OULUN YLIOPISTO
UNIVERSITY of OULU

Advantages and challenges of using capture-the-flag games in cyber security education

University of Oulu
Department of Information Processing Science
Bachelor’s Thesis
Juho Holmi
08/09/2020

Abstract

The world around us is digitalising fast and internet is almost everywhere, which makes cyber security an inevitable part of our lives. This thesis explored if capture-the-flag (CTF) games are viable solution to teaching cyber security. Research method used was a narrative literature review. 16 academic sources were reviewed, nine of which used quantitative research methods.

Prior research showed that capture-the-flag games had a positive impact on participants' motivation and engagement levels. In some studies, capture-the-flag games were found to lead to statistically better learning results and better understanding of computer security. Other resulting advantages were better practical knowledge in cyber security, increased grades and increased confidence in cyber security skills.

Organising such games was found to be a challenging job and consequently, knowledge is required from both organisers and participants of capture-the-flag games. Capture-the-flag game environments are complex and support staff is needed in organising such games. Designing the challenges to be appropriately challenging was found to be a difficult task and a related problem was challenge avoidance. Quality assurance was found to be an important, but often overlooked part of the design process.

In some papers, plagiarism was mentioned being a trouble. Automated approval of flag submissions in the games could lead to students illicitly sharing flags. Besides plagiarism, other ethical implications of teaching offensive computer security methods were a concern to many authors, but no quantitative research on this topic has so far been conducted.

Keywords
Cyber security, capture-the-flag, education, gamification, hacking

Supervisor
Dr. Piiastiina Tikka, University lecturer

Foreword

Thanks for Piiastiina Tikka for her positive and patient attitude towards my never-ending questions.

Juho Holmi

Oulu, 2020

Table of Contents

1. Introduction

In cyber security context, capture-the-flag (CTF) games are competitions, where one's goal is to find hidden flags in a certain computer environment. The environment can encompass a single web page or it can span across a whole network of computers. The two most common types of CTF games are *Jeopardy* and attack-defense. A *Jeopardy*-style competition usually has multiple categories that each have multiple tasks to solve. In an attack-defense competition the participating teams are given a network or a host machine, which they need to defend while trying to exploit the other teams.

The main purpose of this study is to study how CTF games benefit education and also study the possible disadvantages and challenges rising from the format. Scope of this study is not strictly CTF games. Other forms of gamified and offensive forms of cyber security education are studied, whenever deemed relevant. Therefore, the primary research question is "*what are the advantages and disadvantages of using capture-the-flag games in cyber security education*". A secondary research question is "*is there any quantitative evidence of found advantages and disadvantages*".

Motivation for using this topic comes from many directions. First, I have personally found CTF games to be a fun and rewarding way to learn different cyber security aspects. Second, the world around us is digitalising fast and the internet is almost everywhere, which makes cyber security an inevitable, although usually seemingly quite invisible part of our lives (as long as it is not compromised). Third, I study information processing science, but the total number of compulsory cyber security courses in my curriculum is one (1) and there are not many optional courses, which I find rather underwhelming.

Benefits of using CTF games in cyber security education include higher student motivation (McDaniel, Talvi and Hay, 2016; Katsantonis, Fouliras & Mavridis, 2017) and better practical knowledge resulting from the approach (Burns, Rios, Jordan, Gu & Underwood, 2017; Ariyapperuma & Minhas, 2005). Challenges stemming from the format include high knowledge requirements from both the organisers and the participants (Burns et al., 2017; McDaniel et al., 2016; Werther, Zhivich, Leek & Zeldovich, 2011) and complex technical requirements (Dabrowski, Kammerstetter, Thamm, Weippl & Kastner, 2015; Chung & Cohen, 2014). Some sources also expressed concerns regarding ethical issues of teaching students offensive techniques (Logan & Clarkson, 2005; Conti, Babbitt & Nelson, 2011), while other sources were not so concerned (Dabrowski et al., 2015; Mirkovic & Peterson, 2014).

Research methodology used in this thesis is a narrative literature review. It is the lightest form of literature reviews. In short, its purpose is to condense prior research, but it does not necessarily provide the most analytic outcome. (Salminen, 2011.)

The main contribution of this thesis is that it answers to the primary research question "*what are the advantages and disadvantages of using capture-the-flag games in cyber security education*". Also, some of the findings are backed by quantitative research, thus the secondary research question “*is there any quantitative evidence of found advantages and disadvantages*” is at least partly answered. Findings can be utilised in cyber security education. A summary of suggested good practices and possible improvements collected from the sources is also given.

Structure of the thesis is as follows. First, the most important concepts regarding this thesis are explained. Second, the research methods used in constructing this thesis are explained. Third, prior research around the topics of this thesis is analysed. Fourth, the findings of this thesis are discussed. Fifth, this thesis’ findings, contribution, restrictions and recommendations for future research are summarised. Sixth and last, the references used in this thesis are listed.

2. Important concepts

The primary concepts around the topic of this thesis are explained in this chapter.

2.1 Capture-the-flag (CTF) games

Capture-the-flag games are competitions where one’s goal is to find hidden flags in a certain environment. The environment can encompass a single web page or it can span across a whole network of computers. The flags are usually random strings of characters with a certain prefix, which makes it easy for competitors to spot a flag when they see it. (McDaniel et al., 2016.)

Many sources (Gavas, Memon & Britton, 2012; Raman, Sunny & Acuthan, 2014) mention DEF CON 1996 as one of the oldest or even the first ever CTF arranged, so CTFs have been around for roughly 20 years.

The two most common types of CTF games are *Jeopardy* and attack-defense. Other formats exist too. (CTFTime.org, 2020.) This thesis mostly covers the attack-defense and Jeopardy games.

A *Jeopardy*-style competition usually has multiple categories and each category has multiple tasks to solve. Categories can include web exploitation, forensic analysis, cryptography, binary analysis and many other topics. Teams or individuals get points by solving tasks, which can be solved sequentially or in random order, depending on how the organisers have decided. The amount of points rewarded depends on the designed difficulty of the task. In the end, the competitor with the most points is the winner. (CTFTime.org, 2020.)

In an attack-defense competition teams are given a network or a host machine, usually containing a flag which they need to defend while trying to capture-the-flag from the other teams’ machines. Before the teams can start attacking each other, there may be a period that teams can use to patch their systems, develop exploits and tactics and do other activities they deem necessary. Points are awarded for successfully defending own premises and exploiting the other teams. Again, team with the most points in the end is the winner. (CTFTime.org, 2020.)

2.2 Cyber security

Cyber security is a broad topic and many definitions for it can be found in the literature. Craigen, Diakun-Thibault, & Purse (2014) propose a following definition:

> *“Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign* de jure *from* de facto *property rights.”*

I find this definition to be adequately broad, but still understandable, save probably two terms, *de jure* and *de facto*. *De jure* means legally recognised, while *de facto* means in reality. So, essentially cyber security means protecting cyberspace (-enabled systems) from anything that is not legal to do.

Financial losses caused by cyber crime are likely to be very high, but are difficult to measure for many reasons. Brecht & Nowey (2013) have analysed different sources and have found estimations ranging from 560 million dollars to one trillion (million million) dollars. Since those numbers are from year 2013 and the significance of IT infrastructure has grown much up to these days, the numbers have very likely increased annually.

