

# Enhancing Cybersecurity Skills by Creating Serious Games

Valdemar Švábenský  
Masaryk University  
Faculty of Informatics  
Institute of Computer Science  
Brno, Czech Republic  
svabensky@ics.muni.cz

Milan Cermak  
Masaryk University  
Faculty of Informatics  
Institute of Computer Science  
Brno, Czech Republic  
cermak@ics.muni.cz

Jan Vykopal  
Masaryk University  
Institute of Computer Science  
Brno, Czech Republic  
vykopal@ics.muni.cz

Martin Laštovička  
Masaryk University  
Faculty of Informatics  
Institute of Computer Science  
Brno, Czech Republic  
lastovicka@ics.muni.cz

## ABSTRACT

Adversary thinking is an essential skill for cybersecurity experts, enabling them to understand cyber attacks and set up effective defenses. While this skill is commonly exercised by Capture the Flag games and hands-on activities, we complement these approaches with a key innovation: undergraduate students learn methods of network attack and defense by creating educational games in a cyber range. In this paper, we present the design of two courses, instruction and assessment techniques, as well as our observations over the last three semesters. The students report they had a unique opportunity to deeply understand the topic and practice their soft skills, as they presented their results at a faculty open day event. Their peers, who played the created games, rated the quality and educational value of the games overwhelmingly positively. Moreover, the open day raised awareness about cybersecurity and research and development in this field at our faculty. We believe that sharing our teaching experience will be valuable for instructors planning to introduce active learning of cybersecurity and adversary thinking.

## CCS CONCEPTS

• **Social and professional topics** → **Computer science education**; • **Security and privacy** → *Network security*;

## KEYWORDS

cybersecurity, game-based learning, project-based learning

### ACM Reference Format:

Valdemar Švábenský, Jan Vykopal, Milan Cermak, and Martin Laštovička. 2018. Enhancing Cybersecurity Skills by Creating Serious Games. In *Proceedings of 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE'18)*. ACM, New York, NY, USA, 6 pages. <https://doi.org/10.1145/3197091.3197123>

*ITiCSE'18, July 2–4, 2018, Larnaca, Cyprus*

© 2018 Copyright held by the owner/author(s). Publication rights licensed to the Association for Computing Machinery.

This is the author's version of the work. It is posted here for your personal use. Not for redistribution. The definitive Version of Record was published in *Proceedings of 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education (ITiCSE'18)*, <https://doi.org/10.1145/3197091.3197123>.

## 1 INTRODUCTION

As the importance of securing computer systems grows, so is the cybersecurity workforce shortage. It is expected that by 2022, 1.8 million jobs that require cybersecurity expertise will be unfilled [11], stressing the importance of educating security professionals. An efficient security education balances theoretical knowledge and concepts, traditionally taught at universities, with practical applications in real-world settings.

To complement traditional courses on computer networks and security at our faculty, we developed two practical, project-oriented courses on cyber attacks and defense. We focus especially on adversary thinking, a crucial skill for cybersecurity experts who must be able to think like an attacker in order to set up effective countermeasures. While this skill can be exercised in Capture the Flag games, challenges, and competitions, our courses introduce an innovative approach. The learners are guided to create a serious security game deployed at the KYPO cyber range [19], which allows emulating real threats and attacks in a controlled environment.

With respect to the thorough literature survey below, we claim that our courses are unique in combining a serious game project with hands-on cybersecurity. In this paper, which can be of particular interest to fellow security instructors, we share a detailed description of the design, content, and assessment methods of the courses. Next, we present and analyze student surveys. Finally, we share the lessons learned in three semesters of teaching and continuously innovating the courses. We highlight that the students' projects transfer to practice. All learners present their results to other students of the faculty at an open day event, and the best games are even used for further training by our security team.

