1-2022

Lessons learnt conducting Capture the Flag CyberSecurity Competition during COVID-19

Kee Hock TAN

Eng Lieh OUH
Singapore Management University, elouh@smu.edu.sg

Lessons Learnt Conducting Capture the Flag CyberSecurity Competition during COVID-19

Kee Hock Tan
Cyber Security Group
Government Technology Agency
Singapore
tan_kee_hock@tech.gov.sg

Eng Lieh Ouh
School of Computing and Information Systems
Singapore Management University
Singapore
elouh@smu.edu.sg

***Abstract*—This innovative practice full paper describes our experiences conducting cybersecurity capture the flag (CTF) competition for cybersecurity enthusiast participants (inclusive of both tertiary students and working professionals) local and abroad during the COVID-19 pandemic. Learning and appreciation of cybersecurity concepts for our participants with little to no technical background can be challenging. Gamification methods such as capture the flag competition style is a popular form of cybersecurity education to help participants overcome this challenge and identify talents. Participants get to apply theoretical concepts in a controlled environment, solve hands-on tasks in an informal, game-like setting and gain hands-on active learning experience. CTF competitions can be held at physical locations or virtually. However, the COVID-19 pandemic catalyses all major events that are traditionally held physically to go virtual (likewise for physical CTF events). The pandemic limits our physical interactions, changes the dynamics of our engagements with the participants and how participants learn. We have to adapt our CTF competition design and conduct it in a virtual format during the COVID-19 pandemic that is compliant with local pandemic regulations as well.**

This paper describes these adaptations for a semi-international CTF competition conducted for our participants. We conduct the competition entirely virtual and adapt the cybersecurity exercises to be attempted without the participant's physical presence. While we devise ways to validate participants' involvement, it is still more challenging to limit cheating than in a physical environment. However, with appropriate mitigating controls in place (reducing risks to acceptable levels), we were able to achieve similar outcomes compared to a physical event despite the lack of physical interactions. Over 1400 participants registered for our competition, and with the help of over 40 staff, we successfully conducted this 48 hours virtual CTF competition. We further analyse the participants' online activity during the competition, their survey responses after the competition and derive our lessons learnt. We hope that these experiences, analysis and findings are useful for educators or organisers who wish to adopt online CTF to improve the learning outcomes of teaching cybersecurity education.

***Index Terms*—Computing skills, higher education, continuing education, cybersecurity, capture the flag**

I. Introduction

Introducing technical computing concepts such as cybersecurity can be a challenging task for educators to teach and students to comprehend and get motivated about this subject. Hands-on learning techniques such as Capture The Flag (CTF) competition allowing participants to explore security concepts in a real world have been proposed to address this challenging task.

As shared by Chung [1], CTF presents a variety of problems (known as challenges) to the participants. Each challenge contains some form of security vulnerability or security-related task that must be exploited or completed. Upon completion, the challenge will yield higher levels of access or reveal an answer. These answers are often used to form flags or being the actual flag itself, which will be exchanged for points. In which, the teams will be ranked based on the points accumulated. Participants rely on their cyber security knowledge and ability to apply them to solve the challenge.

McDaniel et al. [2] used CTF for their GenCyber camps found it to be a very effective way to provide students to link security concepts back to real-world incidents or common implementations. Beltran et al. [3] in their study showed that students find these CTF competitions to be more interactive, collaborative, useful and motivating compared to individual virtualized exercises. Leune et al. [4] surveyed students taking cybersecurity class before and after participating in CTF found that these sessions increases student engagement and lead to more well-developed skill. Ouh et al. [5], [6] discover that implementing lab CTF exercises for students to discover threats and vulnerabilities and design mitigating solutions do improve their learning outcomes for a secure architecture design.

Ford et al. [7] successfully implemented CTF unplugged in an offline environment with students reporting a significant gain in their cybersecurity knowledge, confidence and comfort level after participation. Hoffman et al. [8] and Childers et al. [9] highlight the need to consider structural issues when establishing such cybersecurity competitions at the national level for universities. The structural decisions to conduct these competitions physically at centralized or multiple sites result in different resource requirements and costs, a factor which institutions need to weigh against the potential benefits.

When COVID-19 successfully forced a global shutdown of face-to-face and offline activities in many sectors, including education, it is no longer an option to consider physically on-site(s) or offline but a necessity for CTF to be conducted completely virtual. This paper focuses on our experience

in organising a cybersecurity CTF competition - STACK the Flags 2020, completely virtual and conforming to the COVID-19 regulatory requirements.

