Visualization for Spectators in Cybersecurity Competitions

Chao Peng*
School of Interactive Games and Media,
Rochester Institute of Technology, NY

David Schwartz†
School of Interactive Games and Media,
Rochester Institute of Technology, NY

Daryl Johnson‡
Department of Computing Security,
Rochester Institute of Technology, NY

Bill Stackpole§
Department of Computing Security,
Rochester Institute of Technology, NY

Chad Weeden¶
Esports and CyberSecurity Range,
Rochester Institute of Technology, NY

Jacob Marcovecchio‖
School of Interactive Games and Media,
Rochester Institute of Technology, NY

Drake Richards**
School of Interactive Games and Media,
Rochester Institute of Technology, NY

Chris Fogle††
School of Interactive Games and Media,
Rochester Institute of Technology, NY

Christopher Brown‡‡
School of Interactive Games and Media,
Rochester Institute of Technology, NY

Victoria Walrond §§
School of Interactive Games and Media,
Rochester Institute of Technology, NY

Abstract

The goal is to raise awareness and encourage learning cybersecurity principles by making competitions appealing to a wider audience. In an effort to make events compelling, attractive, and watchable, the researchers will develop systems to support visualizations and make the transactions between teams in different cybersecurity competitions easy to comprehend. In informing and educating the audience on the intricacies of the competition through engaging visualizations, cybersecurity competitions will be opened up to a world beyond just participants. In doing so, we can potentially attract new talent into the field. Our team seeks to make prototype visualizations for key actions in various student cybersecurity competitions and assess spectator understanding of key principles of the competition.

Index Terms: Human-centered computing—Visualization—Visualization techniques; Human-centered computing—Visualization—Visualization design

1 Introduction

Student competition is intrinsic to the pedagogy of cybersecurity education [24]. Cybersecurity pedagogy embraces competition, as evidenced by multiple competitions [3, 13]. RIT hosts one such event, the Collegiate Penetration Testing Competition (CPTC) [22], which is *"a vehicle for up and coming cybersecurity student teams to build and hone the skills required to effectively discover, triage, and mitigate critical security vulnerabilities"* (`www.rit.edu/cybersecurity/academics`). CPTC differentiates itself from other cybersecurity competitions by allowing offensive measures to evaluate and discover weaknesses without "harm" to the target. CPTC includes several soft assessments such as writing a pen-testing proposal, written assessment and mitigation reports, and a final presentation to the "C-level" executives of the target company. However, we have observed that CPTC and related competitions are missing a key element: *visualization*. From the spectators' point of view, as shown in Figure 1, all they see are the participants frantically typing away on keyboards and occasionally hearing an exclamation of success - "woo-hoo!".

Figure 1: Participants at RIT's cybersecurity competitions.

Despite a wealth of knowledge about teaching and learning through visualization, especially within cybersecurity education [4, 15, 19], attention to the spectators' perspective has been lacking. To outside observers, the competition looks like a giant black box with little or no insight into what goes on inside. Based on our observations in CPTC, spectators are usually limited to the competitors themselves, their friends and families, hosts, and sponsors. With spectators providing audience feedback, oversight by industry professionals, and an opportunity to teach the public about the importance of funding cyber defense, we see a critical need for providing an improved spectator experience.

Visualization for the benefit of the spectator is commonplace in other live streaming venues today as illustrated by telestrator systems [14, 27]. For example, the visual line of scrimmage and first down overlay on a football field or the highlighting of the hockey puck. Imagine you were at a party but did not speak the language. You could still obtain a working knowledge of who the players were by simply observing those who were communicating and with whom. Network traffic analysis works on a similar principle. The content of the messages is not critical to one's understanding of how the traffic is flowing and which of the hosts are sending or receiving traffic.

