StarsCTF: a Capture the Flag Experiment to hack Player Types and Flow Experience

Divina Naiara Vitorino[1], Geiser Chalco[2], Ig Ibert Bittencourt[3]

Abstract

Keywords: *CTF, cybersecurity, gamification, flow theory, player types*

A cybersecurity professional is expected to have a range of skills and abilities in order to have an ideal performance as a professional. In order to increase the engagement of professionals and students, gamification has become a powerful ally. In this study, we present StarsCTF, a Capture the Flag designed to assess player types and their levels of engagement during the gaming experience. In a paired experiment, the individual Jeopardy format (called Open World) was used and a new mode was developed, including new game elements (called DMC). Our results show that the Achievement and Immersion profiles were the most positively impacted due to the presence of game elements that favored these profiles. Open World mode performed better than DMC, so the possibility that freedom to solve challenges in a random order is an important factor in the progression of the competition is being evaluated.

[1] Pós-Graduanda em Computação Aplicada à Educação, USP, divina.vitorino@usp.br

[2] Orientador, UFAL, geiser@usp.br

[3] Orientador, UFAL, ig.ibert@ic.ufal.br .

Cite as: Vitorino, D. & Chalco, G. & Bittencourt, I. (2020). StarsCTF: a Capture the Flag Experiment to hack Player Types and Flow Experience. Anais dos Trabalhos de Conclusão de Curso. Pós-Graduação em Computação Aplicada Educação Instituto de Ciências Matemáticas e de Computação. Universidade de São Paulo.

Introduction

Cybersecurity is the area within Information Technology responsible for protecting devices, as well as the information stored on those. Therefore, it is the responsibility of this professional to ensure the security of the entire environment (networks, applications, information, operating systems) as well as the education of the end user [Kaspersky 2020]. Threats like phishing (theft of information or money), Ransomwares (machine is encrypted after the installation of malicious software) and denial of service attacks (to damage the target company's infrastructure) [Alerta Security 2018] are just a few examples of the challenges faced by professionals in this area. From 10 organizations in Latin America, four suffered a security incident in the last 24 months [Deloitte 2020].

According to research conducted by the Information Systems Audit and Control Association (ISACA), IT knowledge and hard skills (30%) are the second biggest gap on cybersecurity professionals. The estimated time to fill an open position is between three and six months. On the other hand, the same survey also found that the level of confidence in preparing students at universities for the real problems is low (46%). Despite this, 64% of Latin companies require a university degree to fill an entry-level position. Currently in Brazil, registered with the Ministry of Education (MEC), has 80 Information Security undergraduate courses which 63 are active, 18 of which are online. The dropout rate on high degree courses in Information Security in 2018 was 36.6% [BRASSCOM 2019].

In order to increase the engagement of students and cybersecurity professionals in their studies, a proposed solution is the use of gamified environments. The most accepted definition of gamification is the use of game elements in non-game contexts [Deterding et al. 2011]. But gamification and games do not share the same meaning. For Zimmerman (2004), the word game reflects a concept and not a closed category with established standards. However, it has more formal rules than playing, such as: (i) voluntary participation, (ii) rules (iii) take the player to a fantasy world, (iv) Confrontations - individual or group and (v) Outcome - quantified reward for classifying the player's performance [Zimmerman 2004] .

The use of gamification in cybersecurity enables the training of practical skills in a safe environment, developed for learning and which allows trial and fail. This learning method, called Challenge Based Learning, allows the participant to propose solutions to a presented problem, thus encouraging the development of soft skills, such as the ability to solve problems. As it is a complementary activity, there is (in most cases) a pedagogical schedule to be followed, allowing the approach of several subjects, going beyond the content studied. In this scenario, the teacher has more of a tutor role, with the objective of helping the participant to reach the goal [Mansurov 2016].

In this study, we cover the use of the gamified environment called Capture the Flag (CTF) and its impacts on engagement. Capture the Flag is a Cybersecurity competition to solve tasks. The resolution of these tasks is called “flag” and should be submitted at the server that is hosting the competition to earn points and can be played individually or in teams. The competitions can be in online or in-person format, usually

within events. They are usually organized independently by information security communities or within schools and universities [Brown 2019].

The aim of this study was to assess how each player type is impacted by the Capture the Flag experience by analyzing their levels of engagement using the Flow experience and Player type assessment as metric. The flow experience helps to understand how engaged the participant was in the activity and whether it was truly enjoyable and memorable [Mirvis and Csikszentmihalyi 1991].

Our research findings identified that the game elements used satisfy the Achievement and Immersion player types. Socializer was not favored in this game mode. The Open World mode (traditional gamification) performed better than the DMC environment. We found that the participants were unable to advance a medium-level cryptography challenge. Therefore, the possibility of solving challenges out of order can have an impact on the player's performance.

This paper is organized as follows: in Section 2, a background with the History of Capture the Flag and its definition. Also the works related to gamification, cybersecurity and flow. Section 3 presents the definition of Gamification and section 4 the definition of the Flow Theory. Section 5 contains the methodology and execution of the experiment. Section 6 presents the analysis, interpretation of the results and limitations of the study. In part 7, the Conclusion and Future Works.

2. Background

2.1 History of Capture the Flag

The first Capture the Flag competition happened in 1996 at a hacker convention named DEF CON, at Las Vegas, Nevada. The competition had occurred since then, but only in 1999 there was a formal format with a scoreboard, that was made manually by judges. At this edition there were only four teams [DEF CON Communications [S.d.]]. DEF CON is an annual convention created by Jeff Moss that had its first edition in June 1993 and not only brings together Information Security professionals, researchers and students, but also journalists, lawyers, public government employees and so on. The event consists of lectures from various segments, labs (called villages – each one has a specific subject, like offensive or defensive security), workshops and lots of activities running simultaneously [Fahs 2019].

