Cybersecurity Education: From Beginners to Advanced Players in Cybersecurity Competitions

Lindsey J Thomas, Moises Balders, Zach Countney,
Chen Zhong*
Dept. of Informatics and Computer Science
Indiana University Kokomo
{thomalin, balderam, zcourtne, chzhong}@iu.edu
*Corresponding author

Jun Yao
Dept. of Electrical Engineering
University of Texas at Arlington
jun.yao@mavs.uta.edu

Chunxia Xu
School of Foreign Languages
Nantong University, China
xcx@ntu.edu.cn

***Abstract*—Cybersecurity competitions have been shown to be an effective approach for promoting student engagement through active learning in cybersecurity. Players can gain hands-on experience in puzzle-based or capture-the-flag type tasks that promote learning. However, novice players with limited prior knowledge in cybersecurity usually found difficult to have a clue to solve a problem and get frustrated at the early stage. To enhance student engagement, it is important to study the experiences of novices to better understand their learning needs. To achieve this goal, we conducted a 4-month longitudinal case study which involves 11 undergraduate students participating in a college-level cybersecurity competition, National Cyber League (NCL) competition. The competition includes two individual games and one team game. Questionnaires and in-person interviews were conducted before and after each game to collect the players' feedback on their experience, learning challenges and needs, and information about their motivation, interests and confidence level. The collected data demonstrate that the primary concern going into these competitions stemmed from a lack of knowledge regarding cybersecurity concepts and tools. Players' interests and confidence can be increased by going through systematic training.**

***Index Terms*—cybersecurity education, human-subject study, learning needs, cybersecurity competition**

I. Introduction

Cybersecurity competitions have been shown to be an effective approach for promoting student engagement through active learning in cybersecurity [1]. Players can gain hands-on experience in puzzle-based or capture-the-flag type tasks that promote learning [2], [3]. However, beginners with limited knowledge in cybersecurity usually suffer from those tasks due to the lack of knowledge or abilities of using tools. To enhance student engagement, it is important to study the experiences of beginners to better understand their learning needs.

NCL [1] is a national cybersecurity competition which was founded to provide an ongoing virtual training ground for collegiate students to develop, practice, and validate their cybersecurity skills. Players of all levels can participant in NCL. The NCL challenges are designed around industry-recognized objectives such as the CompTIA Security+ and EC-Council Certified Ethical Hacker (CEH), and they are categorized into three levels of difficulty: easy, medium and hard. All of the challenges are provided in a virtual environment so that players can easily access to them by logging into a website. Besides, NCL provides lab-based exercises in its virtual "gym" to players. NCL offers two game season per team and each NCL game season lasts for about two months.

To enhance players' engagement in cybersecurity competition, it is important to study the learning experiences of beginners to gain better understanding of their learning needs. To achieve this goal, we conducted a case study from the beginner perspective which involved 11 undergraduate students participating in one NCL game season: 3 of them have participated in the NCL before, the rest have any no experience. Questionnaires and in-person interviews were conducted before and after NCL games to collect players' feedback on their experience, learning challenges as well as needs, and information about their motivation, interests and confidence level. Given the collected, we did both qualitative and quantitative analysis. The results demonstrate that the primary concern going into these competitions stemmed from lacking of knowledge regarding cybersecurity concepts and tools. Systematic training increases the overall performance and comprehension of cybersecurity, and therefore increases the players' interests and confidence

The contribution of the study mainly comes from the understanding of the learning needs from the beginners' perspective. When exposed to systematic training and the peer mentoring of advanced players, beginners have the potential to succeed even more. This beginner-to-advanced type training expedites skill gain, allowing for enhanced performance.

II. Methodology

A case study was conducted during an academic term, which lasted for four months. All 11 undergraduate students participated NCL competition from March to April. NCL includes three games in one season, pre-season game, individual game, and team game. Students were offered a series of training during the first two months before the NCL games started. The topics of training includes network traffic analysis, web security, cryptography, basic reverse engineering. Interviews and questionnaires were conducted after each NCL game to collect the subjects' opinions and feedback.

[1] https://www.nationalcyberleague.org/

978-1-7281-2504-6/19/$31.00 ©2019 IEEE

A. *Participants*

11 undergraduate students participated in the case study. All of them are majored in Informatics and Computer Science. There are 4 sophomores, 4 juniors, and 3 seniors. 3 of them have participated NCL before, and the remaining 8 students have no prior experience. Figure 1 demonstrates the diversity among the participants.

