



Eliciting Requirements for a Student-focussed Capture The Flag

David Szedlak and Andrew M'Manga

EasyChair preprints are intended for rapid dissemination of research results and are integrated with the rest of EasyChair.

November 19, 2020

Eliciting Requirements for a Student-focussed Capture The Flag

David Szedlak
Department of Computing
Bournemouth University
Poole, Uk
dszedlak@gmail.com

Andrew M'manga
Department of Computing
Bournemouth University
Poole, Uk
ammanga@bournemouth.ac.uk

Abstract—The current consensus is that a lack of skilled young persons entering the cyber security industry is contributing significantly to the accrescent cyber security skills gap. However, little progress has been made in terms of handling key contributing factors – cyber security education. While Capture The Flag (CTF) exercises in cyber security education present some of the necessary requirements, we hypothesise that the current CTF forms do not possess the requirements necessary for promoting student engagement and learning. The paper presents the results of a study aimed at identifying the requirements of a student-focused CTF.

Index Terms—cyber security education, skills gap, user-centered requirements, capture-the-flag.

I. INTRODUCTION

As the threat within cyber security grows with the ever-increasing demand for skilled cyber security professionals, it is increasingly important to supply the industry with highly skilled professionals. The gap in proficiency within the cyber security industry remains highly adverse, as the demand for cyber security professionals continues to grow substantially faster than the overall IT and labour market. This disproportion exists exponentially while the global economy's dependency on computer networks as an economic engine increases, proving cyber security to be an increasing international security concern [13].

The UK national Cyber Security strategy identified the need to strengthen cyber-security skills as a key issue. Specifically, to this research, the lack of young people entering the profession and insufficient exposure to cyber and information security concepts in computing courses [7], which leads to an underutilisation of time within security teams, having to teach graduates the skills required for the job.

Proof of this lies within the majority of IT employers believing that education programs are not fully training students to enter the cybersecurity industry, with only 23% believing otherwise [6]. If such a pitfall does exist within the current education environment, this should prompt the research into what issues employers are having with graduates going into cyber security. One of the most consistent criticisms facing cybersecurity education programs is that an over-emphasis on theory and 'book learning' prevents

students from developing the practical skills they need [14]. Consistently, surveys show that organizations rate hands-on experience and certification attainment highly when hiring [4].

This provides the education sector with the unique opportunity to integrate hands-on forms of learning into their cyber security related courses – with CTF as a prime example. Regrettably, CTF's in education are rarely designed, taking the user's (student) requirements into account - motivating the research question:

What requirements should be taken into consideration to design an effective student-focused CTF?

This paper aims to contribute to the cyber security education environment by providing research and analysis of CTF tools on a student's educational development. We consider the related work on the cyber security skills gap, security education and promotion of student's cyber security interest in Section II, before presenting our data collection approach in Section III. The data is analysed in Section IV, from which findings are used to develop a prototype in Section V. We conclude and discuss future work in Section VI.

II. RELATED WORK

A. The Cyber Security Skills Gap

The Cybersecurity skills gap refers to the gap in fundamental skills required for a career in cybersecurity within the comprehensive pool of cybersecurity professionals and job applicants. The threat within cyber security grows at a continuously alarming rate, as technology and attack vectors continue to evolve, the pool of adequately skilled cyber security professionals remains insufficient, with little to no evidence demonstrating any improvement with regard to reducing the skills gap [9]. Evidence of this skills gap comes from a survey by CSIS which found that 82% of employers report a shortage of cybersecurity skills, and 71% believe that this talent gap causes measurable damages to their organisations [4].

ISACA provide yearly surveys on cybersecurity professionals. In 2018, they found that 61% of organisations believe

that less than 50% of all applicants for cybersecurity jobs actually have the skills required for the job [11]. Alarming however, this has increased over statistics received from their 2015 survey, which stated that in 2015, 52% of organisations believed that less than a quarter of all applicants had the necessary skills for the position [4].

