Emotional Analysis of Learning Cybersecurity with Games

Maria Valero*, Lei Li*, Hossain Shahriar*, Shahriar Sobhan†, Michael Handlin*, and Jinghua Zhang‡
*Information Technology Department, Kennesaw State University
†CyberSecurity Institute, Kennesaw State University
‡Computer Science Department, Winston-Salem State University

***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.**

***Index Terms*—Emotional parameters, cybersecurity, games.**

I. Introduction

The cyber-attacks continue to rise with more technical sophistication and increasing impact throughout the globe [2]. 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 [3]. In higher education, cybersecurity is traditionally taught in undergraduate programs; and more recently, specialized cybersecurity graduate programs were created to meet the industrial demand [4]. An emerging trend in cybersecurity education is to increase the awareness of cyber attacks and prevention through "digital games" [5]. Playing games is a widespread activity across race, gender, and socioeconomic status [6] and have the potential to teach different scenarios and contexts, besides being affordable [5]. The engagement feature and interactivity of digital games make them good medium to teach cybersecurity. How ever, how can we know if those games are an 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 post tests, we can gain more insights if we can exam a person's brain activities when playing games.

This work was supported in part by the Kennesaw State University Institute for Cybersecurity Workforce Development, and the research computing resources and technical expertise via a partnership between Kennesaw State University's Office of the Vice President for Research and the Office of the CIO and Vice President for Information Technology [1].

In this paper, 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 [7] 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 [8].

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.

This paper is organized as follows: Section II provides an overview of cybersecurity games; Section III discusses various parameters used in our study; Section IV highlights experimental design, while Sections V and VI present the results and concludes the paper, respectively.

II. Cybersecurity with Games

Many approaches aim to teach cybersecurity using different types of computer games. In 2020, Coenraad et al. [9] presented a systematic review of 181 cybersecurity digital games that can be found in the Apple App Store, the Google Play Store, Steam, and the web broadly. The study was mainly focused on determining which cybersecurity content is being conveyed through digital games and which cybersecurity practices are promoted. The authors also analyzed the characteristics of the games such as game development, audience, playtime, visual realism, camera view, etc. However, the level of engagement of the participants respecting the presented content is not analyzed. Galikova et al. [10] presented preliminary work on proposing guidelines for creating technical cybersecurity games in a higher education context. The guidelines include identification of learning outcomes,

designing of challenges/tasks and solutions, creating anti-cheating policies, designing game narratives, and privacy considerations. However, no guideline was designed for participant engagement in the game. One research that does consider engagement was presented in 2021 by Karagiannis et al. [11]. In this study, the authors examined how instructional design could be applied and how computer games can be a learning environment for acquiring the basic skills and experience in fundamental cybersecurity topics. The role of engagement in this study was analyzed from the perspective of game design. When playing games, participants are called to solve complex problems and participate without experiencing fatigue, while in a comfortable learning task [11]. However, the analysis of these factors is mainly conducted from the game point of view and not from the real feelings of the participant.

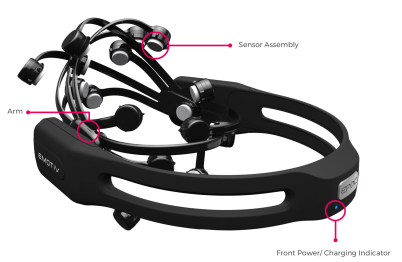
In 2020, Zhang et al. [12] present a game to teach an important concept in cybersecurity, buffer overflow. The engagement level of the participants in six learning components was evaluated using classroom experience reports and surveys. Results showed that 90.5% of students strongly agree or agree that the learning objectives of the buffer overflow game were met. Also, surveys asked if the participant enjoyed the learning experience.

To enhance the previous studies, we propose to objectively analyze the level of engagement, excitement, focus, relaxation, the interest of the participants while they are playing games that teach cybersecurity. We believe that our work can help advance the knowledge of the impact of the games in the interest of the participants in a specific learning topic.

