2022 IEEE/ACM 44th International Conference on Software Engineering: Software Engineering Education and Training (ICSE-SEET)

# Putting Security on the Table: The Digitalisation of Security Tabletop Games and its Challenging Aftertaste

Marco Gutfleisch
Marco.Gutfleisch@rub.de
Ruhr University Bochum
Bochum, North Rhine-Westphalia
Germany

Markus Schöps
Markus.Schoeps@rub.de
Ruhr University Bochum
Bochum, North Rhine-Westphalia
Germany

Sibel Sayin
Sibel.Sayin@rub.de
Ruhr University Bochum
Bochum, North Rhine-Westphalia
Germany

Frederic Wende
frederic.wende@rub.de
Ruhr University Bochum
Bochum, North Rhine-Westphalia
Germany

Martina Angela Sasse
Martina.Sasse@rub.de
Ruhr University Bochum
Bochum, North Rhine-Westphalia
Germany

## ABSTRACT

IT-Security Tabletop Games for developers have been available in analog format; with the COVID-19 pandemic, interest in collaborative remote security games has increased. In this paper, we propose a methodology to evaluate the impact of a (remote) security game-based intervention on developers. The study design consists of the respective intervention, three questionnaires, and a small open interview guide for a focus group. A validated self-efficacy scale is used as a proxy for measuring effects on participants' ability to develop secure software. We tested this design with 9 participants (expert and novice developers and security experts) as part of a small feasibility study to understand the challenges and limitations of remote tabletop games. We describe how we selected and digitalised three security tabletop games, and report the qualitative findings from our evaluation. Setting up and running the virtual tabletop games turned out to be more challenging and complex for both moderator and participants than we expected. Completing the games required patience and persistence, and social interaction was limited. Our findings can be helpful in building and evaluating a better, more comprehensive, technically sound and issue-specific game-based training measure for developers. The methodology can be used by researchers to evaluate existing and new game designs.

## CCS CONCEPTS

• **Social and professional topics** → **Computing education**; • **Security and privacy** → **Software security engineering**.

## KEYWORDS

security, software engineering, developer education, serious games


*ICSE-SEET '22, May 21–29, 2022, Pittsburgh, PA, USA*

ACM ISBN 978-1-4503-9225-9/22/05.
https://doi.org/10.1145/3510456.3514139

**ACM Reference Format:**
Marco Gutfleisch, Markus Schöps, Sibel Sayin, Frederic Wende, and Martina Angela Sasse. 2022. Putting Security on the Table: The Digitalisation of Security Tabletop Games and its Challenging Aftertaste. In *44nd International Conference on Software Engineering: Software Engineering Education and Training (ICSE-SEET '22), May 21–29, 2022, Pittsburgh, PA, USA.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3510456.3514139

## 1 INTRODUCTION

Game-based methods are widely used to create awareness of, and to impart knowledge about a topic. [49]. Collaborative game-based training approaches are seen to be particularly effective because they can strengthen individuals' socio-communicative competences as well as increase knowledge [41]. Playing games to learn about a specific topic - such as security - requires participants to actively communicate about the topic in the game session. This is thought to be a promising way to achieve a sustained improvement in practice in team-based work environments, such as software engineering, where traditional training interventions have been found to have no lasting effect [33]. Based on previous studies, our hypothesis is that collaborative security games have the potential to be good icebreakers to increase communication about security among team members, and help to increase self-efficacy in individual team members. To test this, we designed a study in which we could monitor communication among teams, and assess self-efficacy based on a validated self-efficacy questionnaire [44] targeted at developers.

To test the design and to find out the limitations and challenges in advance, we conducted a small feasibility study. The goal of the study was to answer two primary research questions:

**RQ 1** What are the advantages and opportunities of using remotely conducted IT security tabletop games to educate software professionals on information security?

**RQ 2** What are the challenges and limitations of remote IT security tabletop games as an education tool for software engineers?

We start by reviewing existing literature on game-based learning tools in general, and for software developers in particular. We describe the setup we created, the execution of the security game session as well as the interviews and questionnaires we used as instruments to collect feedback from the participants. The parts of the feasibility study that deviate from the original design (e.g. the

execution of the third questionnaire) are explicitly mentioned in the methodology. Since we only conducted a few game sessions with a small number of participants, our report will only focus on qualitative parts of the design.