In Brazil, the first registered competition happened in 2004 at the H2HC – Hackers to Hackers Conference, in Brasilia, DF and was opened to the general public (conference attendees and people that connected through an external connection with a server that hosted the challenges). Created by Rodrigo Branco and Filipe Balestra, H2HC is the oldest Brazilian Hacker Conference. The event occurs annually in São Paulo and has technical lectures about Information security from intermediate to advanced level. According to the organizers the main objective of promoting the CTF competition is to

encourage the community to collaborate and evolve productively. This is so important that the challenges are developed by volunteers (verbal information).[4]

Figure 2.1.1. First edition's H2HC Site [Internet Archive 2004]

BSides SP has a 24-hour CTF. BSides is an event about Information Security and hacker culture to share information between researchers, professionals and students from all ages. The format is inspired by Security BSides conferences that occur in several countries around the world. Here in Brazil the conference was created by Alberto Fabiano (*in memoriam*), Anchises Moraes, Ranieri Romera e Thiago Bordini and occurs annually in São Paulo since 2011. In 2012, the adoption of the name BSides occured [Garoa Hacker Clube 2012].

Figure 2.1.2.First BSides editions numbers [Anchises Moraes 2013]

CryptoRave also has a 24-hour CTF organized by the security community. CryptoRave is an annual conference organized using crowdfunding with the purpose of disseminating widely concepts of privacy, internet freedom and digital security. It was inspired by the international movement called Cryptoparties [Cryptorave 2020]. The parties have a do it yourself format, what makes possible a massive replication around the world.

[4] Rodrigo Branco and Filipe Balestra, H2HC organizers on August, 2019

Figure 2.1.3. Site for Cryptorave São Paulo's First Edition ["CryptoRave 2014 - 24 horas pela liberdade e privacidade na rede" 2014]

The first Roadsec CTF was in 2014 and it is called Hackaflag. It was a local competition, so only the attendees that were on the event could join. Since 2017 it has an online phase in addition to the traditional local model. Roadsec was idealized by Anderson Ramos and is a traveling event that occurs annually in several cities of Brazil. In each city there is a competition and all the winners go to the finals in São Paulo, where the winner of the year is known. In 2020, due to COVID-19 Hackaflag takes place monthly at online events (verbal information).[5]

Figure 2.1.3.Announcement of the Hackaflag final at Roadsec São Paulo 2014[Jovem Nerd 2014]

A new competition emerged in 2020, called Ultimate Hacker Championship (UHC). Conceived by Igor Rincon and Carlos Vieira, the competition takes place online weekly and is broadcast live on the social network Twitch [Equipe TecMundo 2020].

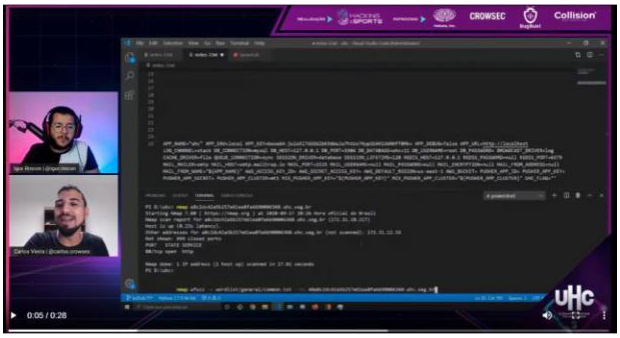

Figure 2.1.4.Streaming the UHC CTF competition on Twitch

There are several local CTF competitions in other Brazilian states that occurs inside conferences, i.e AraHacker (Arapiraca – Alagoas), JAMPASEC (João Pessoa –

[5] Information provided by Boot Santos, Hackaflag organizer in August 2019.

Paraíba), CAJUSEC (Aracaju – Sergipe), Darkwaves (Natal – Rio Grande do Norte)[6], BHACK (Belo Horizonte – Minas Gerais) and also online competitions, often announced at CTF Time [CTFtime team 2012].

2.2. Capture the Flag

The Capture the Flag (CTF) is a competition where the main purpose is to exploit or defend vulnerabilities of a system or application. CTFs are competitions composed of several challenges (commonly called challs) and the main objective is to find the flag that generally can be hidden inside files, pieces of source code, images and so on. There are used Information Security topics to build the challenges, i.e Cryptography, Steganography (encrypted messages hidden on images), Forensic, Reverse Engineering, Mobile Device Security, Web, etc [McDaniel et al. 2016].

The CTF can be played individually or the participant can be part of a team. There are four types of CTF competitions: Jeopardy, Attack/Defense, Mixed and King of the Hill (Table 1.2.1).

Table 2.2.1 CTF Types

Jeopardy	Attack/Defense	Mixed	King of the Hill (KoTH)
A set of categorized tasks. The more complex the task, the higher the score. When the competition ends, the winner is the team (or player) that has the largest amount of points.	Each team has a set of hosts with vulnerable services. The team has time to prepare softwares to correct vulnerabilities and to develop exploits (malicious software). The team must protect their own hosts and attack the opponent to save points.	When both Attack/Defense and Jeopardy are mixed at one competition, like the iCTF, organized by University of California	The objective is to gain the control of one or more hosts. After that occurs, the team that could do it is responsible for its defense. In case of a new invasion, the attacking team becomes a defender. [Bansal 2019].

The rules for the competition may vary from one to another since there is no standard for it. The organization can choose the rules that fit better for the CTF event.

2.3. Related Work

The use of Capture the Flag as an engagement tool in the study of Cybersecurity has been showing good results in different scenarios. A case study proposed by Feng(2016) with 51 students using the game element narrative, concluded that students had a positive

[6] They have a competition called CTW – Capture the Wave. It is an event focused on security for wireless networks - http://www.darkwaves.zone/ctw.html

experience with this format collecting data using a survey. The narrative was built based on a known book story (the Divergent series) and as the story progresses, there is an increase in the degree of difficulty of the challenges. The author did not explore the possibilities of developing a specific story for this event or make any analysis involving player types and flow experience using validated frameworks [Feng 2016].

Ros et al. [Ros et al. 2020] conducted a quasi-experiment carried out with 248 students of Computer Science in the discipline of Cybersecurity, concluding through statistical analysis that there is a correlation between better grades and participation in extracurricular activities. The activity, conducted in an online format and with optional participation, was designed using Kopler's four degrees of freedom (exploring the scenes, making mistakes, testing identities and improving strategies) and the constructivist learning theory. To stimulate the construction of mental models, the metaphor strategy was used. At the end of the experiment, it was found that in addition to having higher grades, the group of students who chose to participate had less tendency to abandon the discipline. The authors did not evaluate player types and flow experience using validated models.