The paper presents the organiser's (as referred to as Organising Committee) considerations, CTF competition design and highlights the key lessons learnt in organising a virtual CTF. The event was a semi-international CTF with a participation requirement of having at least 1 Singaporean / Permanent Resident (PR) in a team (up to 4 members). It was 48 hours, jeopardy style-ed CTF, covering 11 different cybersecurity domains. A total of 1405 participants from 24 different countries registered for the CTF. The paper timely captures the additional considerations when organising a CTF during the COVID-19 pandemic, whereby constraints were introduced by the local health regulatory authority to combat the pandemic.

II. Background

In recent years, the number of CTF events organised has shown strong growth. This was exhibited on ctftime.org [10], a popular CTF event site, showing an increasing number of CTF events being registered on the site every year. Both international and local CTFs can be conducted on-site or virtual. However, the arrival of the COVID-19 pandemic prompted a drop in CTF events that are conducted on-site in 2020 (as observed in Fig. 1).

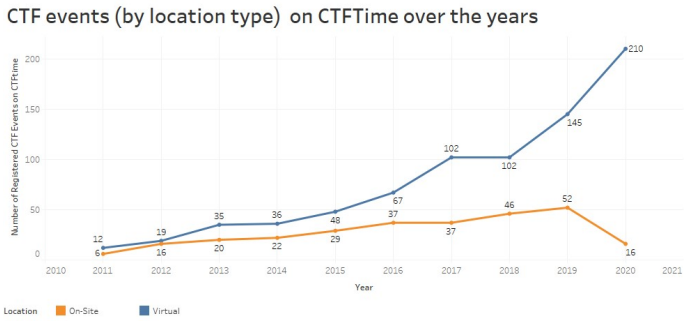

Fig. 1. Number of CTF events registered by location type on ctftime.org over the last 10 years

This is likely due to countries having entered a complete or partial lock-down state, which makes on-site events impossible to conduct. In Singapore, to combat the spread of COVID-19, various measures were implemented. Of which, two of the key deciding factors in conducting on-site events are restrictions on i) social gathering size; and ii) allowing the conduct of large scale events (i.e. conferences). CTF events often have a varying scale of difficulty, which in turn attracts different types of participants. For example, Google CTF [11] and Defcon CTF [12] attract skilled cybersecurity professionals. In contrast, events like picoCTF [13] and HSCTF [14] are designed for high school students. Within Singapore, most of the local CTF events were targeted at students. While various local community groups organised CTF events for the general public, it is often not organised at a similar scale. Thus, the Organising Committee organised a semi-international cybersecurity CTF during Phase 2[1]. The entire event was conducted virtually while adhering to various restrictions in place (due to COVID-19).

III. Competition Design

A. Target Audience

The CTF event was designed to target both cybersecurity professionals and tertiary students. The student population was further segmented into two different groups (based on Singapore's educational system or equivalent). Below is the listing of the participation categories:

1) Category 1 - Open;
2) Category 2 - Universities and Polytechnics; and
3) Category 3 - Junior Colleges, Integrated Programmes and Institutes of Technical Education

The CTF is a team-based event (up to 4 members), with a mandatory requirement of having at least 1 member who is a Singapore Citizen or a Singapore Permanent Resident (PR). Since it is a virtual event, the infrastructure and conduct have to be designed and implemented in a way that is readily accessible for participants all over the world.

B. Operations Requirement

To support the 48 hours event, sufficient staffing is required to respond to i) participants enquiries; ii) any technical incidents; and iii) any other matter. To facilitate the handling of inquiries from the participants, a ticketing system based on Discord called "Tickets" [15] was used to manage participants' enquiry. As the combined prize pool for Top Prizes is worth SGD $57000, there is a need to verify further the validity of the winning team's CTF experience. It is in the Organising Committee's interest to ensure that the prize pool is given to deserving winners. A video interview will be conducted for the eligible winners (top 3 teams of each participation category) as part of the validation process.

C. Infrastructure Requirements

The infrastructure for the CTF event needs to be i) scalable; ii) highly available; and iii) globally accessible for the event to be successful. The Organising Committee took the "Cloud First" strategy [16] to meet the unique technical demands of running a CTF. Thus, a combination of cloud services was used. The infrastructure can be further divided into core and support infrastructure. The core infrastructure is entirely managed by the Organisting Committee and requires specific customisations due to the unique requirements of the CTF. Thus, customised codes were used for the core infrastructure. The support infrastructure relies heavily on commercial off-the-shelves services or products.

