Code Hunt as Platform for Gamification of Cybersecurity Training

Sandro Fouché
Computer and Information Sciences Department
Towson University
Towson, MD USA
sfouche@towson.edu

Andrew H. Mangle
Computer and Information Sciences Department
Towson University
Towson, MD USA
amangle@towson.edu

ABSTRACT

The nation needs more cybersecurity professionals. Beyond just a general shortage, women, African Americans, and Latino Americans are underrepresented in the field. This not only contributes to the scarcity of qualified cybersecurity professionals, but the absence of diversity leads to a lack of perspective and differing viewpoints. Part of the problem is that cybersecurity suffers from barriers to entry that include expensive training, exclusionary culture, and the need for costly infrastructure. In order for students to start learning about cybersecurity, access to training, infrastructure and subject matter experts is imperative. The existing Code Hunt framework, used to help students master programming, could be a springboard to help reduce the challenges facing students interested in cybersecurity. Code Hunt offers gamification, community supported development, and a cloud infrastructure that provides an on-ramp to immediate learning. Leveraging Code Hunt's structured gaming model can addresses these weaknesses and makes cybersecurity training more accessible to those without the means or inclination to participate in more traditional cybersecurity competitions.

Categories and Subject Descriptors

D.2.5 [**Software Engineering**]: Testing and Debugging; K.3.1 [**Computers and Education**]: Computer Uses in Education; K.3.2 [**Computers and Education**]: Computer and Information Science Education

General Terms

Security

Keywords

Cybersecurity, Education, Gamification, Software Testing

1. INTRODUCTION

Our nation faces a shortage of Cybersecurity professionals; "A shortage exists, it is worst for the federal government, and it potentially undermines the nation's cybersecurity." [4]. Cybersecurity competitions have been used to promote cybersecurity training, assess participant knowledge, and develop skills to protect against cyber attacks. Competitive cybersecurity games have been successful in engaging, assessing, motivating and building student knowledge [1]. Additionally, such competitions enrich the security community by collecting information that can be used for experimentation in the security field [7]. These competitions are usually short duration, highly-intense affairs and cater to certain groups.

Preparing for cybersecurity events also requires significant time commitment and resources that are not available to everyone. Competitions focus on domain-specific knowledge, but there is a lack the skill building exercises to assist those just starting out. Few competitions provide training before the event or separate individuals into categories based on their abilities as Nowicki et al. recommended [5]. To succeed at national and many local competitions, participants need significant training, support equipment and access to costly infrastructure. Exacerbating these issues, the adversarial nature of traditional cybersecurity competitions limits their engagement to those students who thrive in such environments. Additionally, the participation costs – including equipment, registration, time, and travel limit access to financially disadvantaged communities. Consequently these barriers to entry make cybersecurity study and practice less attractive to already underrepresented populations such as women and minorities [6].

Code Hunt presents a unique opportunity to broaden the inclusiveness of cybersecurity training. It is an interactive educational gaming platform that aims to develop programming skills in an engaging environment. Code Hunt leverages search-based testing and cloud services to provide fresh content and evolving challenges for beginning and intermediate level developers using a web-based platform [2]. While the platform has been used in formal educational settings (colleges, high schools, MOOCs, and competitions), its potential use in informal settings (self-training and personal enrichment) can lead to a sea-change in cybersecurity education. Code Hunt represents a framework that supports individual learning and competition without traditional infrastructure costs. Participants can utilize a range of connected devices (mobile, tablets, and computers) and can access the content anytime, anywhere. Removed from traditional educational environments the opportunity exists for students to

CHESE'15, July 14, 2015, Baltimore, MD, USA
ACM. 978-1-4503-3711-3/15/07
http://dx.doi.org/10.1145/2792404.2792406

engage with cybersecurity education in private at their own pace, without fear of the stigma, judgement, or ridicule that classroom settings can engender. The challenge for Code Hunt and other methods of gamification is to provide both feedback and support for training which requires expanding the focus from competition and practice to also include instruction [3][5].

2. PROPOSED SOLUTION

Using games to improve cybersecurity have been successful in engaging learners, assessing knowledge, and motivating students [1]. For a student, we propose that web-based security games are ideal for developing interest and knowledge in the cybersecurity domain. Leveraging web-based tools which work across multiple platforms and devices with anytime availability offer an inviting and inclusive approach to cybersecurity. Existing competition and practice sites such as picoCTF (`http://www.picoctf.com`) and OverTheWire (`http://overthewire.org`) provide alternative strategies for encouraging and assessing learning but often direct participants to search for the answer instead of taking advantage of learning opportunity.

Our position is that Code Hunt's successful model represents a platform to achieve the goals of educating, training and developing cybersecurity professionals. By providing an opportunity to leverage a fun and entertaining platform, Code Hunt could be extended to introduce the concepts of Application Security and IT auditing to a wider audience. Adding gamification training for introductory cybersecurity topics (auditing, application, and development security) expands the successful approach of Code Hunt to a new audience. This paper is not the first to suggest such an approach – Xie et al. suggested secure coding exercises for Code Hunt [9]. While< that paper focussed solely on cybersecurity problem sets based on production code samples more suitable for experienced programmers, we propose creating a series of Code Hunt exercises paired supplemental resources targeted being inclusive to novice programmers. This gentler approach to cybersecurity education would augment the previous proposal with three new assets: introductory tutorial texts, hand-crafted, incremental exercises, and support materials to assist learners to understand the concepts behind the challenges.