Kam et al. [Kam et al. 2020] conducted an experiment with 133 undergraduate students about the importance of Ethical Hacking using SQL Injection exercises, showing that flow and task significance had significant effects on students' motivation. The study suggests that the use of flow for providing fun and enjoyment, is an element that can help to engage students and cybersecurity professionals in learning a more complex content. The authors explored a single topic (SQL Injection), so the students who have more knowledge in it will consequently get better grades. To evaluate the Flow state, a questionnaire was created and validated internally, and the player type was not evaluated.

Nguyen et al. [Nguyen et al. 2018] conducted a literature review on Capture the Flag live competitions identified the ten biggest problems in this format (regardless of style, Jeopardy, Attack-Defense or Mixed) and proposed an analysis scheme. We considered using the model to verify the adherence of our scenario, however the authors did not present any form of validation of the construct and the form of calculation[Katsantonis et al. 2017]. Nguyen and colleagues (2018) argue that Information Security should have a specific pedagogical theory, due to the different characteristics of the area. This theory should be oriented to collaborative learning, the training context must connect with the knowledge acquired by the learner and learning focused on experimentation and communication. In this study they also expose the lack of empirical evidence and evaluation information in many papers.

A deeper analysis at an experimental level on how Capture the Flag can be a powerful tool to engage students is needed. The usage of statistically validated psychometric models can help to collect more assertive data and consequently improve the design of gamification experiences. As far as we know, our study is the first that analyzes the player type of the CTF player.

3. Gamification

Gamification is the use of game elements in contexts that are not games. A non-game context is a context where the main objective is not entertainment [Deterding et al. 2011]. The game differs from play due to the existence of clear rules and objectives, since playing is usually improvised and with little or no organization. The first registered use of the Gamification term was in 2008, but the massive adoption occurred only in the second half of 2010. There are two types of gamification: the extrinsic, where known game elements (like points, badges and progress bars) are developed at the environment and the intrinsic that has the objective of motivating and engaging users [Marczewski 2015]. The game elements are elements found in most, but not necessarily all games and are one of the necessary blocks to build a memorable experience for the player.

However, it is important to consider that not all players have the same motivation to play. In order to evaluate and classify the various types that exist, studies were conducted, considering the different aspects of a player's personality (like behaviors, pleasures). Bartle's (1996) model focuses on player behavior and has four categories (i) Killers, (ii) Achievers, (iii) Explorers and (iv) Socializers. Based on Bartle's player types, Yee (2006) proposes a more detailed model, focused on behavior and preferences, with three main components and ten subcomponents: (i) Achievement (Advancement, Mechanics, Competition), (ii) Social (Socializing, Relationship, Teamwork) and (iii) Immersion (Discovery, Role-playing, Customization, Escapism). Also, this study shows a strong correlation between motivations and gender [Dixon 2011]. Nacke and colleagues (2011) developed the BrainHex model, that uses player satisfaction and neurobiological mechanisms. This model, that suggests analyzing the players as archetypes and the experience individually, has seven categories (i) Seeker, (ii) Survivor, (iii) Daredevil, (iv) Mastermind, (v) Conqueror, (vi) Socializer and (vii) Achiever [Nacke et al. 2014].

Questionnaires are applied to know and evaluate a player's type. In this study, the Brazilian questionnaire QPJ-BR was used to conduct evaluations of this type. QPJ-BR stands for Questionário de Perfil de Jogador – Brasil and is a validated adapted version from Yee's Player Types. It uses the same three main components (Achievement, Immersion and Socializer) to classify the player. The translation was done with the help of nine judges and each item was approved by two of them. In case of disagreement, a third one evaluated, as a tiebreaker criterion. The adaptation was made observing the cultural and linguistic aspects, since the main objective was to be a comprehensive questionnaire for any type of games, regardless of platform. After the translation, a linguistic validation was conducted by judges that were not specialists in player's typologies and also a face validity, to make sure that all the components and subcomponents from Yee's original model were covered [Andrade et al. 2016].

4. Flow Theory

The Flow state is used to define an optimal experience. These experiences represent the moment of the overcoming of a complex task [Mirvis and Csikszentmihalyi 1991]. During the flow, all the attention is directed to achieve the goal. According to

Csikszentmihalyi (1991), for an activity to drive the participant to the flow state, it is necessary that it has the following characteristics: (i) clear objectives, (ii) immediate feedback, (iii) tasks with the possibility of completion, (iv) immersion that removes the concerns, (v) high concentration on the task, (vi) a sense of control of the own actions,(vii) ignore feelings (like hunger and pain), (viii) change of the conception of time and (ix) autotelic experience. These characteristics are as known as dimensions.

The proposed model shows the psychological states that are activated according to the stimulus that is received during the performance of the activity (Figure 4.1). The reaction varies according to the balance between the required skills and the proposed challenge. The closer to equilibrium, the greater the chances of reaching the flow state. If this state is reached, the individual experiments specialize sensations (to be capable of executing a task with more knowledge), pleasure and satisfaction, indicating that internal expectations have been met.

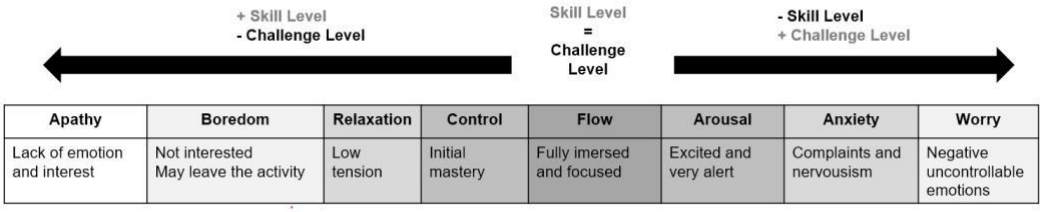

Figure 4.1. Flow Emotional States

Since Flow is an experience, a method is needed to measure it. To perform this measurement, the Flow State Scale is one of the available validated resources. This questionnaire aims to measure the flow state in several activities and the questions reflect all the nine Csikszentmihalyi's dimensions.

