Our Experiences on the Design, Build and Run of CTF

Jun-Gyu Park[*]
SysCore Lab.
Sejong University
Seoul, South Korea
wnsrb3001@gmail.com

Sang-Hoon Choi[*]
SysCore Lab.
Sejong University
Seoul, South Korea
csh0052@gmail.com

Hyun-il Kim[**]
Dept. of Conversions Science
Kongju National University
Kongju, South Korea
hyunil89@kongju.ac.kr

Hong Dowon[***]
Dept. of Applied Mathematics
Kongju National University
Kongju, South Korea
dwhong@kongju.ac.kr

Ki-Woong Park[†]
Dept. of Computer and Information Security
Sejong University
Seoul, South Korea
woongbak@sejong.ac.kr

***Abstract*— CTF is well-known for its approach to attracting more students to the field of computer security. Competition in the CTF can create competent and diverse cybersecurity personnel. For this reason, computer security education for high school students is becoming increasingly important. In this paper, we describe our experiences in a second year of designing, building, and running a CTF to provide effective computer security education for middle and high school students. Our CTF has three factors that observation on flag sharing, providing two hints, and adjusting difficulty levels of challenge. In order to verify the validity of the designed CTF, we ran a CTF for 87 students in middle and high school in 2017 and 2018. Then we analyzed the above three factors based on the collected data.**

Keywords—Capture the Flag, Education, Cyber Security

I. Introduction

Capture The Flag (CTF) is well-known for its approach to attracting more students to the field of computer security [1, 2, 3, 4, 5]. Competition in the CTF can create competent and diverse cybersecurity personnel [6]. For this reason, computer security education for high school students is becoming increasingly important [7].

We designed CTF to provide effective computer security education for middle and high school students. Our CTF is a Jeopardy style competition that solves the challenge to obtain the flag and authenticates the flag to score points [8]. Because the online competition is easy for beginners to access [9], we have adopted the online CTF competition. Each challenge has the same flag. Because of this, it is possible to share the flag obtained by other teams and to submit it. We designed the coin system to observe such flag sharing. To access each challenge, participants must open the challenge of paying coin and participants cannot submit a flag for a challenge that is not open. When attempting flag sharing to submit the correct flag of a challenge that is not open, the corresponding behavior is logged.

We provide two hints to each challenge to assist beginners in resolving the challenge. Providing hints is not a new idea [10], but we do not offer hints without restriction. The initial hint is locked, and you can open it if you want support for the challenge. Even if a flag is submitted for the same challenge, the participant who opened the hint gets a lower score than the participant who did not open the hint.

(a) CTF in 2017

(b) CTF in 2018

Fig. 1. CTF for Middle and High School Students in 2017 and 2018

It is also important to look for a good way to involve beginners in the CTF [10, 11, 12]. However, because of the difficulty levels that does not care about beginners, beginners' access to CTF is limited. To mitigate entry barriers to CTF, we provide challenges of suitable difficulty levels that

†: Corresponding Authors

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIP) (NRF-2016R1A4A1011761) and supported by Institute for Information & communications Technology Promotion(IITP) grant funded by the Korea government(MSIT) (No.2018-0-00420, Development of Serverless Cloud Computing technology for resource allocation and usage measurement by API call unit)

participants with insufficient security knowledge can address. Each challenge was configured so that it could be solved without using a tool as much as possible. In addition, in some cases it is necessary to use a tool, we have provided tools to help participants solve the challenge.

In this paper, we analyze the collected data to check the validity of the designed CTF. We ran our CTF for middle and high school students for two years as shown in Fig 1. Our CTF has three factors that observation on flag sharing, providing two hints, and adjusting difficulty levels of challenge.

The compositions of this paper are as follows. In Section 2, we describe the three factors of the CTF that we designed, built and ran. Section 3 describes the data analysis results collected to verify the validity of each factor. Finally, Section 4 describes the conclusion.

II. CTF System for Middle and High School Students

This section describes the Jeopardy type CTFs held in 2017 and 2018. Our CTF has three factors: coin system for observing flag sharing, two hints for supporting challenge resolution, and adjusting difficulty levels of challenge. Our CTF designed to effectively educate computer security for beginners who do not have a high level of security knowledge.

