Benjamin Acuff and Ankur Chattopadhyay
acuffb1@mymail.nku.edu | chattopada1@nku.edu
Northern Kentucky University - School of Computing and Analytics

CRACK-ERS

(Crack Riddles Applying Cybersecurity Knowledge - Escape Room Scenario)

Abstract

We created an unplugged game that is designed to introduce beginners to different cybersecurity topics through gamification. By providing a unique beginner-friendly and riddle-based approach to foster interest in cybersecurity, CRACK-ERS focuses on team play, simplicity, and inclusivity, unlike existing games like CyberStart. The novelty of CRACK-ERS lies in its non-traditional design as an unplugged CTF (Capture The Flag) with an adventure scenario-driven script, encouraging participants to solve cybersecurity-related riddles. In this work, we present the game's development, its evolution, and its impact on participants' cybersecurity interests, as evidenced by the analysis of quantitative and qualitative data collected through survey responses from high school community members who played the game. Results indicate our unique approach successfully engaged both students and teachers, fostering a positive learning experience, user awareness, and overall interest in cybersecurity topics. In response to the challenges posed by the global pandemic in 2020, CRACK-ERS emerged as a virtual adaptation to engage students in cybersecurity remotely. This study explores how gamification, teamwork, and problem-based activities influence the experiences and motivation of participants. To our knowledge, CRACK-ERS is the first hybrid model CTF that combines the escape room style, riddle-based, and story-driven elements for beginners. Since 2020, we have employed CRACK-ERS in high school outreach workshops, remote cybersecurity sessions, summer camps, and distance learning events aiming to introduce CTFs and basic cybersecurity concepts in a user-friendly, competitive way. There is limited prior work on escape room styled, riddle-based, unplugged CTF that is focused on effectively engaging beginners-level high school participants in a virtual learning mode. We aim to address this research gap.

Motivation and Background

CRACK-ERS was designed to fulfill a gap, as well as a need for unplugged, beginner's level, learner-friendly escape room game styled, riddle-based CTF s to engage high school community members virtually and to build cybersecurity awareness plus interests in a fully-remote setting, where outreach workshops, learning sessions and camps were being run online via Zoom. This project began with the following specific design constraints and particular requirements:

- An entirely virtual learning environment with fully remote participants
- No dependency on specialty software tools, like Wireshark, that need prior setup
- Supportable using Zoom and similar online conferencing software

While designing the escape room, it was important to keep in mind that it was a game, albeit an educational one. Games are meant to interest, engage, and tell its own story. The project members recognized the need that all games have, which is for a cohesive design and a story-based adventure theming. The requirement of creating this in a virtual environment, like Zoom, made the project quite challenging, as in a virtual environment one cannot rely on physical props. The participants also using different hardware was a factor that further limited the options of virtualizing the escape room themed game. In more traditional CTF with cybersecurity challenges, it is assumed that the participant may have access to a VM (virtual machine), web-based tools, or apps to support their learning. In this circumstance we could only reasonably expect that the participant would have access to the internet.

Project Goals

Our research project has seven main goals for participants:

- *To stimulate interest in cybersecurity among participants*
- *To create an unplugged and non-traditional cyber CTF/game*
- *To expose participants with no technical background or prior cybersecurity knowledge to cybersecurity topics and concepts*
- *To help participants, with little or no experience with CTF s, build confidence in cracking/solving cybersecurity challenges, so that they are better prepared for taking on the more challenging, traditional cybersecurity CTF challenges*
- *To create a game-based cybersecurity learning environment, that engages students from both STEM and non-STEM backgrounds*
- *To develop a beginner friendly, unique unplugged CTF, which enables building of problem solving, riddle cracking and teamwork skills in participants, and mentorship relation between moderators and a mentor-mentee relation between moderators and team members*