## 2 RELATED WORK

To map the current landscape of similar courses, we searched for existing university courses and literature as well as curricular guidelines for cybersecurity education. We examined course catalogs of the 10 currently top-ranked computer science (CS) universities based on research and teaching (as listed in QS and THE World University Rankings, respectively). In the course catalog of each university, we searched for topics such as (cyber)security, networks, or cryptography. The search was restricted to the CS and engineering

departments. We discovered relevant courses, for example, MIT's Network and Computer Security<sup>1</sup>, dealing with cryptography, secure programming, or internet security. Most often, the courses were taught using a combination of lectures, (group) homework assignments, (group) projects, student presentations, and a final test. However, we did not find any course dealing in-depth with penetration testing, learning by teaching, and creating serious games in a cyber range as our courses do.

We also examined related papers from the past 5 years on major CS education conferences such as ACM SIGCSE, ITiCSE, ICER, and USENIX ASE (formerly 3GSE). The publications describe learning cybersecurity skills in a practical and engaging way by using video games [16], Capture the Flag events [15], and even card games [4]. Gamification of cybersecurity courses by adding a background story [2], competitive game elements [3], or experience points [14] is popular, resulting in increased student motivation, interest in security topics, and performance. While hands-on cybersecurity labs described in literature [10, 17] cover similar content as our courses, they do not include a serious game project as a teaching method. On the other hand, existing game development courses [6, 20] focus mostly on programming or game design as such but not on cybersecurity.

### 3 DESCRIPTION OF THE COURSES

This section describes the current model of our two courses, the Introductory and the Follow-up. We established the model after three semesters of experience. The courses are offered for CS university students and include 12 weeks of 2-hour sessions plus homework assignments. Table 1 lists the learning outcomes of both courses<sup>2</sup>. Table 2 provides the schedule and the structure of the courses.

The courses follow recent standards and comprehensive curricular guidelines for cybersecurity education, namely these NSA/DHS CAE Knowledge Units [9] and corresponding NIST NICE competencies [8]: cyber defense, cyber threats, networking concepts, network defense, and penetration testing. Moreover, the courses strongly correspond with NCC Information Security Curricula [1] courses Network Security I and Ethical Hacking. Finally, they cover selected topics of the following knowledge units in the Joint Task Force Cybersecurity Curricula [11]: Data integrity and authentication, Network Defense, and System Control, along with adding extra features described in this section.

Apart from connecting to the cybersecurity education guidelines, the courses also employ methods grounded in pedagogical theory and teaching practice [12]. The sessions include a combination of lectures, supervised student practice, and group work. Using the terminology of an extensive survey of active learning methods in computer science [13], we focus on *integrating labs with lectures*, *cooperative learning*, and *project-based learning*.

#### 3.1 Cyber Attack Simulation (Introductory)

The first course focuses on the basics of offensive cybersecurity. It provides both theoretical and practical experience to students, who

elaborate a game project on penetration testing in teams of two people (three if the total number of students is odd). The course is intended for at most 18 undergraduates (sophomores and juniors) who passed prerequisite courses on privacy and computer networks and systems, can read technical papers, and write in English.

In the first session, students play an exemplary security game to see what we expect from their project. During the first, theory part of the course, lectures and exercises introduce students to security topics. The acquired knowledge and skills are used in the second, project part of the course during the creation of Capture the Flag games, whose form is described in [18]. The course ends with the Open Day event, where the students publicly present their games.

The theory part of the course explains cybersecurity topics based on lecturers' practical experiences from the day-to-day operation of a university computer security incident response team (CSIRT). Students get familiar with common attacks (such as scanning, exploits, and threats specified by the OWASP Top 10 project), basics of forensic analysis, and attack detection and mitigation. During the sessions, students perform hands-on exercises to immediately verify their theoretical knowledge in practice. Each student has own learning sandbox in the KYPO cyber range containing attacking and vulnerable machines. The sessions are followed by weekly homework assignments, which involve using serious games created in the previous course runs, tasks in the learning sandbox, or freely available online resources<sup>3</sup>.