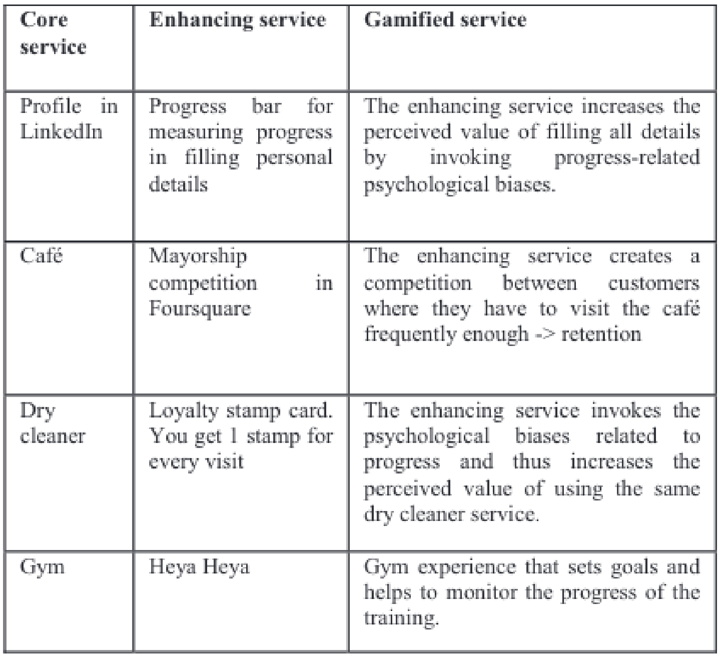
2.3 Gamification

Gamification is an essential keyword in the context of this thesis. Huotari & Hamari (2012) define gamification as

> *“a process of enhancing a service with affordances for gameful experiences in order to support user's overall value creation”.*

The term affordance may not be previously known to many readers. Merriam-Webster (“Affordance”, n.d.) defines it as

> *“the quality or property of an object that defines its possible uses or makes clear how it can or should be used”.*



Core service	Enhancing service	Gamified service
Profile in LinkedIn	Progress bar for measuring progress in filling personal details	The enhancing service increases the perceived value of filling all details by invoking progress-related psychological biases.
Café	Mayorship competition in Foursquare	The enhancing service creates a competition between customers where they have to visit the café frequently enough -> retention
Dry cleaner	Loyalty stamp card. You get 1 stamp for every visit	The enhancing service invokes the psychological biases related to progress and thus increases the perceived value of using the same dry cleaner service.
Gym	Heya Heya	Gym experience that sets goals and helps to monitor the progress of the training.

Figure 1: Examples of gamification (Huotari & Hamari, 2012).

In the aforementioned definition of gamification, affordance can refer to any qualities of the service system that contributes to the emergence of gameful experience. Examples of gamification can be seen in Figure 1.

2.4 Hacking

Merriam-Webster (“Hacking”, n.d. a) defines hacking as

> *“gaining illegal access to (a computer network, system, etc.)*“

and Cambridge Dictionary (“Hacking”, n.d. b) as

> *“the activity of using a computer to access information stored on another computer system without permission, or to spread a computer virus*.“

However, according to Raymond (1991), the term hacker originated at Tech Model Railroad Club (TMRC), a student organisation at the Massachusetts Institute of Technology (MIT) at the sixties. One of the many original definitions (which are quite the opposite to the meaning today) for it is

> “*a person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary”*. (Raymond, 1991.)

Also, according to Raymond (1991), hacker ethic states that

> “*The belief that information-sharing is a powerful positive good, and that it is an ethical duty of hackers to share their expertise by writing open-source code and facilitating access to information and to computing resources wherever possible.*”

Thus, originally, the words hacker and hacking contained very little allusions of criminality. However, in this thesis, hacking refers to the definitions by Merriam-Webster and Cambridge Dictionary, as they are the meanings mostly used nowadays. Still, it is worth noting that in CTF games most offensive activities are naturally allowed and creative thinking encouraged, so in a way, the hackers taking part in CTF contests are hackers mostly in the original sense of the word.

3. Research methods

The research methodology used in this thesis is a narrative literature review. Narrative literature review is “the lightest form of literature reviews. In short, its purpose is to condense prior research, but it does not necessarily provide the most analytic outcome. (Salminen, 2011.)

In the beginning, the Scopus database was mostly used for finding source literature. One notable problem is that both "*cybersecurity*" and "*cyber security*" are valid forms (the difference mainly comes down to whether writer is using US English or British English), so both should be used in searches. I chose to use the British English form "cyber security" when writing my text.

I started the search for sources with “*capture AND the AND flag AND cyber AND security*”, which yielded 61 search results. By changing the expression to “*capture AND the AND flag AND cybersecurity*”, the number of search results decreased to 31. Here, logical operators can be used to include both variants, by changing the query to *capture AND the AND flag AND ("cyber security" OR cybersecurity)*, which yielded 64 results. “*Capture AND the AND flag AND ("cyber security" OR cybersecurity) AND education*” yielded 25 results. Unfortunately, many of the sources found with these search terms did not actually concern cyber security education at all or were of low value.

Since the amount of valuable sources found via Scopus was quite low, I expanded my search to Google Scholar and ACM and IEEE libraries. Among these, Google Scholar was not particularly helpful in finding sources, since the amount of results is usually simply so high. In case of ACM and IEEE libraries, narrowing a simple "*capture the flag*" query by selecting the publication types helped to find many sources.

I also referenced a less academic source for defining the concepts regarding the topic of this thesis, namely CTFTime.org (2020). It should be noted that no author information is present on the CTFTime.org website, but many sources cited in this thesis seem to use CTFTime.org as a credible source.

Source lists of documents found using aforementioned search tools were also very helpful in finding more valuable sources. This path had an increased significance in the later part of writing process.

Some of the sources were also found using simple Google searches around the topic, even accidentally. In the end, I estimate that roughly one third of the sources were from Scopus, one third from the source lists of other sources and the rest mostly from either ACM or IEEE libraries.

Source verification was done using Ulrichsweb and Finnish-language Publication Forum (Julkaisufoorumi). Specifically, I tried to make sure that the bulk of references were from papers that Publication Forum rates at the minimum of level one (1, so-called basic level) whenever Publication Forum recognised the publication.

A special characteristic of sources around this topic seems to be that an overwhelming majority of the sources are conference papers. This may of course stem from the fact that cyber security, computer science and gamification are rather modern topics and most sources are from 2010s.

The main selection criteria for sources was that to be included in this study, they had to somehow cover educational side of capture-the-flag games, even if it was not their main focus. Of course, credible sources regarding purely cyber security education by utilising capture-the-flag games were not very prevalent, so I had to expand this thesis to also include other forms of education that take advantage of gamification.

3.1 Restrictions

A common restriction shared between most of the sources was that they did not use scientific approach in assessing the educational advantages and disadvantages of gamified cyber security education. The papers described education methods in a very report-like, informal fashion and mostly did not use any quantitative research methodologies nor used any theoretical backgrounds.

This is also noted by Hendrix, Al-Sherbaz and Bloom (2016), who found that research methodologies of most of the sources describing cyber security training games could not stand rigorous scrutinization and Katsantonis et al. (2017), who state that majority of the papers studied by them did not collect empirical data.

As to collecting empirical data, Werther et al. (2011) state between the lines that getting answers to surveys from participants is hard, and suggest raffling small prizes to those who answer. Furthermore, self-reporting proficiency levels is not always the most reliable way to obtain data, as is noted by Mirkovic, Tabor, Woo & Pusey (2015): they found out that teams formed based on the self-reported skills were not equal in skills, as was the original intention.

4. Prior research

Reported benefits of using capture-the-flag games in cyber security education include

- higher student motivation (McDaniel et al., 2016; Katsantonis et al., 2017) and
- better practical knowledge (Burns et al., 2017; Ariyapperuma & Minhas, 2005).

Reported challenges stemming from the format include

- high knowledge requirements from both organisers and participants (Burns et al., 2017; McDaniel et al., 2016; Werther et al., 2011) and
- complex technical requirements (Dabrowski et al., 2015; Chung & Cohen, 2014).

