Revolutionizing the Visual Design of Capture the Flag (CTF) Competitions

Rukman Senanayake[1](✉), Phillip Porras[1](✉), and Jason Kaehler[2](✉)

[1] SRI International, Menlo Park, CA 95125, USA
{rukman.senanayake,phillip.porras}@sri.com
[2] Asylum Labs, 1735 Wharf Road, Suite A, Capitola, CA 95010, USA
j.kaehler@asylumlabsinc.com

Abstract. There are a variety of cyber-security challenge tournaments held within the INFOSEC and Hacker communities, which among their benefits help to promote and identify emerging talent. Unfortunately, most of these competitions are rather narrow in reach, being of interest primarily to those enthusiasts who are already well versed in cyber security. To attract a broader pool of younger generation participants requires one to make such events more engaging and intellectually accessible. The way these tournaments are currently conducted and presented to live audiences is rather opaque, if not unintelligible to most who encounter them. This paper presents an ongoing effort to bridge the presentation gap necessary to make cyber security competitions more attractive and accessible to a broader audience. We present the design of a new but familiar model for capturing the interplay, individual achievements, and tactical drama that transpires during one form of cyber security competition. The main user interface and presentation paradigm in this research borrows from those of established e-sports, such as *League of Legends* and *Overwatch*. Our motivation is to elevate the current format of cyber security competition events to incorporate design and presentation elements that are informed by techniques that have evolved within the e-sports community. We apply the physics models and battlefield visualizations of virtual world gaming environments in a manner that captures the intellectual challenges, team achievements, and tactical gameplay that occur in a popular form of cyber security tournament, called the Capture The Flag (CTF) competition. Our goal is to make these events intellectually accessible to broader audiences, to engage a broader and more diverse talent pool of competitors, and to increase the awareness and interest in cyber security among the general public.

Keywords: Cyber security · Capture the Flag · Visualization · Cyber education · National cyber league

1 Introduction

Those who have attended one of the growing lists of INFOSEC or hacking conferences will have likely been exposed to an increasingly competitive skills-building event called a Capture the Flag competition (CTF). CTFs regularly draw security professionals, enthusiasts, government IT specialists, and a wide range of collegiate teams

A. Moallem (Ed.): HCII 2019, LNCS 11594, pp. 339–352, 2019.
https://doi.org/10.1007/978-3-030-22351-9_23

from around the world. Participants pit their skills against each other as they attempt to defend (and in some cases attack) complex applications, computing devices, and even whole computer networks. These competitions have grown in competitiveness and sophistication, even to the height of one venue requiring competitors to create entirely autonomous agents that can discover vulnerabilities, auto-patching their networks, and produce and launch exploits without human assistance [5].

The experiences and skills that result from such competitions help to inspire and develop cyber security talent that the technology-dependent world needs within its workforce [1–4]. In the U.S., these competitions are sponsored by government organizations such as the Defense Advanced Research Projects Agency (DARPA) [5] and the National Science Foundation (NSF), and by leading IT companies across the commercial sector. Internationally, countries in the EU and Asia similarly invest in CTF competitions [6, 7], as part of their strategic investments of building cyber defense skills and identifying desperately needed talent. In fact, ctftime.org tracks more than 200 distinct CTF competitions that take place around the world [9].

No single universally followed model governs CTF competitions. The rules, duration, and the players' network configurations deviate considerably from venue to venue. However, we broadly categorize CTF competitions into three general forms:

- **Blue Team Competitions:** focus entirely on developing defensive skill. In these competitions, participants are granted time to analyze a common configuration of applications and computing assets, derive defenses, and are then evaluated based on their ability to protect these assets from attacks launched by a single Red Team (an offensive cyber-attack team).
- **Red-Team/Blue-Team Competitions:** blend both offensive and defensive objectives. Teams must race to uncover a wide range of vulnerabilities that have been implanted into a common configuration of applications and network components, which each team must administer. Teams must then patch and reconfigure their applications and network to neutralize the vulnerabilities, while weaponizing and launching exploits that compromise the security of those other teams that may have not yet succeeded in protecting their computing assets.
- **Red Team Competitions:** involve individuals, working alone or on teams, who are presented with a common set of applications or computing assets, and are competitively measured by their abilities to construct exploitations against these components.