During the project part of the course, student teams create their own game. The instructors form the teams based on students' performance in the exemplary game and a subsequent survey. The aim is to pair less skilled or less experienced individuals with advanced learners to simulate real workplace. Afterward, students are introduced to the basics of creating serious games. Then, they select a game topic, such as exploiting a vulnerability to gain access to a system, from a list of predefined topics. Each team proposes a story of the game, designs its levels, and prepares virtual machines in the cyber range on which the game will be played. During the sessions, each team presents the proposal to other students and lecturers and receives feedback to improve the proposal. The results are tested by members of the CSIRT, allowing the teams to find out how experts react and how the game can be adjusted. The entire course is concluded by the Open Day event where the visitors (usually students from the whole faculty) play the created games under the guidance of the student authors. Based on the feedback received at the event, the students finish the games including supplementary materials and submit them to instructors for the final evaluation.

Although the course is taught in the Czech language, all materials used by instructors or prepared by students (for both the presentations and projects) are in English. However, the instruction itself and communication within students' teams is conducted in Czech. This is motivated by the fact that English is considered a common language in the cybersecurity field, but also by the concern that communication only in English might create a barrier for those less fluent in the language.

<sup>1</sup><https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-857-network-and-computer-security-spring-2014/index.htm>

<sup>2</sup>Selected learning outcomes correspond to the following NIST NICE [8] knowledge, skills, and abilities descriptions: K0003, K0005, K0013, K0070, K0106, K0177.

<sup>3</sup>Such as <https://www.hackthissite.org> or <https://hack.me/>.

**Table 1: The learning outcomes of both the Introductory and the Follow-up course**

	Cyber Attack Simulation (Introductory)	Cyber Defense Tutorial (Follow-up)
<b>Knowledge</b>	Describe the stages of a cyber attack	
	Understand system and application security threats and vulnerabilities (e. g., authentication attacks, DoS attacks, MitM attack, OWASP Top 10 vulnerabilities)	
	Name cyber defense and vulnerability assessment tools and their capabilities	
	Explain laws, regulations, policies, and ethics related to security and privacy	
<b>Skills</b>	Perform penetration testing focused on a particular threat or vulnerability	Secure a particular network service or application (e. g., Apache or Wordpress)
	Use a cyber range both as a learner and as a designer of games running in it	Perform penetration testing of the service or application
<b>Experience</b>	Give a presentation explaining the vulnerability selected for the game	
	Practical work in small teams (Introductory) or individual (Follow-up) including setting up and maintaining systems, assessing their vulnerabilities, and developing a new serious game or a gamified training tutorial	
	Give two presentations of the final project (Test run and Open day) and instruct learners who use it	

**Table 2: The schedule and the structure of both the Introductory and the Follow-up course**

Week	1	2	3	4	5	6	7	8	9	10	11	12	18
<b>Introductory</b>	Exemplary game	Network security basics, hands-on labs, homework				Game design tutorial, topic choice		Presentations, consultations			Test run	Open day	Final result
<b>Follow-up</b>	Topic choice	Concept consultations		Concept final-ization		Technical consultations			Presentation				

### 3.2 Cyber Defense Tutorial (Follow-up)

The second course is offered for at most 6 students who passed the Introductory course. This number of students enables the instructor to advise student projects thoroughly.

The students learn how to secure a particular network service or application by designing a gamified tutorial on that topic. The tutorial consists of step-by-step instructions that enable the learner to secure the service or application running on a host in the cyber range. This part may be followed by automated attacks against the service or application, immediately enabling learners to test whether their countermeasures were set properly. Students are allowed to enroll in the course repeatedly in multiple semesters if they choose different project topic each time.