Some sources express concerns regarding the ethical issues of teaching students offensive techniques (Logan & Clarkson, 2005; Conti et al., 2011), while other sources are not so concerned (Dabrowski et al., 2015; Mirkovic & Peterson, 2014).

Some sources also talk about the competitive aspects (Dabrowski et al., 2015; Vykopal, Svabensky & Chang, 2020), good practices and possible improvements to the format (Eagle, 2013; Werther et al., 2011).

In the chapters 4.1 – 4.6, prior research about these is described in more detail. Please refer to Appendix A for a summary of source attributes and limitations. For a quick peek to sources' limitations, the columns named *research methods* and *theoretical background* can be useful.

4.1 Previous literature reviews

Katsantonis et al. (2017) reviewed 34 papers in their study of cyber security education based on live competitions and as a part of their study, summarised and categorised the problems and issues identified in the analysed papers.

Regarding the competitions' aims, they found three different drawbacks: the aim of contests is usually to measure skills, but not necessarily education; contests usually fail to properly link the tasks and approaches to the real life; and certain factors force the contests to only focus on a restricted set of topics, which in turn lessens the number of topics learned by participants.

Regarding the learning process, they also found three different drawbacks: even though contests are often tailored for specific groups, designers still struggle to implement appropriately difficult challenges; if the contestants compete against each other, the results are not comparable and repeatable and contestants may not be able to refine their approaches iteratively; and partial credit is not supported.

Regarding the organisational and functional aspects, they found four drawbacks: organising a contest is demanding resource- and preparation wise; expert support personnel are often needed both before and during the the event; a strict quality assurance process is needed; and because of high costs, organisations are pushed to organising the events less frequently. (Katsantonis et al., 2017.)

Hendrix et al. (2016) conducted a literature review of serious games aimed at cyber security education, but their scope was more broad, ranging from board games to Sims-style 3D virtual world games. The study addressed only two CTF games.

4.2 Advantages

McDaniel et al. (2016) credit hacking competitions because they are exciting and thought-provoking. Based on two years experience, they have found CTF to be a very effective tool in providing students with a basic knowledge of common issues in computer security. They note that gamification of cyber security challenges made the CTF approach very successful and also motivated the students to learn the techniques needed in the challenges by themselves, which is also noted by Katsantonis et al. (2017) in their literature review. In similar fashion, Chothia & Novakovic (2015) describe a virtual machine -based CTF framework used in their university-level cyber security course. According to the post-course questionnaire, students rated the course fifth most difficult offered by the school, but they also rated it either the most or the second-most worthwhile course they took and the overall opinion of the course was highly positive.

Chapman, Burket & Brumley (2014) describe their experience of organising PicoCTF, a browser-based CTF game primarily targeted at high school students. They used a post-game online survey directed at both students and teachers to assess the impact of the game. Overall results were positive. 67% of students thought they learned more by playing the game than they normally learned by going to classes and 76% of the teachers reported that their students put more effort into the game than into normal classes. Every teacher who answered would encourage their students to engage in the next year’s game. (Chapman et al., 2014.)

In the post-course survey by Burns et al. (2017), a clear majority (83%) of the students felt that the CTF exercises included in the course helped them to truly understand computer security. Werther et al. (2011) also believe that CTF as a valuable pedagogical tool in teaching computer and network systems and offensive components of CTF result in deeper general understanding of computer science. Chothia & Novakovic (2015), however note that submitting valid flags still does not necessarily prove a deep understanding of the topic.

Suggested deeper understanding is shown in practice by Chothia & Novakovic (2015), who found a very strong relationship between students submitting valid flags and getting good grades from the written submissions. They suggest that the ability of a student to complete CTF-style challenges is a useful assessment technique for academic cyber security courses. Ariyapperuma & Minhas (2005) compare two cohorts in their paper. First group was given traditional laboratory sessions and second group conducted the laboratory sessions as online cyber security games. According to them, the second group using online cyber security games achieved statistically significantly better results in the grades.

Werther et al. (2011) analyse a CTF competition arranged at MIT Lincoln Laboratory. A survey, which was arranged amongst participants after the competition to examine its educational value, indicated that students had learned much about computer security. The survey (n=22) covered both pre- and post-competition reflections of participants. On a 10-point scale, participants reported on average a 1.4 point improvement in the confidence in their computer security skills and a 1.1 point increase in interest in computer security. (Werther et al., 2011.)

The main finding of the empirical study by Mink & Greifeneder (2010) is that students who participated in the course using offensive approach tended to find more vulnerabilities in the administrative test compared to those who studied defensive approaches. This is relevant because CTF games usually require studying and employing offensive methods. Mink & Greifeneder (2010) conclude that using offensive approach lead to better understanding of information security and higher motivation among students, partly because finding a vulnerability is easier than proving a system is free of vulnerabilities. Although, Logan & Clarkson (2005) argue that no research had (as of 2005) found a direct positive correlation between hacking skills and consequentially improved network security.

Continuing with the advantages, Dabrowski et al. (2015) describe their experiences over a decade of using gamification to teach two cyber security courses to university students. Overall reaction from students has been largely positive, especially gaming concepts and practical security challenges have been highly liked. For example, 96% of answerers either agreed or strongly agreed with the claim "*I enjoyed the gaming-like concept of the practical security challenges*", 97% either agreed or strongly agreed with the claim "*I prefer practical security challenges over conventional exercises*" and 67% either agreed or strongly agreed with the claim that gamification approach draws more students to IT security. (Dabrowski et al., 2015.)