1) Core Infrastructure

The core infrastructure is meant to provide access of the

[1]Phase 2 refers to Singapore's COVID-19 response. More information about Phase 2 can be found here: https://www.gov.sg/article/moving-into-phase-2-what-activities-can-resume

CTF to the participants. It has two critical services to provide:

- CTF Platform Service - provides CTF administration related services. These services include activities from Pre-CTF, In-CTF and Post-CTF (as defined by Kucek and Leitner [17]).
- CTF Challenge Service - provides hosting services of the challenges. These services allow users to access the actual challenge environment and conduct attacks against it.

For both systems, they are hosted in the cloud. Depending on the nature of the challenge, specific challenges are hosted on specific Cloud Service Providers (CSPs). For example, challenges related to AWS Simple Cloud Storage (S3) are hosted on Amazon Web Services (AWS).

As highlighted by Rai et al. [18] container based infrastructure significantly reduces the resource requirements. Thus, the infrastructure design is heavily influenced to use containers as much as possible. Refer to Fig. 2 and Fig. 3 for the design of the system.

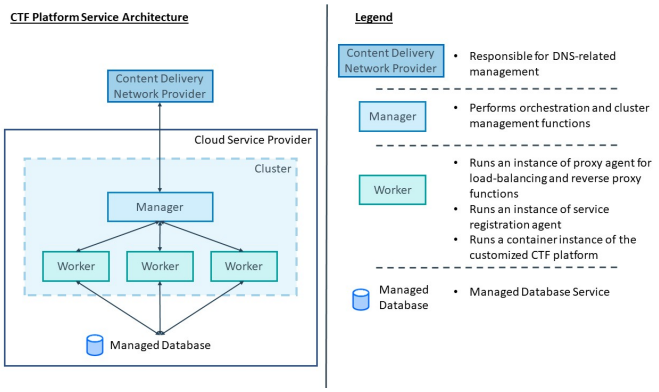

Fig. 2. System component(s) of the CTF Platform

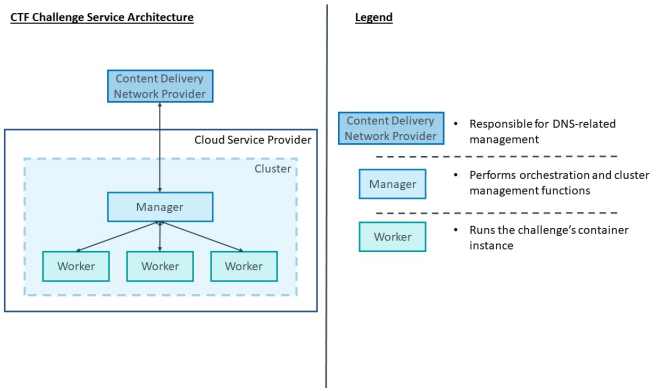

Fig. 3. System component(s) of the CTF Challenge Service

2) Support Infrastructure
The support infrastructure is to provide any other support to facilitate the conduct of the CTF. These services are (not restricted to): i) file hosting; ii) instant messaging; iii) video-streaming, and iv) word processor. A variety of Software As A Service (SAAS) solutions were used. For example, Discord, Google Drive, Google Docs, Youtube, Dropbox. The support infrastructure allows for instant communications and information to be quickly disseminated to the participants.

D. CTF Challenge Design

The challenges were developed with the following set of directions (based on the Organising Committee's institutional considerations):

- Reflective of real-world implementation and design
  To increase the learning value of each challenge, the narrative of the challenge and its corresponding design should be reflective of cybersecurity issues observed in real-world systems.
- Avoid hardware-related challenges due consideration of various COVID-19 measures and conduct of virtual CTF.
  Use of hardware in CTF challenges greatly increases the complexity of the competition administration (i.e. delivery of hardware, troubleshooting). Should there be a need for hardware-related challenges, it should be created in a way in which it is repeatable and consistent. For example, using the output of the hardware (i.e. network packet capture files) and use it as part of the challenge.
- Varying levels of difficulty
  As the participants range from tertiary students to working cybersecurity practitioners, challenges should be developed with varying difficulties to ensure that the participants of varying skill sets are able to participate in the CTF. This is to increase the engagement of the participants. Most challenges are designed to be accessible by all participation categories (Category 1/2/3). The impetus behind such design is to facilitate the Mastery Awards. The selection criteria for Mastery Awards is common throughout all 3 participation categories. The purpose is to identify teams who specialise in a certain niche. However, there are some challenges that are participation category-specific.
- Varied challenge domains
  A total of 11 different challenge domains were i) Binary Exploitation; ii) Cloud; iii) Cryptography; iv) Forensics; v) Internet of things (IoT); vi) Miscellaneous; vii) Mobile; viii) Open Source Intelligence (OSINT); ix) Reverse Engineering (RE); x) Social Engineering (SE); and xii) Web. This is to ensure variety and increase the exposure of cybersecurity issues in these domains.
- Consistent theme
  Having a consistent narrative for the challenges allows participants to follow through more easily. This is in line with Chung and Cohen's work [19], as they highlighted that having a story or theme that provides the glue between the challenges helps to keep the competitors involved in the competition.

