RC^{3}TF, an Augmented Reality CTF: A case study in improving cybersecurity pedagogy for the undergraduate research laboratory

Dr. Brian Robert Callahan*

Information Technology & Web Science Program
Rensselaer Polytechnic Institute
Troy, NY, United States
callab5@rpi.edu
0000-0002-1797-8633

Sanya Joseph*

Information Technology & Web Science Program
Rensselaer Polytechnic Institute
Troy, NY, United States
joseps2@rpi.edu
0009-0000-0343-809X

Shoshana Sugerman*

Information Technology & Web Science Program
Rensselaer Polytechnic Institute
Troy, NY, United States
sugers@rpi.edu
0009-0002-9058-6828

Quinn Colognato*

Information Technology & Web Science Program
Rensselaer Polytechnic Institute
Troy, NY, United States
cologq@rpi.edu
0009-0005-1274-4685

Aanya Mehta

Information Technology & Web Science Program
Rensselaer Polytechnic Institute
Troy, NY, United States
mehtaa8@rpi.edu
0009-0002-5651-3385

Tanvi Mehta

Information Technology & Web Science Program
Rensselaer Polytechnic Institute
Troy, NY, United States
mehtat2@rpi.edu
0009-0005-2243-0196

Emily Goldman

Information Technology & Web Science Program
Rensselaer Polytechnic Institute
Troy, NY, United States
goldme5@rpi.edu
0009-0007-3064-106X

Mary Cotrupi

Information Technology & Web Science Program
Rensselaer Polytechnic Institute
Troy, NY, United States
cotrum@rpi.edu
0009-0005-3985-012X

Ishneet Kaur

Information Technology & Web Science Program
Rensselaer Polytechnic Institute
Troy, NY, United States
kauri@rpi.edu
0009-0007-6157-3549

Victoria Cai

Information Technology & Web Science Program
Rensselaer Polytechnic Institute
Troy, NY, United States
caiv@rpi.edu
0009-0009-7290-9081

Gabriel Bezerra

Information Technology & Web Science Program
Rensselaer Polytechnic Institute
Troy, NY, United States
bezerg@rpi.edu
0009-0002-1690-0073

Adam Kaplan

Information Technology & Web Science Program
Rensselaer Polytechnic Institute
Troy, NY, United States
kaplaa2@rpi.edu
0009-0008-9318-2670

Arielle Revis

Information Technology & Web Science Program
Rensselaer Polytechnic Institute
Troy, NY, United States
revisa@rpi.edu
0009-0003-1511-8351

Lala Liu

Information Technology & Web Science Program
Rensselaer Polytechnic Institute
Troy, NY, United States
liul14@rpi.edu
0009-0009-0074-4011

Samuel Leung

Information Technology & Web Science Program
Rensselaer Polytechnic Institute
Troy, NY, United States
leungs2@rpi.edu
0009-0009-2677-9490

* Co-first authors

Elif Kulahlioglu

Information Technology & Web Science Program
Rensselaer Polytechnic Institute
Troy, NY, United States
kulahe3@rpi.edu
0009-0008-3026-3123

Rachel Schneider

Information Technology & Web Science Program
Rensselaer Polytechnic Institute
Troy, NY, United States
schner5@rpi.edu
0009-0004-4844-9779

Mikah Schueller

Information Technology & Web Science Program
Rensselaer Polytechnic Institute
Troy, NY, United States
schuem@rpi.edu
0009-0008-0752-4145

Quinn Sharp

Information Technology & Web Science Program
Rensselaer Polytechnic Institute
Troy, NY, United States
sharpq@rpi.edu
0009-0006-6032-8755

James Porvaznik

Information Technology & Web Science Program
Rensselaer Polytechnic Institute
Troy, NY, United States
porvaj@rpi.edu
0009-0007-3820-8711

***Abstract*- Augmented Reality, an interactive experience that blends the digital world with the physical world, offers unique experiences for training the next generation of cybersecurity professionals. Capture-the-Flag (CTF) tournaments impart a broad array of offensive (red team) and defensive (blue team) cybersecurity skills to its participants. In this paper, we present our augmented reality CTF, called the Rensselaer Cybersecurity Collaboratory Capture-the-Flag (RC³TF). The RC³TF transforms Rensselaer Polytechnic Institute's campus into a computer network where each building on campus takes on the role of a specific device and the walking paths and other connections between the buildings represent the topology of the network itself. As players traverse campus physically, the RC³TF mobile application, akin to Pokémon Go, presents the relevant geolocation-positioned challenges. This paper focuses specifically on the experiences of the nineteen undergraduate students who worked to design and implement the RC³TF. We explore the pedagogic experience afforded by having students of all cybersecurity skill levels work together to build a larger educational project. Students speak in their own words how the project contributed to their cybersecurity knowledge and community building on campus. We present this case study as a novel insight into how faculty at other universities can quickly and effectively teach cybersecurity concepts through unique research opportunities such as developing cybersecurity pedagogy for their university community and beyond.**