The proposed methodology and the report of our feasibility study can be built upon in future studies with a bigger sample size to evaluate if remote game-based security tabletop games improve developers' security skills.

## 2 RELATED WORK

*Game-Based Learning.* When looking at the possible advantages of game-based learning, the characteristics that stand out most are a high grade of intrinsic motivation for the learner and the stimulation of strategic thinking and decision-making [24]. In software engineering, game-based learning can improve core generic competences like the ability to work in a team or to communicate [41]. Another benefit is the increase of self-efficacy in handling unclear situations [27] regarded as one, if not the most important trait in human interaction with IT security [34]. One important distinction that has to be made is the difference between "conventional" and "serious" games. Serious games are explicitly designed to have an educational purpose, and are not primarily intended to be played for entertainment [1].

*Educational Card- and Board Games.* Research shows that card- and board games can have a positive learning effect in a variety of fields: they can improve mathematical skills in children [18, 25], teach people about topics such as medicine [15, 47], engineering [2], software engineering [32], language [30], and increase computational thinking [4]. Furthermore, they can have a positive effect on the expansion of social interactions [3], with games dating back up to the bronze age having the function of "social lubricants" [14].

*Serious Cybersecurity Games.* In the realm of IT security, different forms of serious games have been studied. Capture-the-flag (CTF) competitions, for example, are designed as races, in which different teams try to find digital "flags" hidden in code [7]. "King of the hill" is another game, in which participants practice performing and defending against penetration testing [5]. Additionally, "Build-it/Break-it/Fix-it" serves as a practice tool for building and attacking secure software [35, 36]. The aim of these competitions is to grant participants the possibility to practice and demonstrate their IT security skills, and have been shown to be a successful educational tool [10, 11]. Other examples for serious games are software testing games [21], anti-phishing games [38, 46], and story-driven and gamified cyber security courses [12, 16].

In summary, there is a vast landscape of cyber security games, which differ in the depth of content, use of gamification, and available platforms, and are part of a rapidly evolving gaming scene [13].

*Self-Efficacy and IT Security.* Self-Efficacy - the belief in one's own abilities to mobilise the motivation, cognitive resources, and actions needed for a specific task [31] - has been identified as an important element in driving individual users' IT security behaviour [34]. The so-called self-efficacy in information security (SEIS) not only influences technology use and secure behaviour, but also the intention to continue security efforts [34]. Game-based learning can have a positive effect on self-efficacy [27]. An example of a serious game which promotes self-efficacy in IT Security is "Hacked Time" [8, 9], a point-and-click adventure game, in which the player travels through time to help dealing with a security breach. The game has been shown to improve the player's security attitude and self-efficacy for using cybersecurity tools [9]. Votipka, Abrokwa and Mazurek built and evaluated a 15-item self-efficacy scale as a proxy for measuring developers' security skills [44].

## 3 METHODOLOGY

At first, in section 3.1, the game selection, adaption and realisation is explained. Afterwards, the procedure of the study (section 3.2), its analysis (section 3.3), as well as the participants' demographics (section 3.4) are explained. The complete questionnaires can be found in our replication package.[1]

### 3.1 Game Selection, Adaptation & Realisation

*Games.* In preparing the study, we had to select from available games on the topic of IT security. The selected games came from a list assembled by IT security specialist Adam Shostack [40], and was supplemented by games found through a thorough online research done by the researchers (The full list of chosen games with software developers as an imaginable target group can be found in table 1). After this first selection, the games were assessed based on a series of criteria: being a boardgame, available and obtainable, finishable in 60 minutes, relevant for several development departments, digitaliseable without huge modifications, available in English, playable with 4 to 8 players, designed for developers as a target group or imaginable to be adapted for developers, and offering a discussion base for IT-Security content. Five of the games listed fulfilled all of the criteria. We then created digital versions of these games (see section 3.1). Two authors conducted a walkthrough of all games, with one taking the role of the moderator. We found two of the five games ("The agile App Security Game" and "Backdoors and Breaches") not suitable (in terms of complexity and/or content) and removed them from the upcoming sessions. The final list consisted of the following games:

- *Elevation of Privilege* [39]: Designed to introduce developers to the method of threat modeling, it is a competitive card game for 3 to 6 players. The 74 playing cards consist of different cyber security anti-patterns based on the "STRIDE" framework for security threats. Playing a card consists of describing it to the other players and explaining how it works in the game.
- *Pivots and Payloads* [42]: A board game for 2 to 6 players. The aim of the game is to teach players about the methodology of penetration testing. Players roll dice and move around the board, which is divided into the 8 stages of pen-testing.
- *[d0x3d!]* [23]: A cooperative board game for 2 to 4 players. Players assume the role of hackers and try to infiltrate a network consisting of 24 machines, steal data and escape.