No matter what the form of competition, CTFs share in the need for participants to conduct in-depth analyses, followed by (either or both) some form of software development or system administration. These phases of a CTF competition involve significant intellectual challenges that are designed to test the participant's technical skills. Unfortunately, for the CTF audience—even one dominated by the technically savvy—viewing these activities is about as engaging as watching small groups of students work on challenging homework problems. These competitions are slow paced, and often take place over an entire day or multiple days. Often, such as at DEFCON [8], the progress that slowly unfolds during the competition is presented to the audience in spreadsheet form, capturing simple statistics as each team progresses in defending their networks or testing exploits. However, embedded within the CTF competition are moments of technical achievement, significant tactical decisions [10], and instances of sophisticated adversarial attacks whose outcomes decide which team will win, and *how* and *why* they have succeeded.

In this paper we present a foray into the design of one form of CTF competition (the Red-Team/Blue Team form) as a visually engaging e-sport tournament. To do this, we impose a structure on the CTF competition, design and develop the visual elements of an intuitive virtual environment in which the players compete, and introduce techniques for isolating individual achievements, team interplay, and scoreboard presentation. We propose a battlefield visualization, which achieves a tradeoff between the number of teams present versus our desire to deliver single-camera presentations of the entire CTF competitions. We offer a novel visualization that captures all elements of the competition.

The contributions of this paper including the following:

- We define a CTF competition framework that deconstructs the event into a series of discrete activities that are performed, often in parallel, by members of each team. We discuss the anticipated sizes of teams and visual elements that are designed to isolate individual skills and team achievements.
- We present a 3-D virtual battlefield paradigm as the landscape on which the CTF competition is played. Our prototype is built using the Unreal game engine [11], which provides full camera virtualized movements that enable a CTF narrator (an event broadcaster) to navigate and visually isolate elements of the competition.
- We introduce a visual ontology of cyber-attacks, network and application architecture, and cyber defense functions. These elements are designed using familiar physics and semantics that enable unsophisticated audiences to grasp major status milestones and dynamic events as initiated by teams and referees.
- We discuss the motivations and challenges of taking a highly complex, slow-paced, and intellectually dense event and re-envisioning it as a visually engaging and intuitively familiar competition. Success in this activity can help CTFs expand their important role in promoting and identify an increasingly critical skill that is globally underserved.
- We design a novel *narrator-centric* presentation layer for the broadcast function, which allows for a subject matter expert to communicate, live, with the audience regarding the actions taking place within the virtual environment. Due to the complexity of the domain, knowing *when* and *where* to look is a substantial issue. Our system gives the narrator a camera ‘switcher’, enabling the focus to shift to action within the field of play as the competition unfolds.

2 Related Work

In the last decade, a great deal of investment has been made to study the impact of gamifying certain areas of cyber security, such that complex host and network events can be readily understood by a wider audience [14–16]. There are many well-documented advantages to such an approach [17]. Toward a model of cyber gamification, it is possible to focus on sub-domains of cyber security to specialize in skills development [18, 19]. Such efforts can target a range of demographics, from students in high schools [20, 21] to entry-level professionals [22].

CTF and Cyber Grand Challenge (CGC) style competitions are becoming increasingly popular as a means to identify new talent in the cyber security domain [9]. There are many CTF competitions formats, most of which have been studied to understand their efficacy in identifying talent, as well as popularizing the field of cyber security [22–24]. In addition, there is a drive to investigate which competition format can be used most broadly [25–27]. The lessons learned form DARPA's CGC format is also well understood and documented [28–30]. Given the current understanding of the impact we have on the format of CTF competitions and given the many differing formats being used, we hypothesize that in our case, we could exercise a degree of freedom in structuring certain elements of the CTF format to facilitate a visual gamification experience. We also posit that the format we propose simplifies certain logistical and technological pain points.

3 Conceptual Overview

When considering the real-time visualization of a highly complex environment with millions of concurrent events happening for a sustained period, the primary conceptual consideration is one of abstraction. In producing a game design, we have chosen a 'top-down' approach, which is narrator-centric and provides an over-watch perspective that is tailored to provide third parties with a visual understanding of the field of play. To determine best practices here, we looked primarily at e-sport events and traditional broadcast television sports.

The first and most essential challenge one finds when attempting to re-envision a CTF competition is that there exist no universal rulebook that specifies how all such competitions are conducted. CTFs have formed organically, and are subject to the preferences of their sponsors and organizers, including iterative improvement from past experiences. CTF organizers also evolve the rules and structure to adjust the difficulty of the challenges. This is to keep pace with the sophistication of the participants and their hacking tools, which are improving at a remarkable pace.

3.1 The Game Structure

Through our analysis of prior CTF competitions, and from communications with both participants and organizers, we have distilled several important commonalities in rules and competition structure that exist across Red-Team/Blue-Team CTFs. Further, in defining our canonical CTF game structure, we are sensitive to avoid decisions that reduce the applicability of the design, excluding the problem of scalability. The game design presented here will not scale to large-numbers of teams, albeit we are agnostic to the number of players that can participate within a single team [12].