Game-Based CTF Learning Activity Overview

In order to share cybersecurity concepts with participants with no technical background, it was necessary to weave the foundational knowledge necessary to solve the challenges themselves. They are unable to use case-based reasoning in the traditional sense, being unfamiliar with some of the terms, but they can be encouraged to take what they do know, examine which parts they do not know and compare the two to compel their research as they work to find a solution. In our CRACK-ERS activity, we encourage participants to use whatever tools they had available to them. They are allowed and encouraged to use pencil/pen and paper, to make use of internet searches, and to engage in teamwork for solving the assigned challenges. The novelty of our game-based CTF lies in its unplugged and adventure-story telling based escape room style script design. We make effective utilization of the Zoom breakout room feature for a nifty game implementation. It was also part of our strategy to create challenges on different cybersecurity topics that would present players with various problem scenarios that are realistic and thought provoking. One of the goals while designing this game was to find various ways to challenge participants so that they must apply problem solving plus riddle cracking skills. Concepts and words that may be outside the scope of non-native English speakers were used as contextual clues. In other words, if a participant had to internet search something, then we wanted it to be an experience that led them to go out of the comfort zone and think out of the box. The original version of CRACK-ERS, which is also known as the Escape the Breakout Room (ETBR) game, is an unplugged CTF, which is intended to engage a wide range of participants from different backgrounds, including both students and teachers at the K-12 level, and is user-friendly without the need of a tech setup process (other than having to join a Zoom call for online participation), for playing the game. The incorporation of hints is meant to help players look in the correct direction (on a need basis), while competing with peers, and gaining valuable CTF experience by solving challenges on their own.

Challenge 2 - Exploit
root@serverterminal:~#
I always knew I was the best
Now I put your cyber team to the test
Nothing this bad since EternalBlue
I have put my hackz on you.
Solve this puzzle if you have wisdom
You should have known to patch this system.
Hint 1: What is the key word in the riddle?
Hint 2: What exactly did EternalBlue exploit?
Solution(s): Windows SMB, SMB, Server Message Block

Figure 1: This shows an exploit-based riddle challenge from CRACK-ERS, a list of its scripted hints, and its solution.

Challenge 5 - Cipher
root@serverterminal:~#
Now I ask "Et tu Brute?"
Solve this crypto message
2 save the day.
Hint 1: Part of the riddle is a quote. How could that be helpful?
Hint 2: A cipher is encoding your phrase. What can you shift to make this work?
Hint 3: Who did Brutus betray, and what does that have to do with a cipher?
Solution: cool your jets betrayed me

Figure 2: This shows a cipher-based riddle challenge from CRACK-ERS, a list of its scripted hints, and its solution.

Results

We surveyed 87 high school participants who were able to experiences CRACK-ERS through Northern Kentucky University cybersecurity summer camps and cybersecurity outreach events. Survey questions number five and six, asking the student about their overall interest in cybersecurity before and after engaging in CRACK-ERS, were of particular interest to us as this was the initial motivation for developing the game. Namely, increasing the number of potential students who might pursue cybersecurity as a major and career interest. The results found a general increase through various levels of interest. It was also found that of all survey participants to date, 21% reported having little to no previous experience with cybersecurity and that they were somewhat or extremely likely to pursue resources or opportunities leading to a career in cybersecurity after engaging in CRACK-ERS. It was found that 57% of those who initially answered that they had no interest at all before the game had an increased interest afterward; 14% increasing to a slight interest and 43% jumping to a moderate interest.