We made minor modifications to some games, without changing their character, to expose software developers to the basics of IT

[1] https://doi.org/10.6084/m9.figshare.19107635

**Table 1: Security games with software developers as an imaginable target group**

| IT Security Games | Description |
|---|---|
| The Agile App Security Game [45] | *Card game* in which the players take the role of an agile development team that needs to prioritize and implement security enhancements to avoid threats. |
| Backdoors and Breaches [37] | *Card game* in which the Players roleplay different IT- security attack tactics. |
| Control-Alt-Hack [17] | *Card game*, in which players take the role of ethical hackers to complete various tasks and missions. |
| OWASP Cornucopia [19] | *Card game* in which players need to use Threat-Modeling to find weaknesses (for web applications). |
| Protection Poker [48] | *Cooperative card game* in which players pass security knowledge around the team and build risk mitigation into iteration planning. |
| OWASP Snakes And Ladders Web Apps [20] | *Board game* in which players traverse a "Snakes and Ladders" board, climbing "secure coding practices" and descending "application security risks". |
| OWASP Snakes And Ladders Mobile Apps [20] | *Board game* similar to the one above, the difference being the focus on mobile controls and risks. |
| Dungeons and Data [6] | *Cooperative role-playing game* in which players take the role of employees of a fictional company, each round dealing with different security incidents. |

security, the analysis of software vulnerabilities, and how to mitigate these with appropriate countermeasures. The game "[d0x3d]", for example, was complemented by a rule, which required the explanation of how specific "Security-Attacks" worked.

*The Moderator.* The study coordinator (one of the authors) assumed the role of the "moderator". The moderator had a series of tasks, including the technical set-up before the study and conducting the group interview after each session. The moderator introduced the game concepts to the participants, brought in knowledge if needed, answered questions, and occasionally directed participants back to the game principles. The moderator was a security expert, but we created cheat sheets for every game as a reminder: a list of the games' elements, background knowledge, and one possible attack and relevant countermeasure per game.

*Digitalisation & Technical Set-Up.* We converted each of the three games into digital format, including cards, figures, playing fields, etc., using the open-source software "Vassal"[43]. "Vassal" allows the digitalisation of games and their playing mechanics, in addition to the subsequent playing with several players. We set up a virtual machine for each player using Google Cloud, and prepared everything so that the participants only had to connect via the Remote Desktop Protocol to join a game session.

## 3.2 Study Procedure

After being recruited, participants received a link to complete the pre-questionnaire. Via the email addresses that were given, a convenient time and date for the game session were set. After a group of four to five participants took part in the remote (but recorded) game session, they had to fill out a second short questionnaire. The group was then interviewed by the moderator to explain and discuss their impressions and thoughts on the game and its execution. This concluded the study. But within the original design, it is planned that participants have to complete an additional questionnaire a few weeks after the gaming session to also measure long-term effects. In figure 1, the procedure of this study is visually depicted.

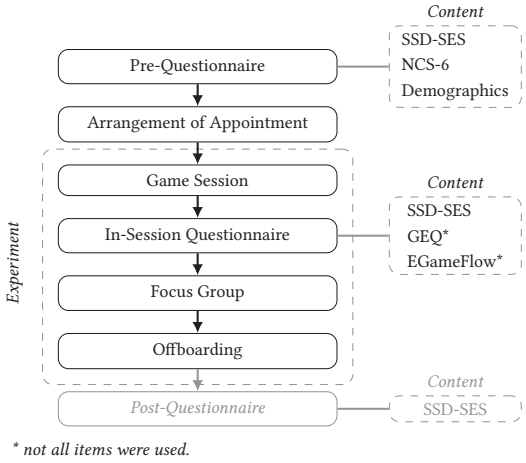


**Figure 1: Overview study procedure**

*Recruiting.* We recruited participants via personal contacts. We screened interested people to make sure that they were over 18 years old, had some practical experience in software development or IT security, or were enrolled in an academic degree program on those topics. Our institution did not have an institutional review board (IRB) for non-medical studies, but we adhered to the national and EU data protection and privacy regulation, conducted a risk assessment, and provided participants with a study description including data handling and consent forms. We informed them that they could terminate the study at any time without negative consequences.