Our CTF is designed as a team-based competition for two or more teams, with an idealized size of between 6 to 8 teams (for visual scale of the battlefield). All teams are provided an identically configured network, which includes host and network misconfigurations that can enable other teams to infiltrate their opponent networks. In addition, each team is given a required set of applications (or *test apps*) that must be run and maintained accessible on the team's network at all times. Access to each team's test apps are continually probed by competition referees, who will penalize a team for any unresponsive or corrupted application. Unfortunately, the test apps are purposefully embedded with one or more critical security flaws that render them vulnerable to attack by any other team that can weaponize an exploit faster than the team hosting the test app can patch the vulnerability.

Blue-Team Responsibilities: Each team must demonstrate their administrative security skills by identifying and removing all configuration vulnerabilities from their network. In addition, the team must reverse engineering, discover, and patch all vulnerabilities in each test apps while not degrading the referee's access to the test app. These defensive actions require significant time and skill, and failure to remove a security weakness will render the team's network exploitable, and thereby subject to score reductions. These configuration flaws and test app vulnerabilities are unknown in number, thus removing any certainty from a team that it has fully protected its assets from attack.

Red-Team Responsibilities: In parallel with their defensive challenges, teams must also demonstrate their skills in offensive operations. While each configuration flaw and test app vulnerability represents a threat to the team that must be removed before points are lost, they also represent opportunities to generate exploits that can be launched against the other teams, thereby earning points in the competition depending on the outcome.

Visualizing Tactical Game Play: An essential objective in presenting a CTF competition is that of accurately visualizing the improvement that each team makes to their defensive posture, as well as their progress in constructing and launching exploits. Capturing defensive progress translates to visualizing the installation of patches to the set of vulnerable test apps, and the removal of network flaws that were delivered within each team's network. Exploit construction, network scanning for reconnaissance purposes, and exploit execution are also vital to visualize. Combined, these defensive posture changes and offensive actions do not just capture distinctions in the speed and skills of teams, but also capture purposeful tactical game play that teams employ, which may ultimately decide which team will win.

Some teams will focus on the immediate and comprehensive installation of defenses as quickly as possible, while on the other extreme there may be teams that employ their resources toward exploit generation to strike first. However, every exploit and network scan performed by one team enables other teams to observe the exploit or scan pattern, thereby revealing an attack surface that may not have been apparent or properly addressed. Exposing an attack (or scan), particularly one that is unsuccessful, reveals *threat intelligence,* which may help other teams harden their defenses and create their own exploit variants) [10].

3.2 Implementation of the Battle Space

Visualization of a tournament requires an ability to perform fine-grained monitoring of the actions of contestants, referees, and selective events that occur on the hosts and networks in the field of play. The instrumented platform that we use to capture these activities is already integrated into existing contests, but we impose additional surveillance requirements.

Team Assets: Game participants are provided with an instance of a Linux VM running [31]. Kali is a Linux OS Distribution that is designed for the penetration testing community, and includes a wide assortment of hacking tools that are typically used in these competitions. We augment Kali with OS extensions that enable the monitoring of key activities that are used to track each team member: process execution, file IO operations, administrative functions, and network connections. We also introduce a requirement that all teams must post exploit binaries or script that they intend to run into a team-designated exploit directory. All attacks and scans produce process executions that result in connections to external networks. Any process that performs these external connections but is launched from a directory outside the designated directory will result in a penalty.

Game Assets: Hosts that are located in each team's protected network are similarly instrumented with OS extensions that monitor all processes, file IO operations, authentication operations, and network operations. We employ system call monitoring extensions that produce records that are correlated with network flow records (using SRIFlow [32]). A correlated record captures the process ID, application name, the user ID of the participant who launched the process, and the source and target IPs, ports, and protocol involved in the flow. This information drives both visual elements of the game display and is used by the referees to detect various rule violations.

Referee Actions: Referees provide a continual stream of network probes that analyze the state and availability of each team's network assets and test apps. The outcome of these flows is visualized in the game environment as health and status indicators per host and test app. In addition, referees continually analyze all network flows from each team, inspecting each for rule violations that represent out-of-bound probing and exploit executions that are launched from outside the designated attack directories.

4 The Visualization Layer

A natural physical model that captures many of the key aspects of the CTF competition is that of a battlefield, composed of each team's network and test apps visualized as cities. This approach presents a familiar grounding for audiences to interpret the status per contestant, and for understanding when exploits are launched from one team into the cityscape of another team. A successful attack is viewed with a visual indicator of structural damage to the target host or test app, which is represented as a physical structure. We discuss the model and visual elements below.