In this work, we investigate ways to visualize events in cybersecurity competitions, so that non-technical spectators can follow, understand, and appreciate the happenings during the competition. We think it is important to develop a visualization tool that can be integrated into common cybersecurity tools to make them easier to understand. Key actions can be visualized as specific illustrations

*e-mail: cxpigm@rit.edu
†e-mail: disvks@rit.edu
‡e-mail:daryl.johnson@rit.edu
§e-mail: bill.stackpole@rit.edu
¶e-mail: cewics@rit.edu
‖e-mail: jxm5725@rit.edu
**e-mail: dwr2966@rit.edu
††e-mail:cjf2245@rit.edu
‡‡e-mail: cxb4531@rit.edu
§§e-mail: wtw1820@rit.edu

978-1-7281-8262-9/20/$31.00 ©2020 IEEE

and game-like representations to make the competition appealing to spectators. Ultimately we hope to encourage non-technical spectators in learning cybersecurity principles.

The rest of paper is organized as follows. In Section 2, we review some existing work from the literature related to visualization for cybersecurity competitions. Section 3 proposes two topics that we think are worthy of in-depth studies in order to develop meaningful and appealing visualizations for non-experts. Section 4 describes a visualization prototype we have developed for a small-scale cybersecurity competition at RIT. Section 5 concludes our current work and Section 6 proposes a roadmap for future work.

2 Related Work

Wicked6^{TM} [11] is a recent attempt at gamifying cybersecurity exhibitions. On August 8th, 2019, teams competed in the HyperX Esports Arena in Las Vegas through a platform called Project Ares which acted as a game hub for the competition. The event included casting, commercial breaks, and screen sharing. However, the visualization of the event was limited and revolved around basic screen capturing from one competitor to another. The tone also came off as monotone, tracking what every team was doing was difficult, and there was a lack of shown progression to the audience.

Turner et al. [23] presented the LUCID, which is a visualization system attempting to create a central spectator interface using a combination of host/network visualization, live feed, and an emphasis on animated commentators. While cybersecurity competitions are known to be beneficial to competitors and cybersecurity experts, the primary goal of LUCID is improving spectator experience and improving spectators' ability to understand cybersecurity competitions. In the LUCID, the visualizations of the events happening during competitions are portrayed as tables and slideshows, which do not seem appealing to non-experts. Later, Ruth et al. [1] added a virtual commentator subsystem to the LUCID. The virtual commentator is a upper-body female avatar programmed with synthesized motions and speeches. It interacts with spectators using facial expressions, hand gestures, and speeches. The commentator subsystem is complementary to the visualizations of competition events. Human-like behaviors and speeches from the commentator can help spectators capture exciting moments in the competitions, but the contributions to the visualizations of the events are still limited.

Kaehler et al. [20] aimed to make competitions more attractive and accessible to spectators. They adopted a 3D virtual battlefield paradigm as the landscape of the competition, which was built in the Unreal game engine. The visualizations were presented as layers of gameplay elments that are commonplace in battlefield video games. Particularly, each team's network and test applications were illustrated as small cities. Attacking from one team to another was animated as the buildings' structural damages, which are visual indicators of damage to the network, host, or test applications. On-screen texts and percentage bars as scoring indicators were used to show each team's competing status. The gameplay elements were easy for non-experts to understand and make sense of cybersecurity competitions. Their work still had lots of space for improvement, such as incorporating visuals to show dynamic and strategic decisions as the competition is running, defensive-offensive balance within a team, instant replays, and telestration graphics.

Garae et al. [10] presented a user-centric visualization framework to help the analysis of security-related attack behaviors. To understand how attacks occur, they collected a large set of attack behavior data from the past cybersecurity challenge events, and described the developing challenges of visualizations such as data processing speed,web graphics performance, and frontend (e.g., graphical assets, interface layouts) and backend (e.g.,storage, data analysis) compatibility. The framework was complex and revealed to have challenges in integrating multiple programming languages and achieving high performance. The visualization features of their visualization are aimed to display the attack correlations between two teams, represented as visually connected dots. While this could be useful for spectators to understand who were communicating, the events of the competition, including interactions, decision makings, and scoring, were not captured by the framework.