Keywords: *Augmented reality, Capture-the-Flag, Red team, Blue team, Cybersecurity, Pedagogy, Gamification*

1 INTRODUCTION

Capture-the-Flag (CTF) tournaments offer a unique, hands-on approach to learning a vast corpus of cybersecurity skills. Participants often learn skills ranging from offensive hacking, what we might consider red teaming, to open source intelligence, network traffic analysis, log reading, and other defensive techniques considered to be part of the blue team. Indeed, CTF tournaments have proven so popular that large CTF websites such as ctftime.org always show CTFs to participate in every day of the year, and over 8500 students from across the United States participate in the National Cyber League competition, a United States-based collegiate-level CTF tournament held once per academic semester in the Fall and the Spring [1]. Tens of thousands of students each year learn cybersecurity skills through these CTF tournaments.

The success of the format has been well-studied in the literature. CTF tournaments are known to provide highly motivating settings [2], perceived social and technical benefits for participation [3], with an analysis of approximately 3600 CTFs yielding a core educational skillset of coding, cryptography, reverse engineering, binary exploitation, forensic analysis, and web exploits being the major focus across this sample [4].

However, these tournaments tend to follow a relatively cookie-cutter format: students are locked away in front of their computers for a set period of time, solving challenges in front of a screen in a hyper-competitive format that may not be particularly forgiving or understandable for the newcomer. Indeed, concerns over some of these problems inherent in the traditional CTF model have been documented in the literature as negative factors preventing initial or continued participation in such events [3].

While the traditional model of CTF events is effective at teaching the requisite skills, we wonder if there could not be other avenues to explore for how a CTF tournament is implemented and played. Exploring the potential for alternative models can provide new insights into improving the traditional model as well as overcoming the need for students to rapidly grow skills in a variety of subdisciplines in the field in order to be competitive in today's graduate education and job market.

In this paper, we introduce the Rensselaer Cybersecurity Collaboratory Capture-the-Flag (RC³TF), an Augmented Reality CTF tournament designed at Rensselaer Polytechnic Institute (RPI). This project enrolled nineteen undergraduate students across several disciplines, including Information Technology & Web Science (ITWS), Computer Science, Electrical and Computer Engineering, Business, and humanities such as Science & Technology Studies.

As the RC³TF was conceived as a multi-semester, multi-year project, and the work is ongoing, we specifically reflect on the first stage which was undertaken in this academic year: the design and iteration of the overall narrative for the RC³TF and the development and refinement of challenges within.

This paper and its methodology are designed to be self-reflexive; to that end, we are presenting how students developed as cybersecurity professionals in the process of developing the RC³TF. It is the students themselves who will be offering their first-hand accounts as to their growth and improvement in the foundational skills of the discipline as evidenced by their designing, coding, and running the RC³TF.

It is our hope that by introducing the RC³TF and letting the student researchers share their insights in their own words, we demonstrate the value of unique pedagogic experiences and inspire others to take on the challenges of adopting these practices into their own cybersecurity research laboratory as a project to enhance undergraduate educational outcomes in the cybersecurity discipline.

2 BACKGROUND

The Rensselaer Cybersecurity Collaboratory (RCC) has a history of using cybersecurity pedagogy both as a methodology for improving the cybersecurity posture at RPI and for rapidly educating students from a wide variety of disciplines and skill levels cybersecurity concepts. Some examples of this work include producing cybersecurity awareness training for campus through an analysis of the benefits and limitations of using Generative AI for such purposes [5], developing an optimized implementation of Shor's algorithm for RPI's quantum computer [6], developing a part-of-speech analyzer using quantum machine learning to learn about the potential for quantum algorithmic bias [6], and developing quantum preprocessing for enabling Internet of Things (IoT) devices to act as intrusion detection systems (IDS) and other security devices [7].

It is well-understood that the cybersecurity industry struggles to attract and retain talent; studies done in the industry show a workforce gap of millions of qualified professionals [8] with significant belief that firms are understaffed [9]. Research has been undertaken to identify the pedagogy interventions needed to most quickly close the skills gap [10], identifying employment trends, challenges, and opportunities for those who will learn cybersecurity skills en route to closing the skills gap [11], and how closing the skills gap, and by extension we argue the workforce gap, is critical to maintaining global competitiveness [12].