The Visualization Layer represents the majority of effort in this research as the team had a number of simultaneous goals. The overall visual 'look' needed a strong 'theme' to appeal to casual observers and have a 'cool' factor often seen in video games, including the use of sport team mascots that convey both the organization and the successes and damages incurred. We chose giant robots to represent the Teams, and small cities to represent their networks, with buildings as the machines in the network and abstract spheres to indicate the actual binaries themselves, illustrated in Fig. 1.

There are 4 categories of actor:

Players: are shown as a photograph or live video with icon representing the current tool they are using. Player highlighting is an important aspect of game competitions that is largely absent from current CTFs, and we posit that for widespread popular acceptance, a critical aspect of audience engagement involves the ability to identify and highlight the successes and setbacks of individual players within a team. Thus, our game design pays significant attention toward bringing the competitors themselves forward in game visualizations, with the goal of creating “star players”.

Binaries: test apps are a primary game element that provides the central focus for much of the competition. Teams distinguish their strategies and score points based on their ability to produce defensive patches, maintain availability, or succeed in producing exploits against these test apps (binaries).

Flags: the primary scoring indicators in a CTF competition. A team receives a Flag when it penetrates an opponent’s binary successfully.

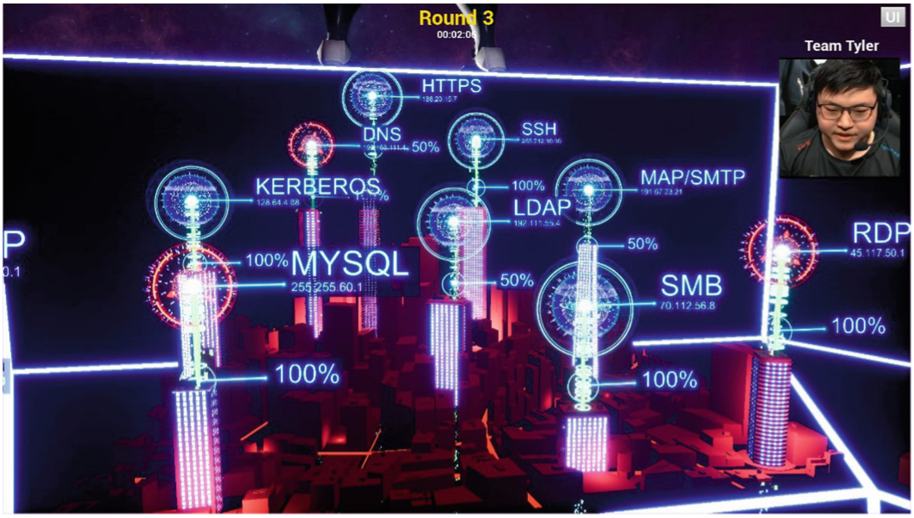

Fig. 1. Illustration of a team’s hosts, test-apps, and network. The test-apps are labeled by the binary name and colored based on their patch status.

Exploits: Table 1 presents the *method* a team will use to retrieve an enemy flag. An exploit is launched as an attack, which becomes a central focus of action in the visualization. However, the attack visualization must not just capture the launch, but must also provide a visual indication of what method of attack the audience is witnessing. We represent 6 basic attack types and two types of “network scans”.

As a secondary element, we show the patches themselves and the process of them being published to all other teams. This patch-publishing requirement means that teams must share with each other every applied patch, as it is instantiated, in their own test apps. This is due to a rule that was recently added to some mature CTFs (Fig. 2).

Table 1. Seven default attack methods are defined, Column 2 identifies the visual representation of the exploit method defined in Column 3.

Attack 0	Flare bullet	Brute force authentication
Attack 1	Green bullet	Misconfiguration exploit
Attack 2	Red bullet	Unintended data exposure
Attack 3	Red laser	SQL injection
Attack 4	Green laser	Application fuzzing
Attack 5	Missiles	Remote code execution
Attack 6	Robot bug swarm	Denial of service
Attack 7	Network scan	Network scan (green is standard, orange is out of bounds)