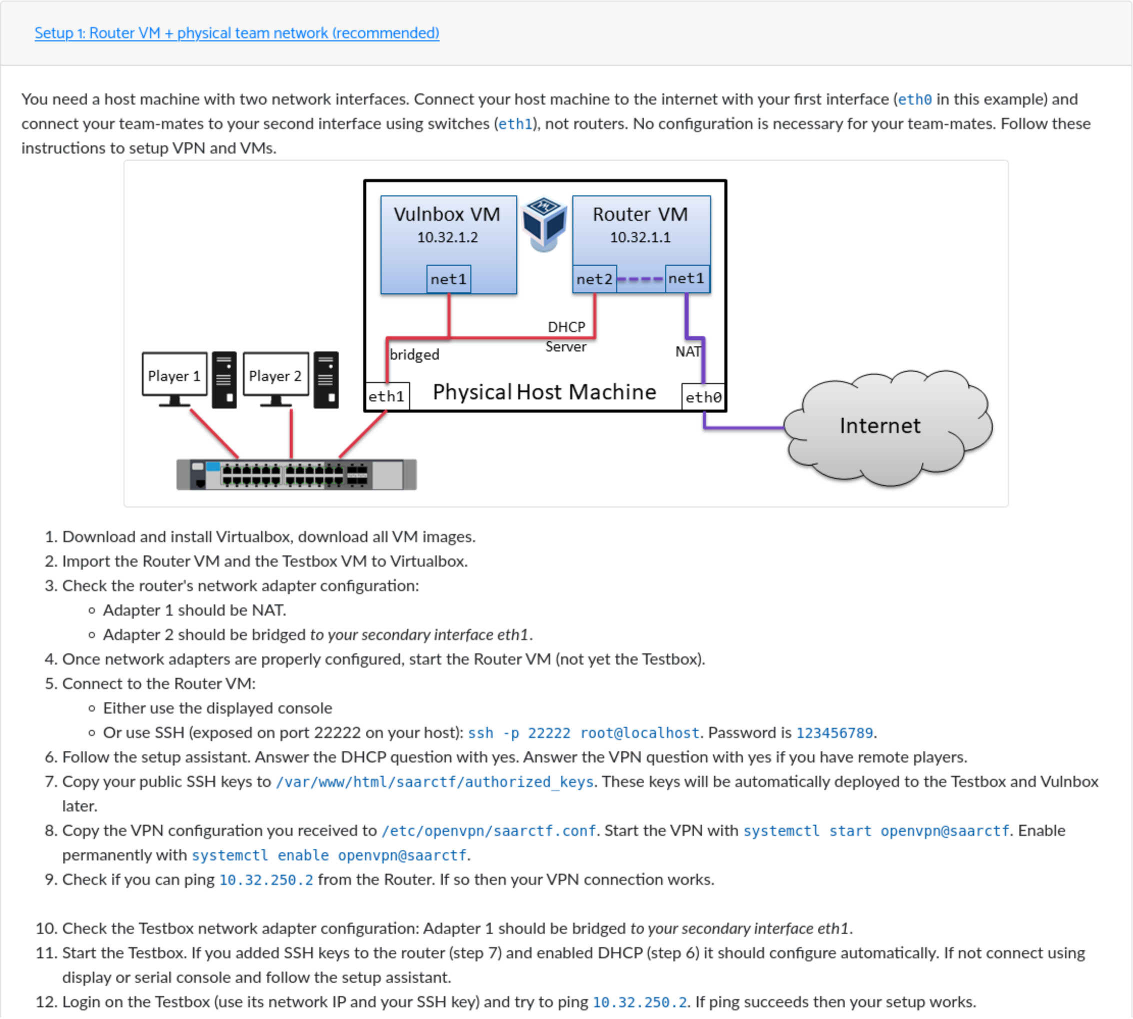
Similar findings are covered by Vykopal et al. (2020), who analyse an university-level course held at a Singapore university that utilised CTF games as homework assignments. The data analysed included the CTF platform logs (such as logins and flag submissions), two surveys and students’ marks from other course assessments. After the CTF games, 16 out of 13 students answered they would prefer CTF games over traditional homework assignments. Statistical analysis also showed a statistically significant positive correlation between students’ total CTF score (including points from bonus challenges) and their marks from other types of course assignments. The same was also true for correlation between students’ total CTF score including points from bonus challenges and mark from the midterm quiz. The correlation coefficient between students’ total CTF score including points from bonus challenges and final exam was practically the same. (Vykopal et al., 2020)

Mirkovic et al. (2015) describe a distributed denial-of-service (DDoS) -themed CTF workshop hosted at ACM Richard Tapia 2015 conference. The participants were undergraduate and graduate level students. Pre- and post-workshop quantitative surveys were used to analyse participants’ change in engagement and self-efficacy in skills needed during the workshop. Analysis of the quantitative data reveals that both engagement and self-efficacy increased during the workshop. For example, before the workshop, 20% thought they were “*confident that they could write rules for iptables to filter traffic with some characteristics, e.g. by protocol, sender IP, length, TCP*” but after the workshop, the number increased to roughly 50%. Qualitative data also revealed that the participants felt that they had gained knowledge of cyber security and network monitoring. Also, participants mentioned that they were “*excited to learn packet [monitoring]* (motoring in the original text, presumably a typing error) *and learn how to observe the data flows in the network*”. A limiting factor for the credibility of this study was the low number of matched-pair answers, which was only five, as was also mentioned by the authors. (Mirkovic et al., 2015.)

Conti et al. (2011) regard CTFs as valuable tools in education and went as far as saying that every information security education program should include CTF competitions in order for the students to get sufficient knowledge. The same is also noted by Mink & Greifeneder (2010), who concluded their findings by saying that information security courses should teach offensive aspects.

4.3 Challenges and disadvantages

Participating in capture-the-flag games requires lots of technical knowledge, both from organisers and participants, a fact that is mentioned by many sources. McDaniel et al. (2016) have noticed that a number of participants lack even some very basic skills, such as using tabs in a browser, that limit their ability to effectively solve the challenges.



Setup 1: Router VM + physical team network (recommended)

You need a host machine with two network interfaces. Connect your host machine to the internet with your first interface (`eth0` in this example) and connect your team-mates to your second interface using switches (`eth1`), not routers. No configuration is necessary for your team-mates. Follow these instructions to setup VPN and VMs.

1. Download and install Virtualbox, download all VM images.
2. Import the Router VM and the Testbox VM to Virtualbox.
3. Check the router's network adapter configuration:
   - Adapter 1 should be NAT.
   - Adapter 2 should be bridged *to your secondary interface eth1*.
4. Once network adapters are properly configured, start the Router VM (not yet the Testbox).
5. Connect to the Router VM:
   - Either use the displayed console
   - Or use SSH (exposed on port 22222 on your host): `ssh -p 22222 root@localhost`. Password is `123456789`.
6. Follow the setup assistant. Answer the DHCP question with yes. Answer the VPN question with yes if you have remote players.
7. Copy your public SSH keys to `/var/www/html/saarctf/authorized_keys`. These keys will be automatically deployed to the Testbox and Vulnbox later.
8. Copy the VPN configuration you received to `/etc/openvpn/saarctf.conf`. Start the VPN with `systemctl start openvpn@saarctf`. Enable permanently with `systemctl enable openvpn@saarctf`.
9. Check if you can ping `10.32.250.2` from the Router. If so then your VPN connection works.

10. Check the Testbox network adapter configuration: Adapter 1 should be bridged *to your secondary interface eth1*.
11. Start the Testbox. If you added SSH keys to the router (step 7) and enabled DHCP (step 6) it should configure automatically. If not connect using display or serial console and follow the setup assistant.
12. Login on the Testbox (use its network IP and your SSH key) and try to ping `10.32.250.2`. If ping succeeds then your setup works.

Figure 2: An example of a CTF competition team network configuration (SaarCTF, 2020).

Similarly to McDaniel et al. (2016), Burns et al. (2017) mention that 13% of students on their course gave up on the course CTF exercises due to not having enough computer administration skills or having too low-end hardware and that only 8% of students could discover the flags by themselves (without reading the hints provided). Werther et al. (2011) also highlight the same: participation requires considerable a priori domain knowledge and because of that, majority of computer science students are excluded from CTF events. Figure 2 shows an example of a possible network configuration that a team has to perform when participating in a CTF competition.

Players who cannot solve any challenges quickly stop playing. Most CTFs do not support giving partial credit, which means students do not get any points by getting close to the solution; it's either all or nothing. This may be a challenge, but it can also pose as a factor differentiating motivated and driven students from those who are not. (Chung & Cohen, 2014.)

Dabrowski et al. (2015) also note that grading of submissions needs to be automated in order to give students immediate feedback, which in turn increases the engagement levels of participants. However, as Chothia & Novakovic (2015) point out, plagiarism is a potential problem if submitting flags is the only way of solution verification.

Vykopal et al. (2020) also mention encountering plagiarism. Since they collected transaction logs from the CTF portal, they were able to see if: (1) two or more students submitted the same flag within a short period of time, (2) submitted a flag without actually downloading the file containing the flag or (3) submitted flags to consecutive locked challenges (solving one challenge unlocks the next) within a suspiciously short time frame. By analysing the logs they caught three students, who admitted submitting flags acquired from peers. (Vykopal et al., 2020.)

Students do not always play by the rules of the competition. For example, Werther et al. (2011) write that some students removed executables from their machines which the CTF infrastructure relied upon in grading the points. Also, while the organisers did try to capture all the network traffic generated during the competition, the capture file was corrupted, which in turn prevented them to investigate potential volume-based denial of service (DOS) attacks, which were forbidden during the competition. (Werther et al., 2011.) Chung & Cohen mention that there are known cases when students have attacked the CTF website itself and have attacked other teams using the website.