3 Topics

3.1 Cybersecurity Competitions as Games

Cybersecurity indulges in various kinds of competitions across the space, each with a different set of parameters and goals necessary to "win" an event. These competitions can be generalized into four unique categories: (1) *Defensive* competitions revolve around designing and protecting a network against a series of attacks. *The National Collegiate Cyber Defense Competition* [26] is arguably one of the most notable competitions in this space; (2) *King of the Hill* [2] is a competition which focuses around multiple teams fighting for control over a large network, such as the Information Security Talent Search (ISTS) competition at RIT; (3) *Capture the Flag* competitions [9, 25] are arguably the most popular kind of competition. They can either exist in Jeopardy style through challenges that award points, or in an attack/defense style where teams or individuals are meant to protect servers; and (4) there exists CPTC [22]: an offensive styled competition allowing teams to infiltrate networks without causing harm to its target.

Each competition is specialized around one of these four general categories. Each is created with unique parameters, different software, different scoring, and is completed over different time frames. Some competitions may take a few hours, and some others may take multiple days. However, each competition still uses core language and includes key actions across every variation. To explain this as an analogy, let us take the game of chess. Chess in its simplest form is a composite of two players, a game board, and unique game pieces. These players tend to have a piece of paper with a written language that allows games to be recreated. However, Chess also has unique variations (e.g., Crazyhouse Chess, Suicide Chess, and Atomic Chess [6]). In each variation, like Cybersecurity Competitions, the parameters of the game change. Yet the core gameplay and language remain intact.

Cybersecurity competitions all revolve around the same core gameplay and language, as chess does. Yet, by researching and identifying the "written language" of cybersecurity competitions, a clearer board is created with parameters that can be altered for unique competition. A generalized visualization framework should include an infrastructure of scene management and an intact rendering engine to rasterize fundamental graphical elements, while supporting dynamic scene synthesis with adaptive components and flexible assets, so that the uniqueness and key actions in different competitions can make sense to spectators. Those components and assets can be made of customizable modules. For example, the modules can be team avatars (e.g., heroes, fortification models, vehicles), scoring viewing systems (e.g., health bars, occupied territories), offensive and defensive animations (e.g., projectile launching, air striking), and theme graphics templates (e.g., battlefields, geographical maps). By extension, these modules, which resemble actions a player or team may take, can always be recreated and constructed visually. In other words, this will decompose the framework into separate processes, such as managing data and scenes, constructing graphical representations, and rendering, and therefore create a real-time game-like environment where visualizations are created dynamically to immerse spectators.

3.2 Visualization through Event Production

Visualization creates a visual workspace making network activities and events traceable and revealing the story hidden inside cyber security data [8]. When considering visualization for the benefit of the spectator, the definition extends beyond that of a created system

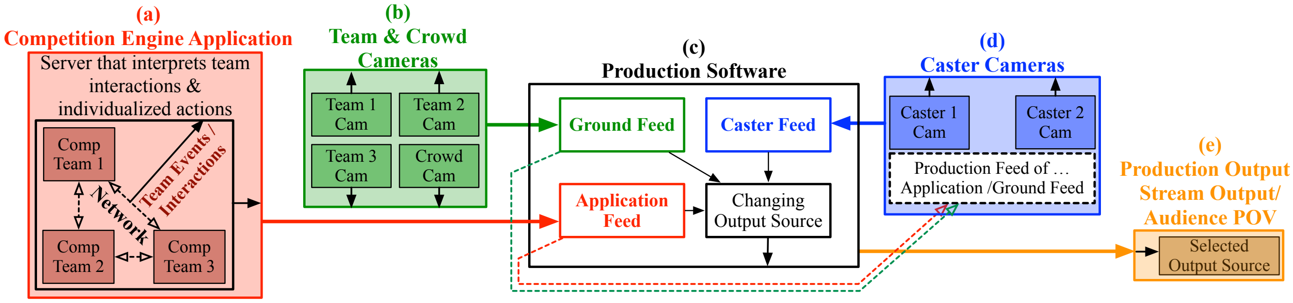

Figure 2: The architecture of the visualization tool for ISTS competition. (a) is the cybersecurity competition engine that monitors the competition real-time and displays visualizations sent for production. (b) includes the views of the crowd and competitors captured by camera operators used in production. (c) is the production software that dynamically manages all input feeds and selects the appropriate output meant from spectators. This software also sends different video feeds to casters for context of "gameplay" events. (d) includes the casters/analysts specific views captured by camera operators used in production. (e) includes the finalized output views in which spectators can see across different platforms.

of applications monitoring network activities and creating visual representations of what happens. Visualization for the spectator includes the totality of broadcasting and event production. We identify the following items that we think are worth of discussions.