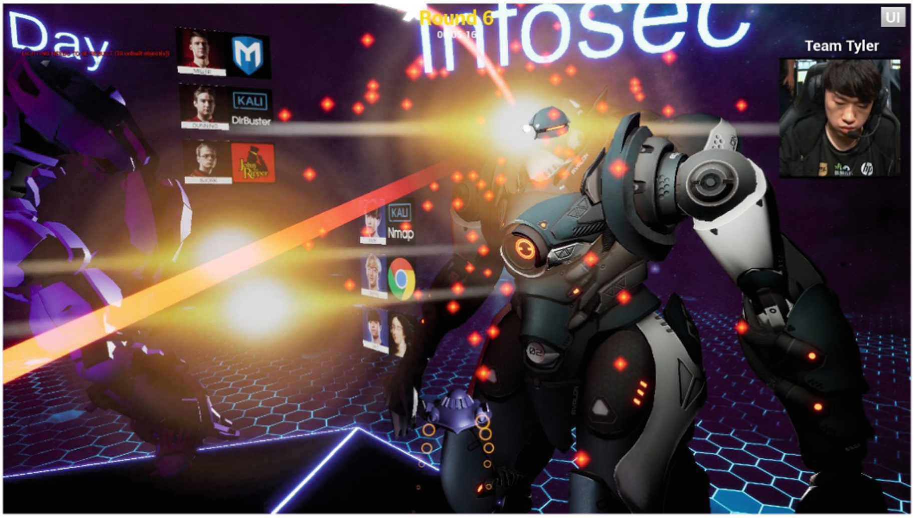

Fig. 2. Illustration of an exploit that is launched and credited to a specific player. Designation of the responsible team is indicated through the mascot, and the exploit method is visually represented by the shape and color.

Teams may also publish corrupt (or infected) patches, such that other teams must take great care. This adds an interesting dynamic to the core decision process teams face during real competitions. We also include the notion of an "infection," in which a team has successfully penetrated an opponent's network.

As the competition progresses and players attack each other's assets, the system ingests the Event Layer information and visually links the action to the appropriate actor:

> *Team A decides to target Binary 2 and Binary 3 from Team B. Their best SQL team member just completed a SQL vulnerability patch and rapidly pivots to constructing the SQL exploit. The visualization will show him working on that attack, and when he releases it on the network, we will see the Team A giant robot fire a red laser at the Team B buildings that host Binary 2 and Binary 3. If the attack succeeds, the building "explodes" and a flag will be seen flying from that location to the feet of Team A.*

The system is live. However, some programmatic attacks that occur in milliseconds are visualized over a synthetic duration for the human audience. This aspect of sequentially staging visual events is incident-based rather than live-traffic based. Once a team has hit a given target (say 20 flags) or the competition clock has hit a predetermined end-point, scores are tallied and results are presented.

4.1 E-Sport Tools Layer

If you watch a professional sporting event (or e-sports), you will notice what a critical role the narrator (broadcaster) plays. Having a subject matter expert (SME) who can talk about the competition while it progresses and point out the nuances, strategies and specifics make the entire spectator experience vastly more rewarding and engaging. However, unlike traditional sports where the ‘action’ is usually centered around a particular area on the field or court (usually ‘the ball’), in CTF’s we have a highly decentralized field of play, with many actors performing a wide range of activities in parallel. This presents a substantial challenge for the ‘broadcast’ aspect of the application. *What should we be looking at?*

This is where the ‘Broadcaster’s interface’ becomes critical. This is a set of onscreen functionalities that only the broadcaster will see. Conceptually, our prototype CTF game engine incorporates a camera ‘switcher’ (borrowed from broadcast TV facilities), where a variety of cameras allow the broadcaster to quickly pivot the audience to follow the action, and then narrate the particular event or strategy. This view includes both in-game actions and separate ‘Data Pages’ that provide historical data about players, teams, and the test app challenges. Figure 3 illustrates an example of a broadcaster perspective with camera selection.

‘Scoping,’ represents another critical component of the Broadcasters Interface. Since these playfields can get quite chaotic, it is often desirable to remove aspects of