We take these calls very seriously and combine these insights with pedagogic experiences not often afforded to students in order to create unique cybersecurity research opportunities primarily at the undergraduate level.

3 DEVELOPING CHALLENGES

Once the team was assembled, we agreed to hold in-person weekly meetings with as many students as possible. This decision turned out to be extremely beneficial, as we will see in the Discussion section, as it provided all the students with exposure to the very wide gamut of cybersecurity knowledges necessary to create a complete CTF.

We began our project by developing challenges for RC³TF. This aspect of the project required us to think quite deeply about how to effectively incorporate augmented reality into a broader event. Our initial concept was to produce our CTF using both Virtual Reality (VR) and AR technologies. We were hopeful that we would be able to purchase VR devices to help develop the RC³TF. Unfortunately, we were unable to

purchase any devices as that was not a permitted expense from our grant.

After some deliberation once learning that we were unable to purchase VR devices, we quickly switched gears to a new kind of tournament style. We devised a Pokémon Go-style game in which our campus would be transformed into a computer network. In this arrangement, the buildings on campus would be assigned a "role," such as a switch, router, or workstation, and the pathways connecting the buildings would more-or-less be considered Ethernet cabling, or other connections between the "devices." Using a web application we would design and some geolocation, players could physically navigate RPI's campus and be presented with challenges germane to their location.

We drafted up ideas to augment existing common CTF challenges using AR technology. To best get an understand of the kinds of challenges we would be adapting to the AR world, we participated in a number of CTF tournaments, most notably the National Cyber League, but also others such as the University of North Dakota Cyber Hawks CTF, UConn CyberSEED, and more.

Figures 1-3 showcase our iterations of our campus network diagram, with Figure 4 being the final diagram of the RPI campus transformed into a computer network. We can see the initial idea grow to cover the entire campus network, with later iterations adding concepts of difficulty to the locations.

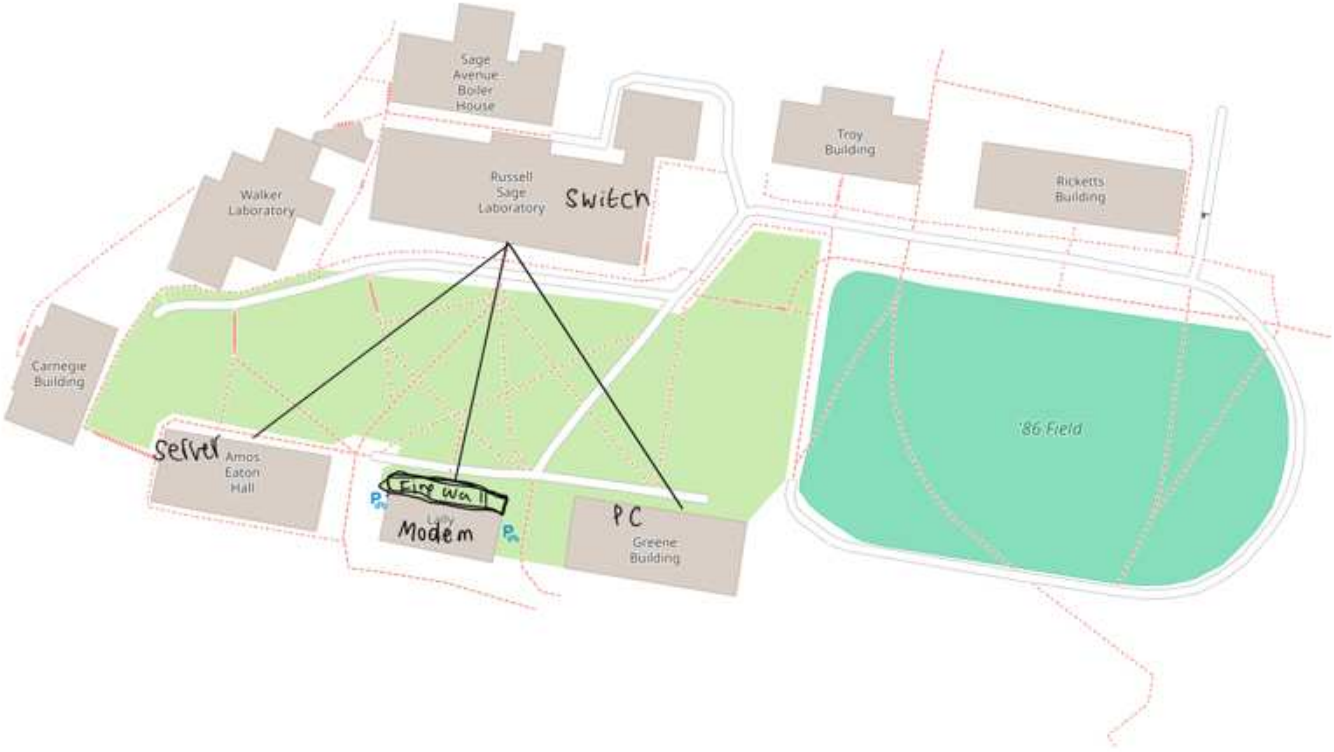

Figure 1. First iteration of transforming the RPI campus into a computer network.