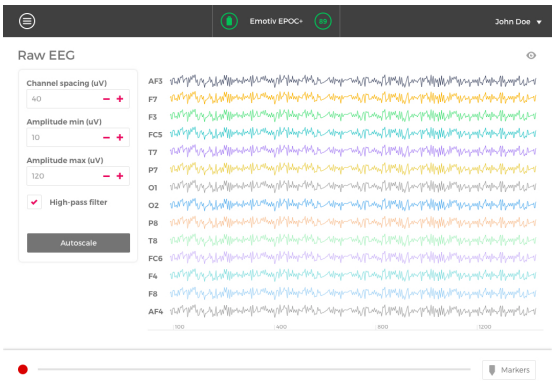
III. Electroencephalogram and Emotional Parameters

The Electroencephalogram or EEG is a signal that indicates the time change of electrical potential caused by the brain activity [13]. This signal is different from person to person and mostly depends on age, gender, vigilance, and other factors. However, the features of the signals are the same, so this allows their analysis and processing [13]. Invasive, partially invasive, and non-invasive methods can be used to capture EEG. In the invasive methods, electrodes are placed to the grey cerebral cortex during surgery. This procedure ensures a high-quality signal; however, it may produce also brain damage [14]. In the partially invasive methods, the electrodes are implemented inside the skull, but outside the brain. The quality of the signal is good and the risk of brain damage is less; however, it still requires surgery procedures [15]. During non-invasive methods, the EEG signal is a capture from the surface of the head [16]. This method, also known as Brain-Computer Interface (BCI), is secure, and it does not require invasive procedures.

The BCI Emotiv EPOC+ device [7] neuroheadset, captures signals using the non-invasive method, specifically by measuring voltage potentials from the skull surface. Figure 1(a) shows the BCI neuroheadset and Figure 1(b) an example of EEG signal. The neuroheadset allows capturing six performance metrics (i) engagement, (ii) focus, (iii) excitement, (iv) stress,



(a)



(b)

Fig. 1: (a) The BCI Emotiv EPOC+ Neuroheadset.

(v) relaxation, and (vi) interest, that are related to human emotions. The engagement performance metric measures the level of attention on a specific task. The focus performance metric is also related to attention, but also with concentration on the specific task. The excitement measures the level of arousal, and the stress performance metric is a measure of the level of challenge associated with the specific task. Finally, the relaxation metric determines the ability of the subject to regain composure after immersion in the task, and the interest performance metric gauges the extent to which a subject is attracted or averse to the task.

IV. Experiment Design

A. Research Ethics

The Institutional Review Board (IRB) at Kennesaw State University granted permission to conduct this research study (Study #IRB-FY21-481). The study was completely non-invasive and posed no physical harm to participants. Letters of consent were provided and signed by participants where we explained the purpose of the research, risks, compensation, and their right to drop the study at any moment without consequences. We assured participants of the confidentiality and anonymity of their information and data.

B. Experiment Design

1) Selected Games: Two of the major topics when teaching cybersecurity are the problems generated with buffer overflow and access control. Despite extensive research over the past decades, buffer overflow has been the number one security

vulnerability in applications for many years [12]. Buffer overflow is a type of software error that can lead to a program crash, data corruption, and security breaches. A buffer overflow occurs when a program overruns the buffer's boundary and overwrites adjacent memory [17]. On the other hand, learning effective access control mechanisms is primordial for improving cybersecurity. In this study, we use two games. Game 1 is referred to as "Buffer overflow" game. In this game, students learn important concepts of buffer overflow including call stack illustration, simple buffer overflow, overwriting a variable, overwriting a return variable, redirecting, and countermeasures. Game 1 was developed by [12] and is a web-based interactive visualization tool that was developed using the Unity game engine. All scripts were written in C# programming language using Visual Studio Community IDE. Currently, this tool was built to the WebGL format through Unity and uploaded to a web server to be played as an online game [12]. Game 2 is referred to as "Access Control" game. In this game, students learn concepts related to access control including discretionary access control, reading and accessing files, permission change, etc. Both games are available online in [18] and [19].