In order to evaluate the Flow, two measures are necessary: (i) Dispositional Flow Scale (DFS): Questionnaire used to measure the tendency to experience flow before an activity, and (ii) Flow State Scale (FSS): Questionnaire used to assess whether the participant reached the flow. In total, there are 36 questions for each questionnaire, four for each dimension of the flow. For more accurate results, the ideal is that the assessment is made from recent experiences [Jackson and Eklund 2002].

5. Material and Methods

This work is framed as applied research in which our theoretical contribution covers an exploratory study in the scientific literature to elaborate a gamification design for CTF events based on the conditions of flow theory. We also implemented and evaluated this design through empirical study. In this sense the research methodology approach during this work was conducted as a Paired Experiment Design. The paired experiment evaluates two measures of the same participant under different conditions, usually called treatment and control. This method was chosen to reduce the variability of responses among those involved in the experiment [Hanson [S.d.]].

5.1. Design

There were two Capture the Flag designs in two sessions (event Day 1 and event Day 2). The former design, called Open World, was a traditional Gamification format individual Jeopardy-style CTF with challenges developed by instructional designers. The latter design was called DMC, which stands for Dynamics, Mechanics and Components. The new one was built using the same challenges developed by the designers but presented with other game elements (Figure 5.1). The chosen elements for DMC were: (i) Emotions, (ii) Narrative, (iii) Progression, (iv) Challenges, (v) Feedback, (vi) Points. An original story was created using the Hero's Journey and adapted to the existing challenges, which were organized in progressive order of difficulty[7].

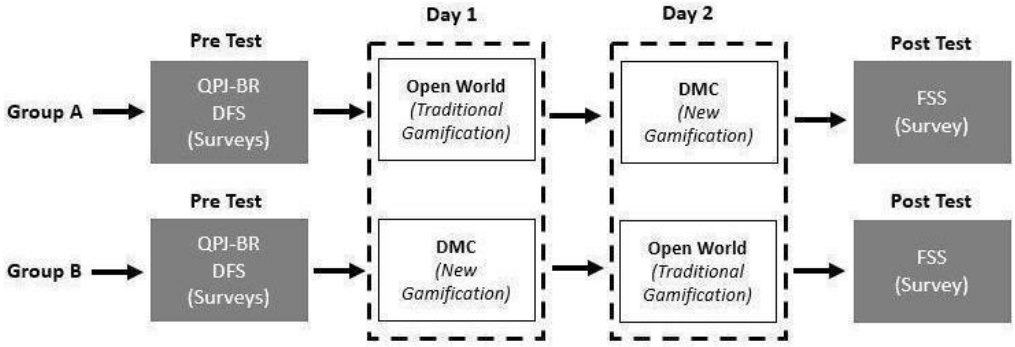

Figure 5.1.1 Experiment Design

The selection of the participants was based on convenience and without a probabilistic sample. The target population of the experiment was higher education students in Information Security or related areas (undergraduate and graduate) and professionals. The participants were aware that the data collected during their participation in the events would be used for scientific research purposes and the consent was collected in the instruments used.

5.2. Hypothesis

The objective of this study was to analyze how each player type was impacted by the Capture the Flag experience and to achieve this, we used the Flow scale as a metric. We developed two hypotheses to support this objective:

RQ1: What is the impact of flow experience on player types?

Hnull: *There is no correlation on the variance between player type and flow experience*
H1: *There is a correlation on the variance between player type and flow experience*

RQ2: What is the impact of the flow experience on the performance of the players based on the game mode (Open World or DMC)?

7 To read the CTF story, access this link: https://bit.ly/3l6RvBg

Hnull: *There is no correlation on the variance between the player performance and the game mode*
H1: *There is a correlation on the variance between the player performance and the game mode*

5.3. Instruments

The instruments used for data collection were the following: (i) Questionário de Perfil de Jogador (QPJ-BR): Portuguese validated survey to collect and identify the different player types. The participants of the competitions answered this instrument before the CTF events. (ii) Dispositional Flow Scale (DFS): Portuguese version. The participants of the competition answered the survey before the experience to evaluate the predisposition of flow state for CTF events . and (iii) Flow State Scale (FSS) Portuguese version. The participants answered the survey after the experience to evaluate the flow experience of participants during the OpenWorld and DMC design[8]. (iv) CTFd Platform data: the available reports on the platform were used to measure the performance of the participants.

5.4. Experiment Execution

The elaboration of CTF events was divided into the phases: Development, Pilot Experiment and Execution. In the Development, instructional designers were invited to build the challenges. Three cybersecurity professionals were invited to deploy the platform and build the challenges for the pilot experiment. Among the available options, we chose the CTFd, an open source project, because of the possibility of extracting a larger amount of data from the competitions, which would allow a complete analysis [9].

For the Pilot Experiment, ten Information Security professionals were invited to join. The platform used to host the challenges was prepared for a competition and challenges were developed, just like a real scenario. So, they registered at the platform and received a token to gain access to the competition. The participants were randomly distributed between the two available environments. From ten participants invited, seven joined the competition, four on Open World and three on DMC. The pilot experiment was useful to test the infrastructure and observe the CTF Player behaviors. The most experienced CTF players gave relevant feedback that was used to improve the game design and experience for the live competition.

For the Execution, we conducted two Capture the Flag events, Day 1 and Day 2, organized as on-line individual competitions. Both were 24-hour events and occurred in June 2020. The challenges built by the invited designers were used and the participation

8 Access the instruments used in this link: https://bit.ly/2GDCWWZ
9 Access the platform configuration in this link: https://bit.ly/3nixucS

was open to anyone wishing to play, leaving participation in both events voluntary. To gain access to the platform, the player must previously register with a valid email address. Participants who signed up received a token 48 hours before the competition, which guaranteed access to one of the environments (Open World or DMC).

There was a unified ranking for the two environments per competition day. The player who scored the most amount of points after the analysis of the event organizers was declared the winner. To encourage participation, there was an award for the winners and the players who answered all the forms received a certificate of participation.