*Pre-Questionnaire.* To provide a quantitative way of examining and analysing the effects of the training session, three questionnaires with slightly different contents were used.

The pre-questionnaire included the 15 items of the validated Secure Software Development Self-Efficacy Scale (SSD-SES) [44], which is used as a proxy for measuring developers' security skills. Additionally, we added the validated six-item version of the Need for Cognition Scale (NCS-6) to the pre-questionnaire, which measures people's tendency to enjoy thinking and engaging in cognitive activity [29]. The NCS-6 was added with the intention to examine a possible positive correlation between this character trait and the self-efficacy scale, as well as the enjoyment of this game-based training method measured in the in-session questionnaire. Both sets of items were rated on a 5-point Likert-scale.

Furthermore, the first questionnaire contained some general demographic questions about their age, gender, nationality, job and education and some more specific ones about their skills and experience regarding information security and software development.

*Game Session.* On the date of the gaming session, the participants joined the virtual conference room and the moderator gave an introductory presentation about the basic functions of "Vassal"

and the rules and mechanics of the game they would play. Afterwards, they were each given remote desktop access to separate virtual machines that were connected to the respective Vassal game session.

*In-Session Questionnaire.* The in-session Questionnaire included items of the SSD-SES [44]. Additionally, we selected items of the Game Experience Questionnaire (GEQ) [26] (to measure game players' experience) and the EGameFlow scale [22] (to measure game players' enjoyment) that added together made up 16 items in total. The items were rated on a 5-point Likert scale.

*Focus Group.* After completing Questionnaire 2, a group interview was conducted to discuss the impressions and thoughts on the game session and review the participants' opinions on how effective the games were in conveying IT security knowledge.

We kept the focus group session open-ended and used the following questions as a guide:

(1) What did you like or dislike about the game in general, content-wise and visually?
(2) Do you think you could motivate your developer colleagues to partake in a game session like this with you?
(3) Did the game session motivate you to continue to read up on IT security topics on your own?
(4) Would you want to play other IT tabletop games with a different core topic, e. g. usability or performance?

*Post-Questionnaire.* Questionnaire 3 was supposed to be filled out by the participants approximately one or two months after the game session in order to analyse potential long-term effects of the training. It mainly included the items of the SSD-SES [44] and a few questions to rule out the possible influence of having gained significantly more expertise in security topics since the last questionnaire through work or otherwise. Since this was out of the scope of our feasibility study, we did not send our participants the post-session questionnaire.

### 3.3 Analysis

The game sessions and the focus group interviews were recorded and transcribed. Both were analysed using thematic analysis [28]. With using the focus group interviews, three of the authors iteratively designed a coding tree using the two primary research questions stated in the introduction section as a guideline. Afterwards, two authors re-coded the interviews independently, and also coded the verbal statements made during the game sessions.

### 3.4 Participants

9 people participated in this study, 6 were male, 2 female, and 1 chose the option not to identify. Their ages ranged from 23 to 30 (M = 26, SD = 1.89). Group 1 consisted of 4 participants and played the three games "Pivots and Payloads", "[d0x3d!]" and "Elevation of Privilege". Group 2 consisted of 5 participants and only played "Elevation of Privilege". The majority of the participants had a similar academic background and were therefore already familiar with each other. 5 were either currently studying for a bachelor's or a master's degree in IT security. One was a Ph.D. student in a security-focused area and three others were experienced software developers.

## 4 REPORT ON THE FEASIBILITY STUDY

Because we only tested the selected games with 2 different groups, consisting of 9 participants in total, the quantitative results aren't reported in detail. In addition, the first group played all games in a row which is why not all in-session questionnaires were filled out. Hence, we only focus on the qualitative results. The planned maximum of two hours for the entire session, including the focus group interview, varied slightly from session to session.