In contrast to the Introductory course, students work on their projects individually and from the beginning, without the theoretical introduction by instructors. The whole course is driven by students rather than teachers. Since the students completed the Introductory course, they already have experience in creating a game in the cyber range. This allows them to focus on the project topic chosen in the first week. In the following weeks, they elaborate the game outline on their own at home and consult ideas and issues they encounter with the instructor at course sessions. Besides the consultations, the sessions contain brief lectures on game tutorial creation essentials, including automation of installation and host configuration in the cyber range or orchestration of attacks execution. The students also advise the learners from the Introductory course, since we believe that advice from peers has a larger impact on the students compared to the instructors. Similarly as in the first course, the students present and discuss their projects to get

feedback not only from the instructor but also from their classmates. The test run and the Open Day is shared with the Introductory course, followed by a final submission 6 weeks afterward.

## 4 PROJECT ASSESSMENT METHODS

### 4.1 Formative Assessment

While working on their game, students receive formative feedback in three settings: presentations of project milestones to the class, consultation sessions with the course tutors, and a test run of the game with security experts. All three occasions are detailed below.

*4.1.1 In-class presentations.* Both courses require the students to present their progress in brief talks. Students are given the structure of the presentation with the aim to help them focus on the content (e. g., explaining details of the vulnerability). The time limit of 5 to 10 minutes should force them to prioritize the key messages. The talks provide opportunities to receive feedback, both on the content and the presentation delivery, not only from instructors but also from peers. This is beneficial for the presenting team and even for other classmates observing the comments.

*4.1.2 In-class consultations.* In-person or e-mail consultations of students' projects is a prevalent method of the formative assessment, especially in the Follow-up course. Although students are instructed to find answers to their questions within the class or from open sources first, they are encouraged to ask the instructors for help with the cyber range. Learners often struggle with the configuration of virtual hosts, the specifics of a cyber range and the underlying virtualization platform, or the game structure (decomposing the attack stages into individual game levels). Since many problems are



**Figure 1: Open Day, students present their projects to peers**

recurring each semester, the instructors have the solutions ready, which saves the students a lot of time.

**4.1.3 Test run.** One week before the Open Day, cybersecurity experts review the students' projects and provide feedback so that the students can perfect the game. The test run is an informal live session that takes two hours. The reviewers play the game and immediately discuss its aspects with the student team.

## 4.2 Summative Assessment

The students present their projects to a broad audience after incorporating formative feedback from classmates, tutors, and experts. Finally, the teachers review and mark the final revision of each project. Both occasions are detailed below.

**4.2.1 Open Day.** At the end of the semester, all students of both courses present the games they created on the Open Day event. As Figure 1 shows, the event is very informal, with the goal of promoting the games of our students. During the event, our labs are open to the whole faculty so that anyone can freely come and try any of the students' games.

**4.2.2 Final project review.** After the Open Day, students have the last chance to improve their projects, which they then submit to instructors for a final evaluation. The instructors deploy the projects in the cyber range from scratch to check whether the submission is functional and contains all essential parts, such as documentation of host configuration in the cyber range. Students of the Follow-up course have to use a specific input format that can be processed by a tool for automated installation and configuration, such as Ansible.

## 4.3 Student Surveys from the Third Semester

We now report data and findings from the test run and the Open Day that took place at the end of the third semester, in December 2017. In this semester, we had 18 university students (16 males, 2 females), 15 of which were enrolled in the Introductory course and divided into 7 teams, plus 3 individuals from the Follow-up course.

**4.3.1 Test run.** 10 members of the CSIRT volunteered to test the projects. We assigned each tester to one of the 10 student projects with the intention to match the topic of the game and the tester's expertise. Before playing, we informed the testers about the goal of the game, prerequisites, and the estimated time of the gameplay. After playing, the testers completed a survey asking to compare the announced and actual time of playing and rate the educational

value of the game, its completeness, and overall quality. The game's educational value was rated on the following scale: None, Small, Medium, High, Huge. The game's degree of completion was rated on a scale from 0 (totally unfinished) to 10 (release candidate). Finally, the game's overall quality was rated on the following scale: Poor, Sufficient, Good, Very good, Excellent.