Dabrowski et al. (2015) note that arranging a course like theirs, which has a hundred or more participants and various challenges, takes time to develop. They started with two physical servers and a script-based approach and have in a decade moved to a more unified and automated solution using Python, database and virtual machines. Logan & Clarkson (2005) remind that proper lab network configuration is especially important, as the exercises may contain activities that are legal only if strictly confined to the lab environment and continue to say that if the lab network is not properly isolated, there may be a risk of breaking the law or university accepted use policies.

Many CTF games consist of individual puzzles or challenges. Quality assurance is an essential part of challenge development, but it is often overlooked, which leads challenges to be improperly valued or even unsolvable. Broken websites are a common problem amongst CTF competitions. (Chung & Cohen, 2014.)

Chung & Cohen (2014) also note that challenge avoidance is an unsolved problem in CTF games, since many participants judge the difficulty of the task solely based on the points that are given by solving the task. A related problem is noted by McDaniel et al. (2016), who noticed that most of the students proceeded through challenges in sequential order, even though the order in which the challenges can be undertaken was not restricted in any way. However, Vykopal et al. (2020) note that challenge chains can help students more easily perceive recommended challenge execution order.

McDaniel et al. (2016) point out that the generational gap between CTF organisers and participants made the participants to not understand some of the hints provided by the organisers. Similarly, the after-game survey conducted by Vykopal et al. (2020) indicated that hints were the most dissatisfying piece of the game. Last, McDaniel et al. (2016) found the concluding wrap-up session not to engage students in a conversation.

4.4 To compete or not to compete

Capture-the-flag games are inherently competitive in their nature and many sources mention competition as a positively motivating factor for students. In their post-course questionnaire, Dabrowski et al. (2015) asked students how they regarded the competitive aspects, i.e. the live scoreboard, of the course. Results were quite mixed. 63% of the answerers neither disagreed or agreed, disagreed or strongly disagreed with the claim that competition incentivised them to put more effort in the course. Roughly two thirds neither disagreed or agreed, disagreed or strongly disagreed with the claims that they tried to be better than other students or spent extra effort to show up in the competition scoreboard.

Vykopal et al. (2020) asked the students in the after-game survey (N=16) about how they perceived the scoreboard feature. On a 5-point likert scale ranging from 0 = *Not at all* to 4 = *Very much,* median of the answers was *1 (Slightly)*. Students also did not seem to talk much about their scores with their peers, since the median answer to this was also *1 (Slightly)* on the same scale.

4.5 Ethical and legal aspects

Ethicalness of cyber security education is addressed more in detail by Logan & Clarkson (2005). They argue that most of the information security courses with hands-on lab exercises concentrate too much on the offensive and technical side of information security and present an unrealistic view of what skills are needed to become an information security professional. However, Mirkovic & Peterson (2014) argue that benefits of teaching students to attack systems outweigh the negative [ethical] aspects of doing so. According to them, students cannot really learn to defend against the attacks without being exposed to adversarial behaviour.

According to Logan & Clarkson (2005), an overwhelming majority of attacks against financial companies have come from insiders exploiting non-technical vulnerabilities, such as organization procedures and processes and have not required much technical skills. Course designers should also keep the inevitable failure of security measures in mind when designing the content of the labs. Students should also practice recovering from detected intrusions and practice planning for disasters instead of focusing purely on offensive methods. (Logan & Clarkson, 2005.)

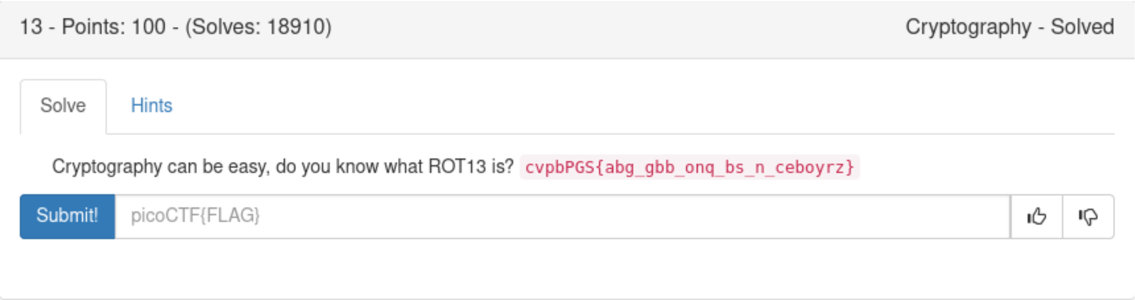
Since hacking competitions always involve activities that can be used for both good and evil, it is necessary for the educators to also incorporate the ethical implications of the skills and techniques that students will learn (Conti et al., 2011). Logan & Clarkson (2005) reviewed computer science major requirements of NSA-certified Centers of Academic Excellence in Information Assurance (CAE) Universities and looked if they include and/or require their students to include ethics or legal issues courses in their degree programs. Roughly two thirds (62%) had such courses, but 66% of schools did not require undergraduate students to attend such courses. Logan & Clarkson (2005) fear that by omitting ethical and legal side of information security from the degree programmes, universities could be training both “good guys” and “bad guys”. Students, however, do not always seem to think so darkly: Dabrowski et al. (2015) note that 82% of students did not agree with the claim that "*gamification might cause students to lose touch with the ethical questions regarding hacking*".

4.6 Good practices and ways to improve

In his text, Eagle (2013) compares pure CTF competitions to military exercises of same sort. Main differences between the two are that in CTF competitions, the organisers usually do not prepare the contestants for the competition nor do they offer any post-competition analysis of why and how teams performed the way they did. In military exercises however, competitors are often given exact prerequisites for attending the exercises and a detailed feedback after the exercise regarding their performance and deficiencies. If the challenge in question is a competition, releasing references to material relevant for solving the problems, walkthroughs explaining the necessary steps and guides detailing how the problem was constructed could be helpful in aiding students to learn from the games. Also, in case of an attack-defense competition, a full content of the network traffic generated during the competition and a detailed time line of successful attacks could enable teams to self-assess their activities. If the challenge is more of an educative type, in addition to ways described in previous sentences, links to material relevant for solving the problems can help participants. Walkthroughs explaining the necessary steps to solve the problems can also help many participants learn by example. (Eagle, 2013.)

Worthiness of walkthroughs was also observed by McDaniel et al. (2016), who state that an introductory walkthrough, which helped the students catch at least one flag early in the game, encouraged students to continue solving the challenge. They also note that the first few challenges needed to be easier, so that they were less likely to make frustrated students drop out of the game. An example of a educational CTF is given by Werther et al. (2011). The MIT Lincoln Laboratory CTF described in their paper offered pre-competition lectures, labs, wiki pages and a mailing list to help students prepare for the event. Chung & Cohen (2014) mention involving a peer-level organizer, i.e. a fellow student, in the development process of the CTF to ensure that the challenges are appropriately challenging.

Many private competitions offer prizes and while academia cannot compete with those prizes, Conti et al. (2011) and Mirkovic et al. (2015) mention other ways to incentivise participation in educational hacking competitions: integrating CTFs into curriculum, giving books as prizes and publicly recognising those who do well in the competitions.