### 4.1 Advantages & Opportunities

*More specific topics.* In general, the participants found the topics to be too broad and wished for more specific and practical game topics: *"You actually want to have concrete questions or explanations and then concrete counter-questions."* — [P4]. Especially regarding software developers as the target group, participants found it important that the practicability was considered more. One practical approach could be replacing a fictive system, as it is used for applying threat modeling in Elevation of Privilege, with a system or subsystem that the participants work with. Testing their own product would make the game more enjoyable and attractive for the participating group. Additionally, the identified security issues can be recorded directly, and this, in turn, generates an added value for the team as well as the management.

*Cheat sheets.* The cheat sheets used by the moderator were regarded as an indispensable tool for the game sessions. All games require a person with security expertise to intervene when problems arise and also actively drive communication forward. In our case, we played with participants who did not have immense knowledge about security. Many attacks and practical examples were prepared on "cheat sheets" in advance and were brought into the discussion if necessary. Here, the moderator had knowledge about security and the cheat sheets turned out to be extremely helpful. Additional well-prepared help for the facilitator seems to be an important aid for gaming groups without much expertise themselves or access to an expert.

*Diverse participants.* Regarding the composition of teams playing the game, participants pointed out benefits when it comes to the diversity of the players, but also regarding the similarity of players. For one, diversity was deemed important for promoting the sharing of knowledge between different players with different backgrounds. Regarding the similarity of the group, the benefits that were pointed out were the shared practical experience and an already established sense of cohesion to help the flow of the games: *"It has advantages and disadvantages when people are all together in a development group. The advantage is that they all know what they are talking about because they all know the same system. The disadvantage is that they have less variation in it. In other words, they know fewer types of attacks and so on, because they all have a similar background."* — [P4].

### 4.2 Challenges & Limitations

*Importance of the moderator.* The moderator turned out to be a very important role in the execution of the games. It was necessary that one person guided the players through the games and added pointers and suggestions where it was needed. Not only we noticed this, but also the participants: *"I also thought it was good that the host, you,*

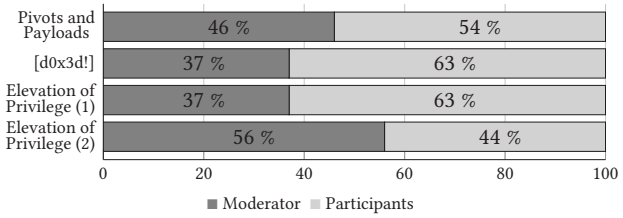


**Figure 2: Results of speech shares of the moderator and the participants ($n = 9$)**

*for example, can always intervene immediately if it really goes in a completely wrong direction. Or that you suggest something in the right direction so that it can be discussed further."* — [P6]. The importance of the moderator is highlighted in the speech shares of the participants. Figure 2 shows the speech shares of the moderator (dark grey) and the other players (light grey). The chart shows that the moderator talked more than the other players, in one case having even more than half of the speech shares of the session. What we also observed were frequent changes of speakers between individual players and the moderator. However, this was rarely the case among the players themselves implying a general confusion about the rules or a lack of confidence in their understanding of the game since they were mostly awaiting the moderator to answer questions and explain things. Already during the piloting, we noticed that there was a need to initiate discussion or provide content. This also proved true during our game sessions. All of this further indicates the relevance of the moderator and its explanatory role.

*Technical Issues.* The technical side of the study was criticised in different ways. For one, the RDP-Setup was deemed problematic for establishing a stable and performant connection: *"So the RDP setup worked miserably, you already know that."* — [P4]. The software "Vassal" was seen as partly confusing in some aspects: *"In addition to that, I started with just my laptop screen, which is not that big, and then I had to zoom in and out a lot to get an overview. And move things back and forth [...]"* — [P6]. While the technology was functional, there is still room for improvement in terms of usability. Hence we would suggest using a more attractive and more usable platform.

*Fundamental security knowledge needed.* What became clear in the interviews and during the games was that a fundamental knowledge of the players about IT security was essential for the experience. In all of the games, participants criticised the suitability of the games for software developers that have no basic knowledge about security themes. For "[d0x3d!]": *"Well, if you don't have a background, I really don't see how that's going to help."* — [P4]. From the point of view of complexity, we would classify the participants' entry into the games as rather hard. We think that there is still potential in research to develop and test (remote) educational games that are able to impart not only complex but also basic knowledge about security and to open a discussion about security-relevant topics.