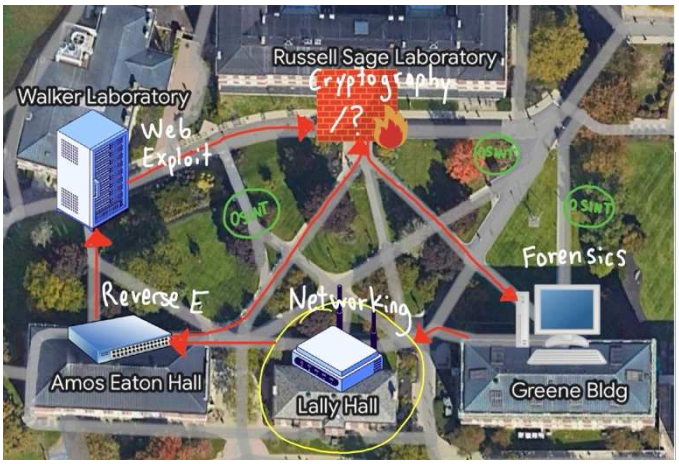

Figure 2. Adding more locations to the campus map, with challenges in the pathways between buildings.

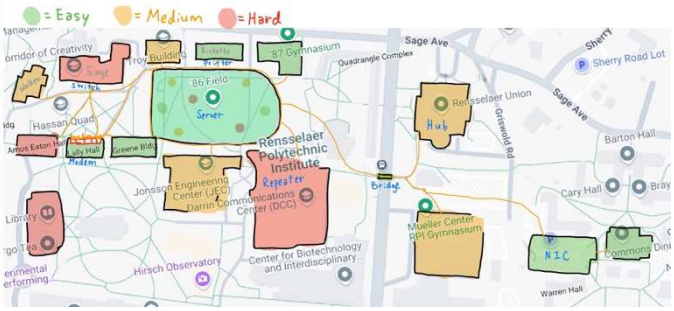

Figure 3. Adding the concept of difficulty to the locations.

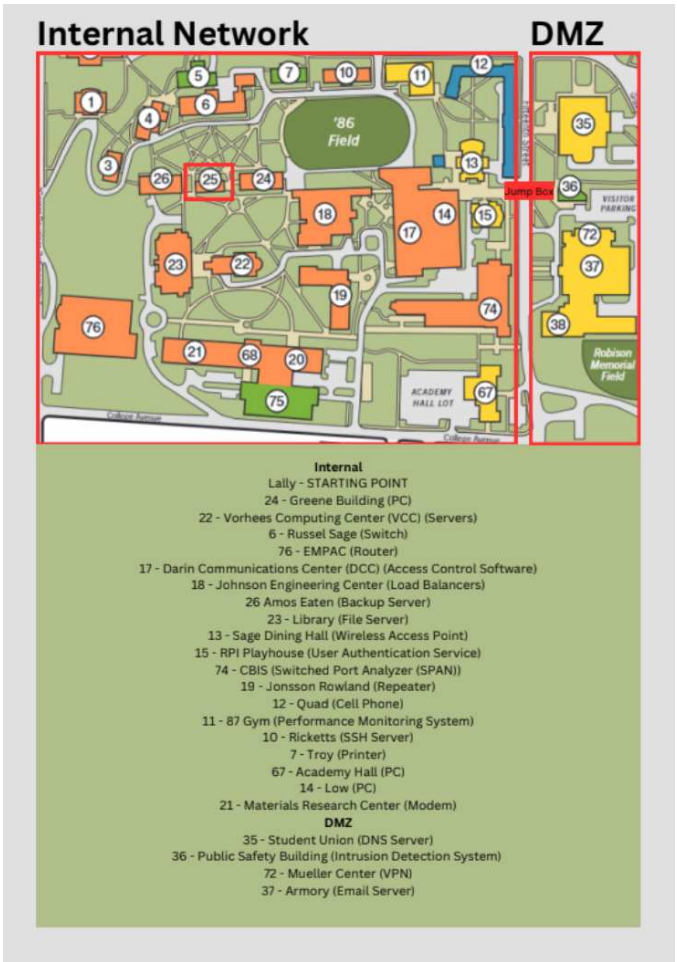

Figure 4. Final diagram of RPI campus presented as a computer network.