2) Participants: To recruit participants for this experiment, we send out a promotional flyer to students inside Kennesaw State University using the College mail list. The study was applied to 12 subjects ages between 18 and 50 years old. Subjects belonged to different University Departments such as Information Technology, Computer Science, Information Systems, and Software Engineering with some background in cybersecurity and enough skills to play online games. The gender distribution of the participants was 70% male and 30% female. Each subject was assigned randomly either the buffer overflow or access control game.

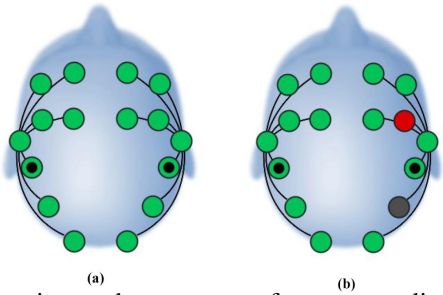
3) Data Collection Preparation: Participants were asked to fill out a pre-survey before they arrived at the data collection center. The pre-survey collected information about the previous experience of the participant with online games. We placed the Emotiv Neuroheadset over the head skull of the participants. Figure 2 shows different participants in the data collection setting using the neuroheadset.

To effectively collect EEG signals, it is necessary to prepare the headset and the applications and adjust the headset with the skull. We found the physical design of the Epoc+ neuroheadset has deficiencies in terms of maintaining the contact quality above 98%, which is required for accessing various features and getting expected readings. Fig. 3 presents the contact quality between the skull and the electrodes during the evaluation that reaches 100 % (Figure 3a) and 61 % (Figure 3b).

4) Collected Variables: Participants played the games for a period no longer than 20 minutes. During that time, we collect brain signals related to six performance parameters that are closely related to human emotions while doing an activity. The (i) engagement, (ii) focus, iii) excitement, (iv) stress, (v) relaxation, and (vi) interest parameters were collected. Each of the performance metrics is estimated with a 0.1 Hz frequency. For each metric, the neuroheadset provides five data

(a) (b) (c) (d)

Fig. 2: Data collection process. (a) female subject playing buffer overflow game. (b) male subject playing buffer overflow game. (c) female subject reading instructions for access control game. (d) male subject playing access control game.



(a) (b)

Fig. 3: Overview and percentage of contact quality of Epoc+ Neuroheadset. (a) 100% contact quality. (b) 61% contact quality.

parameters. Those are:

- **Scaled Data** shows the raw data scaled on a 0 to 1 scale to provide more context for each individual's score. Values near to 1 represent a major presence of the parameter metric.
- **Raw** shows the raw values outputted from the performance metric algorithm, which can range from single digit negative number to single digit positive numbers.
- **MIN/MAX** sets lower and upper bounds for the scaled data and are calculated from the current mean and variance of the raw data.
- **ACT** indicates performance indicator. If ACT value is 1, it means active. When ACT is 0, it means poor quality and/or noise

Figure 4 shows an example of scaled data for each one of the six performance metrics in a period of 5 minutes with a sampling rate of 0.1 Hz.

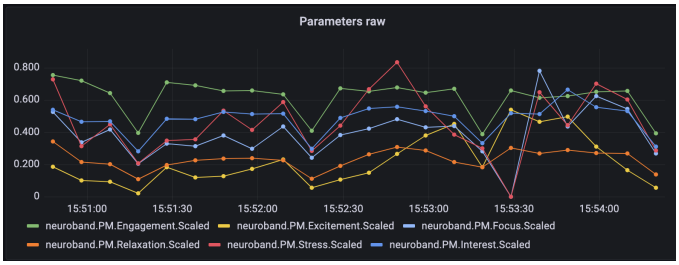


Fig. 4: Scaled data from engagement (green), excitement (yellow), focus (light blue), relaxation (orange), stress (red), interest (dark blue).

