students could ask CSE students after CTFs if their observations of the CSE group did indeed reflect what they were going through. CSE students could also let CJ students know what might improve their methodological skills by offering suggestions on the best unobtrusive observational strategies and what extra/other questions to ask.

Of course CSE students also benefit from CCJ students. For instance, CCJ students would offer a more structured approach into individual and group thought and decision-making processes. CSE students may thus learn as they are interviewed by CCJ about what they experienced, which will make them more cognizant of cyberattack/security processes.

4. Improving *validation* and *transparency* in CTF Evaluation: most of the current means of evaluating CTFs are surveys and interaction logs [2]. While these instruments are undoubtedly important, they offer a more "gappy, black box account" by answering questions such as 'What is happening?' [4, 6]. Qualitative research is process-oriented and answers the 'why or how is it happening'; it is thus effective in unpacking these process mechanisms and offers insights into "unforeseen relationships, and generates new insights" into phenomena [as cited in 9].

There are two main challenges to MEL. First, the logistics of the CTF exercise would make MEL problematic as CS and CCJ students are engaged in separate activities: the former group attempts to solve technical challenges, while the latter group is observing behaviors. Each group is busy with its respective experiential learning process, which makes CSE/CCJ interaction during the CTF exercise moot. Any such interaction would hinder the objectives of discipline-specific experiential learning.

Second, interacting pre and post CTF exercises may be difficult as both CSE/CCJ students may be exhausted and/or frustrated after their respective tasks. Each group may experience fatigue or may not have the desire to communicate with the other. Furthermore, CSE students may not be comfortable having their behaviors observed and thus may not be able to fully concentrate on their CTF exercise. This, in turn, may make CCJ students feel uncomfortable with observing as they realize their presence is distracting to CSE students.

These challenges at implementing MELs could be managed in the following ways:

1. Have a few *hybrid* CTF teams that comprise both CSE and CCJ students. Here the CSE and CCJ students would be from the same university, meet on a regular basis, and do ‘dry runs’ before going live at the actual CTF. Not only would this enable strong bonds and trust between the students well before the CTF, it would also allow for continuous discussions and feedback to both CCJ and CSE students, which would improve their methodological and technical skills respectively.

2. If students are from different universities and as such do not get the chance to establish prior contact, CCJ and CSE students can talk to each other briefly before the CTFs. Once students know each other well they are more likely to be comfortable. CCJ students will be more comfortable interviewing and observing students without having to worry about how CSE students feel about their presence. Similarly, CSE students are more likely to chat with CCJ students during moments of frustration/victory; CCJ students can thus capture these raw emotions, which might otherwise be difficult to investigate.

3. If the first two options are not possible, CSE students can talk to CCJ students during breaks to capture feelings and emotions; these conversations could be for very short time frames (approximately 10-30 seconds), which would offer nice verbal snippets from participants that complement the observations.

4. Any of the above suggestions could be coupled with audio/video recordings of CSE teams during CTFs. A simple audio recorder could be placed in the vicinity of the CSE group that would capture every verbal communication between team members. Additionally, video recorders could also capture the group’s movements and facial expressions as they progress through the CTF. This approach has several advantages. First, CSE students who wish to remain focused on the CTF can do so without having to speak with any CCJ students. Also, if CSE students are exhausted and have experienced frustrations that they do not wish to share at that time, also do not have to converse with CCJ students. And at a later date, students can meet up to go over the audio/video and chat. Second, this audio and/or video recording would offer a valuable and complementary data source in addition to pure observations and interviews conducted by CCJ students. Of course, if both CSE and CCJ students are willing and able to meet at a later time, they can view the video and/or listen to the audio together and discuss the experiences, which can be further cross-checked with the observation data. This would improve the validation of the data and allow both CCJ and CSE students to build on their research and attack techniques respectively.