After transforming our campus into a computer network, we needed to craft a larger narrative that would give the players motivation to participate in the CTF. Drawing inspiration from RPI's past, specifically an intrusion in May 2021, we developed a narrative that presented a university under immediate attack; players would need to tap into both their knowledge of cybersecurity and of campus in order to get the campus network fully restored.

Next, we needed to develop challenges that would make sense for each location. We planned out 35 challenges for the RC[3]TF, at least one for each area that we identified, with many having multiple challenges. A typical challenge design document is demonstrated in Figure 5.

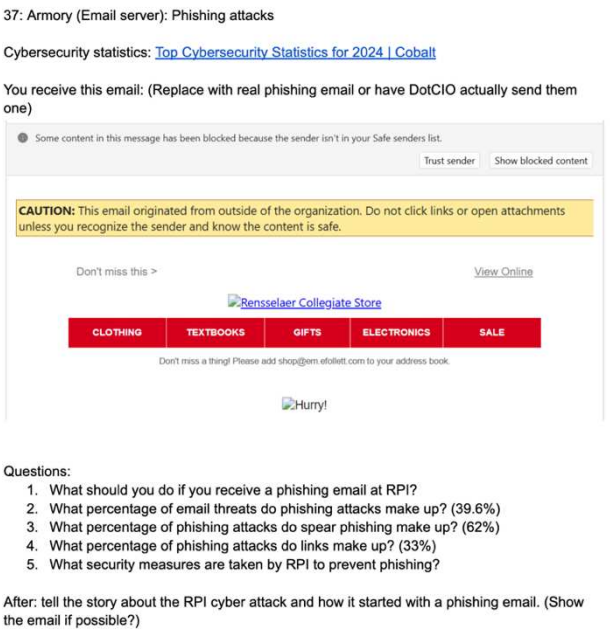

Figure 5. Challenges design document for phishing attacks.

Finally, students worked together to flesh out the ideas for these different challenges. This aspect of the

RC[3]TF is predominantly where the research aspect took place; students were expected to on their own research the challenges they were to design and implement.

Challenges were ultimately divided into a number of broader categories depending on how we envisioned the players coming into contact with them. For challenges that are directly tied to a particular device type, those challenges would offer a hands-on activity that culminated in obtaining a flag that earned points. For example, entering the library would give the players access to the File Server challenges. Importantly, entering the library also meant that challenges germane to other devices would no longer be accessible to the players; we believe this helps add to the immersiveness of the overall experience, where players need to physically move around campus in order to progress with the overall story.

The second type of challenge would be "random encounters" not unlike our inspiration Pokémon, where walking around campus from building to building would sometimes generate story-based narratives about real-world cybersecurity breaches, with simple question and answers for players to obtain points.

After this, we did get to work at the initial coding of challenges. While this is mostly incomplete, we will report on this aspect of the RC[3]TF and its pedagogic benefits in future work.

4 DISCUSSION

Our student co-authors come from a variety of different expertises: cybersecurity, computer science, design, data science, management, humanities, and more. Students were split up into core teams depending on their role in the overall production of RC[3]TF: a visual design team, a challenge design team, and a coding team. Each team had a student leader who oversaw the everyday production of the outputs of each team.

In our discussion, we will turn our attention to our student researchers, who were given the opportunity to reflect on their experiences over the course of the year. We will discuss four relevant themes from across the student researchers: deepening of cybersecurity knowledge, improved articulation of cybersecurity knowledge, honing of supplemental skills outside of cybersecurity that can be fed back into improving cybersecurity knowledges and professionalization, and fun.

It is our belief that these themes represent the kinds of experiential learning, a type of learning that prioritizes experience towards learning and development [13], that we believe go beyond simply participating in CTF tournaments.

4.1 On deepening cybersecurity knowledge

One common topic among our student researcher reflections was how working on the RC[3]TF contributed to a further deepening of their knowledge of topics. Even when students were already very knowledgeable in a topic, through coursework and/or CTF player participation, developing their own CTF helped to create further expertise.

One of our student participants described learning about buffer overflow and network-based attacks in a way beyond participating in coursework, and were able to gain a deeper insight into how these attacks are carried out in the real world—in no small part because designing CTF challenges requires deep research into not only the nuts-and-bolts of the attacks themselves, but how adversaries actually carry them out.