The announced time for all the games ranged from 15 to 45 minutes, with 30 minutes on average. Among the 10 testers, 4 reported that the estimate was accurate  $\pm 10$  minutes. The remaining 6 of them played longer than estimated, for additional 20 minutes on average. This shows that even in a relatively short game, the students tend to underestimate the required time. Next, 9 out of 10 testers stated that the games have a High educational value, with the possible usage in university or professional education. The completeness ranged from 4 to 8, with the median being 6.5. The overall quality spanned the whole scale, with the median being Good. Finally, there was a very strong Spearman correlation between completeness and quality rating ( $\rho = 0.97, p < 10^{-6}$ ).

**4.3.2 Open day.** Each of the 7 student teams from the Introductory course was given two computers to run their game; the 3 Follow-up course students had one computer each. Topics of all the games along with the basic prerequisites were displayed on a huge screen (see the top right corner of Figure 1). If a visitor selected a game, the student team introduced him/her to the rules and assisted with any difficulties, if the player needed help. We encourage self-reliance in our students, so the teams were fully responsible for attending to the visitors the whole time. Still, the instructors were ready to resolve any technical issues with the cyber range.

After finishing the game, each player reflected on the game in a brief anonymous online questionnaire. The questionnaire was filled in privately on a separate computer so that the players would not be influenced by the presence of the game creators. In the survey, the players rated the educational value of the game and its overall quality on the same 5-step Likert scales we used in the test run. We also measured the total play time of the players. Finally, the players described their learning experiences, so that we could see if the game was perceived as educational, and optionally wrote a subjective comment for the creators, instructors, or organizers.

In total, 41 game plays in teams of one to three people occurred. We report only the aggregate results instead of examining the games separately, due to a small number of participants in each individual game. All of the players provided feedback on the game. The educational value was rated as Medium (9), High (27), and Huge (5). The overall quality was rated as Sufficient (1), Good (10), Very good (23), and Excellent (7). The play time ranged from 5 to 70 minutes, with the median and average being 40 minutes. We attribute the large variance of the time to the fact that some players experienced technical difficulties and had to wait, to different skill levels of the attendees, and to their different game strategies (some just skipped through the game, others wanted to finish it without asking for any hint). We avoid comparing the data of expert reviewers and the attendees, as these two groups perceive the game differently.

The self-reported learning experiences included mostly working with Linux Terminal, using offensive security tools in Kali Linux distribution, and game-specific learning outcomes, such as packet analysis in Wireshark, securing Apache server, or understanding

particular vulnerabilities. Of the 41 player teams, 24 included optional comments, which were overwhelmingly positive: 10 students used the word “super” in their feedback, 5 especially appreciated how helpful and supportive the student tutors were, and 3 other explicitly asked the organizers to hold more events like this. Only 4 comments were slightly negative: 2 students would have appreciated more precise instructions for playing (that is, what tasks they are supposed to accomplish), and 2 students were bothered by experiencing technical difficulties with the cyber range.

**5.1.3 Limitations of the observations.** The results of the evaluation mentioned above come from a relatively small sample of 18 students. Next, although we encouraged honest feedback, we cannot eliminate the possibility that expert reviewers in the test run might have provided less strict assessment due to student teams being present with them. Finally, the attendees of the Open Day were self-selected, mostly male university students with interest in cybersecurity. While 41 gameplays is a sufficient sample, some of them included groups of two or three people playing one game together (and subsequently, completing the questionnaire together).

## 5 LESSONS LEARNED

This section shares 6 successes and 5 challenges we experienced over the three semesters of teaching and continuous innovation of our courses. These lessons were distilled based on both our observations and feedback of the total of 46 enrolled students, which was gathered by online surveys and informal discussions.

### 5.1 Successes

**5.1.1 A motivating impact of the final presentation.** The Open Day motivates students to work on their project, since they know it will be applied in practice. The students gain an authentic experience of working with a real audience to which they have to present the projects. At the same time, the event poses a strict deadline and pressure.