Team interactions. At cybersecurity competitions, it is important to remain cognizant of the human interaction elements that exist through these competitions. For instance, CPTC includes human injections that are required to be dealt with from members on the team. There is also dialogue within a team environment that can be listened into, potential for caster elaboration as aid to any visualized scenes, team presentations, and other moments throughout competition which encourage more than just a baseline application.

2D vs. 3D graphics. There are both strong advantages and disadvantages to using 2D and 3D graphics for visualization. 2D visualization is less time consuming to make, and especially with a more minimalist style, it can simplify tasks and actions to spectators. However, if there is not a lot of actions happening on the screen, it can be a struggle to keep audience attention with 2D visuals. When done right, 3D visualization can enhance visual attention [7, 12, 17]. At the same time, 3D visuals are more time consuming to make, and they can often overcomplicate the spectator view.

Competitor-centric view vs. field-centric view. The event production may utilize different camera views to capture close-up and long shots of the scene. The competitor-centric view is responsible for the visualization covering specific actions of individual competitors. For example, a virtual camera can be established to take close-ups following the actions of a hero avatar. This can be used to highlight a competitor's outstanding effort. An extreme close-up shot can be used to intensify the dramatic interest by, for example, showing destruction details of a fortification 3D model or capturing the competitor's facial emotional expressions. The field-centric view can give spectators a visualization of the general situation regarding the competition. It provides an over-watch perspective with visual representations of the field of play. It is capable of showing which team is dominating or having the momentum in the competition. Thus, visualization of the complete competition should be a combination of competitor-centric view and field-centric view.

4 Prototype: A Visualization Tool for ISTS

Over the course of the last year, our team has investigated and created a small-scale mock-up of visualization framework through using RIT's ISTS competition. ISTS is an annual attack/defend type of competition where colleges from around the country compete for the coveted title of ISTS champion. Competitors are faced with a wide variety of challenges which are designed to cover as many facets of computing security, system administration, networking, and programming. These challenges include code review, architecture design, incident response, and policy writing – all while defending a completely student-built infrastructure [16]. Comparing to CPTC, ISTS is smaller scale and it includes multiple teams fighting one another to penetrate a network in a controlled environment. ISTS is also locally hosted, less dynamic, and less complex overall.

A group of students from RIT's Golisano College of Computing and Information Sciences worked alongside faculty to conceptualize and bring to life a small-scale visualization framework. By identifying key cybersecurity events triggered through the competition, including reverts, exploits, services (taken down/up), and connection strength, each action was provided some sort of visual queue. As shown in Figure 2, using a server which tracked network activities and events at the ISTS competition, the activities and events could be caught and sent into multiple applications.

The first application functions as a control panel to the visualizer. No different than a remote control can move a robot, this control panel received real time updates from a server monitoring the network teams worked through. Users could then show unique visualizations based on the monitored activity or manually submit information necessary to recreate visualizations for spectators.

The second application acts as an interpreter to both the control panel and the server. This application has multiple screens, no different than an American Football game has multiple camera angles, that can be altered and controlled. Additionally, this application can be set to interpret data from either the real time server or through manual submission. It is here where the physical visualizations would be shown onto a screen. The application allows for visualizations of selected competitors or of the entirety of the competition.

This framework allows for live streaming with broadcasting software, such as Open Broadcasting Software [18] and XSplit [21]. Through the availability of this broadcasting software and a server/control panel/visualizer system, cybersecurity hackathons become exponentially more available to the public. Additionally, they become marketable to an untouched audience curious about the field of work, similar to esports.