For the first event (Day 1), 223 participants signed up to participate. They were distributed between the two available environments. One hundred sixty-one tokens were manually distributed by email 24 hours before the competition (the participants that subscribed to the competition after the manual distribution were automatically assigned to Open World mode). 73 participants attended the competition, divided between the Open World (53) and DMC (20) environments.

In the second event (Day 2), there was the return of participants from the first and the addition of new registrants, totaling 121 registrations. All participants that registered in the first event received a token manually sent by email, totaling 157 tokens distributed for DMC mode and 96 for Open World. Forty-six participants attended, 42 of which played in DMC mode and four in Open World. Due to a problem in the email system, the tokens needed to be available on the platform, so new participants could join the competition without the need of manual intervention.

5.5. Gaming the System Episodes

Gaming the System is an act practiced by the player in an attempt to obtain a good result using system properties instead of using the knowledge learned. These are typical behaviors of gaming the system (i) asking for help repeatedly until the correct answer is obtained (ii) sequence of attempts with a low interval to guess the answer (iii) frustration and (iv) anxiety. [Baker 2008]

It was foreseen in the rules of the game that after the end of the competition, the StarsCTF organizers would make an analysis before the winner's name was released. In the First Event, a case of gaming the system was detected through manual analysis where, at the end of the competition, the first three placed players had the same score. Through the analysis of the score evolution curve and submission interval, it was possible to identify that the first two were playing together, which was against the rules[10]. The fact affected the result of the competition and the third place was announced as the legitimate winner. In the second, an analysis was made of the scoring evolution of the first placed player and he was announced as the winner. However, in a later analysis to prepare the dataset, we found that two players connected in the two available experiences, in order to accumulate more points. The fact did not affect the result of the competition.

10 To know the report generated from this analysis, access this link: https://bit.ly/3jASdGG

6. Results

In this section we present the analysis performed and the results found.

6.1. Dataset Reduction

On Day 1, 73 participants attended the competition, 53 played on Open World mode and 20 on DMC mode and we considered valid the data from the participants who answered the three questionnaires: QPJ-BR, DFS (pre test) and FSS (post test), totalizing 18 participants, 10 for Open World and 8 for DMC. Data collected from players who engaged in gaming the system were also excluded from the analysis.

On Day 2, 46 participants attended the competition, 42 played on DMC mode and 4 on Open World mode. Due to the exclusion of data from the gaming the system episodes, the samples did not have a reasonable amount of data for analysis in both environments, so the sample was discarded.

6.2. Data Analysis

Analysis Pack for Excel was used for Data analysis. To do the validation of the hypotheses, we used non-paired Student's t-test and Pearson's Correlation Coefficient, considering a Confidence Interval of 95%.

6.3. First Event - Day 1

For the analysis of ***RQ1:*** *Evaluate the impact of flow experience on player types*, we considered 14 participants. Four outliers were detected and removed. To calculate the player type, we consider the participant's score in the three categories - achievement, immersion and socializer - and not just the one with the highest score, after all the three have interference in their profile, with different intensities (Figure 6.3.1).

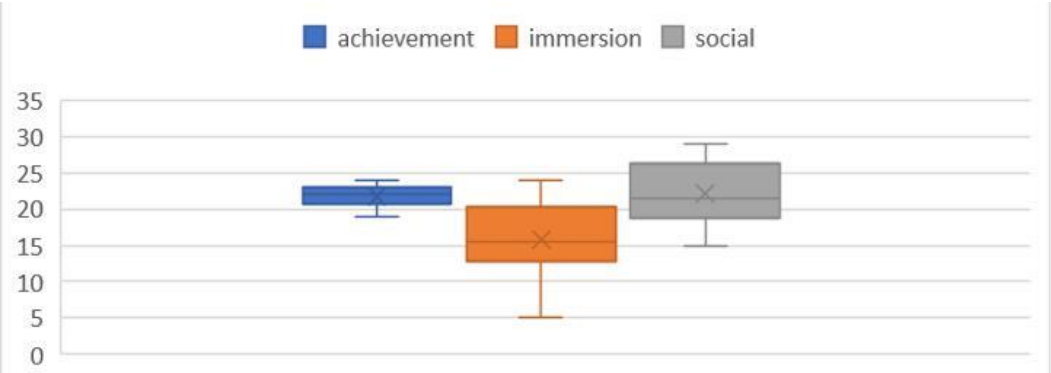

Figure 6.3.1 Player Types

We used a non-paired t-test with the data collected in the DFS (before the competition) and FSS (after the competition) questionnaire to check for significant variance (Table 6.3.1). We found significant variances on dimensions 1, 6 and 9.

Table 6.3.1 t-value for Flow Experience

Flow Dimension (DFS x FSS)	t-value	p-value
dimension 1	1.7056	0.0007
dimension 2	1.7247	0.0530
dimension 3	1.7056	0.1134
dimension 4	1.7081	0.0873
dimension 5	1.7056	0.2158
dimension 6	1.7207	0.0184
dimension 7	1.7108	0.1519
dimension 8	1.7081	0.0862
dimension 9	1.7056	0.0178

significant = $p < 0.05$

Also, we did a correlation analysis to see if there was a positive or negative impact for each player type and what the weight of this correlation is - weak, moderate or strong (Tables 6.3.2, 6.3.3 and 6.3.4). For these measures, we consider the Dancey & Reidy Psychology scale [Akoglu 2018], which varies positively and negatively between -1 and +1. For values from 0.1 to 0.3 the correlation is considered weak, from 0.4 to 0.6, moderate, from 0.7 to 0.9 strong and 1 indicates a perfect correlation. Considering moderate and strong correlations, on player types, for achiever we found dfs-dimension5 and fss-dimension9 , for immersion fss-dimension1, fss-dimension5, fss-dimension6, dfs-dimension9 and fss-dimension 9 and for socializer fss-dimension2, fss-dimension3, fss-dimension5, dfs-dimension6, fss-dimension6, dfs-dimension9 and fss-dimension9.