*Remote Gaming and Social Communication.* When it comes to the remote gaming aspect of the study, many participants didn't feel as comfortable as when playing "offline" with other players at the table: *"It is still a success of this game that you have set themes and I think you have that much more when you sit comfortably around a table and drink your beer and play cards and think about your software than when you have to sit here at your computer. It's not that comfortable with your mouse and keyboard, you have to click things back and forth. A handful of cards is just easier."* — [P4]. Playing remote may be an alternative when it comes to bridging distances, but may be a hindrance for social communication, especially if the games consist of topics that the players are not familiar with. From the point of view of the participants and the moderator, this was very challenging. The non-verbal communication was almost completely missing. Finding the perfect moment to join a discussion turned out to be more difficult remote. Discussions were almost non-existent and a lot of content had to be introduced by the moderator. In addition, it was difficult for the moderator to assess if the content was received and understood by the participants. The fact that the technology was not particularly appealing and that there was only little or no space on the screen for the small videos from the conference tool, further discouraged communication. We have actively adapted two of the games with the basic idea to promote communication. Nonetheless, we had the overall impression that all tested game concepts in the digital form are not optimal under the given circumstances to involve everyone, as it would be the case in a local setting. However, the difficulties may be due to the fact that some participants were not familiar enough with the topic and may have felt insecure. But that would also apply in practice, where we cannot assume that every software professional is familiar with security.

## 5 CONCLUSION

We have presented a research design that can be used to evaluate the impact of (remote) security game interventions. A replication package is included to provide additional material used, which can help the research community to design and improve future experiments to test similar educational approaches with a security focus. Our findings should also help in the creation of new game-based learning interventions that focus on teaching and improving developers' security skills and self-efficacy.

Furthermore, we provided the results of a feasibility study. We only had a small number of participants, two teams, and only one team managed to play all 3 games. The games did not run smoothly from a technical point of view, and communication between team members was too challenging to elicit the information we were looking for. Thus, the study showed that creating digital versions of the tabletop games, and measuring their impact on software developers was more challenging than we had imagined. In hindsight, we should have anticipated that games that work in a face-to-face context don't generate as much participation in a remote context, and require much more steering from a moderator. To address the security training needs of software teams in a remote setting, we need innovative approaches that take a cue from successful online games, not tabletop ones.

## ACKNOWLEDGMENTS

Funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy – EXC 2092 CaSa – 390781972. The authors would like to thank Yasemin Acar for her valuable feedback in designing the study.

## REFERENCES


[1] Clark C Abt. 1987. *Serious games*. University press of America.

[2] MT Azizan, N Mellon, RM Ramli, and S Yusup. 2018. Improving teamwork skills and enhancing deep learning via development of board game using cooperative learning method in Reaction Engineering course. *Education for Chemical Engineers* 22 (2018), 1–13.

[3] Erin E Barton, Elizabeth A Pokorski, Erin M Sweeney, Marina Velez, Stephanie Gossett, Jia Qiu, Celia Flaherty, and Maddisen Domingo. 2018. An empirical examination of effective practices for teaching board game play to young children. *Journal of Positive Behavior Interventions* 20, 3 (2018), 138–148.

[4] Matthew Berland and Victor R Lee. 2011. Collaborative strategic board games as a site for distributed computational thinking. *International Journal of Game-Based Learning (IJGBL)* 1, 2 (2011), 65–81.

[5] Kevin Bock, George Hughey, and Dave Levin. 2018. King of the hill: A novel cybersecurity competition for teaching penetration testing. In *2018 {USENIX} Workshop on Advances in Security Education ({ASE} 18)*.

[6] Josh Bressers. 2018. Dungeons and Data. https://www.rsaconference.com/library/blog/role-playing-an-incident-except-its-fun

[7] Peter Chapman, Jonathan Burket, and David Brumley. 2014. PicoCTF: A game-based computer security competition for high school students. In *2014 {USENIX} Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*.

[8] Tianying Chen, Jessica Hammer, and Laura Dabbish. 2019. Self-efficacy-based game design to encourage security behavior online. In *Extended Abstracts of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–6.

[9] Tianying Chen, Margot Stewart, Zhiyu Bai, Eileen Chen, Laura Dabbish, and Jessica Hammer. 2020. Hacked Time: Design and Evaluation of a Self-Efficacy Based Cybersecurity Game. In *Proceedings of the 2020 ACM Designing Interactive Systems Conference*. 1737–1749.