The CTF event was designed with a shared challenge environment in mind. Thus, it will not provide a dedicated environment for each participating team. The primary

Fig. 4. Breakdown of platform activities by participation category

considerations behind such a design is to reduce cost and complexity of administering these challenges. The challenges will be planned to be released in the organisation's Github repository [20] after the CTF event. A total of 67 challenges were developed for the CTF event.

IV. CTF Competition Conduct

A total of 1405 participants (437 teams) registered for the event. The participants come from a total of 24 different countries (including Singapore). Due to unforeseen technical issue, the event was extended by 1.75 hours, lengthening it to a total of 49.75 hours. In addition, 1191 support tickets were raised (by participants) and resolved (by Organising Committee) during the event.

A. Comparison of CTF Platform Activities by participation category

There are three types of platform activities that are measured:

1) Correct Flag Submission: Number of successful flag submission (percentage of running total within the participation category)
2) Incorrect Flag Submission: Number of unsuccessful flag submission (percentage of running total within the participation category)
3) Hints Unlocked: Number of hints unlocked (percentage of running total within the participation category)

To better visualise the activities, the three measurements are normalised using the respective percentage of the running total within the participation category. Refer to Fig. 4 for the breakdown of platform activities by participation category. Notable Observation(s) are:

1) Unsuccessful flag submission activities for Category 1 peaks 4 hours from the start of the CTF, followed by Category 2 (7 hours) and finally, Category 3 (27 hours). This is likely due to the difference in playing strategy and CTF veterancy of participating teams.
2) There are no visually observable differences for successful flag submission and hint unlocking activities within the participation categories.
3) CTF platform activities are generally very low in late night and early morning hours (2am - 8am) of the day. However, on the first day, CTF platform activities were consistently high till late at night. This is likely due to the start of the CTF on Day 1 (4th December), 9pm. A notable observation for Category 2 participants is that they do have a tendency to stay "active" longer, as seen in the early hours of Day 2 (5th December).

B. Incidents / Observations made during the competition run

During the competition run, several incidents occurred which had potential impact or impacted the competition run. *The description, impact and action(s) taken by the organising committee of each incident are as listed.*

1) Inaccessible challenge files
   Due to the sudden spike in file access, the service provider blocked the challenge files access. Participants were not able to access the challenge files for approximately 1.5 hours. The organising Committee re-hosted the challenge files on another file hosting provider (AWS S3). Due to the downtime, the CTF is extended by 1.75 hours.
2) Local Internet Service Provider (ISP) outage
   A small number of participants reported internet connectivity issues. Competition conduct was not

impacted as the connectivity issues only affected a small group of users. The internet connectivity was restored shortly (https://cutt.ly/8bCwEZo) after the competition started. No action taken was taken by the Organising Committee.

3) Reports of cheating cases
   A small number of participants reached out to the organisers to report cheating cases and challenge leakages in forums. Suspected cheating teams were given a warning. Additional reviews and investigations were planned by the Organising Committee to be conducted, should the suspected teams qualify for any of the prizes. Since the suspected teams eventually did not qualify for any of the prizes, no further review or investigation was conducted. Thus, there was no impact on the competition execution. *Cheating cases such as plagiarism are also discovered in other CTF competitions. Vykopal et al. [21] investigated and discover patterns of plagiarism. They recommend strict rules to be announced to participants upfront.*
4) Suspected dummy teams
   Dummy teams are teams who did not participate actively during the CTF but yet incur huge negative scores. These teams are often suspected of unlocking hints without incurring cost on their "main" team. A few teams appeared to have incurred negative scores (significant value) towards the end of the competition. No impact on the competition execution as the suspected teams do not qualify for any of the prizes. Organising Committee disqualified suspected dummy teams. Organising Committee allowed for disqualified teams to directly appeal to the Organising Committee should the disqualification be wrongly made.
5) Interaction with OSINT Challenge Target
   To improve the realism of the OSINT related-challenge, a real-life target was used. However, some participants did not adhere to common Operational Security guidelines for investigations (not to interact with the target) and interacted with the target via social media. While there is no immediate impact on the competition, it may result in reputation damages to the Organising Committee. The Organising Committee issued statements to the participants not to interact with the target and to use solely what was already available on the internet. In addition, the Organising Committee apologized to the target and resolved the matter amicably.
6) Inaccessible scoreboard towards the end of the competition
   Towards the end of the CTF, participants were continuously accessing the scoreboard around the same time. As a result, the servers were overwhelmed and participants were not able to view the scoreboard for a short period of time. The Organising Committee re-scaled computing resources responsible for the CTF platform. The service recovered shortly after (approximately 15 minutes).