B. Cyber Security Education

A qualified cybersecurity professional is someone who has sufficient practical and theoretical knowledge on the fundamental security concepts within cybersecurity. Poor outlooks from professionals in industry on the cybersecurity education environment, in addition to the lack of departments in US universities with a Certified Association Executive (CAE) designation [5], conclude that the current education environment does not consistently provide any guarantee that graduates are qualified to go into the cybersecurity industry. To elaborate, evidence shows that the current education environment is failing to teach graduates the necessary practical skills for a job in cybersecurity. One of the most consistent complaints that faces cybersecurity education programs is that there is a considerable over-emphasis on theory, which prevents students from developing the practical skills they need [14]. As a result, employers are left dissatisfied because graduates are lacking essential practical experience as well as an understanding of the computing and information security fundamentals. A 2016 CSIS survey of IT employers revealed that only 23% of employers believe graduates are trained sufficiently to enter the cyber security industry [4].

Practical skills are consistently shown to be rated highly when evaluating new hires [10], which is why it is imperative that education programs focus the curriculum to ensure that students are provided with a platform to achieve mastery in the fundamental concepts of cyber security [3].

C. Promoting Students Cyber Security Interest

Students who lack interest in a topic will not attempt to understand certain concepts but will at best focus on memorizing answers or finding ways around material that they perceive as boring [15]. Therefore, the development of education programs promoting student retention and interest is paramount. One such approach familiar to this problem is gamification.

Gamification is a process comprising of the application of game-like elements in a non-game context in order to motivate learner behaviour [12]. A detailed comparative analysis of the effects of gamification on student learning at the university of Hong Kong [8], verifies the practice of gamification as beneficial to student education.

Capture the Flag tools exhibit gamification by delivering challenges that introduce users to a variety of cyber security concepts at differing degrees of difficulty. The area of focus

that CTF competitions aim to measure are vulnerability identification, exploit development, tool development and trade-craft. There are currently three main types of CTFs [2]. These are: Jeopardy-style. Attack-Defence style and Mixed CTFs.

Capture the Flags can be used in education, as a means of motivating students to learn the basic security concepts required for a career in offensive cyber security. Beginners are often put off of CTF competitions due to frustrating first experiences within their first attempts at them. Research has revealed the cause of this to be that the majority of CTF challenges are not appropriately designed for beginners, which leads to beginners getting stuck and giving up [1]. Without guidance, beginner students miss essential learning goals and take longer to learn concepts [16].

CTFs usually cover a variety of cyber security topics. The names of these topics vary depending on the name the host is most familiar with. A research analysing the popularity of 909 category names used in CTFs revealed “crypto”, “web”, “reverse”, “forensic”, “pwn” and “misc” as the most common names given by CTF hosts to each major category’s corresponding area within cyber security [1].

III. DATA COLLECTION

Data elicitation begun by reaching out to a university’s cyber security society for participation. The society was chosen in preference to the university’s final year ethical hacking students as in had members ranging from the first to the final year of university progression. For training, the society used an in-house developed CTF, picoCTF (<https://picoctf.com/>), and OverTheWire (<https://overthewire.org/wargames/>).

As a first step, the society’s president and vice president were interviewed on student experience with CTF tools and what improvements they would like to see. The interview took approximately 30 minutes and was recorded. Knowledge gained from the interview aided the design of a questionnaire used as the main data elicitation approach due to interview time limitations. The questionnaire was setup on Jisc online surveys (<https://www.onlinesurveys.ac.uk>) and the link emailed to the society’s members - of which eight responded.

Examples of questions used in the questionnaire included:

- Where the instructions provided by the CTF tools satisfactory?
- Which sub-genre of challenges did you find most engaging and why?
- Do you find any of the CTF tools used in your studies to be lacking any particular sub-genre of challenges? If so, please elaborate.
- What has your experience with these tools been like? Please give a brief review of your experience with these CTF tools.

- Have the CTF tools delivered a diverse set of challenges with varying degrees of difficulty?
- What is your verdict on the practical knowledge gained by the CTF tools and the effect on your educational development?
- Have there been opportunities for you to apply your practical knowledge within your course?
- How much of an influence do you think these CTFs have provided, regarding the desirability of a career in Cyber Security?

IV. DATA ANALYSIS

A. Quantitative Analysis

The first part of analysis was quantitative - facilitated by Jisc online surveys dynamically generated graphs. From the analysis, the results seem to indicate that our hypothesis (*the current CTF forms do not possess the requirements necessary for promoting student engagement and learning*) was not correct, or that it did not apply to the cohort as illustrated below.