[10] Ronald S Cheung, Joseph P Cohen, Henry Z Lo, and Fabio Elia. 2011. Challenge based learning in cybersecurity education. In *Proceedings of the International Conference on Security and Management (SAM)*. Citeseer, 1.

[11] Ronald S Cheung, Joseph Paul Cohen, Henry Z Lo, Fabio Elia, and Veronica Carrillo-Marquez. 2012. Effectiveness of cybersecurity competitions. In *Proceedings of the International Conference on Security and Management (SAM)*. The Steering Committee of The World Congress in Computer Science, Computer …, 1.

[12] 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 ({ASE} 17)*.

[13] Merijke Coenraad, Anthony Pellicone, Diane Jass Ketelhut, Michel Cukier, Jan Plane, and David Weintrop. 2020. Experiencing cybersecurity one game at a time: A systematic review of cybersecurity digital games. *Simulation & Gaming* 51, 5 (2020), 586–611.

[14] Walter Crist, Alex de Voogt, and Anne-Elizabeth Dunn-Vaturi. 2016. Facilitating interaction: Board games as social lubricants in the Ancient Near East. *Oxford Journal of Archaeology* 35, 2 (2016), 179–196.

[15] Maria Cutumisu, Siddhi D Patel, Matthew RG Brown, Caroline Fray, Patrick von Hauff, Thomas Jeffery, and Georg M Schmölzer. 2019. RETAIN: a board game that improves neonatal resuscitation knowledge retention. *Frontiers in pediatrics* 7 (2019), 13.

[16] 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 (3GSE 15)*.

[17] Tamara Denning, Adam Lerner, Adam Shostack, and Tadayoshi Kohno. 2013. Control-Alt-Hack: the design and evaluation of a card game for computer security awareness and education. In *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. 915–928.

[18] Jessica Elofsson, Stefan Gustafson, Joakim Samuelsson, and Ulf Träff. 2016. Playing number board games supports 5-year-old children's early mathematical development. *The Journal of Mathematical Behavior* 43 (2016), 134–147.

[19] OWASP Foundation. 2012. OWASP Cornucopia. https://owasp.org/www-project-cornucopia/

[20] OWASP Foundation. 2014. OWASP Snakes And Ladders. https://owasp.org/www-project-snakes-and-ladders/#:~:text=OWASP%20Snakes%20and%20Ladders%20%2D%20Web,widely%20known%20Top%20Ten%20Risks.

[21] Gordon Fraser, Alessio Gambi, Marvin Kreis, and José Miguel Rojas. 2019. Gamifying a software testing course with code defenders. In *Proceedings of the 50th ACM Technical Symposium on Computer Science Education*. 571–577.

[22] Fong-Ling Fu, Rong-Chang Su, and Sheng-Chin Yu. 2009. EGameFlow: A scale to measure learners' enjoyment of e-learning games. *Computers & Education* 52, 1 (2009), 101–112.

[23] Mark Gondree and Zachary Peterson. 2012. [d0x3d!]. https://d0x3d.com/d0x3d/get_the_game.html

[24] M Helm and F Theis. 2009. Serious Games als Instrument in der Führungskräfteentwicklung. *Handbuch E-Learning* 29 (2009).

[25] Nicole M Hendrix, Robin L Hojnoski, and Kristen N Missall. 2020. Promoting numeracy skills through board game play. *Young Exceptional Children* 23, 2 (2020), 100–111.

[26] Wijnand A IJsselsteijn, Yvonne AW de Kort, and Karolien Poels. 2013. The game experience questionnaire. *Eindhoven: Technische Universiteit Eindhoven* 46, 1 (2013).

[27] Michael Kerres, Mark Bormann, and Marcel Vervenne. 2009. Didaktische konzeption von serious games: Zur verknüpfung von spiel-und lernangeboten. *Medien-Pädagogik: Zeitschrift für Theorie und Praxis der Medienbildung* (2009), 1–16.

[28] Udo Kuckartz. 2014. *Qualitative text analysis: A guide to methods, practice & using software*. SAGE, Los Angeles and London and New Delhi and Singapore and Washington, DC.