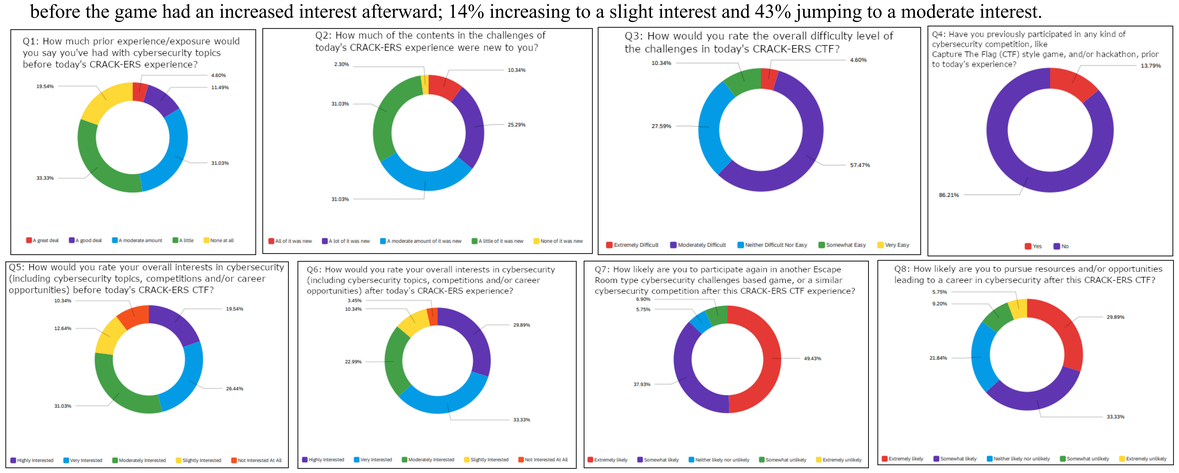

Figure 3

Future Work and Summary

Based on user/player feedback and our long-term vision for our unplugged, escape room style CTF game-based learning activity, we plan to expand our work in the following ways:

- **Enhance Into A Web-based Version and Add New Features:** We aim to expand our unplugged CTF game-based learning activity by transforming it into a wen-based CTF game tool, and by implementing a leaderboard plus points system, timer functionality, dynamic challenge progression, collecting and implementing more cybersecurity challenges, and a web hosting service for the game.
- **Implement A Web-based Version:** Although our game is currently implemented via Zoom in an unplugged CTF format, it requires one human moderator for each Zoom breakout room for narrating the game script and presentation of challenges. A major improvement goal is to transform this game into a web version, where it can be played individually or in teams on computers or mobile devices without needing human moderators.
- **Refine CTF Contents:** We would like to enhance the current beginner-friendly CTF challenges by refining the game contents to increase the user experience of true immersion and engagement. We intend to improve the escape room aspect by adding additional story videos and game characters.
- **Expand Audience:** We intend to like to reach out to a broader audience with our CRACK-ERS game-based learning activity by offering the game at cybersecurity outreach events, such as summer camps, workshops, and technology conferences. We would like to see it being used in more K-12 schools for students and for K-12 teacher professional development.

Our CRACK-ERS activity was created to increase cybersecurity awareness and interest among high school students. Survey data shows that our combination of an unplugged escape room style CTF game with a beginner-friendly approach created an impactful and memorable learning experience. We plan to expand our game-based learning activity's scope to further cybersecurity awareness and address the shortage of unplugged, beginner's level, learner-friendly escape room themed, riddle-based CTF s.

References

1. Bettina Schneider, Trupti Zanwar. CySecEscape – Escape Room Technique to Raise Cybersecurity Awareness in SMEs. International Conference - The Future of Education
2. Dr Etienne Wenger-Trayner, Beverly Wenger-Trayner. Learning in a Landscape of Practice. Routledge, 2014.Ge Jin, Manghui Tu, Tae-Hoon Kim, Justin Heffron, and Jonathan White. 2018. Game based cybersecurity training for high school students. In Proceedings of the 49th ACM Technical Symposium on Computer Science Education. ACM, Baltimore, MD, 68-73. https://doi.org/10.1145/3159450.3159591
3. E. Beguin et al., "Computer-Security-Oriented Escape Room," in IEEE Security & Privacy, vol. 17, no. 4, pp. 78-83, July-Aug. 2019, doi: 10.1109/MSEC.2019.2912700.
4. Emanuel Löffler, Bettina Schneider, Petra Maria Asprion, Trupti Zanwar. "CySecEscape 2.0 - A Virtual Escape Room To Raise Cybersecurity Awareness". International Journal of Serious Games, 2021-03-09.
5. Ge Jin, Manghui Tu, Tao-Hoon Kim, Justin Heffron, Jonathan White. "Game based Cybersecurity Training for High School Students". SIGCSE '18: Proceedings of the 49th ACM Technical Symposium on Computer Science Education, 2018-02.
6. Kevin Daimi, Guillermo Francia III. Innovations in Cybersecurity Education. Springer, 2020.
7. Lave, J., & Wenger, E. Situated Learning: Legitimate Peripheral Participation. Cambridge University Press, 1991.
8. Mandar Shivapurkar, Sajal Bhatia, Irfan Ahmed. "Problem-based Learning for Cybersecurity Education". CISSE, 2020-07-30.
9. Lene Hayden Taraldsen, Frode Olav Haara, Mari Skjerdal Lysne, Pernille Reitan Jensen & Eirik S. Jenssen (2022). A review on use of escape rooms in education - touching the void, Education Inquiry, 13:2, 169-184, DOI: 10.1080/20004508.2020.1860284