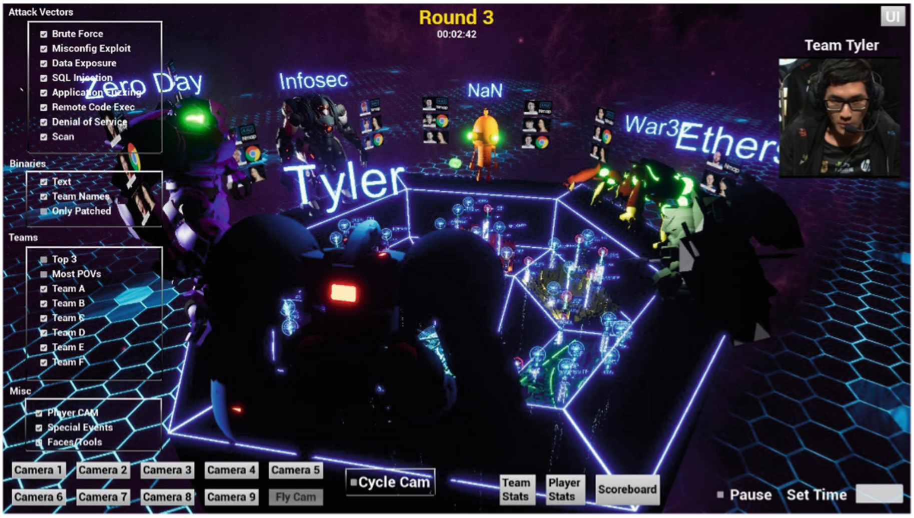

Fig. 3. An example of the broadcaster view with the camera selection options.

the visualization to discuss a particular detail. Broadcasters can toggle the display of each kind of attack, for example to show ONLY Misconfiguration Exploits, or can remove certain teams and to show isolated interactions between Team A and B. Providing these tools during the presentation enables the broadcaster to minimize visual clutter, so that the narration can be translated to the visual display with less confusion.

Finally, Data Pages are analogous to the 'stats' shown in broadcast sports and e-sports. We have seam sheets, leaderboards and individual sheets. The Team-sheets update with game information, for example if a player has been red-carded for illegal activity (such as an out-of-bounds scan or launching external network activity from a process that is launched outside the exploit directory) (Fig. 4).

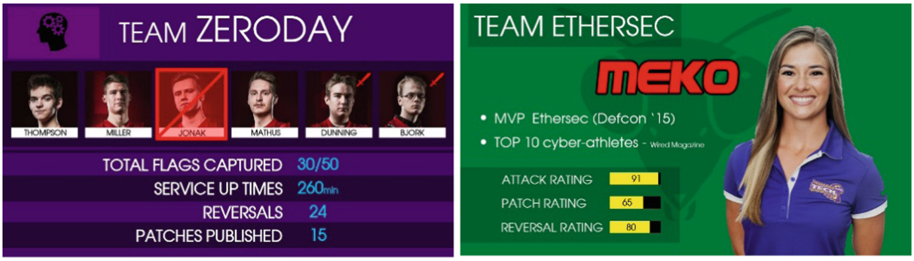

Fig. 4. Example data pages that highlight team and individual statistics.

4.2 An Example Parameters of a CTF E-Sport Competition

We have designed and constructed demonstration e-Sport games using the design described in this paper. The following briefly summarizes the parameters that were used within this demonstration.

Starting with the high-level goal to make CTF competitions accessible and enjoyable to the widest possible audience, we began by imposing a set of constraints for this particular e-sport inspired visualization. Specifically, we chose to show a red-blue CTF, with the following parameters:

- Number of teams: 6
- Number of members per team: 6
- Which tools are provided: Kali, IDA pro, Nmap, Chrome, Wireshark, Metasploit, DirBuster, SQLmap, Nessus, Burpsuite, and John the Ripper
- Number of binaries per team: 9
- Event duration: 12 h

It is important to note that these constraints are somewhat arbitrary and that the actual world of CTFs has a wide range of possible configurations. With this in mind, our core system is flexible and could support a fair amount of variation if required. We consider this current design as a starting point for a robust and extensible framework.

5 Future Work and Discussion

As the existing CTF game engine framework evolves, there are a several open problems that were deemed beyond the scope of our present design. This section enumerates the limitations of our work and acknowledges several open technical challenges.

Tournament Extensibility and Scalability. An ideal visualization framework should handle a wide range of arbitrary devices and configurations. For example, recently, IoT-based CTF competition have emerged in recognition of the ongoing security challenges that these devices now pose [13], We see natural extensions to our current battlefield motif. However binary test applications, and the network administrative functions involved in Blue-Team activities are less relevant. The system should also visually scale to the number of players, teams, and binaries, in an automated and graceful way. This is perhaps the most significant challenge in CTF game design. Procedural geometry and rule-based modeling offer potential solutions on the 3D layout construction, while more flexible interim data-formats could drive the configuration of the battle space. Finally, the visual ontology of discriminating among exploit classes is currently fixed in number. We would like to extend this vocabulary through better instrumentation and a more robust event description syntax.

A Granular Representation of Traffic Content. The current instrumentation of the hosts and network focus on flow-level analysis, in which the type of attack must be designated by the application from which it is launched. However, the internal size, structure, and content of flows can offer insights into the methods and outcomes of an exploit attempt. Deep packet inspection, which is not performed in the current prototype, would enable the visualization of the responses of the hosts and test apps as they encounters probes and exploits. These responses can offer insights into how Blue-team defenses are performing as new connections from the opponents are parried.