6. Future Directions

As with any experiential learning, MEL has its shortcomings (much like CTFs as discussed above), but the benefits far outweigh these (also much like CTFs). Promoting innovative research, dismantling of disciplinary boundaries, enhancing student experiences, and improving the evaluation effectiveness of CTFs are all reasons in favor of MEL.

The MEL approach also would help CTF organizers greatly, with designing skill-specific exercises, getting effective and timely feedback, which can be used in future CTF designs, and, perhaps, most importantly, making CTFs more student/participant-driven thereby making them even more enjoyable and educational in the future.

Acknowledgements

This material is based upon work supported by the National Science Foundation under Grant No. 1453040.

7. References

[1] Association for Experiential Education
http://www.aee.org/

[2] Chapman, P., Burket, J. & Brumley, D. (2014). PicoCTF: A Game-Based Computer Security Competition for High School Students. Proceedings of USENIX 2014.

[3] Chung, K. & Cohen, J. (2014). Learning Obstacles in the Capture the Flag Model. Proceedings of USENIX 2014.

[4] Davis, A., Leek, T., Zhivich, M., Gwinnup, K. & Leonard, W. (2014). The Fun and future of CTF. Proceedings of USENIX 2014.

[5] Dunning, T. (2008). *Natural and Field Experiments: The Role of Qualitative Methods*. Retrieved November 24, 2012. Online at http://www.thaddunning.com/wp-content/uploads/2009/12/DesignBased_QualMethods_v2.pdf

[6] Howe, K. (2004). *A Critique of Experimentalism*. Qualitative Inquiry, 10(1), pp. 42-61.

[7] Kolb, D. A. 1984. Experiential learning: Experience as the source of learning and development. New Jersey: Prentice-Hall

[8] Kolb, A. Y., & Kolb, D. A. (2005). Learning styles and learning spaces: Enhancing experiential learning in higher education. *Academy of management learning & education*, *4*(2), 193-212.

[9] Maxfield, M. & Babbie, E. (2005). *Research Methods For Criminal Justice and Criminology 4th Edition*. Wadsworth Publishing.

[10] NIU.edu (n.d.). "Experiential Learning". Retrieved April 10, 2015. Online at http://www.niu.edu/facdev/resources/guide/strategies/experiential_learning.pdf

[11] Poh, P., Soetanto, R., Austin, S., & Adamu, Z. A. (2014). International multidisciplinary learning: an account of a collaborative effort among three higher education institutions.

[12] Pusey, P., Tobey, D. & Soule, R. (2014). An Argument for Game Balance: Improving Student Engagement By Matching Difficulty Level with Learner Readiness. Proceedings of USENIX 2014.

[13] Rege, A., Ferrese, F., Biswas, S., & Bai, L. (2014). Adversary dynamics and smart grid security: A multiagent system approach. Proceedings of the 7th International Symposium on Resilient Control Systems (ISRCS). Institute of Electrical and Electronics Engineers (IEEE). pp. 1-7. IEEE Catalog Number: CFP1469H-ART [ISBN: 978-1-4799-4187-2] DOI: 10.1109/ISRCS.2014.6900101.

[14] Smith, S., Tillman, D., Mishra, P., Slykhuis, D., Alexander, C., Henriksen, D., Church, R. & Goodman, A. (2014). Building Multidisciplinary Connections: Intersections of Content, Creativity, and Digital Fabrication Technologies. In Society for Information Technology & Teacher Education International Conference (Vol. 2014, No. 1, pp. 2506-2510).

[15] Sydnor, S., Sass, M. S. M., Adeola, M., & Snuggs, T. (2014). Qualitative Analysis of Multidisciplinary College Students in an International Alternative Break Course'. The Online Journal of Quality in Higher Education, 27.

[16] University of California Davis (UC Davis). (2011). 5-step experiential learning cycle definitions. http://www.experientiallearning.ucdavis.edu/module1/el1_40-5stepdefinitions.pdf