In a question asking the student whether they found past CTF tools to be lacking in any particular sub-genre (i.e. web, crypto, etc), 62.5% of respondents stated they did not believe any of the CTF tools were lacking in a particular sub-genre of challenges. The findings are illustrated in Fig. 1.



Fig. 1. Student opinion on previous CTF tool's sub-genre consistency

Another question, this time focusing on the diversity of challenges and incremental difficulty showed that students felt that CTFs in use were adequately designed. In response to this question 62.5% of students stated that they felt CTF tools had provided a diverse set of challenges with varying degrees of difficulty and at a sufficient level. The findings are illustrated in Fig. 2.



Fig. 2. Student opinion on challenge diversity and incremental difficulty of CTF tools in use

When asked about sufficiency of learning material and guidance in CTF tools, 62.5% of students as illustrated in Fig. 3 also stated they were content with the tips and learning material provided.



Fig. 3. Student opinion on the sufficiency of learning material and guidance in CTF tools

Final responses that stood out were those in reference to the question whether CTF tools were readily accessible on demand. 50% agreed, while 25% disregard, and 25% selected other (illustrated in Fig. 4). The findings suggested that not only did a larger percentage of the students feel that the CTF tool in use had the necessary requirements for their learning, they were also available when required.

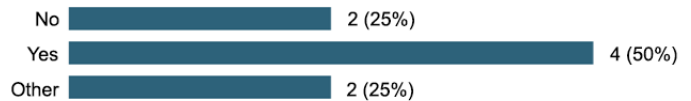


Fig. 4. Student opinion on availability of CTF tools

B. Qualitative Analysis

The second part of analysis was qualitative - focussed on the students' written responses. As we only had eight respondents, use of function-specific qualitative data analysis tools was not required. The qualitative analysis proved beneficial as it highlighted the key requirements not evident in the quantitative results. Excerpts from student responses are presented throughout the section to illustrate the findings.

- The first finding indicated that a variety of challenges was seen as a key requirement. This was advocated in the following response:

"I think a range of challenges is always a good thing... Most people have different interests and areas of expertise" [S4].

- A second observation was that the students felt incremental difficulty was an essential feature in the CTF design:

"...Incremental difficulty is also something that is important to incorporate into CTF tools" [S4].

"I think the most important component of CTFs, especially those targeted at a diverse group with different abilities is gradual increase in difficulty..." [S1].

- Another key requirement was the need for sufficient guidance for beginners. This was clearly expressed in the following responses:

"In regard to instructions, this could mean more instruction and guidance for early questions/challenges" [S2].

"Step-by-step guidance but you forfeit half the points for that section" [S7].

“Maybe after each sub-genre further reading on where to look if you’re stuck on a particular CTF question...” [S6].

- The students also expressed the need for information on the comparison between real world attack vectors and the challenges within CTFs:

“Definitely real-world application, i.e. useful links or guidance on how you can further develop a particular area that could potentially help you get a specific job role because of your passion for a niche sub-genre” [S7].

- As an overall, the students felt that the CTFs where a positive contribution to their practical knowledge and educational development:

“Absolutely! Before CTFs I had zero technical knowledge. Through CTFs I have learned an array of technical skills and applied them to challenges that may help me in the real world when I start my security consultant role. Not only do CTFs help technical skill development, but they help develop “softer” skills such as teamwork, communication, leadership etc” [S1].

“A lot of the practical challenges certainly relate to a lot of the theory lectured in my course enabling practical experience to further emphasise defined concepts” [S5].

- The participant also supported the notion that CTFs encourage students to pursue a career in cyber security.

“I am interested in a career in cyber security. CTFs hosted by our society have the ability to widen knowledge as well as introduce to different types / forms of security.” [S6]

“Yes, I am - having done ctfs have made me realise that there’s a lot to cyber security and i’d like to invest more time into it! yes, they might help me to understand or get into the mindset of how to break and question things, they will definitely give me patience” [S1]

V. FINDINGS

A. CTF Requirements

The goal of the study was to identify the requirements that should be taken into consideration to design an effective student-focused CTF. While the study did not identify student training and engagement inadequacies in the CTFs used by our participants, it however, highlighted areas that require focus in the development of future student-focused CTF tools.