5) Data Storage and Visualization: In order to process the collected data, we extract the information from EmotivPRO software and import them into a stream data database. We developed a Python script to extract the data and import it into our own database. The extracted data is sent to a Cloud (High-Computing Performance - HCP Cloud) in real-time by following HTTPS (Hypertext Transfer Protocol Secure) security protocol and storing it in a powerful stream-data database InfluxDB [20]. For visualizing the data, we employed Grafana tool [21] to show the performance parameters with a timestamp for easy analysis.

V. Results and Discussion

As mentioned before, 12 subjects contributed to the experiment by playing cybersecurity games while using the neuroheadset to collect their EEG signals.We ensured that the data was collecting by getting a 100% contact quality of the neuroheadset and the subject. We randomly assigned the type of game to play. Eight (8) subjects played game #1 – Buffer Overflow, and four (4) participants played game #2 – Access Control. After the study, each participant filled out a post-survey that asks them about the emotions that they experiment during the experiment. None of the participants had played cybersecurity games in the past. Table I presents the preliminary results from the survey that also serve as a comparison with the signals obtained from their brains; subjects ranged from 1 to 10, being 1 the lowest level and 10 the highest level of engagement, excitement, stress, relaxations, focus, and interest while playing the game.

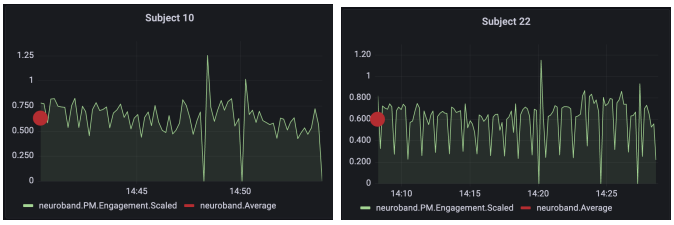
TABLE I: Level of performance metrics provided manually by the subjects after completing the experiment

Performance Metric / Level	1	2	3	4	5	6	7	8	9	10
Engagement	10%	10%	0%	0%	10%	30%	20%	10%	0%	10%
Excitement	10%	0%	20%	0%	40%	20%	0%	10%	0%	0%
Stress	50%	0%	0%	0%	37.50%	0%	12.50%	0%	0%	0%
Relaxation	10%	10%	0%	20%	20%	0%	10%	10%	10%	10%
Focus	0%	0%	10%	10%	0%	10%	50%	0%	20%	0%
Interest	0%	0%	10%	0%	10%	20%	10%	30%	0%	20%

First, the level of engagement reported by the subjects in both games was about levels 6, 7, and 8. This means that the majority of subjects reported being engaged with the games in all their phases. Figure 5 shows the level of engagement of the subjects taken from their brain signals from the subjects who played "Buffer Overflow" and Figure 6 shows the same but with "Access Control".

(a) (b) (c) (d)

Fig. 5: Example of level of engagement of four subjects playing the Game "Buffer Overflow". The red dot is the average of the engagement. (a) Subject 1. (b) Subject 3. (c) Subject 7. (d) Subject 11

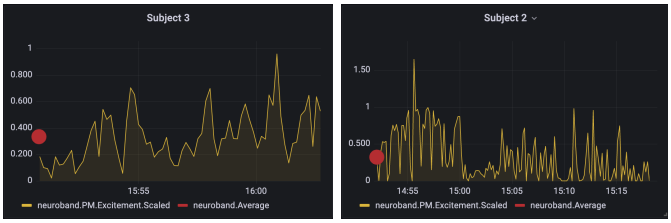


(a) (b)

Fig. 6: Example of level of engagement of two subjects playing the Game "Access Control". The red dot is the average of the engagement. (a) Subject 10. (b) Subject 22.