TABLE I
MEAN RATINGS FOR CTF EVENT

Rating	Category 1	Category 2	Category 3
R-1	4.0108	3.8235	3.6222
R-2	4.2473	4.3162	4.2889
R-3	4.1075	4.1029	3.9778

V. EVALUATION AND ANALYSIS OF THE CTF COMPETITION

A. Post-Event Survey - All Teams

The Organising Committee conducted a post-event survey towards the end of the CTF, and flags were given out when the survey was completed by the respective teams. The survey aims to understand how the competition fare and identify areas for improvement.

1) What is the rating for the CTF event?
   The event enjoyed a positive rating overall. A total of 3 different metrics were captured:
   - On a scale of 1 to 5, how would your team rate your experience in STACK the Flags? (as referred to as R-1 - "Experience Rating")
   - How was the overall conduct of STACK the Flags? (as referred to as R-2 - "Conduct Rating")
   - How would you rate the support provided by STACK the Flags's Organising Committee? (as referred to as R-3 - "Support Rating")

   There is a drop-down list of 5 options (value 1 - 5) for each of the above questions. The scores provided in Table I are the mean rating per participation category. The mean rating is calculated below (rounded to 4 decimal place) with a maximum attainable score of 5.
2) What is the impression of the CTF event?
   Mostly positive feedback (visualised using wordcloud [22]) were received for the CTF event. The list of questions and its associated word cloud as shown in Fig. 5, 6 and 7 allows us to infer the general impression of the CTF event:

Fig. 5. Question: What does your team like the most about STACK the Flags?

Fig. 6. Question: What are the area(s) that can be further improved?

Fig. 7. Question: Any other comments? You can leave a message for the Organising Committee too!

3) What type of challenges do the participants like?
The top 3 challenge domains are i) Open Source Intelligence (OSINT); ii) Miscellaneous; and iii) Web.
   - OSINT challenges are generally more well liked as it is a domain type with the lowest barrier of entry (difficulty of learning / picking up skills within the domain).
   - Miscellaneous challenges are often challenges that cannot be classified into other challenge domains within the CTF. Miscellaneous challenges are often designed to be unconventional challenges. Thus, they tend to be more ”fun”.
   - Web challenge domain is de facto for many CTFs. Thus, there is a great familiarity or expectation by the participants that CTFs will have web challenges.
4) What the participants have to say about?
The following list contains the summarised feedback provided by the participants. Positive comments or encouragements from the participants were not shown as the listing is focused on the means to improve the CTF. The points below were abstracted and summarised to convey the key learnings from the participants' feedback.

Feedback from all 3 participation categories:

- Use of an alternative file hosting service provider. There are known file-hosting sites which automatically block file downloads when there is a spike in traffic (as witnessed in the CTF event) and should be avoided. Participants suggested to have a backup file-hosting site available such as AWS S3 when the main file-hosting site becomes unavailable.
- Clearer challenge description and hints
- Challenges should be more directed/deliberate/focused
- Include educational/preparatory materials (tools/videos) as part of the CTF or within the challenge
- Training before/during the CTF
- Greater range of difficulties in challenges (especially on introductory ones)
- Improved CTF infrastructure (responsiveness, availability)

Feedback unique to Category 1 and 2:

- Prevent the registration of dummy teams
- Improve challenge file(s) naming convention
- Periodic release of hints (for unsolved challenges)
- Varied Discord channels for formal/informal conversations (use of voice channels, setting up channel for topic-specific conversation such as “music”)

Feedback unique to Category 1 and 3:

- Points should be more fairly distributed
- Improve reporting mechanism to report misconducts by participating teams (planting of fake flags/disqualify uncooperative teammates)

Feedback unique to Category 1:

- Longer CTF duration
- More communication options alternative to Discord
- Administrative instructions, and conduct information can be clearer
- Introduce controls to use smaller challenge files
- Challenge dependencies should be scoped and directed
- Provide earlier confirmation of event registration
- More variety of prizes

Feedback unique to Category 2:

- CTF to be conducted on the Weekday
- Shift Polytechnic students to category 3
- Clearer flag format and number of flag submission
- More guidance provided by the challenge setters during the CTF execution

Feedback unique to Category 3:

- Administrators should be more professional

B. *Winning Teams Interview*

A total of 9 interview sessions were conducted with the top 3 winning teams. While the purpose of the interview was to validate their participation in the CTF, feedback was sought to improve the CTF conduct. The summary of their feedback is highlighted below:

- "Gating" of challenges should be contained within their respective domains. "Gating" refers to challenge dependency. Kucek and Leitner [17] explain that dependency essentially means that solving one challenge is the prerequisite for accessing another. If possible, the depth of "gating" should be limited as a larger depth will cause the completion of the series of challenges to be "tiring" and difficult to follow.
- To reduce the amount of "guess-work" needed to solve challenges, there can be more "signposting" within the challenge. Chung and Cohen [19] highlighted that a well-designed challenge should lead the competitor through its own solution process. The challenge inherently provided the needed digital breadcrumbs for the participant to move towards the solution.
- Dynamic scoring should be more evident. During the CTF, the effects of dynamic scoring are not apparent. This address problems arising from competition organizers and challenge developers misunderstanding of the challenge's difficulty and ambiguousness. A more apparent dynamic scoring can address the market forces by reacting to the solves accordingly. Such incidents are not uncommon and have been observed in various CTF events. For example, such an issue was observed in Cyber Security Awareness Worldwide (CSAW) CTF 2013, whereby Kung and Cohen [19] shared that both challenge developers and competition organizers misunderstand the ambiguity of the challenge and how competitors would approach the challenge. This resulted in a drastic drop in solves for the challenge compared to other challenges in the same category and complaints.

C. Organising Committee's observation(s) on conducting virtual CTF

The following observations highlight key observations made by the CTF event's Organising Committee:

1) Challenges / Pain Points
   - Difficulty in assessing/conducting the investigation of cheating cases, validation of the participating team's CTF experience, and enforcing fair gameplay. For on-site CTFs, various controls can be implemented to reduce the risk of cheating, such as physical isolation of teams, network restrictions, or physical inspection. These on-site controls can be hard to implement for virtual CTFs. As a result, other controls such as video interviews of winners (especially for awards with a substantial prize pool) have to be conducted to validate winners' identity and participation authenticity.
   - Difficulty in validating participant's information - Lack of Know Your Customer (KYC) processes. It can be difficult to validate the information from foreign participants. For example, educational pathways in Singapore are different from those of the United States of America. The mapping of educational pathways to ensure fair participation can introduce significant overhead due to the potential combinations. Different countries have different systems to verify such information. Thus, as part of the control, the Organising Committee mandated the requirement of having 1 Singapore/PR in the participating team as a form of mitigating control. The assumption made here is that having a local representative allows for easier probe/conduct of investigation should there be a need.
2) Benefits
   - Significant cost reduction
     For physical events, additional costs such as venue and equipment rental and food have to be factored in.
   - Access to the wider community
     Virtual events allow the global community to access the event. For virtual CTFs, anyone with a working computer and internet access can participate. However, it may introduce unpredictability to the CTF demand (access to a bigger market), which translates to the cost (eventually) to provision the necessary computing resources.
   - Compliance with COVID-19 measures
     A virtual CTF event, is in general compliant with most COVID-19 measures. However, CTF organisers should to be mindful of the maximum size of social gathering affects the number of members in each team.
   - Reduced event administration
     Depending on the nature of the organisation, certain administration processes might be introduced, such as evaluation planning, hiring of additional staff to do crowd control (especially for large-scale events) and physical security for on site events. A virtual CTF takes place in the comfort of the participants' homes and these controls tend not to apply.