**5.1.2 Constraining student efforts.** If students are given too much freedom, the complex task of creating a cybersecurity game might be daunting. By specifying constraints such as possible topics, network topology, number of levels, and maximum time, we lowered the barrier for students to start working on the project. Moreover, having a precise specification of the expected result helped the students deliver results of a higher quality. A further restriction on the maximum team size reduced communication overhead and allowed students to focus on the task itself.

**5.1.3 The expert review.** A test run of the scenarios is helpful for the students, as their game is played and reviewed by independent cybersecurity experts. The students can observe how the expert interacts with the game and subsequently improve it. Moreover, the testers can practice skills or enhance knowledge in a different way from their everyday work.

**5.1.4 Recognizing issues early.** Regular checkpoints and especially in-class presentations of the project helped identify and correct students efforts. For example, students who explained the vulnerability exploited in their game to their classmates improved their understanding of it after receiving feedback. However, teams who started with presenting the game proposal realized later that the

vulnerability works differently than they thought, which resulted in losing one week of preparation.

**5.1.5 Popularizing cybersecurity at the faculty.** The Open Day builds cybersecurity awareness, substantially promotes our research group and CSIRT, and helps to find new collaborators: especially students for capstone projects, final theses, or further runs of the course. After the third Open Day, we encountered a major increase of requests for thesis supervision or other collaboration.

**5.1.6 Contributing to research and development.** The practical contributions of the courses include developing new serious games applicable for future training, creating opportunities to perform cybersecurity and educational research, and testing of the cyber range. While the platform was being developed, the students and teachers of the courses using it acted as implicit testers, who discovered and reported numerous bugs and feature requests.

### 5.2 Challenges

**5.2.1 Technical infrastructure requirements.** Preparing and employing the cyber range poses an additional burden for both instructors and students. The platform must be in a stable release version and with operational support, as any outages seriously hinder the lessons. We recommend working in the team of at least two lecturers, so that one can fully focus on the content and the other provide technical assistance. In order to relieve teachers of some work, the game creators should have access to the following operations in the cloud: restarting a machine, creating a snapshot, reverting the state of the machine, and editing the game content.

**5.2.2 Preparation and implementation effort from instructors.** Compared to lectures, running hands-on cybersecurity courses introduces a lot of extra work. Apart from technical infrastructure described above, the instructors have to organize the test run and the Open Day, both of which require substantial effort in managing different games real-time on a complex cyber range. What is more, even after the game successfully passes Open Day and final review of the teachers, it still needs further improvement and fine-tuning by experts before it can be used in training sessions.

**5.2.3 Selecting a vulnerability.** The students often select a particular vulnerability for their game that cannot be replicated. The reason is that it has been already fixed in used software, or the vulnerable version is not available anymore, or the current version of the used operating system will not run it anymore. As a result, they are forced to look for a new one and even redesign the game. A possible solution is that instructors would provide a list of vulnerabilities applicable for each selected topic.

**5.2.4 Team formation and teamwork.** As in many other project-oriented courses, the students face the challenge of self-managing a small team. Most of the students report they enjoyed working in a team without experiencing common team issues such as social loafing. However, some students expressed their wish to have more organized and efficient teamwork. Making group processes explicit, for example, by discussing Tuckman stages [7] with the students, can help overcome this issue. Arguably, this would also improve all students in teamwork, since unless group processes are taught explicitly, working on a team project teaches teamwork

only implicitly [5]. Another difficulty is the grouping into teams itself, which we will explore in our future work.

**5.2.5 Students underestimating complexity of the project.** Creating the game is more complicated than students expect, even though we gradually introduced several checkpoints throughout the semester (see 5.1.4). Although the students play the exemplary game at the beginning, a brief survey showed that this was not enough for the most to gain a solid understanding of what will involve developing their project. Even when we added extra time for project development at the expense of theory, most teams completed the majority of work only two weeks before the Open Day. Nevertheless, a comment we often hear from students at the end of the course is “I wish we started working on this in advance”. Perhaps adding more strict checkpoints mirrored in grading could increase motivation for continuous work during the semester. Right now, we do not grade the course, only give a Pass/Fail mark.