The average engagement range from subjects playing "Buffer Overflow" game (0.532) was slightly lower than participants playing "Access Control" game (0.671). We believe that this is due to the interactivity between the game and the subject. For example, "Buffer overflow" game presents initially some concepts and reading slides followed by an interactive short-time game. We can notice that when the subjects were playing the short-time game, the engagement increase compared with the time they were reading concepts. On the other hand, the "Access Control" game is a long interactive game. The subjects keep the engagement during the game. The peaks in the engagement were produced when the subjects achieve a new level in the game. With the level of excitement, subjects reported values mostly between 5 and 6. Figure 7 shows two examples of two subjects playing different games. For those playing "Buffer overflow" the excitement average was 0.35 and 0.489 for those playing "Access Control". We can notice from Figure 7a that while playing "Buffer Overflow" the subject was less excited at the

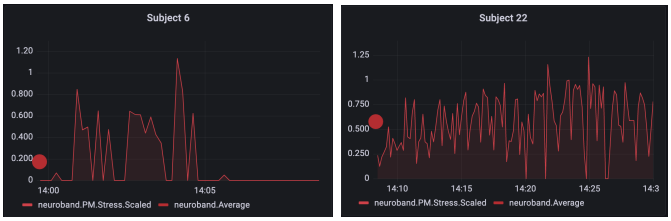
beginning and increased during the game. On the other hand, Figure 7b shows that the participant was more excited at the beginning of the "Access control" game than at the end. This could be due to the subjects start to get used to the rhythm of the game. For example, "Buffer Overflow" presents different dynamics during the game (mixing of thinking and playtime), so it seems that subjects were excited to see what it is coming next.



(a) (b)

Fig. 7: Example of level of excitement. The red dot is the average of the engagement. (a) Subject 3 playing "Buffer Overflow". (b) Subject 2 playing "Access Control".

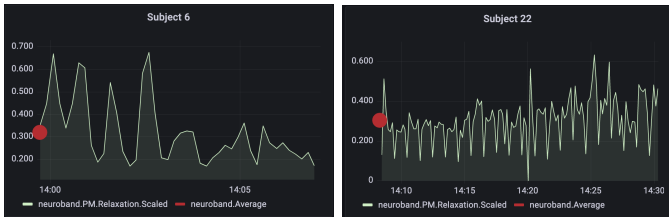
Regarding the level of stress, the subjects presented great variations from one and another. Regardless of the game, they were playing, we detect high and low levels of stress in subjects. For example, Figure 8a shows a participant playing "Buffer overflow" with low levels of stress at certain points, especially at the end of the game, and Figure 8b display the stress level of subject 22 while playing "Access control" game. Comparing with Table I, half of the participants reported not experiencing stress during the experiment, however, this was not exactly what the brain signals reported.



(a) (b)

Fig. 8: Example of level of stress. The red dot is the average of the engagement. (a) Subject 6 playing "Buffer Overflow". (b) Subject 22 playing "Access Control".

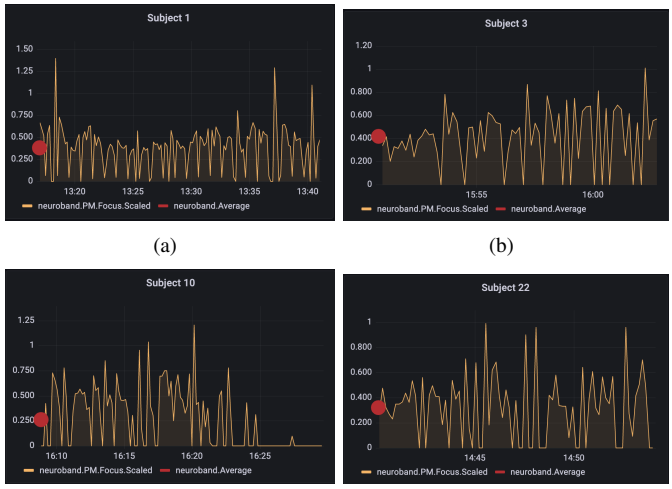
Participants also self-report high levels of relaxation during the experiment regarding the game they were playing. As relaxation can be seen as an opposite measure of stress [22], we compare the relaxation values of the participant to verify the readings of the stress performance metric. For comparison purposes, Figure 9 shows the relaxation measurements from subjects 6 ("Buffer Overflow") and subject 22 ("Access control"). As expected, subject 6 experienced higher relaxation peaks as he/she presented less stress. Regarding subject 22, the relaxation levels constantly varied during the game. In general, subjects presented an average of the stress of 0.512 and relaxation of 0.401 for "Buffer Overflow" game, and an average of the stress of 0.496 and relaxation of 0.422 for "Access control". So, we did not find significant differences between both games. We assume that the level of stress and relaxation depends on the person's personal attitudes instead of the played game.