D. Challenges / Pain Points - Summary

1) Service outages by external entities
   For example, local ISP service outages.
2) Unfair gameplay related
   For example, cheating cases, uncooperative teammates, dummy teams, colluding, challenge leakages.
3) Challenge design related
   For example, challenge itself, description, hints, instructions, related namings, challenge files, flag format, flag submission, "gating" / dependencies may be unclear.
4) Infrastructure related
   For example, computing resources not provisioned adequately, inaccessible challenge files, unresponsive scoreboards.
5) Gameplay / Competition Design
   For example, uneven point distribution for each challenge, an unbalanced number of challenges per domain, the periodic release of hints (for unsolved challenges), lack of challenge difficulty ranges.
6) Lack of formal and informal communication alternatives
7) Lack of preparatory materials for the CTF
8) Difficulty in ensuring the validity of participants information (KYC)

E. Controls / Innovations / Recommendations

The following section discusses a list of proposed items that can be potentially considered by CTF organisers addressing the concerns raised by the participants and pain points observed from organising the CTF event (in the previous sections). Some of these areas are relatively new and not widely implemented/seen in CTFs. They have a varying degree of cost (time, human resources), and it may be too expensive to be implemented in actual CTF conduct. Financial costs are not included in the considerations for the proposed list below. In addition, the list is non-exhaustive; they are curated from a combination of observations made from popular CTF events and recommendations from the Organising Committee.

1) Use of Singpass - government-backed identity services [23]
   - Deters unfair gameplays (cheating and creation of dummy teams) and improves KYC processes. The assumption made here is that the use of official information endorsed by relevant authorities deters unfair gameplays. Use of official information allows participants to be identifiable. Reactive controls such as blacklisting of participants on future events can be enforced using this information.
   - Introduces complexity to the registration process. In addition, not all government have such digital services offering, and not all citizens may have access to such digital services (e.g. age requirement)
2) Applying Automatic Problem Generation (APG) techniques for CTF challenges.
   - As shared by Burket et al. [24], APG techniques create new versions of problems, called problem instances, that get distributed among teams. APG can ensure that each team receives a different flag for a given problem, mitigating the threat of copied or leaked flags
   - Encourages and improves the CTF experience authenticity as participants have to be able to complete the challenge.
   - Increased complexity for processing flag submission and challenge development. Also, not all challenges are suitable for APG.
3) Standardised CTF Administration and Challenge Development Guidelines
   - Refers to guidelines referenced internally/externally for the organisation and administration of the CTF. [2]
   - Addresses challenge, game-play and competition design-related issues. Avoid common mistakes if strictly adhered ("gating" issues, CTF scoring configurations such as dynamic scoring, unclear challenge description, hints, challenge itself and other potential incidents. Acts as Quality Assurance (QA) control for game-play, challenge and competition design.
   - May hamper innovation (it is common for challenge setters to have differing opinions on how CTF challenges should be developed). There is no one-size-fits-all guidelines available as the organisers often have a unique set of considerations in organising CTFs.
4) Use of Machine Learning (ML)/Artificial Intelligence (AI) to detect behavior deviations [3]
   - ML/AI is useful to detect deviations and provide first line of detection for potential participants behavior deviations from the "norms". Subsequently, the Organising Committee can investigate the deviations. Intervention is still needed due to the possibility of false positives.
   - Novel approach to improve fair game-play and deter unfair practices - can be used to detect potential dummy accounts and collusion between teams.
   - Increases complexity of infrastructure.

VI. Conclusion and Future Work

CTF events are useful means not just to educate but also to facilitate community growth. However, to actualise large scale CTF events require considerable amount of effort and resources. The information captured in this paper can be useful for organisers who want to organise events of a similar scale. In addition, the paper also highlights the impact of the COVID-19 pandemic on CTF conduct. It was observed that the COVID-19 pandemic has little impact on the design of the CTF. However, CTF organisers should still be mindful of the social gathering restrictions as they may have direct impact on the team size. This is assuming team members may gather physically to participate in the CTF together.

Moving forward, given the growing market need for cybersecurity professionals, CTF events will continue to be a "norm". In fact, companies recognise the value of CTF and, in some cases, use CTF events as part of their hiring requirements[4]. Thus, the need to innovate and improve CTF conduct becomes paramount. As such, the Organising Committee is keen to expand the scope and depth of post-event analysis by redesigning and building more targeted data pipelines (for example, challenge server interactions, server availability metrics/monitoring controls) in the next iteration of the CTF event. The primary motivation is to continuously improve CTF engagement and experience through data.

Acknowledgment

The authors would like to thank Chong Rong Hwa, Terence Teo, Lorraine Ong, David Quay, Bjorn Lim, Leon Chua, Winston Ho, Joel Peh and the CTF event's Organising Committee for their guidance and support to make this work possible.

[2]For example, i) https://cutt.ly/HbkYN1D; ii) https://cutt.ly/6bkYCYB and iii) https://cutt.ly/DbkYV8H. These best practices captured by the community are based on the writers' experience of organising CTF.