## 6 CONCLUSIONS

Learning by doing is a popular approach used in cybersecurity education. In alignment with state-of-the-art curricular guidance, we developed two interrelated undergraduate courses that apply learning by teaching in the interactive virtual environment of KYPO cyber range. Students design serious games with the topic of cyber attack or defense, which they then present at the Open Day. They have to cope with numerous interdisciplinary tasks throughout the semester while exercising a broad spectrum of technical and soft skills: system administration, penetration testing, game design, teamwork, project planning, communication, and presentation.

Our experience from three runs of the courses is that they have a strongly beneficial impact on cybersecurity education and research at our faculty. Students rate the courses positively, since they exercise adversary thinking in real-world settings. They can see the practical results of their work during the semester and at the end when presenting their game to their peers. Feedback from attendees of the Open Day shows they enjoyed the event and it attracted some of them to the cybersecurity field. This is highly valuable for security research groups at the faculty, which engages junior collaborators on their research and development projects.

Among the challenges we identified, we suggest prospective instructors who may consider introducing similar courses in their settings, to especially mind the following one. Both courses highly depend on the cyber range hosting the created games. We advise to run them on a stable infrastructure since the topic itself is complex, and every outage of the infrastructure disrupts the sessions. Besides, covering all learning objectives of the Introductory course may lead to shallow instruction in individual areas (network security, system security, game design). The complexity of the cybersecurity field would accommodate two courses, for instance, one covering only the theory and another entirely dedicated to the project.

## ACKNOWLEDGMENTS

This research was supported by the Security Research Programme of the Czech Republic 2015-2020 (BV III/1-VS) granted by the Ministry of the Interior of the Czech Republic under No. VI20162019014 – Simulation, detection, and mitigation of cyber threats endangering critical infrastructure. Martin Laštovička is Brno Ph.D. Talent Scholarship Holder – Funded by the Brno City Municipality.