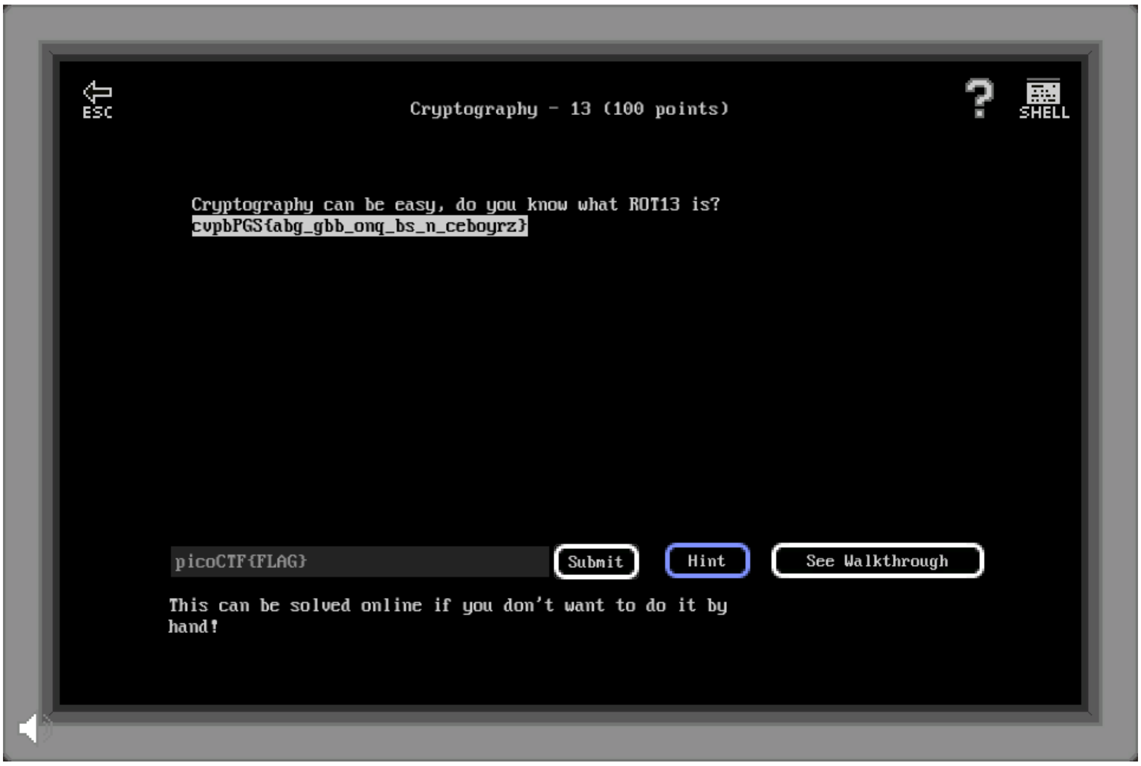


13 - Points: 100 - (Solves: 18910)

Cryptography - Solved

Cryptography can be easy, do you know what ROT13 is? `cvpbPGS{abg_gbb_onq_bs_n_ceboyrz}`

Figure 3: A screenshot of PicoCTF 2019's text-based mode (picoCTF - CMU Cybersecurity Competition, 2020).



Cryptography can be easy, do you know what ROT13 is?
`cvpbPGS{abg_gbb_onq_bs_n_ceboyrz}`

This can be solved online if you don't want to do it by hand!

Figure 4: A screenshot of PicoCTF 2019's interactive game viewer (picoCTF - CMU Cybersecurity Competition, 2020).

As described by Chapman et al. (2014), PicoCTF has a traditional text-based mode and an interactive game viewer mode, between which the participants can choose. Both modes include the same challenges. Usage of the mode depended heavily on the level of the student's education: younger students chose the interactive mode more often than older students, which, according to Chapman et al. (2014), tells that the interactive mode succeeded in engaging younger and less experienced students. Figures 3 and 4 show the difference between PicoCTF 2019's text-based mode and interactive game viewer, when viewing the same challenge.

Vykopal et al. (2020) suggest building flag-sharing detection capabilities into the CTF platform to help in revealing illicit flag sharing by participants. They also stress that collaboration rules and plagiarism detection guidelines need to be clearly defined in the very beginning of the game.

Regarding the fears of teaching offensive capabilities to students, Mirkovic & Peterson (2014) require an ethics slide set to be shown before the CTF exercises and an ethical offense quiz to be passed before students must pass before participating in the CTF exercise. Their CTF implementation also requires students to play both the offensive and defensive part during the game. A post-mortem analysis of the exercise is performed by the instructors after each exercise.

5. Findings and discussion

The primary purpose of this study was to evaluate advantages and disadvantages of using capture-the-flag games in cyber security education based on prior research.

Table 1: Summary of advantages of CTF games in education according to sources

Advantage	**Source(s)**
Improved student motivation	Chapman et al., 2014; Chothia & Novakovic 2015; Dabrowski et al., 2015; Katsantonis et al., 2017; McDaniel et al., 2016; Mink & Greifeneder, 2010; Mirkovic et al., 2015
Better practical knowledge	Ariyapperuma & Minhas, 2005; Mink & Greifeneder, 2010; Mirkovic et al., 2015
Better general understanding of cyber security	Burns et al., 2017; Mirkovic et al., 2015; Werther et al, 2011
Better grades resulting from the approach	Ariyapperuma & Minhas, 2005
Strong indication of overall course performance	Chothia & Novakovic 2015; Vykopal et al., 2020
Increased interest in cyber security	Dabrowski et al., 2015; Mirkovic et al., 2015; Werther et al, 2011
Increased confidence in computer security skills	Werther et al, 2011
More vulnerabilities found	Mink & Greifeneder, 2010

Table 2: Summary of disadvantages of CTF games in education according to sources

Disadvantage	**Source(s)**
High knowledge requirements	Burns et al., 2017; Chung & Cohen, 2014; McDaniel et al., 2016; Werther et al, 2011
Complex technical requirements	Dabrowski et al., 2015; Logan & Clarkson, 2005; Werther et al, 2011
Plagiarism is easy	Chothia & Novakovic 2015; Vykopal et al., 2020
Students try to bend the rules	Werther et al, 2011; Chung & Cohen, 2014
Quality assurance is often overlooked	Chung & Cohen, 2014
Challenge avoidance and challenge order problems	Chung & Cohen, 2014; McDaniel et al., 2016
Hints are hard to get right	McDaniel et al., 2016; Vykopal et al., 2020
Ethical implications are concerning	Conti et al. (2011); Logan & Clarkson, 2005

Table 1 summarises advantages and table 2 summarises disadvantages of using capture-the-flag games in cyber security education. Reported benefits of using capture-the-flag games in cyber security education include higher student motivation (McDaniel et al., 2016; Katsantonis et al., 2017) and better practical knowledge resulting from the approach (Burns et al., 2017; Ariyapperuma & Minhas, 2005).

Reported challenges stemming from the format include high knowledge requirements from both organisers and participants (Burns et al., 2017; McDaniel et al., 2016; Werther et al., 2011) and complex technical requirements (Dabrowski et al., 2015; Chung & Cohen, 2014). High requirements regarding both knowledge and technical requirements are also illustrated by Figure 2.

Some sources also express concerns regarding ethical issues of teaching students offensive techniques (Logan & Clarkson, 2005; Conti et al., 2011), while other sources are not so concerned (Dabrowski et al., 2015; Mirkovic & Peterson, 2014). None of the sources that expressed their concern thought of the ethical problem this way: could teaching defensive methods and system administration skills help potential hackers circumvent the protections more easily? The coin always has two sides.

Some sources also talk about competitive aspects (Dabrowski et al., 2015; Vykopal, Svabensky & Chang, 2020), good practices and possible improvements to the format (Eagle, 2013; Werther et al., 2011).

In total, Tables 1 and 2 both have eight categories each. This summarises the advantages and disadvantages of using CTF games in cyber security education quite well. There are multiple advantages and such games can be a valuable tool, but they have to be used with care, or else there might not be much to be gained.