Table 6.3.2 Socializer x Flow Experience

socializer (DFS x FSS)	r	correlation

dfs_dimension1	-0.1767	weak
fss_dimension1	-0.1324	weak
dfs_dimension2	-0.2015	weak
fss_dimension2	-0.3445	moderate
dfs_dimension3	0.0760	weak
fss_dimension3	0.3251	moderate
dfs_dimension4	0.1778	weak
fss_dimension4	0.2288	weak
dfs_dimension5	-0.2824	weak
fss_dimension5	-0.3564	moderate
dfs_dimension6	-0.0301	moderate
fss_dimension6	-0.4164	moderate
dfs_dimension7	0.0988	weak
fss_dimension7	-0.0896	weak
dfs_dimension8	-0.1823	weak
fss_dimension8	-0.2995	weak
dfs_dimension9	-0.3188	moderate
fss_dimension9	-0.6044	moderate

Table 6.3.3 Immersion x Flow Experience

immersion (DFS x FSS)	r	correlation
dfs_dimension1	-0.2102	weak
fss_dimension1	0.5888	moderate
dfs_dimension2	0.0658	weak
fss_dimension2	0.3707	weak
dfs_dimension3	-0.2583	weak
fss_dimension3	-0.2575	weak
dfs_dimension4	0.0288	weak
fss_dimension4	0.1967	weak
dfs_dimension5	0.1614	weak
fss_dimension5	0.4063	moderate
dfs_dimension6	-0.1315	weak
fss_dimension6	0.4709	moderate
dfs_dimension7	-0.3645	weak
fss_dimension7	0.0968	weak
dfs_dimension8	-0.2836	weak
fss_dimension8	0.2666	weak
dfs_dimension9	-0.4241	moderate

fss_dimension9	0.6191	moderate

Table 6.3.4 Achievement x Flow Experience

achievement (DFS x FSS)	r	correlation
dfs_dimension1	0.0982	weak
fss_dimension1	0.1987	weak
dfs_dimension2	0.1781	weak
fss_dimension2	-0.0842	weak
dfs_dimension3	0.0210	weak
fss_dimension3	-0.1987	weak
dfs_dimension4	0.0099	weak
fss_dimension4	0.1606	weak
dfs_dimension5	0.4090	moderate
fss_dimension5	0.2953	weak
dfs_dimension6	-0.0056	weak
fss_dimension6	0.2614	weak
dfs_dimension7	-0.1631	weak
fss_dimension7	-0.0668	weak
dfs_dimension8	-0.0381	weak
fss_dimension8	0.1138	weak
dfs_dimension9	-0.0126	weak
fss_dimension9	0.4387	moderate

Relating the dimensions with significant variation to the correlation data by player type, we have as a result a table showing the significant variations, the strength of the correlation and the direction of the variation (positive or negative) (Table 6.3.5).

Table 6.3.5 Significant dimensions x correlations

	before(dfs)/post competition(fss)	socializer	immersion	achievement
dimension 1	**dfs**	weak - negative	weak - negative	weak - negative
	fss	weak - negative	moderate - positive	weak - negative
dimension 6	**dfs**	moderate - negative	weak - negative	weak - negative
	fss	moderate - negative	moderate - positive	weak - positive
dimension 9	**dfs**	moderate - negative	moderate - negative	weak - negative
	fss	moderate - negative	moderate - positive	moderate - positive

So, for RQ1, the alternate hypothesis ***H1:There is a correlation on the variance between player type and flow experience*** is valid for Flow dimensions 1, 6 and 9, and null hypothesis ***Hnull: There is no correlation on the variance between player type and flow experience*** for Flow dimensions 2, 3, 4, 5, 7 and 8.

For the analysis of **RQ2:** *Evaluate the impact of the flow experience on the performance of the players based on the game mode (Open World or DMC)*, we considered 18 participants. No outliers were found. To calculate the performance of the player, we divided this analysis in two parts. First, we used participants who played Open World mode and did a correlation analysis using their competition score versus data from the DFS and FSS questionnaires (Table 6.3.6). Then, we performed the same procedure with DMC participants (Table 6.3.7).

Table 6.3.6 Performance x Open World mode

points Open World mode	r	correlation
dfs_dimension1	0.1034	weak
fss_dimension1	-0.3769	weak
dfs_dimension2	-0.4120	moderate
fss_dimension2	-0.2044	weak
dfs_dimension3	0.1167	weak
fss_dimension3	0.2133	weak
dfs_dimension4	-0.5365	moderate
fss_dimension4	-0.6996	moderate
dfs_dimension5	-0.6303	moderate
fss_dimension5	-0.7486	moderate
dfs_dimension6	-0.2999	weak
fss_dimension6	-0.6098	moderate
dfs_dimension7	0.3205	weak
fss_dimension7	-0.0867	moderate
dfs_dimension8	0.4862	moderate
fss_dimension8	-0.7150	moderate
dfs_dimension9	0.0015	weak
fss_dimension9	-0.5798	moderate

Table 6.3.7 Performance x DMC mode

points DMC mode	r	correlation
dfs_dimension1	-0.5270	moderate
fss_dimension1	-0.1677	weak
dfs_dimension2	-0.4488	moderate

fss_dimension2	-0.2651	weak
dfs_dimension3	-0.4048	moderate
fss_dimension3	0.0489	weak
dfs_dimension4	-0.3169	weak
fss_dimension4	-0.4504	moderate
dfs_dimension5	-0.1250	weak
fss_dimension5	-0.2704	weak
dfs_dimension6	-0.5197	moderate
fss_dimension6	-0.2002	weak
dfs_dimension7	-0.4858	moderate
fss_dimension7	-0.6160	moderate
dfs_dimension8	-0.4424	moderate
fss_dimension8	-0.6929	moderate
dfs_dimension9	-0.2299	weak
fss_dimension9	-0.7591	strong

Considering the moderate and strong correlations, we found for Open World dfs-dimension2, dfs-dimension4, fss-dimension4, dfs-dimension5, fss-dimension5, fss-dimension6. fss-dimension-8 and fss-dimension9. For DMC mode, dfs-dimension1, dfs-dimension2, dfs-dimension3, fss-dimension4, dfs-dimension6, dfs-dimension7, fss-dimension7, dfs-dimension8, fss-dimension8 and fss-dimension9. Considering the flow dimensions with significant variance found in the previous hypothesis and related to the participants' performance, we arrive at a table with the relationship between dimensions X performance by game mode (Table 6.3.8).