Another student discussed having only a surface-level understanding of cybersecurity concepts and terminology. Through participating in the development of challenges, the student was able to gain further insight into phishing and encryption.

Yet another student described being part of the team as an avenue for her to gain exposure to previously unfamiliar topics, such as spanning-tree attacks and jump boxes. These are topics that the student may have never had the ability to engage with if not for her participation in the RC[3]TF project. With 35 challenges designed over the course of the year, combined with our weekly in-person meetings, students were able to regularly meet and discuss their work—meaning they were regularly sharing their new knowledge with each other—so that all students were able to engage in a genuine and routine peer learning exercise. Peer learning is well-understood to provide education and psychological benefits to students [14] and we believe this project created an environment for peer learning that goes beyond the simple CTF, which, depending on how the tournament is implemented, may stifle or even forbid peer learning.

Another experienced student described their improved knowledge as follows: "I worked on the Command and Control (C2C) challenge where I needed to create a network traffic capture between an infected host and its server, suspicious binary being used for the communication, and a log file from an infected machine that shows the compromised host. While I had previous knowledge about cybersecurity, I never implemented an attack or knew in-depth how to simulate an attack environment. I broke down the daunting task into sections, slowly developing the challenge to ensure a realistic yet compromised environment. Developing the challenge and seeing how the parts came together taught me more than simply reading about a challenge ever could. I now have real development experience and knowledge I can apply into my future in cybersecurity because of the RC[3]TF."

Perhaps the most revealing sentiment in deepening cybersecurity knowledge was the recognition that cyber threats often have a significant human component to them, not being entirely or solely technical. One of our student researchers described it as such, "[t]hrough this project, I gained a deeper understanding of how cyber threats often exploit human behavior rather than just technical flaws. Many successful attacks depend on user error, urgency, or deception rather than software vulnerabilities alone. My goal for this assignment then shifted to create a balance between the gamification of these common security issues and education. By communicating these principles through game play, users can develop habits of caution and quick recognition in a way that is interactive and accessible." This is a very salient message that may get lost in the simple playing of CTFs or even coursework that students may undertake. It is one thing for us as educators to teach the social factors inherent to cybersecurity; it is quite another for a student to make that realization on their own through the development of their own cybersecurity challenges.

4.2 On articulating cybersecurity knowledge

Students who had no expertise in specific subdisciplines of cybersecurity quickly found themselves very knowledgeable in those areas through their work on the RC[3]TF.

One student researcher who was already fairly advanced described their participation as follows: "One of the challenges I worked on was the Log Analysis challenge, where you have to find an attack through PCAP files. We decided to set this challenge in Academy Hall and the purpose of this challenge is to help the players find unusual activity that is affecting a web server's cache. The players have to look at packet captures and find suspicious behavior, for example HTTP headers or DNS responses that are not matching. The challenge leads them through questions that ask them to analyze IP addresses and find the attacker's IP address. This challenge gave me a chance to learn and create a realistic scenario that helps others also build their cybersecurity skills."

Another student researcher entirely new to the field offered a similar explanation fitting to their emerging knowledge: "As a student whose background did not include much about cybersecurity, this opportunity was a great chance to learn some new concepts. Not only was I able to learn the concepts myself, but I also had the opportunity of diving deep enough into the concepts to design a cohesive and relevant minigame that showcases the content in an accurate way while making a game that is both fun for users to play and helps them understand the concepts in a simple way, even for users who are unfamiliar with said concepts. For example, I was the programmer that created the encryption minigame. As background for this game, I did a lot of research into the different types of encryption and decryption techniques, and the types of technologies used to do said decryption. Once I understood all I could about the topic, I picked a Caesar cypher to showcase an analog form of encryption and decryption, allowing users to understand in a simple form how a basic encryption form works and how automated tools can be used to decrypt the code if it is set to the correct settings. This not only lets users understand these complex concepts in a simple way but also provides a fun visual suitable for all skill levels. Through the development of several of these minigames, I have learned a lot about different aspects of cybersecurity, from encryption to DDoS attacks, all while having fun making the games and making fun for others."

Yet another student researcher demonstrated an improved ability to articulate the human aspect of cybersecurity: "For example, in the phishing related game, players must quickly distinguish between a

legitimate email and a phishing attempt, reinforcing the importance of scrutinizing suspicious messages. In a keylogger inspired game, players must carefully type a password while avoiding detection from an external keylogger, teaching them the importance of awareness when entering sensitive information. Various games incorporate elements like urgency, decision-making under pressure, and pattern recognition. Skills, such as encryption and decryption, are also tested. One must consider physical security risks as well, like the dangers of plugging in an unknown USB device, reinforcing the need for caution beyond just software protections. Striking a balance between simplicity and effectiveness was a challenge, as I had to ensure that each game not only reinforced key cybersecurity principles but also remained accessible to players with varying levels of knowledge."