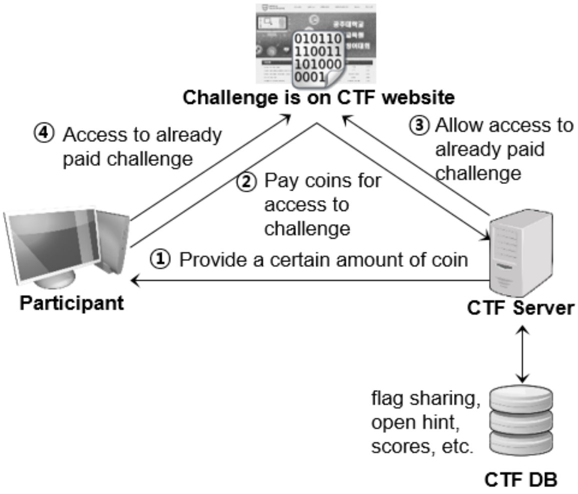
Challenge is on CTF website
④ Access to already paid challenge
③ Allow access to already paid challenge
② Pay coins for access to challenge
① Provide a certain amount of coin
Participant
CTF Server
flag sharing, open hint, scores, etc.
CTF DB

Fig. 2. Our CTF System

A. Coin System

Coin system can observe flag sharing, which share the flag obtained by other teams and submit it. The coin is a virtual currency that must be paid to access each challenge in our CTF. Participants must access the challenge in order to get scores by submitting a flag. In addition, Participants must pay a coin to access the challenge as shown in Fig 2. The participant cannot solve the challenge because he cannot access the challenge if he does not pay a coin. You pay only once for each challenge, and the number of coins to pay per difficulty levels is different. If the correct flag of the challenge that did not pay the coin is submitted, the behavior is to be logged, the submission fails, and scores are not acquired. However, this method has the limitation that it cannot observe flag sharing of a challenge that has already been paid.

B. Provide two Hints

For each challenge, two hints written by the submitter are provided to help solve the challenge. The initial hint is in the lock state and participants can open the hint if participants need help with the challenge resolution. However, it is not fair that participants who open the hint and those who do not open the hint get the same score. Thus, even if the same challenge is resolved, the participant who opened the hint is scored lower than the participant who did not open the hint. Also, participants who open both hints get lower scores than participants who open one hint.

C. Adjust Difficulty Levels of Challenge

Depending on the difficulty levels of the challenge in the CTF, beginners are greatly affected. Therefore, we provide challenges that adequately includes the level of difficulty to solve even those who do not have knowledge of security. In order to lower the entry barriers to CTF, each challenge was configured so that it could be solved without the use of tools. However, the challenge was also created that requires the use of a tool to form an appropriate level of difficulty. Therefore, when it is necessary to use a tool inevitably, we tried to solve the difficulty of solving the challenge by providing the corresponding tool. The difficulty levels of challenge were classified into three (easy, medium, hard). Overall, about four-fifths of the security challenges were easy and medium.

III. Lessons Learned

To validate the designed CTF, we ran our CTF for 87 middle and high school students in 2017 and 2018. They studied computer security theory and practice in advance. The goal of the designed CTF is to learn by themselves and to gain knowledge of security techniques.

A. Flag Sharing Problem

By including the coin system for observing the flag sharing in the CTF, we were able to collect data on flag sharing. Analysis of data collected from two CTFs resulted in flag sharing. As shown in Table I, submissions through flag sharing occurred 9 times in 2017 and 100 times in 2018. The number of students who submitted the shared flag was 4 out of 87(4.59%) in 2017, and 18 out of 87(20.68%) in 2018. According to the analysis results, flag sharing occurred in the CTF, and the number is never small. We want participants to learn and accomplish themselves through the CTF, but there are participants who try to solve the challenge using the wrong way. In addition, the occurrence of flag sharing in CTFs where fair competition is important should never be interpreted lightly and the Organizer should consider measures to prevent it.

TABLE I. Flag Sharing Try Count and Number of Malicious Participants in 2017 and 2018

year	***Flag Sharing Try Count***	***Number of Malicious Participants***
ctf_2017	9	4(4.59%)
ctf_2018	100	18(20.68%)

B. Low Practicality of Hint

The participants were given two hints to support the challenge solution. To verify the validity of the hint, data were collected at opening the hint in each challenge. We analyzed whether the challenge that hints were opened was resolved. As a result of the analysis, the ratio of unresolved is 75.5% in 2017 and 75.6% in 2018. These results indicate that the hints we provided were not useful to the participants. Although the organizer provides hints to the participants from the organizer's point of view to support the challenge resolution, the hint may not actually be helpful. This indicates that there is a difference of views on challenge between the organizer and the participant. When producing hints, the organizer should look at the challenge from the perspective of the participant.

C. High Score Deviation

We analyzed the final scores of the participants after the competition to ensure that the difficulty levels of the challenge were properly adjusted. The analysis method performed Kolmogorov-Smirnov normality test using the statistical program SPSS 25.00. The hypotheses for the normal distribution are as follows.