5.1 Contribution

The main contribution of this thesis is that it answers to the research question "*what are the advantages and disadvantages of using capture-the-flag games in cyber security education*". Findings can be leveraged in deciding what kind of education methods to use in a cyber security course or if a CTF game should even be considered.

A summary of suggested good practices and possible improvements to the format is also given in the last chapter of prior research and column 'implications on practices' of Appendix A.

5.2 Limitations

A distinct limitation of this study was the limited number of sources that used quantitative research methods. Moreover, many sources that collected quantitative data had only collected it within a very limited scope. Thus, many sources can only be seen as providing only anecdotal evidence.

Quantitative research essentially means systematically measuring a phenomenon to transform it to a numerical form. Therefore, quantitative research assumes that the phenomenon can be measured. Quantitative research can measure a wide variety of phenomena, from simple distance measurements to more vague things like how people feel. The data from measurements is analysed for trends and relationships. (Watson, 2015).

Variable is an important term in quantitative research. A variable is a measurable thing like distance or sound pressure level. Variables are divided into two categories, independent and dependent. (Watson, 2015.) If we would be studying the relationship between course grades and education methods (e.g., labs versus CTF games), course grade would be the dependent variable and education method would be the independent variable.

Two broad categories of research design, experimental and survey, exist in quantitative research. In experimental design, the researcher has the ability to manipulate the independent variable to study its effect on the dependent variable. In survey design, data can be gathered by distributing questionnaires, by interviewing or by observation. The data from quantitative research is analysed statistically. Such values as percentages, mode, median and mean can be dug out from the data. Then, conclusions can be inferred from the data using inferential statistics. (Watson, 2015.) Many tools, including SPSS, exist, that are directed towards statistical analysis.

As can be seen based on prior research, this particular subtopic of science needs more research based on quantitative research methods, preferably using both experimental and survey design approaches.

Last, this literature review was not systematic and did not follow strict guidelines in source selection. Many publication databases were left outside literature search because of time limitations.

5.3 Future work

As we have learned in the prior research section, there has been very little formal research about using capture-the-flag games in cyber security education. Quantitative research could be used in the future to compare the impact of the so-called traditional methods of teaching and more hands-on -oriented methods taking advantage of gamification. Of course, this is not a trivial task and may require years of observance.

One aspect that is a little easier to examine and may be done within a period of one course is how students themselves feel the impact of using capture-the-flag games on their study motivation, interest in cyber security and other things. Simple pre- and post-course questionnaires with Likert scales could be used to compare how students' knowledge and motivation increases within the period of the course. More complex relationships, like how likely is it that a student will end up in a cyber security job depending on if he/she took a cyber security course utilising a capture-the-flag game or a traditional lecture-based course, could be analysed, although this would require data from multiple sources and from a long period of time.

A controlled experiment between utilising CTF games versus traditional lab assignments could be organised to study the differences in students' motivation, engagement level, learning results and other appropriate aspects of education.

I also touched the ethical (and unethical) aspects of learning cyber security by playing CTF games. Capture-the-flag games usually include using some kind of offensive methods. Therefore, it would be interesting to investigate if teaching cyber security by using capture-the-flag games leads more students to utilise these skills "on the dark side", ie. penetrating illegally into computer systems and networks. Some sources mentioned that students may be drawn to "the dark side" by introducing them to offensive penetration techniques. It would be very interesting to see proper research done in this area, e.g. what are the causal relationships in this context.

All of the suggested study topics suffer from the same disadvantage: there is a need for controlled data preferably accumulated within a period of multiple courses utilising different teaching methods. Considering that, it is not very surprising that it is hard to find sources that have studied these topics systematically.

6. Conclusions

This thesis explored if CTF games are are viable solution to teaching cyber security. Research method used is a narrative literature review. 16 academic sources were reviewed, nine of which used quantitative research methods. A limitation of this study was the limited number of sources that used quantitative research methods. Many sources can only be seen as providing only anecdotal evidence. This literature review was not systematic and did not follow strict guidelines in source selection. Many publication databases were left outside literature search because of time limitations.

Prior research showed that CTF games had a positive impact on participants’ motivation and engagement levels. In some studies, CTF games were found to lead to statistically better learning results and better understanding of computer security.

Organising such games was found to be a challenging job and knowledge is required from both organisers and participants. CTF environments are complex and support staff is needed in organising CTF games. Designing the challenges to be appropriately challenging is a difficult task and quality assurance is important, but often overlooked part of the design process.

Ethical implications of teaching offensive computer security methods were a concern to many, but no research on this topic has so far been conducted. Automated approval of flag submissions in the games was observed to lead students to illicitly share flags.

Suggestions regarding future research on this topic are: (1) use of more formal methods, namely quantitative research methods, (2) investigate relationship between attending course with CTF elements and likelihood to pick up cyber security career, (3) perform a controlled experiment comparing CTF games and traditional lab assignments and (4) investigate if teaching offensive methods leads students to commit illegal actions with the skills acquired.

7. References

Affordance. (n.d.). In *Merriam-Webster.com dictionary*. Retrieved 17.5.2020 from https://www.merriam-webster.com/dictionary/affordance

Ariyapperuma, S., & Minhas, A. (2005). Internet security games as a pedagogic tool for teaching network security. *Paper presented at the Proceedings - Frontiers in Education Conference, FIE*, , 2005 S2D-1-S2D-5.

Burns, T.J., Rios, S.C., Jordan, T.K., Gu, Q., & Underwood, T. (2017). Analysis and Exercises for Engaging Beginners in Online CTF Competitions for Security Education. *ASE @ USENIX Security Symposium*.

Chapman, P., Burket, J., & Brumley, D. (2014). PicoCTF: A Game-Based Computer Security Competition for High School Students. *3GSE*.

Chothia, T. & Novakovic, C. (2015). An Offline Capture The Flag-Style Virtual Machine and an Assessment of Its Value for Cybersecurity Education. *3GSE*.

Chung, K., & Cohen, J. (2014). Learning Obstacles in the Capture The Flag Model. *3GSE*.

Conti, G., Babbitt, T., & Nelson, J. (2011). Hacking competitions and their untapped potential for security education. *IEEE Security and Privacy*, 9(3), 56-59. doi:10.1109/MSP.2011.51

CTFtime.org. (2020). What is Capture The Flag?. Referenced 29.3.2020, available at: https://ctftime.org/ctf-wtf/

Dabrowski, A., Kammerstetter, M., Thamm, E., Weippl, E.R., & Kastner, W. (2015). Leveraging Competitive Gamification for Sustainable Fun and Profit in Security Education.

Eagle, C. (2013). Computer security competitions: Expanding educational outcomes. *IEEE Security and Privacy*, 11(4), 69-71. doi:10.1109/MSP.2013.83

Gavas, E., Memon, N., & Britton, D. (2012). Winning cybersecurity one challenge at a time. *IEEE Security and Privacy*, 10(4), 75-79. doi:10.1109/MSP.2012.112

Hacking. (n.d. a). In *Cambridge English dictionary*. Retrieved 17.5.2020 from https://dictionary.cambridge.org/dictionary/english/hacking

Hacking. (n.d. b). In *Merriam-Webster dictionary*. Retrieved 17.5.2020 from https://www.merriam-webster.com/dictionary/hacking

Hendrix, M., Al-Sherbaz, A. & Bloom, V. (2016). Game Based Cyber Security Training: are Serious Games suitable for cyber security training?. *International Journal of Serious Games*. 3. 10.17083/ijsg.v3i1.107.

Katsantonis, M., Fouliras, P., & Mavridis, I. (2017). Conceptual analysis of cyber security education based on live competitions. *Paper presented at the IEEE Global*

Engineering Education Conference, EDUCON, 771-779. doi:10.1109/EDUCON.2017.7942934

Logan, P. Y., & Clarkson, A. (2005). Teaching students to hack: Curriculum issues in information security. *Paper presented at the Proceedings of the Thirty-Sixth SIGCSE Technical Symposium on Computer Science Education, SIGCSE 2005*, 157-161.