The Semantics of Player Activity. Perhaps one of the most direct ways in which e-sports draw spectators into the game is by their ability to visualize the activities of the individual players. To appreciate the skills, strategies, and the progression of the game, it is important to understand what the players are doing at a given moment in the contest. This point is particularly relevant to the slow-paced, multi-hour duration of a CTF competition. Audiences are more likely to rotate in among multiple tournaments or attend and return to the tournament rather than engage in monitoring the tournament from beginning to end. We would like methods to visually represent the process of attack construction, as well as methods to visualize vulnerability discovery, and security flaw removal.

Post-Game Analytic Services. We currently collect the bare minimum in analytics. One area for future algorithmic extensions is that of conducting automated comparisons of milestones, such as exploit formulation, exploit execution, test app patch deployment, configuration flow removal, and network scans. The rate and timing of these milestones could facilitate additional narratives that explain team strategies and the skills that are exhibited among the competitors. There may be analogies that arise between CTF gameplay comparisons with existing e-sport competitions that can facilitate a better understanding of the skills and strategies that teams employed during the competition.

A Recommendation System for Broadcasters. When and where spectator attention should be focused may not be obvious? As mentioned earlier, regardless of our effort to abstract the assets and applications of a typical CTF into a familiar physical representation (a city-scape battlefield), there remains the potential difficulty for the audience to always know *where* the most interesting events are happening. Even when a competition is slow paced, the ability to identify when background activity becomes notably interesting may not always be immediately apparent. An expert system could be applied to filter and prioritize events through a series of criteria, and then offer recommendations to the broadcaster of scrutiny-worthy fields of play. Camera activations could also be automatically adjusted to capture action and a single button could allow the broadcaster to zoom based on these recommendations. As the number of teams and players increases, such automation will become increasingly valuable.

6 Conclusion

This paper presents the design of a Cyber CTF competition framework, which employs a 3-D virtual battlefield abstraction that is designed to increase the engagement and understanding of the action that transpires. We present the motivations and challenges of taking a highly complex, slow-paced, and intellectually dense event and re-envisioning it as a visually engaging and intuitively familiar competition. Our prototype framework is designed to model CTFs as an e-sport tournament, with a cityscape abstraction of live networks, hosts, and applications, and a visual ontology of defensive and offensive actions that capture the milestones and events as they unfold. Further, we discuss the ability of this framework to capture the strategic decisions made by the teams, as each must decide how to balance its resources on defensive or offensive activities. Finally, we outline the limitations and open problems that we have encountered during this project.

Acknowledgments. This project was funded by the National Science Foundation (NSF) (Award Number DGE-1824258). The views, opinions, and/or findings contained in this paper are those of the authors and should not be interpreted as representing the official views or policies, either expressed or implied, of NSF.

References

1. Tobey, D.H., Pusey, P., Burley, D.L.: Engaging learners in cybersecurity careers: lessons from the launch of the national cyber league. In: ACM Inroads, New York, NY, USA, March 2014
2. Vigna, G., et al.: Ten years of iCTF: the good, the bad, and the ugly. In: Proceedings of the USENIX Summit on Gaming, Games and Gamification in Security Education (3GSE), San Diego, CA, August 2014