H_0: Participant scores follow a normal distribution

H_1: Participant scores do not follow a normal distribution

The maximum number of points that can be obtained if all the challenges are resolved is 7,000 in 2017 and 10,200 in 2018. As shown in Table II, the result of the competition was 794.94 on average in 2017 and 754.617 in standard deviation. In 2018, the average was 1522.76 and the standard deviation was 1604.081. In our CTF, both the 2017 and 2018 average scores are very low compared to the total score, and the standard deviation is high. When the standard deviation is 0, it means that the scores of the participants are all the same, and the larger the standard deviation, the more the scores are away from the average. In addition, since the significance level value is 0.000, which is less than 0.05, you can reject the null hypothesis of following a normal distribution and draw the conclusion that you do not follow a normal distribution. Therefore, there is a large variation in scores among the participants and a great difference in difficulty levels of challenge per individual. The results confirm that the difficulty levels of the challenge have not been properly adjusted. All scores cannot be the same because of differences in knowledge levels among participants. However, for effective security education, it is necessary to reduce the score difference between the participants through appropriate levels of difficulty adjusting.

TABLE II. Kolmogorov-Smirnov Normality Test

		Score_2017	***Score_2018***
N		87	87
Normal Parameters	Mean	794.94	1522.76
	Std. Deviation	754.617	1604.081
Most Extreme Differences	Absolute	0.182	0.232
	Positive	0.181	0.232
	Negative	-0.146	-0.176
Kolmogorov-Smirnov Z		0.182	0.232
Asymp. Sig. (2-tailed)		0.000	0.000

IV. Conclusion

In this paper, we describe the CTF that was designed, built and ran to effectively educate computer security and inspire security interest. We designed a coin system to observe flag sharing, provided beginners with hints to support the challenge resolution, and adjusted difficulty levels of challenge to ease entry barriers. In our CTF, flag sharing was happening and the hints we provided were not conclusive to the participants. Also, it was not possible to provide effective security training to the participants with the challenge difficulty levels adjustment mistake. We will strive to build a CTF platform that enables effective security training through the experience of such CTF operations.

References

[1] Martin Carlisle, Michael Chiaramonte, and David Caswell, “Using CTFs for an Undergraduate Cyber Education.” 2015 USENIX Summit on Gaming, Games, and Gamification in Security Education, August 2015.

[2] Tom Chothia and Chris Novakovic, “An Offline Capture The Flag-Style VirtualMachine and an Assessment of Its Value for Cybersecurity Education.” 2015 USENIX Summit on Gaming, Games, and Gamification in Security Education, August 2015.

[3] Adrian Dabrowski, Markus Kammerstetter, Eduard Thamm, Edgar Weippl, and Wolfgang Kastner, “Leveraging Competitive Gamification for Sustainable Fun and Profit in Security Education.” 2015 USENIX Summit on Gaming, Games, and Gamification in Security Education, August 2015.

[4] Z. Cliffe Schreuders and Emlyn Butterfield, “Gamification for Teaching and Learning Computer Security in Higher Education.” 2016 USENIX Workshop on Advances in Security Education, August 2016.

[5] Giovanni Vigna, Kevin Borgolte, Jacopo Corbetta, Adam Doupe, Yanick Fratantonio, Luca Invernizzi, Dhilung Kirat, and Yan Shoshitaishvili, “Ten Years of iCTF: The Good, The Bad, and The Ugly.” 2014 USENIX Summit on Gaming, Games, and Gamification in Security Education, August 2014.

[6] Pusey, P., Gondree, M., and Peterson, Z, “The outcomes of cybersecurity competitions and implications for underrepresented populations.” IEEE Security & Privacy 14. 6, 90–95, 2016.

[7] E. Stobert, E. Cavar, L. Malisa, and D. Sommer, “Teaching Authentication in High Schools: Challenges and Lessons Learned.” 2017 USENIX Workshop on Advances in Security Education, August 2017.

[8] Andy Davis, Tim Leek, Michael Zhivich, Kyle Gwinnup, and William Leonard, “The Fun and Future of CTF.” 2014 USENIX Summit on Gaming, Games, and Gamification in Security Education, August 2014.

[9] Burns Tanner J., Rios Samuel C., Jordan Thomas K., Qu Qijun, and Underwood Trevor, “Analysis and Exercises for Engaging Beginners in Online CTF Competitions for Security Education.” 2017 USENIX Workshop on Advances in Security Education, August 2017.

[10] Jan Vykopal and Milos Bartak, “On the Design of Security Games: From Frustrating to Engaging Learning.” 2016 USENIX Workshop on Advances in Security Education, August 2016.

[11] Kevin Chung and Julian Cohen, “Learning Obstacles in the Capture The Flag Model.” 2014 USENIX Summit on Gaming, Games, and Gamification in Security Education, August 2014.

[12] Jelena Mirkovic, Aimee Tabor, Simon Woo, and Portia Pusey, “Engaging Novices in Cybersecurity Competitions: A Vision and Lessons Learned at ACM Tapia 2015.” 2015 USENIX Summit on Gaming, Games, and Gamification in Security Education, August 2015.