(a) (b)

Fig. 9: Example of level of relaxation. The red dot is the average of the engagement. (a) Subject 6 playing "Buffer Overflow". (b) Subject 22 playing "Access Control".

The focus performance metric measures the attention and concentration of the subject while playing the game. Subjects self-report in the post-survey a focus level between 7 and 9, which means that they were paying a lot of attention to the game.



(a) (b)

(c) (d)

Fig. 10: Example of level of focus of four subjects. The red dot is the average of the engagement. (a) Subject 1 playing "Buffer Overflow". (b) Subject 3 playing "Buffer Overflow". (c) Subject 10 playing "Access Control". (d) Subject 22 playing "Access Control"

Figure 10 presents the results of focus for four participants, two of them (Figure 10a and Figure 10b) playing "Buffer Overflow", and the other two (Figure 10c and Figure 10d) playing "Access Control". As can be noticed, the average level of focus was not greater than 0.5 in both games. However, using visual observations, we can state that participants were more focused on the game when the game was interactive instead to only read instructions.

Finally, we studied the interest performance metric that measures if a subject is attracted or averse to the task. We

(a) (b)

Fig. 11: Example of level of interest. The red dot is the average of the engagement. (a) Subject 9 playing "Buffer Overflow". (b) Subject 22 playing "Access Control".

could notice that for both games, the average level of interest of the subjects was greater than 0.550. This can mean that the subjects were attracted to the task of playing games to learn cybersecurity. Figure 11a shows the level of interest of a subject playing "Buffer Overflow" game, whereas Figure 11b presents the interest of a subject playing "Access Control".

As presented, we consider that in general and regardless of the game they are playing, subjects are very interested in the task of learning using games; in this case, learning cybersecurity. However, the interactivity of the game plays an important role in engaging the participants. We noted that participants were more engaged with parts of the games that teach "Access Control" than others that teach "Buffer Overflow" mainly due to the interactivity of the game. The "Access Control" game presents an interactive avatar that interacts with multiple animations in order to learn. Instead, the "Buffer Overflow" game is a mix of reading, questions, and small portions of interactive games. Participants were more engaged in the interactive sections. We also noticed that the initial part of the game is fundamental to hit the excitement of the participants. Good introductions to the game generate more excitement than just text and questions. We noted that the level of stress and relaxation is the same across both games regardless of their interactivity. Finally, we noted that maintain a high level of focus in the game is a difficult task, but parts of the game that require the subject to perform an action generate more focus than long texts to read.

Lastly, we faced few challenges while performing the experiment with the subjects; most of them related to get accurate data and proper placement of the device on the head when the subject has a thick hair style. In some cases, we spent more than 45 minutes placing the device.

VI. Conclusion

In this paper, we analyze six performance metrics (engagement, focus, excitement, stress, relaxation, and interest) obtained from EEG signals of 12 users while playing cybersecurity concept related games to measure the effectiveness of the games to attract attention and engage the participants. We analyzed data obtained from participants while they were playing buffer overflow and access control concepts. We conclude that while participants are interested in learning with games, the interactivity of the game plays an important role in the participant's engagement.

VII. Acknowledgment

The authors want to thank to the CS Department at Winston-Salem State University and the CS Department at North Carolina A&T State University for providing the cybersecurity games used in this work.