[3]Use of ML/AI to identity cheaters in online gaming (https://cutt.ly/obkSleA) or Anti-Money Laundering (AML) (https://cutt.ly/IbkSxYr) can be similarly applied to CTFs.

[4]A sample Job Description requiring CTF experience: https://www.amazon.jobs/en/jobs/1164503/penetration-testing-engineer.

REFERENCES

[1] K. Chung, "Live lesson: Lowering the barriers to capture the flag administration and participation," in *2017 USENIX Workshop on Advances in Security Education (ASE 17)*. Vancouver, BC: USENIX Association, Aug. 2017. [Online]. Available: https://www.usenix.org/conference/ase17/workshop-program/presentation/chung

[2] L. McDaniel, E. Talvi, and B. Hay, "Capture the flag as cyber security introduction," in *2016 49th hawaii international conference on system sciences (hicss)*. IEEE, 2016, pp. 5479–5486.

[3] M. Beltrán, M. Calvo, and S. González, "Experiences using capture the flag competitions to introduce gamification in undergraduate computer security labs," in *2018 International Conference on Computational Science and Computational Intelligence (CSCI)*. IEEE, 2018, pp. 574–579.

[4] K. Leune and S. J. Petrilli Jr, "Using capture-the-flag to enhance the effectiveness of cybersecurity education," in *Proceedings of the 18th Annual Conference on Information Technology Education*, 2017, pp. 47–52.

[5] E. L. Ouh and Y. Irawan, "Exploring experiential learning model and risk management process for an undergraduate software architecture course," in *2018 IEEE Frontiers in Education Conference (FIE)*. IEEE, 2018, pp. 1–9.

[6] E. L. Ouh, B. K. S. Gan, and Y. Irawan, "Did our course design on software architecture meet our student's learning expectations?" in *2020 IEEE Frontiers in Education Conference (FIE)*. IEEE, 2020, pp. 1–9.

[7] 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*, 2017, pp. 225–230.

[8] L. J. Hoffman, T. Rosenberg, R. Dodge, and D. Ragsdale, "Exploring a national cybersecurity exercise for universities," *IEEE Security & Privacy*, vol. 3, no. 5, pp. 27–33, 2005.

[9] N. Childers, B. Boe, L. Cavallaro, L. Cavedon, M. Cova, M. Egele, and G. Vigna, "Organizing large scale hacking competitions," in *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. Springer, 2010, pp. 132–152.

[10] CTFtime.org - All about CTF (Capture the Flag). [Online]. Available: https://ctftime.org

[11] Google CTF. [Online]. Available: https://capturetheflag.withgoogle.com/

[12] Defcon CTF. [Online]. Available: https://oooverflow.io/

[13] Pico CTF. [Online]. Available: https://picoctf.org/

[14] HSCTF - The First CTF by High Schoolers, for High Schoolers. [Online]. Available: https://hsctf.com/

[15] Tickets - The Best Tickets Bot for Discord. [Online]. Available: https://ticketsbot.net/

[16] Is it about time you develop a Cloud First strategy? [Online]. Available: https://venturi-group.com/develop-cloud-first-strategy/

[17] S. Kucek and M. Leitner, "An empirical survey of functions and configurations of open-source capture the flag (ctf) environments," *Journal of Network and Computer Applications*, vol. 151, p. 102470, 2020.

[18] A. S. Raj, B. Alangot, S. Prabhu, and K. Achuthan, "Scalable and lightweight {CTF} infrastructures using application containers (pre-recorded presentation)," in *2016 {USENIX} Workshop on Advances in Security Education ({ASE} 16)*, 2016.

[19] K. Chung and J. Cohen, "Learning obstacles in the capture the flag model," in *2014 {USENIX} Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*, 2014.

[20] GovTech CSG Stack the Flags 2020. [Online]. Available: https://github.com/GovTech-CSG/stack-the-flags-2020

[21] J. Vykopal, V. Švábenskỳ, 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*, 2020, pp. 752–758.

[22] Transform your text into word clouds. [Online]. Available: https://worditout.com/

[23] SingPass - Your Improved Digital ID. [Online]. Available: https://www.singpass.gov.sg/main

[24] J. Burket, P. Chapman, T. Becker, C. Ganas, and D. Brumley, "Automatic problem generation for capture-the-flag competitions," in *2015 {USENIX} Summit on Gaming, Games, and Gamification in Security Education (3GSE 15)*, 2015.