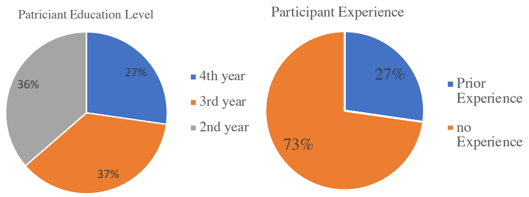

Fig. 1. The background of the participants in the case study.

B. *Training Sessions*

To improve the participants' performance and engagement, training sessions were offered to the participants before the NCL games. All the training practices are hands-on labs. Participants had the chance to learn cybersecurity knowledge and useful tools by solving various problems. The topics covered are as follows.

- Network Traffic Analysis: the participants were taught how to use Wireshark to analyze packet capture (PCAP) files.
- Web Security: multiple wireless security protocols were introduced. Participants gained experience with cracking a wireless password in WEP network, using Wireshark and Aircrack-ng.
- Cryptography and Hashing: ciphers and hashing algorithms were explained, and useful decoding/decryption tools were introduced to the participants (e.g., RSA cracker, John the Ripper).
- Exploration and Enumeration: Source code analysis tasks were introduced and participants learned to use the binary analysis tool (e.g., gdb, IDA).

C. *Case Study Protocol*

At the beginning of the study, a background questionnaire was conducted. Participants were asked about what their strengths and weaknesses were, as well as the level of interest in cybersecurity, motivation and confidence in participating in the NCL games. The rating questions (using 7-point Likert scale) are listed in Table I.

The training session lasted for about two months. We met with the participants twice a week for one hour, offering short lectures and hands-on labs to train them. After the training session, the participants were asked the same questions listed in Table I.

The NCL games happened during the following two months, including the preseason game which lasted for 8 days, the individual game which lasted for 3 days, and the team game which lasted for 3 days. The participants participated in all of the games by working on challenges on the NCL website [2]. We met with the participants once per week in-between the games to address their questions and let them communicate with each other. Peer tutoring was stimulated by encouragement and small awards during the meetings. Besides, the participants could work on the practical labs provided by the NCL gym by themselves. Post-game questionnaires were sent out to the participants after the individual game and team game to collect the feedback on theire game experience and to ask them to rate their level of interests, motivation and confidence using 7-point Likert scale. The rating questions are presented in Table II. We also conducted interviews with the participants to follow up with the questions in order to collect in-depth information about their game experience and feedback. The interviews were unstructured and the questions mainly depended on the participants' response in questionnaire. For example, common questions are "`why do you think ...`" and "`tell me more about ...`".

TABLE I
RATING QUESTIONS IN THE BACKGROUND SURVEY

R1: I am interested in learning cybersecurity.
R2: I feel confident in participating in this NCL.
R3: I consider cybersecurity as a possible career after graduating college.

TABLE II
RATING QUESTIONS IN THE POST-GAME QUESTIONNAIRE

R1: I am interested in learning cybersecurity.
R2: I feel confident in participating in this NCL.
R3: I consider cybersecurity as a possible career after graduating college.
R4: I am motivated to learn some new techniques in this field when participating in the game.
R5: The training so far helps me understand cybersecurity better.
R6: The peer tutoring in-between the NCL game is helpful for me.

III. RESULTS

We found three main concerns that the beginners had when participating in the competition, which are listed as follows.

- **Less motivated due to lack of knowledge.** The participants without prior experience felt intimidated and under prepared to participate in the competition. Sometimes they didn't know how to even approach the challenges. For an example, when presented with a new decoding problem, the participants with experience knew how to use tools to address the problem, while the beginners had no idea on how to solve it.
- **Training benefits the engagement.** During the interview, we asked the participants without prior experience if the training they went through helped them throughout the game. One of the participants initially said "`Having almost no experience left me feeling like I would be incapable of participating in the NCL`". But later he mentioned "`The training that provided me`

[2] https://cyberskyline.com/

with tools and materials in a format that allowed me to gain knowledge and understanding very quickly help my performance and built up my confidence so I was fully engaged"

- **Active interest leads to success.** Participants who held active interest in cybersecurity were able to quickly enhance their performance through the practices and training in the study, although they didn't have prior experience. They could successfully address complex challenges once they were provided with background knowledge, tools and information resources. Besides, we observed that beginner benefited a lot from the peer mentoring of advanced players.