The results of the data analysis describe a set of requirements necessary for designing a student focused CTF tool.

The requirements are summarised below, where requirement 1-3 relate to content, and 4 and 5 relate to guidance:

- 1) A Variety of challenges
- 2) A Range of different challenge categories
- 3) Incrementing difficulty
- 4) Sufficient guidance for beginners such as providing reading material
- 5) Information on the comparison between real world attack vectors and the challenges within CTFs

These requirements coincide with research that has revealed that sufficient guidance is crucial to a CTF aimed at beginners, as without proper guidance beginners miss essential learning goals, which often results in them giving up [1], [16].

B. Prototype

Based on the findings, a prototype CTF aimed at introducing students to key cyber security concepts was developed.

As there are a variety of CTF challenge categories, we prioritised the requirements relating to content (requirements 1-3) using the MoSCoW prioritisation method. Competitions implemented were selected based on minimal design time. This analysis resulted in the design of:

- Web challenges with examples of the OWASP web top ten.
- Cryptography challenges with examples of different encryption and encoding schemes.
- Forensics challenges including examples of file forensics and steganography.
- Miscellaneous challenges that test general skills including Linux command line knowledge, programming knowledge and ability to use a variety of tools.
- OSINT challenges that encourage creativity and reconnaissance.

While Pwn and Reverse Engineering challenges were also feasible, they would take quite an amount of time to develop as they require extensive knowledge and proficiency in low level programming languages and assembly code. The MoSCoW selection of the challenges is illustrated in Fig. 5.

In relation to requirements 4 and 5 on guidance, we implemented the following:

- A cheat sheet page
A page that is designed to point the player in the right direction, with guidance on how to use the tools required to complete the challenges.
- An additional reading material page
A page consisting of links to reading material relevant to the challenges and categories in the CTF.
- Additional information page
A page designed to teach the student about how the challenges in the CTF relate to real world attack vectors in addition to suggestions on where to go after the CTF to further hone their cyber security skills.

A sample page from the prototype page is illustrated in Fig. 6.

Web	
Crypto	
Forensics	
Misc	
OSINT	
Pwn	
Reverse Engineering	

Included
Not included (Wishlist categories)

Fig. 5. Categories included and excluded from the CTF design using MoSCoW

Challenges			
Web			
Don't trust him!	50	One More Name Here	20
Students Union	75	Extremely exciting website...	100
Misc			
Index	5	怪異材料白濁	5
✓	20	Interference	50
Crypto			

Fig. 6. CTF Challenges page

C. Prototype Evaluation

To evaluate the tool's utility, walkthroughs were carried out with three participants, each lasting approximately 30 minutes. The participants were final year computing students, two of which had no prior CTF experience. Due to physical distancing restrictions, the walkthrough was run by the researcher, where the screen was shared online with the participants. On completion, semi-structured interviews were conducted and recorded.

The feedback received from the evaluation was generally positive indicating that the tool had the potential to spark cybersecurity interest and guide students while improving their practical skills. Additionally, the evaluation also revealed that the CTF experience (usage) actually dissuaded some students from a career in cyber security or ethical hacking in particular. Notable feedback is highlighted below:

Q: Are you more interested in cyber security, given the walkthrough of the challenges in this CTF?

A: *"I think so. You showed me things I didn't know of before and because of that I feel like I would be able to do more of these puzzles".*

Q: Would you be interested in doing more CTFs like this in future?

A: *"Yes I would. I do not know whether I'd want to go into ethical hacking per say, but I would definitely be interested in completing more CTFs like this".*

Q: Do you feel the CTF could inspire your interest to take up a career in cyber security?

A: *"No, in fact the opposite. It both seems super daunting to get into, and the fact there are games around how unsafe websites has made me not want to get into it. It's a whole barrel of fish I do not want to have my name next to".*

Q: Any other comment?

A: *"I had some fundamental knowledge necessary for the completion of the challenges, however only at a theoretical level and I didn't know how they were exploited in real life. I thought the addition of the cheat sheet and materials was really nice for the absolute beginners".*

VI. CONCLUSION AND FUTURE WORK

The background research for this study established that CTFs are not suitably designed for beginners, this includes a lack of guidance and suitably designed challenges - which in turn contributes to the cybersecurity skills gap [16]. While our study did not prove that this is indeed the case - possibly due to the limited cohort. The study, however, identified the basic requirements for a student-focussed CTF, from which a prototype was developed.

