Proceedings of the Informing Science + Information Technology Education Conference

An Official Publication of the Informing Science Institute InformingScience.org

InformingScience.org/Publications

Online July 24 – 25, 2024

GAMIFIED CYBERSECURITY EDUCATION THROUGH THE LENS OF THE INFORMATION SEARCH PROCESS: AN EXPLORATORY STUDY OF CAPTURE-THE-FLAG COMPETITIONS

[RESEARCH-IN-PROGRESS]

Albert Tay*	Brigham Young University, Provo, UT, USA	albert_tay@byu.edu
Sebastian Hayes	Brigham Young University, Provo, UT, USA	sh933@byu.edu
Drew Wilson	Brigham Young University, Provo, UT, USA	aw053102@byu.edu
Emmie Hall	Brigham Young University, Provo, UT, USA	elhall279@gmail.com
Dallin Kaufman	Brigham Young University, Provo, UT, USA	kaufman1@byu.edu

* Corresponding author

ABSTRACT

Aim/Purpose	Capture the Flag (CTF) challenges are a popular form of cybersecurity education where students solve hands-on tasks in a game-like setting. These exercises provide learning experiences with various specific technologies and subjects, as well as a broader understanding of cybersecurity topics. Competitions reinforce and teach problem-solving skills that are applicable in various technical and non-technical environments outside of the competitions.
Background	The Information Search Process (ISP) is a framework developed to understand the process by which an individual goes about studying a topic, identifying emotional ties connected to each step an individual takes. As the individual goes through the problem-solving process, there is a clear flow from

The full paper has been published as the following and is being presented at this conference:

Tay, A., Hayes, S., Wilson, D., Hall, E., & Kaufman, R. (2024). Gamified cybersecurity education through the lens of the information search process: An exploratory study of Capture-the-Flag competitions [Research in progress]. *Issues in Informing Science and Information Technology, 21,* Article 1. https://doi.org/10.28945/5313

Abstract published in *Proceedings of InSITE 2024: Informing Science and Information Technology Education Conference*, July 24-25 [online], Article 12. Informing Science Institute. https://doi.org/10.28945/5255

(CC BY-NC 4.0) This article is licensed to you under a Creative Commons Attribution-NonCommercial 4.0 International License. When you copy and redistribute this paper in full or in part, you need to provide proper attribution to it to ensure that others can later locate this work (and to ensure that others do not accuse you of plagiarism). You may (and we encourage you to) adapt, remix, transform, and build upon the material for any non-commercial purposes. This license does not permit you to use this material for commercial purposes.

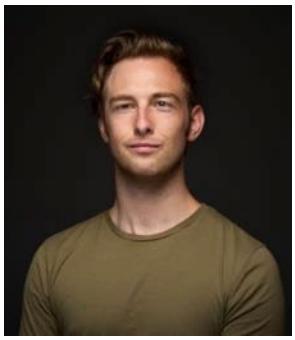
	uncertainty to clarity; the individual's feelings, thoughts, and actions are all interconnected. This study aims to investigate the learning of cybersecurity concepts within the framework of the ISP, specifically in the context of CTF competitions.
Methodology	A comprehensive research methodology designed to incorporate quantitative and qualitative analyses to draw the parallels between the participants' emotional experiences and the affective dimensions of learning will be implemented to measure the three primary goals.
Contribution	This study contributes significantly to the broader landscape of cybersecurity education and cognitive-emotional experiences in problem-solving.
Findings	The study has three primary goals. First, we seek to enhance our understanding of the emotional and intellectual aspects involved in problem-solving, as demonstrated by the ISP approach. Second, we aim to gain insights into how the presentation of CTF challenges influences the learning experience of participants. Lastly, we strive to contribute to the improvement of cybersecurity education by identifying actionable steps for more effective teaching of technical skills and approaches.
Recommendations for Practitioners	Competitions reinforce and teach problem-solving skills applicable in various technical and non-technical environments outside of the competitions.
Recommendations for Researchers	The Information Search Process (ISP) framework may enhance our understanding of the emotional and intellectual aspects involved in problem-solving as we study the emotional ties connected to each step an individual takes as the individual goes through the problem-solving process.
Impact on Society	Our pursuit of advancing our understanding of cybersecurity education will better equip future generations with the skills and knowledge needed to address the evolving challenges of the digital landscape. This will better prepare them for real-world challenges.
Future Research	Future studies would include the development of a cybersecurity curriculum on vulnerability exploitation and defense. It would include practice exploiting practical web and binary vulnerabilities, reverse engineering, system hardening, security operations, and understanding how they can be chained together.
Keywords	cybersecurity, Capture-the-Flag, information search process, gamification

AUTHORS

Albert Tay, an IT & Cybersecurity faculty member at Brigham Young University, received his Ph.D. in Communication and Information Sciences from the University of Hawaii, Manoa. Dr. Tay is co-PI on the NSF CyberCorps Scholarship for Service grant ($3.7 million).

Prior to joining BYU, Dr. Tay managed Utah's Statewide Longitudinal Data Systems program and served as the project director for the IES FY 2015 SLDS grant ($6.7 million). Dr. Tay has also taught IT courses at various universities and managed IT departments and projects in various industries.

Sebastian Hayes is currently a cybersecurity student at Brigham Young University. Sebastian is a teaching assistant for IT & Cybersecurity courses. He also serves as a research assistant at the Cybersecurity Research Laboratory. He is president of the Network Engineering Student Association and program director for Kids Who Code. He participated in NCAE CyberGames (placed 1st in regionals 2022 and 2023) and National Cyber League CTF (placed 3rd in Fall 2023). He has also assisted in creating the BYU public CTF (2022, 2023), BYU STEM Camp CTF (2023), and BYU Cybersecurity Camp CTF (2022, 2023).



Drew Wilson is a Computer Science student at Brigham Young University. Drew is a teaching assistant for Computer Science courses. He also serves as a research assistant at the Cybersecurity Research Laboratory. He is vice president of the Cybersecurity Student Association and is interested in applying machine learning to cybersecurity tools and processes. He has participated in many cybersecurity competitions, including the National Cyber League, where his team placed 3rd, and Hack the Building, which emphasized securing ICS technology against APTs.

Emmie Hall is currently a cybersecurity student at Brigham Young. Emmie works in the Office of Information Technology. She was a teaching assistant for an IT & Cybersecurity course. She also serves as a research assistant at the Cybersecurity Research Laboratory. She participated in NCAE CyberGames (placed 1st in regionals 2023).

Dallin Kaufman is currently a cybersecurity student at Brigham Young. He volunteers at the Cybersecurity Research Laboratory. He also teaches introductory cybersecurity classes and leads the CTF group for the Cybersecurity Student Association. He participated in the National Cyber League Team competition (placed 3rd nationally) and the National Collegiate Cyber Defense Competition (placed 8th nationally).