Table 6.3.8 Significant dimensions x game mode correlations

	before(dfs)/post competition(fss)	**Open Word**	**DMC**
dimension 1	**dfs**	weak - positive	moderate - negative
	fss	weak - negative	weak - negative
dimension 6	**dfs**	weak - negative	moderate - negative
	fss	moderate - negative	weak - negative
dimension 9	**dfs**	weak - positive	weak - negative
	fss	moderate - negative	strong - negative

So for RQ2, the alternative hypothesis ***H1: There is a correlation on the variance between the player performance and the game mode*** is valid for both modes.

6.4. Discussion

For Research Question 1, the correlation between player types and flow experience, we found significant correlation on the following dimensions: (i) dimension 1 - clear objectives, (ii) dimension 6 - sense of control and (iii) dimension 9 - autotelic experience.

The Socializer player type was the least engaged, with all significant flow dimensions tending to a negative variance. The achievers were impacted positively by the autotelic experience (Dimension 9) and the immersion player type had a positive variance on Dimensions 1,6 and 9 on the results after the competition.

Using Yee's table [Yee 2005] of components and subcomponents (Table 6.4.1) to map the elements used on the challenges, it is possible to have an overview of the configuration of the resolved challenges in both environments. The Open World's challenges have elements to satisfy players with high scores in the player type achievement (Challenges, Feedback and Points), and DMC ones have elements to satisfy achievement and immersion player types (Narrative, Progression Restrictions, Challenges, Feedback and Points).

Table 6.4.1 Components and Subcomponents per Player Type

Achievement	Social	Immersion
Advancement Progress, Power, Accumulation, Status	**Socializing** Casual Chat, Helping Others, Making Friends	**Discovery** Exploration, Lore, Finding Hidden Things
Mechanics Numbers, Optimization, Templating, Analysis	**Relationship** Personal, Self-Disclosure, Find and Give Support	**Role-Playing** Story Line, Character History, Roles, Fantasy
Competition Challenging Others, Provocation, Domination	**Teamwork** Collaboration, Groups, Group Achievements	**Customization** Appearances, Accessories, Style, Color Schemes
		Escapism Relax, Escape from RL, Avoid RL Problems

For Research Question 2, the correlation between the correlation between game modes and flow, considering moderate results, we found for Open World: FSS -

Dimension 6 and FSS - Dimension 9, all negative. For DMC: DFS - Dimension 6 and FSS - Dimension 9, also all negative.

Analyzing the platform's data, it was possible to check that the amount of challenges solved on Open World is bigger than the challenges solved on DMC. On Open World the players solved 15 with different kinds of complexity (easy, medium and hard) while on DMC 8 challenges were solved, 7 easy and one medium. The next challenge for DMC was medium complexity. It was possible to identify that one player kept trying to submit the correct flag until the end of the competition, which can lead to thinking of a potential lack of skill and possibility of frustration [Weiss et al. 2016]. So, due to the characteristics of the competition, the freedom to solve challenges in any order also have a direct impact on the score of the players and consequently on their flow experience. On both scenarios not all the available challenges were solved.

The limitations found in the study show points of attention and work possibilities for future research. The most important was the need to redesign the study. Due to the COVID-19 pandemic, the design of the original project was changed to an online format. The available scenario was faithful to those commonly found in CTF competitions however, it was not possible to assess the difference in engagement between in-person and online events. Also, in a first analysis, the type of competition chosen (individual, Jeopardy) did not allow the inclusion of game elements to favor the Social player type. It was not possible to predict in advance the number of participants who would attend the event, since it is quite common to register just before the competition or even with the competition in progress. A method for automatically distributing tokens would be extremely useful to ensure a better distributed sample.

7. Conclusions and Future Works

The purpose of this paper was to evaluate the performance and engagement levels of the experiment participants using the player type and the Flow experience as metrics. We built the experiment environment using an open source tool, CTFd. The environment contained two experiences, one called Open World, which contained game elements normally used in CTF competitions and the other called DMC, which contained the same challenges, but in addition to other game elements. A paired experiment was carried out in two editions in June 2020. Due to a problem in the sample of the second experiment, it was excluded from the analysis and only the sample of the first event was considered, totaling 18 participants.

Relating Player types x flow experience, the Socializer profile was the least affected by the experience, probably due to the chosen format (Individual and Jeopardy). In future studies, it is interesting to assess the difference in the performance of players in individual or group competitions. The profiles Immersion and Achievement had more positive effects, due to the elements present in the competition. In the relation between game mode and flow, all variances were negative. The vast majority of the challenges solved were of easy and medium difficulty in the Open World environment and of easy

difficulty in the DMC mode. Participants failed to solve a medium difficulty challenge (called Kardeco) and were unable to advance the story.

An important fact is that in both environments not all the available challenges were solved, which leads us to believe that either there were too many challenges for the competition or the level of difficulty of the challenges was demanding a lot of time from the participants.

This study advances the literature using psychometric methods validated for the analysis of player types and experience of flow with environments with different gamifications. In future studies a larger and more diverse sample in player types and genres can help build better experiences and attract more talents to the Cybersecurity area.

8. References

Akoglu, H. (1 sep 2018). User's guide to correlation coefficients. *Turkish Journal of Emergency Medicine*, v. 18, n. 3, p. 91–93.

Alerta Security (2018). Segurança da informação: entenda as principais ameaças. https://www.alertasecurity.com.br/seguranca-da-informacao-entenda-as-principais-ameacas/, [accessed on Aug 16].

Anchises Moraes (2013). BSidesSP in a glance. . https://www.slideshare.net/anchises/bsidessp-in-a-glance?smtNoRedir=1, [accessed on Dec 12].

Andrade, F., Marques, L., Bittencourt, I. I. and Isotani, S. (2016). QPJ-BR: Questionário para Identificação de Perfis de Jogadores para o Português-Brasileiro. *Anais do XXVII Simpósio Brasileiro de Informática na Educação (SBIE 2016)*, v. 1, n. Cbie, p. 637.