McDaniel, L., Talvi, E., & Hay, B. (2016). Capture the flag as cyber security introduction. *Paper presented at the Proceedings of the Annual Hawaii International Conference on System Sciences,* , 2016-March 5479-5486. doi:10.1109/HICSS.2016.677

Mink, M., & Greifeneder, R. (2010). Evaluation of the offensive approach in information security education doi:10.1007/978-3-642-15257-3_18

Mirkovic, J., & Peterson, P. (2014). Class Capture-the-Flag Exercises. *3GSE.*

Mirkovic, J., Tabor, A.E., Woo, S.S., & Pusey, P. (2015). Engaging Novices in Cybersecurity Competitions: A Vision and Lessons Learned at ACM Tapia 2015.

picoCTF - CMU Cybersecurity Competition. (2020). Referenced 11.5.2020, available at: https://picoctf.com/

Raman, R., Sunny, S., Pavithran, V., & Achuthan, K. (2014). Framework for evaluating capture the flag (CTF) security competitions. *Paper presented at the 2014 International Conference for Convergence of Technology, I2CT 2014*, doi:10.1109/I2CT.2014.7092098

Raymond, E. (Ed.). (1996). *The new hacker's dictionary*. Mit Press.

SaarCTF. (2020). Referenced 5.9.2020, available at: https://ctf.saarland/setup

Salminen, A. (2011). *Mikä kirjallisuuskatsaus?: Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin.* Vaasa: Vaasan yliopisto.

Vykopal, J., Svabensky, V., & Chang, E. -. (2020). Benefits and pitfalls of using capture the flag games in university courses. *Paper presented at the Annual Conference on Innovation and Technology in Computer Science Education, ITiCSE,* 752-758. doi:10.1145/3328778.3366893

Watson, R. (2015). Quantitative research. *Nursing Standard, 29*(31).

Werther, J., Zhivich, M., Leek, T., & Zeldovich, N. (2011). Experiences in cyber security education: The MIT lincoln laboratory capture-the-flag exercise. *Paper presented at the 4th Workshop on Cyber Security Experimentation and Test, CSET 2011*

Appendix A. Overview of sources

Source	Purpose of the study	Research methods	Theoretical background	Main findings	Implications on practices	Research recommendations
Ariyapperuma & Minhas (2005)	Investigate the suitability of online security games as a pedagogic tool for teaching network security in an educational framework	Quantitative: logs, questionnaires Qualitative: interviews	-	Statistically significantly better results in the grades for CTF group	Results are universal and the methodology can be applied universally (belief)	Evaluate similar online games addressing different subject content
Burns, Rios, Jordan, Gu & Underwood (2017)	Identify the most concerning security issues, create exercises and assess them	Quantitative: surveys	-	83% of students think exercises helped to understand computer security	Provide partial solutions and hints for students	Research defensive techniques and system administration skills
Chapman, Burket & Brumley (2014)	Present game design, evaluation of it and provide insights into students	Quantitative: logs, surveys	-	Positive educational experience according to students and instructors	Younger students benefit especially from visual game-based elements	Perform closely controlled experiments on smaller groups, collect longitudinal data
Chothia & Novakovic (2015)	Analyse how students' performance on the CTF-style challenges correlates with their achievement in the formative assessment and examination	Quantitative: logs, surveys, course grades	-	CTF exercises popular among students, ability to solve them correlates with overall grades	Flag-only grading may lead to plagiarism, so additional assessment techniques needed	Continue analysis of how well acquiring flags in CTF-style challenges corresponds to traditional educational assessment
Chung & Cohen (2014)	Present insights and lessons learned from organising CSAW CTF	Qualitative: insights, lessons learned	-	Solving challenges can be intimidating to beginners etc.	Involve peer-level people in design process	-
Conti, Babbitt & Nelson (2011)	examine untapped competitions' potential and identify those that can energize and enhance information	Article: informal	-	Hacking competitions can help educators infuse learning and excitement into information security education	Every information security education program should include CTF	-

Source	**Purpose of the study**	**Research methods**	**Theoretical background**	**Main findings**	**Implications on practices**	**Research recommendations**
	security education in			programs	competitions	
Dabrowski, Kammerstetter, Thamm, Weippl & Kastner (2015)	Assess results of using gamification in university cyber security courses	Quantitative: surveys Qualitative: interviews	Gamification study by Hamari, Koivisto & Sarsa (2014)	Students enjoy the game-like competitive teaching concept, also raises interest in IT security and pushes to put more effort into the course and practical exercises	Plan to add additional security courses relying on the same gamification concept	-
Eagle (2013)	Describe types of CTF competitions, list their positive and negative aspects, list possible improvements	Article: informal	-	-	Walkthroughs, guides, material, network captures can improve CTF value	-
Katsantonis, Fouliras & Mavridis (2017)	Construct a concept map of live (CTF) competitions	Literature review, conceptual analysis	Learning theories	Drawbacks in competitions' aims, learning obstacles, competitions' organisational and functional issues	Competition attributes can be traded. Analysis scheme developed to help develop future competitions.	-
Logan & Clarkson (2005)	Explore the issues involved in designing an information security course with lab components that involve destructive actions	Qualitative: review universities' curricula Quantitative: statistics of universities' curricula	-	Few universities require students to attend ethics and/or legal issues courses	Use accounts that work only under monitoring. Create course level AUPs (accepted usage policies). Careful consideration in course design recommended.	Include ethics in future studies.
McDaniel, Talvi & Hay (2016)	Assess results of using CTF competition in teaching middle- and high school students	Qualitative: observing	-	Effective way to teach computer security.	Provide introductory challenges to help beginners.	-
Mink & Greifeneder (2010)	Present an experimental setup to evaluate the offensive	Empirical research Quantitative:	-	Teaching offensive aspects leads to a better understanding of	Information security courses should teach	Gather more empirical data and use the presented setup.

Source	Purpose of the study	Research methods	Theoretical background	Main findings	Implications on practices	Research recommendations
	approach in information security education and conduct an empirical study	questionnaires, practical tests		information security and that it is more motivating	offensive aspects	Use more subjects. Expand the tests into other relevant topics.
Mirkovic & Peterson (2014)	Describe class CTF exercises, recount experiences	Report: informal	-	Benefits of teaching students to attack systems outweigh the negative [ethical] aspects of doing so (argument)	Require an ethics slide set to be shown before the CTF exercises and an ethical offense quiz to be passed	-
Mirkovic, Tabor, Woo & Pusey (2015)	discuss experience in using Class Capture-the-Flag Exercises (CCTFs)	Quantitative: surveys (pre and post) Qualitative: interviews	-	CTF exercises improved participants' self-efficacy in practised topics	Balance teams, collect better data, incentivise students to answer to surveys	-
Vykopal, Svabensky & Chang (2020)	Summarise experience from using jeopardy CTF games as homework assignments	Quantitative: surveys, logs, course grades	-	Statistically significant relationship between CTF solving and other forms of assessment. Illicit flag-sharing can be a problem.	Implement means to catch flag sharing. Implement dynamically served hints.	-
Werther, Zhivich, Leek & Zeldovich (2011)	Describe experience in designing, organizing, and running an education-focused CTF, and discuss teaching methods, game design, scoring measures, logged data, and lessons learned	Quantitative: survey, logs	-	Increased confidence in computer security skills. Increase in interest in computer security.	Incorporate feedback in the upcoming years' competitions.	Analyse the CTF effect in more detail in future