An experienced student researcher demonstrated their improved articulation as simplification of complex topics into broadly understandable explanations: "I first worked on teaching challenges related to performance monitoring systems and phishing. I learned extensively about these two topics, condensed the information, and presented it in a way for the user to learn and test their knowledge. This research and writing taught me extensively about the topics themselves and about how to simplify information so any user can comprehend the topic in its entirety."

To wrap up this section, we look at one final insight from the design team: "For a steganography challenge I developed, which involved hiding a solution flag in a password-protected file within the challenge image, I learned more about using the command-line tool Steghide. I also explored how to protect flag and password contents from being revealed in the source code, a fundamental aspect of cyber and code security."

There are hardly any roles within the cybersecurity field that do not in some capacity require the successful communication of what it is the practitioner has done. We found that all our student researchers were able to meaningfully discuss their contributions to the RC[3]TF, regardless of their initial skill level prior to beginning the project.

4.3 On honing supplemental skills

Because we had a wide variety of students who came to the project with many difference expertises, both within cybersecurity and outside it, we tried our best to match certain aspects of the design and implementation of the RC[3]TF with those outside skills.

For example, our lead student researcher for the design team was already well-versed in design thinking, art, and branding. Her primary task focused on the overall visual design language of the RC[3]TF. She explained her honing of her design skills as follows:

"As the design lead on this project, I also developed better design skills by learning how to create cybersecurity challenges that were engaging, educational, and eye-catching. Traditional CTFs have challenges that are fully virtual, so from a design perspective, I knew I had to keep the AR aspect/our campus buildings in mind as well. To support these challenges and make them more accessible, I also used Canva to help design our website, while other team members spent time coding the website: this served as a starting point for the AR CTF. To ensure that participants could easily locate resources, instructions, and challenge specifics, the website needed to be aesthetically pleasing, user-friendly, and educational. As a result, the website was an important aspect of the project, and I was glad to be a part of it, as was participating in this research project."

4.4 On fun

The student researchers routinely reflected on how much fun they had developing the RC[3]TF. Indeed, fun is routinely cited as a core aspect of playing in CTFs both in celebration and critique [15, 16]. We are happy to report that the activity of developing a CTF was also seen as fun by our student researchers. To share just one quote about fun:

"Developing for the RC[3]TF has been an incredibly fun and rewarding way to strengthen my cybersecurity skills, and I'm even more excited to share the final product with other students who may be building their own interest in the field."

5 CONCLUSION

In this paper, we introduced the RC[3]TF, an Augmented Reality-enhanced cybersecurity Capture-the-Flag

experienced being designed by students for students at RPI. We reported on the in-progress state of the RC^{3}TF focused on the early stages of design and early implementation of the RC^{3}TF. Predominantly, we allowed the student researchers, all undergraduates from a variety of disciplines, share their direct experiences working on the project.

The purpose of this report is to highlight that while playing CTFs are known to have benefits for students' educational outcomes, there are additional benefits that can only be realized by having students take on the role of CTF creators. Specifically, we call out deepening cybersecurity knowledge, articulating cybersecurity knowledge, honing supplemental skills, and fun as the four primary benefits our student researchers experienced that go above and beyond classroom experiences and even CTF playing.

It is our hope this report demonstrates the value of unique research-based pedagogic experiences and inspires others to take on the challenges of adopting these practices into their own cybersecurity research laboratory as a project to enhance undergraduate educational outcomes in the cybersecurity discipline.

6 ACKNOWLEDGEMENT

We would like to acknowledge the RPI Teaching and Learning Collaboratory, who funded this research with an internal RPI seed grant.

No Generative AI was used in the research or writing of this paper.

7 REFERENCES

[1] National Cyber League, "The National Cyber League Announces Official Fall 2023 Cyber Power Rankings for High Schools and Colleges," PRWeb, November 20, 2023. [Online]. Available: https://www.prweb.com/releases/the-national-cyber-league-announces-official-fall-2023-cyber-power-rankings-for-high-schools-and-colleges-301993134.html.

[2] N. Childers, B. Boe, L. Cavllaro, L. Cavedon, M. Cova, M. Egele, and G. Vigna, "Organizing Large Scale Hacking Competitions," In Detection of Intrusions and Malware, and Vulnerability Assessment. DIMVA 2010. Lecture Notes in Computer Sciecne, vol. 6201, C. Kreibich and M. Jahnke, eds. Springer: Berlin, Heidelberg, doi: https://doi.org/10.1007/978-3-642-14215-4_8.