3. Cheung, R.S., Cohen, J.P., Lo, H.Z., Elia, F., Carrillo-Marque, V.: Effectiveness of Cybersecurity Competitions (2012). https://www.josephpcohen.com/papers/seccomp.pdf
4. Namin, A.S., Aguirre-Muñoz, Z., Jones, K.S.: Teaching cyber security through competition: an experience report about a participatory training workshop. In: Proceedings of the 7th Annual International Conference on Computer Science Education: Innovation and Technology (CSEIT) (2016)
5. DARPA: Welcome to DARPA's Cyber Grand Challenge – full playlist, July 2016. https://www.youtube.com/watch?v=g5Kt2ayMN0&list=PL6wMum5UsYvZx2x9QGhDY8j3FcQUH7uY0
6. The European Cyber Security Agency: European Cyber Security Challenge. Home page for the EU 2019 CTF Competition. January 2019. https://www.europeancybersecuritychallenge.eu/
7. EY.COM: The Asia-Pacific Cyber Case Challenge, January 2019. https://www.ey.com/cn/en/careers/ey-asia-pacific-cyber-challenge
8. DEFCON: DEFCON 2018 Capture The Flag (CTF) Competition, January 2018. https://www.defcon.org/html/defcon-26/dc-26-ctf.html
9. CTF Time: CTFS, January 2019. https://ctftime.org/ctfs
10. Bao, T., Shoshitaishvili, Y., Wang, R., Kruegel, C. Vigna, G., Brumley, D.: How shall we play a game?: a game-theoretical model for cyber-warfare games. In: Proceedings of the 30th IEEE Computer Security Foundations Symposium, CSF 2017, Santa Barbara, CA, 21–25 August 2017
11. Epic Games: What is the Unreal Engine 4, January 2019. https://www.unrealengine.com/en-US/what-is-unreal-engine-4
12. Samurai CTF Team: We are Samurai CTF and we won Defcon CTF this year (2013). http://www.reddit.com/r/netsec/comments/y0nnu/we_are_samurai_ctf_and_we_won_defcon_ctf_this/c5r9osm
13. Fortinet: Ph0wn: A CTF Dedicated to Smart Devices, November 2018. https://www.fortinet.com/blog/threat-research/ph0wn-a-ctf-cedicated-to-smart-devices.html
14. Boopathi, K., Sreejith, S., Bithin, A.: Learning cyber security through gamification. Indian J. Sci. Technol. **8**, 642–649 (2015)
15. Fink, G., Best, D., Manz, D., Popovsky, V., Endicott-Popovsky, B.: Gamification for measuring cyber security situational awareness. In: Schmorrow, Dylan D., Fidopiastis, Cali M. (eds.) AC 2013. LNCS (LNAI), vol. 8027, pp. 656–665. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-39454-6_70
16. McDaniel, L., Talvi, E., Hay, B.: Capture the flag as cyber security introduction. In: Proceedings of the 49th Hawaii International Conference on System Sciences (HICSS). IEEE (2016)
17. Dabrowski, A., Kammerstetter, M., Thamm, E., Weippl, E., Kastner, W.: Leveraging competitive gamification for sustainable fun and profit in security education. In: USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15) (2015)
18. Adams, M., Makramalla, M.: Cybersecurity skills training: an attacker-centric gamified approach. Technol. Innov. Manag. Rev. **5**(1) (2015)
19. Nakaya, M., Akagi, S., Tominaga, H.: Implementation and trial practices for hacking competition CTF as introductory educational experience for information literacy and security learning. In: Proceedings of ICIA (2016)
20. Chapman, P., Burket, J., Brumley, D.: PicoCTF: a game-based computer security competition for high school students. In: 3GSE, August 2014
21. Dasgupta, D., Ferebee,D.M., Michalewicz, Z.: Applying Puzzle-based learning to cyber-security education. In: Proceedings of the 2013 on InfoSecCD 2013: Information Security Curriculum Development Conference, p. 20. ACM, October 2013

22. Gavas, E., Memon, N., Britton, D.: Winning cybersecurity one challenge at a time. IEEE Secur. Priv. **10**(4), 75–79 (2012)
23. Chung, K., Cohen, J.: Learning obstacles in the capture the flag model. In: 3GSE, August 2014
24. Vigna, G., et al.: Ten years of iCTF: The good, the bad, and the ugly. In: 3GSE, August 2014
25. Chothia, T., Novakovic, C.: An offline capture the flag-style virtual machine and an assessment of its value for cybersecurity education. In: USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15) (2015)
26. Nunes, E., Kulkarni, N., Shakarian, P., Ruef, A., Little, J.: Cyber-deception and attribution in capture-the-flag exercises. In: Jajodia, S., Subrahmanian, V.S.S., Swarup, V., Wang, C. (eds.) Cyber Deception, pp. 151–167. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-32699-3_7
27. Ford, V., Siraj, A., Haynes, A., Brown, E.: Capture the flag unplugged: an offline cyber competition. In: Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education, pp. 225–230. ACM, March 2017
28. Song, J., Alves-Foss, J.: The DARPA cyber grand challenge: a competitor's perspective. Proc. IEEE Secur. Priv. **13**(6), 72–76 (2015)
29. Song, J., Alves-Foss, J.: The DARPA cyber grand challenge: a competitor. In: Proc. IEEE Secur. Priv. (1) (2016)
30. Walker, M.: Machine vs. machine: lessons from the first year of cyber grand challenge. In: Proceedings of the 24th USENIX Security Symposium (2015)
31. Kali.Org: Kali Distribution Page - Our Most Advanced Penetration Testing Distribution, Ever, January 2019. https://www.kali.org
32. SRI International: SRIFlow Distribution Page – Network Flow Auditing for Security and Visualization, January 2019. http://sriflow.csl.sri.com