5 Conclusions

Visualization of cybersecurity enables larger exposure for professionals, and especially decision makers, in the field. The term, visualization, consists of both written applications to visually explain unique identifiable actions taken from competitors at these competitions and the overall event production providing depth to the spectator experience. As demonstrated by the work described in this paper, small scale prototypes can be built and are specified for individual competitions. However, creating a tool that identifies the same actions across all competitions is bound to enable visualization across every competition, revolutionizing cybersecurity competitions. Additionally, this tool (or series of applications used) should work hand in hand with the complete production experience and offer usage across unique identifiable events in different competitions.

6 Roadmap for Future Work

We anticipate that this work will provide the foundation for a comprehensive study of more visualizations and other sensory experiences. We seek to improve the CPTC, which will provide further refinements of the proposed architecture and help to influence other competitions. We suggest the following items to extend this work:

- **Intelligent focus:** given the complexity of the interactions, research into applying eye-tracking, vision, and applying to help spectators know where to focus would likely improve the spectator experience.
- **Cybersecurity competition "engine":** just as game development is helped by game engines, like Unity and Unreal, we anticipate that middleware and scripting environments would greatly assist with incorporative visualizations into the ever-growing variety of competitions. For each event, to rewrite and redo all of the assets, procedural generation, and casting seems arduous.
- **Spectator populations:** we foresee a variety of motivations for this work–to inspire prospective students into cybersecurity, to help with decision makers in industry and government, and to help researchers. For each group, there are multitude of spectators, which means we need to consider spectator survey and the impact that different visualizations might have.
- **Esportsification:** akin to gamification [5, 16], the connections between cybersecurity and esports competitions appear to be very strong, and as such, learning how to adapt and apply the production values of esports could help to enhance the appeal and understanding from these events.

Acknowledgments

We thank all the sponsors for the National CPTC: IBM Security, Google Cloud, Eaton, FireEye, and RIT along with volunteers from Crowe, Uber, HurricaneLabs, nccgroup, and indeed. This work was supported in part by RIT's Center for Cybersecurity Research.

References

[1] R. Agada, J. Yan, and W. Xu. A virtual animated commentator architecture for cybersecurity competitions. In S. Latifi, ed., *Information Technology - New Generations*, pp. 43–50. Springer International Publishing, Cham, 2018.

[2] K. Bock, G. Hughey, and D. Levin. King of the Hill: A novel cybersecurity competition for teaching penetration testing. In *2018 USENIX Workshop on Advances in Security Education (ASE 18)*. USENIX Association, Baltimore, MD, Aug. 2018.

[3] Cyber Security Degrees. A comprehensive list of cyber security competitions. Web, 2020. https://www.cybersecuritydegrees.com/faq/comprehensive-list-of-cyber-security-competitions/.

[4] A. D'Amico, L. Buchanan, D. Kirkpatrick, and P. Walczak. Cyber operator perspectives on security visualization. In D. Nicholson, ed., *Advances in Human Factors in Cybersecurity*, pp. 69–81. Springer International Publishing, Cham, 2016.

[5] S. Deterding, D. Dixon, R. Khaled, and L. Nacke. From game design elements to gamefulness: Defining "gamification". In *Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments*, MindTrek '11, p. 9–15. Association for Computing Machinery, New York, NY, USA, 2011. doi: 10.1145/2181037.2181040

[6] S. Droste and J. Fürnkranz. Learning the piece values for three chess variants. *ICGA Journal*, 31(4):209–233, 2008.

[7] M. S. El-Nasr and S. Yan. Visual attention in 3d video games. In *Proceedings of the 2006 ACM SIGCHI International Conference on Advances in Computer Entertainment Technology*, ACE '06, p. 22–es. Association for Computing Machinery, New York, NY, USA, 2006. doi: 10.1145/1178823.1178849

[8] G. A. Fink, C. L. North, A. Endert, and S. Rose. Visualizing cyber security: Usable workspaces. In *2009 6th International Workshop on Visualization for Cyber Security*, pp. 45–56, 2009.

[9] 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, p. 225–230. Association for Computing Machinery, New York, NY, USA, 2017. doi: 10.1145/3017680.3017783

[10] J. Garae, R. K. L. Ko, J. Kho, S. Suwadi, M. A. Will, and M. Apperley. Visualizing the new zealand cyber security challenge for attack behaviors. In *2017 IEEE Trustcom/BigDataSE/ICESS*, pp. 1123–1130, 2017.