A. Attitude Changes in Participants

We present the participants' responses to the rating questions in the pre-game questionnaire, the 1st post-game questionnaire and the 2nd post-game questionnaire using boxplots. The results are demonstrated in Figure 2. The participants are categorized base on their prior experience in cybersecurity competition. Overall, the ratings are positive. We can find the participants with prior experience provided more stable ratings. Besides, the rating did improve the participants' confidence and interests in learning cybersecurity.

IV. Discussion and Conclusion

Several interesting finds were gathered from the case study. First of all, despite the fact of having almost no prior knowledge of cybersecurity, participants were still able to pick up on how to succeed at these tasks quickly than expected. This finding is consistent with the existing study [3]. While facing initial difficulty at the beginning of the competition, the beginners were able to grasp the concepts and complete the easy-level tasks in a shorter time because of the training and peer support of advanced players, as well as the engaging experience of the games. It is shown that training plays an important role in increasing participants' engagement and interest. Participants who had active interest in cybersecurity were able to quickly enhance their performance in the competition. In the next step, we are going to identify the effective training methods used in the case study in a systematic way in order to develop practical guidelines for guiding beginner players in the cybersecurity competitions.

References

[1] A. Conklin, "Cyber defense competitions and information security education: An active learning solution for a capstone course," in *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)*, vol. 9. IEEE, 2006, pp. 220b–220b.

[2] D. H. Tobey, P. Pusey, and D. L. Burley, "Engaging learners in cybersecurity careers: lessons from the launch of the national cyber league," *ACM Inroads*, vol. 5, no. 1, pp. 53–56, 2014.

[3] D. H. Tobey, "A vignette-based method for improving cybersecurity talent management through cyber defense competition design," in *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research*. ACM, 2015, pp. 31–39.

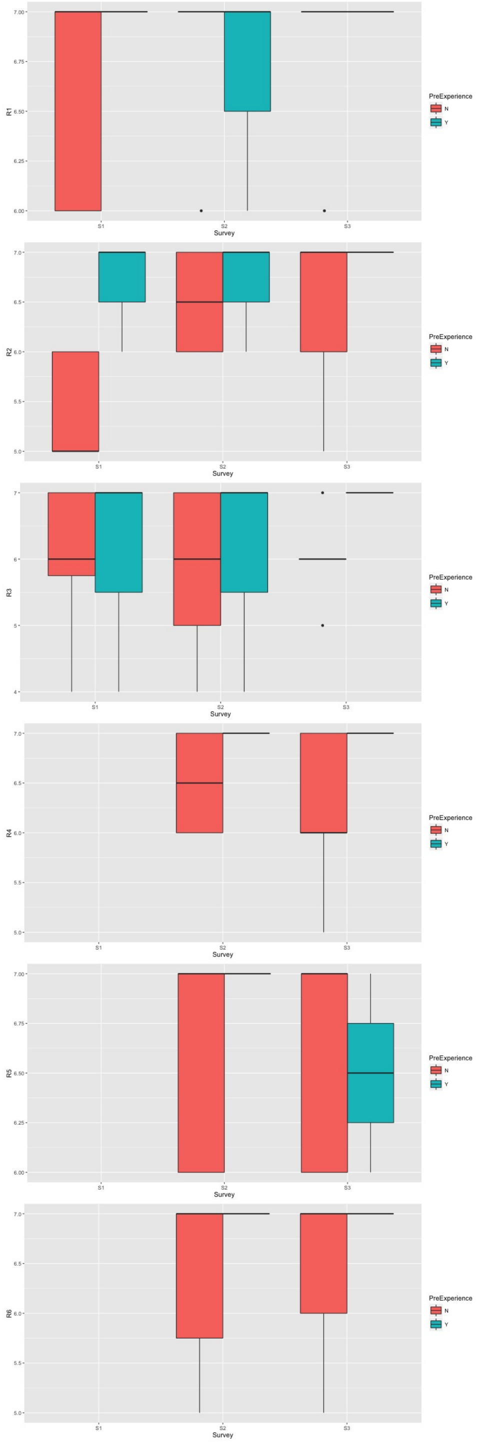

Fig. 2. The boxplots of the participants' ratings to R1, R2, R3, R4, R5 and R6 in background survey, the 1st post-game survey, and the 2nd post-game survey.