Introductory Texts. While the existing Code Hunt implementation is engaging, entertaining, as well as educational, it provides little in the way of introduction to the system or tutorial of programming concepts. The existing implementation works well when paired with traditional classroom instruction, but does not provide enough support for other types of users. Considering the 24x7, global availability of Code Hunt, it makes sense to leverage it as a tool to drive inclusion outside of the classroom. It should be noted that CodeHunt's predecessor – Pex4Fun, did include such introductory texts [8]. To enable use of Code Hunt by a wider range of users, we suggest Code Hunt be paired with carefully selected introductory texts. We propose to investigate whether appropriate material can be culled from existing textbooks and training material or needs to be created to suit a self-directed, online training environment such as Code Hunt.

Incremental Exercises. In their paper [9], Xie et al. advocate the extension of Code Hunt with input validation and access control exercises based on real artifacts from previous work and the NIST National Vulnerability Database (`http://nvd.nist.gov`). While the proposed exercises would be beneficial to more experienced students, they may be beyond the grasp of students just introduced to programming concepts. Instead, we propose the addition of carefully chosen introductory challenges designed to build cybersecurity skills and confidence in parallel. Bishop et al. have indicated a significant drop-off after Code Hunt's first level and have suggested that providing awareness may improve retention but this hypothesis has not been tested [2]. We suggest that an incremental approach that incorporates supplementary material on a question-by-question basis will improve retention and completion of the exercises.

The cybersecurity community often contributes to competition problem sets and would likely be willing to contribute introductory challenges. InfoSec recently held an event proposing Capture-the-Flag style questions and rewarded participants with the best posted solutions (`http://resources.infosecinstitute.com/n00bs`). Each of the created problems were designed to incrementally present an introduction to cybersecurity topics. If resources are constrained, a similar approach may be used to leverage existing Code Hunt community to contribute questions and facilitate the development of training material.

Built-In Support Materials. In addition to the existing clue and hint system, Code Hunt should be extended to provide more robust in-situ instructional aids to support cybersecurity training. These supporting materials would serve to assist learners in understanding the concepts behind the challenges. Including such support within Code Hunt limits distraction and frustration by providing just-in-time learning. Additionally, in platform support materials can be quantitatively analyzed to determine if the user acquired the knowledge to solve the challenge.

Overall, the existing open cloud-based platform could be extended to promote cybersecurity training as well as programming skills. Our proposed changes are intended broaden the reach of Code Hunt and encourage users of various backgrounds to develop cybersecurity skills.

3. REFERENCES

[1] J. A. Amorim, M. Hendrix, S. F. Andler, and P. M. Gustavsson. Gamified Training for Cyber Defence. In *NATO Modelling and Simulation Group MSG Annual Conference*. North Atlantic Treaty Organization, 2013.

[2] J. Bishop, R. N. Horspool, T. Xie, and N. Tillmann. Code Hunt: Experience with coding contests at scale. *Proc ICSE*, 2015.

[3] S. Combéfis and J. Wautelet. Programming Trainings and Informatics Teaching Through Online Contests. *Olympiads in Informatics*, 8:21–34, 2014.

[4] M. C. Libicki, D. Senty, and J. Pollak. Hackers Wanted: An Examination of the Cybersecurity Labor Market. *Hackers Wanted: An Examination of the Cybersecurity Labor Market*, June 2014.

[5] M. Nowicki, M. Matuszak, and A. Kwiatkowska. Teaching secondary school students programming using

distance learning: a case study. In *10th IFIP World Conference on Computer in Education*, pages 246–254, Toruń, Poland, 2013. Nicolaus Copernicus University Press.

[6] R. Shumba, K. Ferguson-Boucher, E. Sweedyk, C. Taylor, G. Franklin, C. Turner, C. Sande, G. Acholonu, R. Bace, and L. Hall. Cybersecurity, women and minorities: findings and recommendations from a preliminary investigation. In *Proceedings of the 2013 Conference on Innovation and technology in Computer Ccience Education Working Group Reports*. ACM, June 2013.

[7] T. Sommestad and J. Hallberg. Cyber Security Exercises and Competitions as a Platform for Cyber Security Experiments. In *Secure IT Systems*, pages 47–60. Springer Berlin Heidelberg, Berlin, Heidelberg, 2012.

[8] N. Tillmann, J. de Halleux, T. Xie, S. Gulwani, and J. Bishop. Teaching and learning programming and software engineering via interactive gaming. In *ICSE '13: Proceedings of the 2013 International Conference on Software Engineering*. IEEE Press, May 2013.

[9] T. Xie, J. Bishop, N. Tillmann, and J. de Halleux. Gamifying software security education and training via secure coding duels in code hunt. *HotSoS*, pages 26–2, 2015.