Baker, R. (2008). Why Students Engage in "Gaming the System" Behavior in Interactive Learning Environments. p. 40.

Bansal, P. (2019). CTF are for Nerds : A Popular myth. https://medium.com/bugbountywriteup/ctf-are-for-nerds-a-popular-myth-54d6647259eb, [accessed on Sep 8].

BRASSCOM (2019). Formação Educacional e Empregabilidade em TI.

Brown, E. (2019). CTF Hacking: What is Capture the Flag for a Newbie? https://cybersecurity.att.com/blogs/security-essentials/capture-the-flag-ctf-what-is-it-for-a-newbie, [accessed on Aug 17].

Cryptorave (2020). Why CryptoParty? https://www.cryptoparty.in/sao-paulo, [accessed on Sep 8].

CryptoRave 2014 - 24 horas pela liberdade e privacidade na rede (2014). https://2014.cryptorave.org/, [accessed on Dec 12].

CTFtime team (2012). CTF Events. https://ctftime.org/event/list/, [accessed on Sep 27].

DEF CON Communications, I. ([S.d.]). A history of Capture the Flag at DEF CON. https://www.defcon.org/html/links/dc-ctf-history.html, [accessed on Sep 8].

Deloitte (2020). Tendências em gestão de riscos cibernéticos e segurança da informação na América Latina e Caribe. . , [accessed on Aug 16].

Deterding, S., Dixon, D., Khaled, R. and Nacke, L. (2011). From Game Design Elements

to Gamefulness: Defining “Gamification.” In *Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments*. , MindTrek ’11. Association for Computing Machinery. https://doi.org/10.1145/2181037.2181040.
Dixon, D. (2011). Player Types and Gamification. . http://gamification-research.org/wp-content/uploads/2011/04/11-Dixon.pdf, [accessed on Sep 5].
Equipe TecMundo (2020). Campeonato ao vivo vai premiar hackers por invasão de sistemas. https://www.tecmundo.com.br/seguranca/154535-campeonato-vivo-premiar-hackers-invasao-sistemas.htm, [accessed on Aug 9].
Fahs, G. (2019). DEF CON: The Ultimate Guide for First-Timers. https://medium.com/@ginnyfahs/def-con-the-ultimate-guide-for-first-timers-516b6ffda705, [accessed on Sep 8].
Feng, W. (2016). A “Divergent”-Themed {CTF} and Urban Race for Introducing Security and Cryptography. . https://www.usenix.org/conference/ase16/workshop-program/presentation/feng, [accessed on Sep 27]. Garoa Hacker Clube (2012). BSidesSP.
Hanson, T. ([S.d.]). Chapter 8 Paired observations. p. 19.
Internet Archive (5 may 2004). :: Hackers 2 Hackers Conference :: http://web.archive.org/web/20040505210502/http://www.h2hc.com.br/, [accessed on Dec 12].
Jackson, S. A. and Eklund, R. C. (jun 2002). Assessing Flow in Physical Activity: The Flow State Scale–2 and Dispositional Flow Scale–2. *Journal of Sport and Exercise Psychology*, v. 24, n. 2, p. 133–150.
Jovem Nerd (2014). Final do H4ck4fl4g acontece hoje no Roadsec em São Paulo - NerdBunker. *Jovem Nerd*. https://jovemnerd.com.br/nerdbunker/final-do-h4ck4fl4g-acontece-hoje-no-roadsec-em-sao-paulo/, [accessed on Dec 12].
Kam, H.-J., Menard, P., Ormond, D. and Crossler, R. E. (2020). Cultivating cybersecurity learning: An integration of self-determination and flow. *Computers & Security*, v. 96, p. 101875.
Kaspersky (2020). O que é cibersegurança? https://www.kaspersky.com.br/resource-center/definitions/what-is-cyber-security, [accessed on Aug 16].
Katsantonis, M., Fouliras, P. and Mavridis, I. (2017). Conceptual analysis of cyber security education based on live competitions. . IEEE.
Mansurov, A. (17 aug 2016). A CTF-Based Approach in Information Security Education: An Extracurricular Activity in Teaching Students at Altai State University, Russia. *Modern Applied Science*, v. 10, n. 11, p. 159.
Marczewski, A. (2015). Game Based Solution Design. https://www.gamified.uk/gamification-framework/differences-between-gamification-and-games/, [accessed on Sep 8].
McDaniel, L., Talvi, E. and Hay, B. (jan 2016). Capture the Flag as Cyber Security Introduction. In *2016 49th Hawaii International Conference on System Sciences (HICSS)*. Mirvis, P. H. and Csikszentmihalyi, M. (1991). Flow: The Psychology of Optimal Experience. *The Academy of Management Review*, v. 16, n. 3, p. 636.
Nacke, L. E., Bateman, C. and Mandryk, R. L. (2014). BrainHex: A neurobiological gamer typology survey. *Entertainment Computing*, v. 5, n. 1, p. 55–62.
Nguyen, T. A., Pham, H., Chi, H. and City, M. (2018). A Design Theory-Based

Gamification Approach for Information Security Training. p. 36–39.
Ros, S., Gonzalez, S., Robles, A., et al. (2020). Analyzing Students' Self-Perception of Success and Learning Effectiveness Using Gamification in an Online Cybersecurity Course. *IEEE Access*, v. 8, p. 97718–97728.
Weiss, R., Turbak, F., Mache, J., Nilsen, E. and Locasto, M. E. (aug 2016). Finding the Balance Between Guidance and Independence in Cybersecurity Exercises. In *2016 USENIX Workshop on Advances in Security Education (ASE 16)*. . USENIX Association. https://www.usenix.org/conference/ase16/workshop-program/presentation/weiss. Yee, N. (2005). Motivations of Play in MMORPGs. p. 46.
Zimmerman, E. (2004). Narrative, Interactivity, Play and Games: Four Naughty Concepts in Need of Discipline. *First person: New media as story, performance, and game*. MIT Press, Cambridge, MA. .