[29] Gabriel Lins de Holanda Coelho, Paul HP Hanel, and Lukas J. Wolf. 2020. The very efficient assessment of need for cognition: Developing a six-item version. *Assessment* 27, 8 (2020), 1870–1885.

[30] Kacper Łodzikowski and Mateusz Jekiel. 2019. Board games for teaching English prosody to advanced EFL learners. *ELT Journal* 73, 3 (2019), 275–285.

[31] Elizabeth M Ozer and Albert Bandura. 1990. Mechanisms governing empowerment effects: a self-efficacy analysis. *Journal of personality and social psychology* 58, 3 (1990), 472.

[32] Giani Petri, Christiane Gresse von Wangenheim, and Adriano Ferreti Borgatto. 2017. Quality of games for teaching software engineering: an analysis of empirical evidences of digital and non-digital games. In *2017 IEEE/ACM 39th International Conference on Software Engineering: Software Engineering Education and Training Track (ICSE-SEET)*. IEEE, 150–159.

[33] Andreas Poller, Laura Kocksch, Sven Türpe, Felix Anand Epp, and Katharina Kinder-Kurlanda. 2017. Can Security Become a Routine? A Study of Organizational Change in an Agile Software Development Group. In *Proceedings of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing* (Portland, Oregon, USA) *(CSCW '17)*. Association for Computing Machinery, New York, NY, USA, 2489–2503. https://doi.org/10.1145/2998181.2998191

[34] Hyeun-Suk Rhee, Cheongtag Kim, and Young U Ryu. 2009. Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & security* 28, 8 (2009), 816–826.

[35] Andrew Ruef, Michael Hicks, James Parker, Dave Levin, Michelle L Mazurek, and Piotr Mardziel. 2016. Build it, break it, fix it: Contesting secure development. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*. 690–703.

[36] Andrew Ruef, Michael Hicks, James Parker, Dave Levin, Atif Memon, Jandelyn Plane, and Piotr Mardziel. 2015. Build it break it: Measuring and comparing development security. In *8th Workshop on Cyber Security Experimentation and Test ({CSET} 15)*.

[37] Black Hills Information Security. 2019. Backdoors and Breaches. https://www.blackhillsinfosec.com/projects/backdoorsandbreaches/

[38] Steve Sheng, Bryant Magnien, Ponnurangam Kumaraguru, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, and Elizabeth Nunge. 2007. Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd symposium on Usable privacy and security*. 88–99.

[39] Adam Shostack. 2014. Elevation of privilege: Drawing developers into threat modeling. In *2014 {USENIX} Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*.

[40] Adam Shostack. 2014. Tabletop Security Games & Cards. https://adam.shostack.org/games.html

[41] Alexander Soska, Jürgen Mottok, and Christian Wolff. 2015. Playful learning in academic software engineering education. In *2015 IEEE Global Engineering Education Conference (EDUCON)*. IEEE, 324–332.

[42] SANS Penetration Testing Curriculum Staff and Faculty. 2018. Pivots and Payloads. https://www.sans.org/blog/sans-pen-test-poster-pivots-payloads-boardgame/

[43] The Vassal Team. 2021. VASSAL. https://vassalengine.org/

[44] Daniel Votipka, Desiree Abrokwa, and Michelle L Mazurek. 2020. Building and Validating a Scale for Secure Software Development Self-Efficacy. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*. 1–20.

[45] Charles Weir. 2018. The agile App Security Game. https://www.securedevelopment.org/2017/10/12/games-to-help-learn-about-secure-development/

[46] Zikai Alex Wen, Zhiqiu Lin, Rowena Chen, and Erik Andersen. 2019. What. hack: engaging anti-phishing training through a role-playing phishing simulation game. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. 1–12.

[47] Alexander M Whittam and Whitney Chow. 2017. An educational board game for learning and teaching burn care: A preliminary evaluation. *Scars, burns & healing* 3 (2017), 2059513117690012.

[48] Laurie Williams, Andrew Meneely, and Grant Shipley. 2010. Protection poker: The new software security" game". *IEEE Security & Privacy* 8, 3 (2010), 14–20.

[49] Leah Zhang-Kennedy and Sonia Chiasson. 2021. A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education. *ACM Comput. Surv.* 54, 1, Article 12 (Jan. 2021), 39 pages. https://doi.org/10.1145/3427920