KSU Proceedings on Cybersecurity Education, Research and Practice

2021 KSU Conference on Cybersecurity Education, Research and Practice

Oct 30th, 3:30 PM - 4:00 PM

Emotional Analysis of Learning Cybersecurity with Games using IoT

Maria Valero
mvalero2@kennesaw.edu

Md Jobair Hossain
Kennesaw State University, mhossa21@students.kennesaw.edu

Shahriar Sobhan
Kennesaw State University, sshobhan@students.kennesaw.edu

Valero, Maria; Hossain, Md Jobair; and Sobhan, Shahriar, "Emotional Analysis of Learning Cybersecurity with Games using IoT" (2021). *KSU Proceedings on Cybersecurity Education, Research and Practice*. 5.
https://digitalcommons.kennesaw.edu/ccerp/2021/Research/5

Abstract

The constant rise of cyber-attacks poses an increasing demand for more qualified people with cybersecurity knowledge. Games have emerged as a well-fitted technology to engage users in learning processes. In this paper, we analyze the emotional parameters of people while learning cybersecurity through computer games. The data are gathered using a non-invasive Brain-Computer Interface (BCI) to study the signals directly from the users' brains. We analyze six performance metrics (engagement, focus, excitement, stress, relaxation, and interest) of 12 users while playing computer games to measure the effectiveness of the games to attract the attention of the participants. Results show participants were more engaged with parts of the games that are more interactive instead of those that present text to read and type.

Location

Online Zoom Session

Disciplines

Information Security | Management Information Systems | Technology and Innovation

WORK IN PROGRESS – EXTENDED ABSTRACT

Cyber-attacks continue to rise with more technical sophistication and increasing impact throughout the globe [1]. There is a high demand for cybersecurity professionals with adequate motivation and reasonable skills to detect, prevent, respond and mitigate the effects of such threats [2]. In higher education, cybersecurity is traditionally taught in undergraduate programs; and more recently, specialized cybersecurity graduate programs were created to meet the industrial demand [3]. An emerging trend in cybersecurity education is to increase the awareness of cyber-attacks and prevention through "digital games" [4]. Playing games is a widespread activity across race, gender, and socioeconomic status [5] and have the potential to teach different scenarios and contexts, besides being affordable [4]. The engagement feature and interactivity of digital games make them good medium to teach cybersecurity. However, how can we know if those games are effective? Is the person playing the digital games really engaged? Is he/she interested? Is this person completely focused on the game, or is he/she distracted? Can we see if these games generate enough attention from the participant that leads to knowledge retention? While answers to these questions can be indirectly measured by surveys and posttests, we can gain more insights if we can exam a person's brain activities when playing games. In this work, we propose to use a Brain-Computer Interface (BCI) to directly read people's brain signals and transferred them into a stream data database to measure their level of (i) engagement, (ii) focus, (iii) excitement, (iv) stress, (v) relaxation, and (vi) interest while playing cybersecurity games. The idea is to perform effective analysis of teaching cybersecurity with games by extracting information from a wearable IoT device. We use Emovit Epoc+ Neuroheadset [6] to read and record brain signals. Emotiv is a bioinformatics company focused on developing varieties of electroencephalography (EEG) based BCIs products with the mission of empowering individuals to understand their brain and accelerate brain research globally.

The main contributions of this paper can be summarized as follows:

1. We analyze the effectiveness of learning cybersecurity concepts using games from the perspective of emotional parameters obtained directly from brain signals.

2. We categorize the level of (i) engagement, (ii) focus, (iii) excitement, (iv) stress, (v) relaxation, and (vi) interest of participants while learning cybersecurity with games.

ACKNOWLEDGEMENT

The work is partially supported by ICWD Summer Research Grant 2021.

REFERENCES

[1] G. Vasiliadis, M. Polychronakis, and S. Ioannidis, "GPU-assisted malware," *Int. J. Inf. Secur.*, vol. 14, no. 3, pp. 289–297, 2015, doi: 10.1007/s10207-014-0262-9.

[2] D. Mouheb, S. Abbas, and M. Merabti, "Cybersecurity Curriculum Design: A Survey," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 11345 LNCS, pp. 93–107, 2019, doi: 10.1007/978-3-662-59351-6_9.

[3] Kennesaw State University, "Master Degree in Cybersecurity," 2021. https://www.kennesaw.edu/master-degrees/cybersecurity/index.php.

[4] M. Coenraad, A. Pellicone, D. J. Ketelhut, M. Cukier, J. Plane, and D. Weintrop, "Experiencing Cybersecurity One Game at a Time: A Systematic Review of Cybersecurity Digital Games," *Simul. Gaming*, vol. 51, no. 5, pp. 586–611, 2020, doi: 10.1177/1046878120933312.

[5] Jesper Juul, "A casual revolution: reinventing video games and their players," *Choice Rev. Online*, vol. 47, no. 12, pp. 47-6689-47–6689, 2010, doi: 10.5860/choice.47-6689.

[6] Emotiv, "Emotiv," *Emotiv*, 2021. https://www.emotiv.com/about-emotiv (accessed Feb. 27, 2021).