[11] J. Gulick, M. Ricci, and M. Galloway. CyberIsASport: A recap of the wicked6 cyber games. Web, Oct. 2019. BrightTALK, https://www.brighttalk.com/webcast/14989/370611/cyberisasport-a-recap-of-the-wicked6-cyber-games.

[12] J. T. Hansberger, C. Peng, V. Blakely, S. Meacham, L. Cao, and N. Diliberti. A multimodal interface for virtual information environments. In J. Y. Chen and G. Fragomeni, eds., *Virtual, Augmented and Mixed Reality. Multimodal Interaction*, pp. 59–70. Springer International Publishing, Cham, 2019.

[13] L. J. Hoffman, T. Rosenberg, R. Dodge, and D. Ragsdale. Exploring a national cybersecurity exercise for universities. *IEEE Security Privacy*, 3(5):27–33, 2005.

[14] D. Jones, S. Rands, and A. D. Butterworth. The use and perceived value of telestration tools in elite football. *International Journal of Performance Analysis in Sport*, 20(3):373–388, 2020. doi: 10.1080/24748668.2020.1753965

[15] G. Markowsky and L. Markowsky. Visualizing cybersecurity events. In *Proceedings of the International Conference on Security and Management (SAM)*, pp. 1–7. The Steering Committee of The World Congress in Computer Science, Computer ..., 2013.

[16] S. Nicholson. *A RECIPE for Meaningful Gamification*, pp. 1–20. Springer International Publishing, Cham, 2015. doi: 10.1007/978-3-319-10208-5_1

[17] C. Peng. Introductory game development course: A mix of programming and art. In *2015 International Conference on Computational Science and Computational Intelligence (CSCI)*, pp. 271–276, 2015.

[18] S. Schirra, D. Holmes, and A. Rhee. Collecting observational data about online video use in the home using open-source broadcasting software. In *Proceedings of the 2018 ACM International Conference on Interactive Experiences for TV and Online Video*, TVX '18, p. 197–202. Association for Computing Machinery, New York, NY, USA, 2018. doi: 10.1145/3210825.3213568

[19] D. Schweitzer and W. Brown. Using visualization to teach security. *Journal of Computing Sciences in Colleges*, 24(5):143–150, 2009.

[20] R. Senanayake, P. Porras, and J. Kaehler. Revolutionizing the visual design of Capture the Flag (CTF) competitions. In A. Moallem, ed., *HCI for Cybersecurity, Privacy and Trust*, pp. 339–352. Springer International Publishing, Cham, 2019.

[21] SplitmediaLabs. Xsplit broadcaster [computer program]. version 1.3. 1403.1202. 2015.

[22] B. Stackpole and D. Johnson. CPTC-a security competition unlike any other. 2019. https://scholarworks.rit.edu/cgi/viewcontent.cgi?article=1956&context=other.

[23] C. Turner, J. Yan, D. Richards, P. O'Brien, J. Odubiyi, and Q. Brown. LUCID: A visualization and broadcast system for cyber defense competitions. *ACM Inroads*, 6(2):70–76, May 2015. doi: 10.1145/2746408

[24] D. T. Verhoeff. The role of competitions in education. In *FutureWorld: Educating for the 21st Century*, pp. 1–10, 1997.

[25] J. Vykopal, V. Švábenský, and E.-C. Chang. Benefits and pitfalls of using capture the flag games in university courses. In *Proceedings of the 51st ACM Technical Symposium on Computer Science Education*, SIGCSE '20, p. 752–758. Association for Computing Machinery, New York, NY, USA, 2020. doi: 10.1145/3328778.3366893

[26] G. B. White and R. Dodge. The national collegiate cyber defense competition. In *Proceedings of the Tenth Colloquium for Information Systems Security Education*, 2006.

[27] Q. Zhou and D. Liu. Interactive visual content sharing and telestration: A novel network multimedia service. In *2010 14th International Conference on Intelligence in Next Generation Networks*, pp. 1–6, 2010.