From a behaviour perspective, the study has shown that with the appropriate design, CTFs can strengthen student's interest in pursuing a career in cyber security and improving their practical skills. However, it has also been established that CTFs have the potential to dissuade those less familiar with the (ethical) hacking aspects of cyber security, who view cyber security as something of a dark-art. This suggests that providing student-focused CTFs is only one step to addressing the cyber security skills gap, but that training on the advantages of the various forms of cyber security is also required in order to change this perception.

For future work, we will conduct further studies with cyber security groups in different universities, while building on the requirements for a student-focussed CTF.

REFERENCES

- [1] T. J. Burns, S. C. Rios, T. K. Jordan, Q. Gu, and T. Underwood, "Analysis and Exercises for Engaging Beginners in Online CTF Competitions for Security Education," in *2017 USENIX Workshop on Advances in Security Education (ASE 17)*. Vancouver, BC: USENIX Association, Aug. 2017.
- [2] R. S. Cheung, J. P. Cohen, H. Z. Lo, F. Elia, and V. Carrillo-Marquez, "Effectiveness of cybersecurity competitions," in *Proceedings of the International Conference on Security and Management (SAM)*. The Steering Committee of The World Congress in Computer Science, Computer ..., 2012, p. 1.
- [3] W. Crumpler and J. Lewis, "The Cybersecurity Workforce Gap," CSIS, Washington, Tech. Rep., 2019.
- [4] CSIS, "Hacking the Skills Shortage," McAfee, Santa Clara, CA, Tech. Rep., 2016.
- [5] M. Dawson, "National Cybersecurity Education: Bridging Defense to Offense," *Land Forces Academy Review*, vol. 25, no. 1, pp. 68–75, Mar. 2020.

- [6] K. Evans, *Human capital crisis in cybersecurity: technical proficiency matters*. Place of publication not identified: Ctr For Strat & Intl Stds, 2010.
- [7] HM Government, "NATIONAL CYBER SECURITY STRATEGY 2016-2021," UK Government, London, UK, Tech. Rep., 2016.
- [8] B. Huang, K. F. Hew, and C. K. Lo, "Investigating the effects of gamification-enhanced flipped learning on undergraduate students' behavioral and cognitive engagement," *Interactive Learning Environments*, vol. 27, no. 8, pp. 1106–1126, 2019.
- [9] ISACA, "State of Cybersecurity: Implications for 2015 - An ISACA and RSA Conference Survey," ISACA, San Francisco, Tech. Rep., 2015.
- [10] —, "State of Cyber Security 2017: Part 1: Current Trends in Workforce Development," Rolling Meadows, IL, Tech. Rep., 2017.
- [11] —, "State of cybersecurity 2018 Part 1: Workforce Development," ISACA, Schaumburg, IL, Tech. Rep., 2018.
- [12] L. McDaniel, E. Talvi, and B. Hay, "Capture the Flag as Cyber Security Introduction," in *2016 49th Hawaii International Conference on System Sciences (HICSS)*. Koloa, HI, USA: IEEE, Jan. 2016, pp. 5479–5486.
- [13] Raytheon, "Securing Our Future: Closing the Cybersecurity Talent Gap," National Cyber Security Alliance, Sterling, VA, Tech. Rep. 2016 Survey Results, 2016.
- [14] S. Sharkey, D. Morin, and J. Hunter, "COMMENTS OF T-MOBILE USA, INC." NIST, Washington, Tech. Rep., 2017.
- [15] P. D. Umbach and M. R. Wawrzynski, "Faculty do Matter: The Role of College Faculty in Student Learning and Engagement," *Research in Higher Education*, vol. 46, no. 2, pp. 153–184, 2005.
- [16] R. Weiss, F. Turbak, J. Mache, E. Nilsen, and M. E. Locasto, "Finding the Balance Between Guidance and Independence in Cybersecurity Exercises," in *2016 USENIX Workshop on Advances in Security Education (ASE 16)*. Austin, TX: USENIX Association, Aug. 2016.