[3] J. Warner and P. J. Guo, "Hack.edu: Examining How College Hackathons Are Perceived By Student Attendees and Non-Attendees," Proceedings of the 2017 ACM Conference on International Computing Education Research (ICER '17), pp. 254-262, doi: https://doi.org/10.1145/3105726.3106174.

[4] T. J. Burns, S. C. Rios, T. K. Jordan, Q. Gu, and T. Underwood, "Analysis and Exercises for Engaging Beginners in Online CTF Competitions for Security Education," 2017 USENIX Workshop onf Advances in Security Education (ASE 17). [Online]. Available: https://www.usenix.org/conference/ase17/workshop-program/presentation/burns.

[5] B. R. Callahan and S. L. Sugerman, "Benefits and Limitations of Generative AI for Cybersecurity Awareness Training," ISC2 Security Congress 2024: Boldly Forward, Oct. 14-16, 2024. [Online]. Available: https://www.isc2.org/Insights/2024/10/ISC2Congress-Generative-AI-for-Cybersecurity-Awareness-Training.

[6] B. R. Callahan, K. Schilp, Q. Colognato, E. Goldman, S. Sugerman, A. Mehta, A. Imanuel, K. Kaii, and H. Rose, "Multidisciplinary quantum cybersecurity research for the undergraduate laboratory," The Journal of the Colloquium for Information Systems Security Education, vol. 12, no. 1, pp. 112-118, 2025, doi: https://doi.org/10.53735/cisse.v12i1.206.

[7] T. Cheng, S. Sugerman, C. Farley, and B. R. Callahan, "Quantum preprocessing for Internet of Things edge computing security devices," Proceedings of the 1st IEEE Conference on Secure and Trustworthy CyberInfrastructure for IoT and Microelectronics (SaTC 2025), Wright State University, Dayton, OH, Feb. 25-27, 2025.

[8] ISC2, "2024 ICS2 Cybersecurity Workforce Study: Global Cybersecurity Workforce Prepares for an AI-Driven World," Accessed: February 25, 2025. [Online]. Available: https://edge.sitecorecloud.io/internationf173-xmc4e73-prodbc0f-

9660/media/Project/ISC2/Main/Media/documents/research/2024-ISC2-WFS.pdf.

[9] ISACA, "State of Cybersecurity 2024: Global Update on Workforce Efforts, Resources, and Cyberoperations," Accessed: February 25, 2025. [Online]. Available: https://www.isaca.org/-/media/files/isacadp/project/isaca/resources/reports/isaca-state-of-cybersecurity_2024_1024.pdf.

[10] F. Goupil, P. Laskov, I. Pekaric, M. Felderer, A. Dürr, and F. Thiesse, "Towards Understanding the Skills Gap in Cybersecurity," Proceedings of the 27th ACM Conference on Innovation and Technology in Computer Science Education Vol 1 (ITiCSE 2022), July 8-13, 2022, doi: https://doi.org/10.1145/3502718.3524807.

[11] R. Vogel, "Closing the cybersecurity skills gap," Salus Journal, vol. 4, no. 2, pp. 32-46, 2016, doi: https://search.informit.org/doi/10.3316/informit.093144667545339.

[12] H. Ruoslahti, J. Coburn, A. Trent, and I. Tikanmäki, "Cyber Skills Gap – A Systematic Review of the Academic Literature," Connections: The Quarterly Journal, vol. 20, no. 2, pp. 33-45, 2021, doi: https://doi.org/10.11610/Connections.20.2.04.

[13] D. A. Kolb, *Experiential learning: Experience as the source of learning and development*. FT press, 2014.

[14] J. M. Hanson, T. L. Trolian, M. B. Paulsen, and E. T. Pascarella. "Evaluating the Influence of Peer Learning on Psychological Well-Being," Teaching in Higher Education, vol. 21, no. 2, pp. 191–206, 2016. doi: https://doi.org/10.1080/13562517.2015.1136274.

[15] V. Ford, A. Siraj, A. Haynes, and E. Brown, "Capture the Flag Unplugged: an Offline Cyber Competition" In Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education (SIGCSE '17), Association for Computing Machinery, New York, NY, USA, pp. 225–230. https://doi.org/10.1145/3017680.3017783.

[16] K. Chung and J. Cohen, "Learning Obstacles in the Capture the Flag Model," 2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE '14), August 18, 2014. [Online]. Available: https://www.usenix.org/conference/3gse14/summit-program/presentation/chung.