References

[1] T. Boyle and R. Aygun, "Kennesaw state university hpc facilities and resources," 2021. [Online]. Available: https://digitalcommons.kennesaw.edu/training/10

[2] G. Vasiliadis, M. Polychronakis, and S. Ioannidis, "Gpu-assisted malware," *International Journal of Information Security*, vol. 14, no. 3, pp. 289–297, 2015.

[3] D. Mouheb, S. Abbas, and M. Merabti, "Cybersecurity curriculum design: A survey," in *Transactions on Edutainment XV*. Springer, 2019, pp. 93–107.

[4] Kennesaw State University, "Master Degree in Cybersecurity," https://www.kennesaw.edu/master-degrees/cybersecurity/index.php, 2021, online; accessed 09 February 2021.

[5] 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," *Simulation & Gaming*, vol. 51, no. 5, pp. 586–611, 2020.

[6] J. Juul, *A casual revolution: Reinventing video games and their players*. MIT press, 2010.

[7] I. Fouad and F. Mohammed, "Using emotiv epoc neuroheadset to acquire data in brain-computer interface," *International Journal of Advanced Research*, vol. 3, pp. 1012–1017, 11 2015.

[8] Emotiv. (2021) Emotiv. [Online]. Available: https://www.emotiv.com/about-emotiv/.

[9] 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," *Simulation & Gaming*, vol. 51, no. 5, pp. 586–611, 2020.

[10] M. Gáliková, V. Švábenskỳ, and J. Vykopal, "Toward guidelines for designing cybersecurity serious games," in *Proceedings of the 52nd ACM Technical Symposium on Computer Science Education*, 2021, pp. 1275–1275.

[11] S. Karagiannis and E. Magkos, "Engaging students in basic cybersecurity concepts using digital game-based learning: Computer games as virtual learning environments," in *Advances in Core Computer Science-Based Technologies*. Springer, 2021, pp. 55–81.

[12] J. Zhang, X. Yuan, J. Johnson, J. Xu, and M. Vanamala, "Developing and assessing a web-based interactive visualization tool to teach buffer overflow concepts," in *2020 IEEE Frontiers in Education Conference (FIE)*. IEEE, 2020, pp. 1–7.

[13] S. Siuly, Y. Li, and Y. Zhang, "Eeg signal analysis and classification," *IEEE Trans Neural Syst Rehabilit Eng*, vol. 11, pp. 141–4, 2016.

[14] D. Taussig, A. Montavont, and J. Isnard, "Invasive eeg explorations," *Neurophysiologie Clinique/Clinical Neurophysiology*, vol. 45, no. 1, pp. 113–119, 2015.

[15] P. S. Reif, A. Strzelczyk, and F. Rosenow, "The history of invasive eeg evaluation in epilepsy patients," *Seizure*, vol. 41, pp. 191–195, 2016.

[16] H. Anupama, N. Cauvery, and G. Lingaraju, "Brain computer interface and its types-a study," *International Journal of Advances in Engineering & Technology*, vol. 3, no. 2, p. 739, 2012.

[17] B. Di, J. Sun, H. Chen, and D. Li, "Efficient buffer overflow detection on gpu," *IEEE Transactions on Parallel and Distributed Systems*, vol. 32, no. 5, pp. 1161–1177, 2020.

[18] WSSU, "2d-access-control," Wssu.edu, 2021. [Online]. Available: https://gamelab.wssu.edu/modules/AccessControlWebGL/ AccessControl.html

[19] WSSU , "2d-buffer-overflow," Wssu.edu, 2021. [Online]. Available: https://gamelab.wssu.edu/modules/BufferOverflowWebGL/ bufferoverflow.html

[20] Influxdata Inc, "InfluxDB," 2019. [Online]. Available: https://www.influxdata.com/

[21] Grafana Labs, "Grafana," 2018. [Online]. Available: https://grafana.com/

[22] J. A. Dusek and H. Benson, "Mind-body medicine: a model of the comparative clinical impact of the acute stress and relaxation responses," *Minnesota medicine*, vol. 92, no. 5, p. 47, 2009.