## REFERENCES

- [1] National CyberWatch Center. 2017. National CyberWatch Center Information Security Curricula Guide. <https://www.nationalcyberwatch.org/resource/curriculum-guide/>. (2017). Accessed: 2018-03-27.
- [2] Tom Chothia, Sam Holdcroft, Andreea-Ina Radu, and Richard J. Thomas. 2017. Jail, Hero or Drug Lord? Turning a Cyber Security Course Into an 11 Week Choose Your Own Adventure Story. In *2017 USENIX Workshop on Advances in Security Education*. Vancouver, BC. <https://www.usenix.org/conference/ase17/workshop-program/presentation/chothia>
- [3] Adrian Dabrowski, Markus Kammerstetter, Eduard Thamm, Edgar Weippl, and Wolfgang Kastner. 2015. Leveraging Competitive Gamification for Sustainable Fun and Profit in Security Education. In *2015 USENIX Summit on Gaming, Games, and Gamification in Security Education*. Washington, D.C. <https://www.usenix.org/conference/3gse15/summit-program/presentation/dabrowski>
- [4] Tamara Denning, Adam Shostack, and Tadayoshi Kohno. 2014. Practical Lessons from Creating the Control-Alt-Hack Card Game and Research Challenges for Games In Education and Research. In *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education*. San Diego, CA. <https://www.usenix.org/conference/3gse14/summit-program/presentation/denning>
- [5] Ville Isomöttönen. 2014. Making Group Processes Explicit to Student: A Case of Justice. In *Proceedings of the 2014 Conference on Innovation & Technology in Computer Science Education (ITiCSE '14)*. ACM, 195–200. <https://doi.org/10.1145/2591708.2591717>
- [6] Stephan Krusche, Barbara Reichart, Paul Tolstoi, and Bernd Bruegge. 2016. Experiences from an Experiential Learning Course on Games Development. In *Proceedings of the 47th ACM Technical Symposium on Computing Science Education (SIGCSE '16)*. ACM, 582–587. <https://doi.org/10.1145/2839509.2844599>
- [7] David L. Largent. 2016. Measuring and Understanding Team Development by Capturing Self-assessed Enthusiasm and Skill Levels. *Trans. Comput. Educ.* 16, 2, Article 6 (Feb. 2016), 27 pages. <https://doi.org/10.1145/2791394>
- [8] NIST. 2017. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. <https://www.nist.gov/itl/applied-cybersecurity/national-initiative-cybersecurity-education-nice/nice-cybersecurity>. (2017). <https://doi.org/10.6028/NIST.SP.800-181> Accessed: 2018-03-27.
- [9] NSA / DHS National Centers of Academic Excellence in Cyber Defense. 2013. Knowledge Units. <http://www.iad.gov/nietp/CAERrequirements.cfm>. (2013). Accessed: 2018-03-27.
- [10] Mike O'Leary. 2017. Innovative Pedagogical Approaches to a Capstone Laboratory Course in Cyber Operations. In *Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education (SIGCSE '17)*. ACM, 429–434. <https://doi.org/10.1145/3017680.3017720>
- [11] Joint Task Force on Cybersecurity Education. 2017. Cybersecurity Curriculum CSEC 2017. <http://cybered.acm.org/>. (2017). Accessed: 2018-03-27.
- [12] Geoffrey Petty. 2009. *Teaching Today: A Practical Guide*. Nelson Thornes.
- [13] Kate Sanders, Jonas Boustedt, Anna Eckerdal, Robert McCartney, and Carol Zander. 2017. Folk Pedagogy: Nobody Doesn't Like Active Learning. In *Proceedings of the 2017 ACM Conference on International Computing Education Research (ICER '17)*. ACM, 145–154. <https://doi.org/10.1145/3105726.3106192>
- [14] Z. Cliffe Schreuders and Emlyn Butterfield. 2016. Gamification for Teaching and Learning Computer Security in Higher Education. In *2016 USENIX Workshop on Advances in Security Education*. Austin, TX. <https://www.usenix.org/conference/ase16/workshop-program/presentation/schreuders>
- [15] Clark Taylor, Pablo Arias, Jim Klopchic, Celeste Matarazzo, and Evi Dube. 2017. CTF: State-of-the-Art and Building the Next Generation. In *2017 USENIX Workshop on Advances in Security Education*. Vancouver, BC. <https://www.usenix.org/conference/ase17/workshop-program/presentation/taylor>
- [16] Michael F. Thompson and Cynthia E. Irvine. 2014. CyberCIEGE Scenario Design and Implementation. In *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education*. San Diego, CA. <https://www.usenix.org/conference/3gse14/summit-program/presentation/thompson>
- [17] Maxim Timchenko and David Starobinski. 2015. A Simple Laboratory Environment for Real-World Offensive Security Education. In *Proceedings of the 46th ACM Technical Symposium on Computer Science Education (SIGCSE '15)*. ACM, 657–662. <https://doi.org/10.1145/2676723.2677225>
- [18] Valdemar Švábenský and Jan Vykopal. 2018. Challenges Arising from Prerequisite Testing in Cybersecurity Games. In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education (SIGCSE '18)*. ACM, 56–61. <https://doi.org/10.1145/3159450.3159454>
- [19] Jan Vykopal, Radek Oslejsek, Pavel Celeda, Martin Vizvary, and Daniel Tovarnak. 2017. KYPO Cyber Range: Design and Use Cases. In *Proceedings of the 12th International Conference on Software Technologies - Volume 1: ICSOFT*. INSTICC, SciTePress, 310–321. <https://doi.org/10.5220/0006428203100321>
- [20] Chang Yun, Hesam Panahi, and Zhigang Deng. 2016. A Multidisciplinary, Multifaceted Approach to Improve the Computer Science Based Game Design Education: Methodology and Assessment. In *Proceedings of the 47th ACM Technical Symposium on Computing Science Education (SIGCSE '16)*. ACM, 570–575. <https://doi.org/10.1145/2839509.2844582>