# Developing and Evaluating a Hackathon Approach to Foster Cyber Security Learning

Abasi-amefon O. Affia[1], Alexander Nolte[1,2], and Raimundas Matulevičius[1]

[1] University of Tartu, Tartu, Estonia,
{amefon.affia, alexander.nolte, rma}@ut.ee
[2] Carnegie Mellon University, Pittsburgh, PA, USA

**Abstract.** Securing information systems and teaching people about how to use them securely is one of the significant challenges of the coming years. There is, however, a considerable lack of feasible approaches to train potential future professionals on security. Hackathons appear to be a good approach because studies have found them to not only be useful to teach participants but also to encourage people to explore the security of information systems. Such benefits cannot materialize without careful planning though. In our paper, we propose and evaluate a set of interventions aimed at fostering security learning amongst hackathon participants. Evaluating our approach, we found that emphasizing the need for idea generation, introducing security talks relevant to the ideas generated, interaction with mentors that come from diverse backgrounds, and the introduction of incentives can encourage security learning among participants.

**Keywords:** Hackathons · Security Learning · Action Research.

## 1 Introduction

Technological advancements have led to the ubiquitous availability of data and continue to shape digital innovation [7]. Industry experts predict there will be 6 billion internet users by 2022 [23] and nearly 26 billion connected devices by 2020 [13]. The increase in devices significantly expands the attack surface for malicious actors, who are continually developing more advanced and scale able tools to e.g. access sensitive user data. It is thus critical to educate future professionals that can build secure systems and train users to use these systems securely.

We propose to utilize the hackathon format as a way to raise interest among potential future professionals and spread security knowledge to the larger population. Hackathons are time-bounded events during which participants from diverse backgrounds form teams and work on projects that are of interest to them [26]. Hackathons have previously been utilized as a tool for education and learning [24,27,16] and in fact, learning has been cited as one of the key motivations for participants to participate [14]. However, there is a need for a hackathon approach that specifically focuses on improving the level of knowledge among those which build or use IT systems.

While learning can be considered an essential part of every hackathon, prior work provides indication that what organizers want participants to learn at a hackathon can be different from what they actually learn or are interested in learning [22]. It is thus necessarily to design a hackathon approach that specifically focuses on activities related to security learning. Addressing this gap we propose and evaluate a hackathon approach anchored around specific interventions by asking the following two related research questions:

**RQ**$_1$. *How can different interventions at a hackathon influence informal learning about security in a social context?*

**RQ**$_2$. *How can these interventions be improved?*

To answer these questions, we conducted an action research study of three teams at a security hackathon. The methods and processes to stimulate security learning were delivered as interventions introduced during the hackathon process. We observed all teams and participants at set intervals during the early, mid, and later phases of the hackathon, administered questionnaires and conducted interviews at the end of the event.

Our results indicate that organising idea generation as a separate event before the hackathon, security talks focused on topics relevant to the hackathon projects, mentor feedback to increase interaction, and a competition style that encourages practising security, foster security learning within the social context of a hackathon.

Our findings thus expand the current body of knowledge related to the use of hackathons as social learning opportunities in a specific context. The contribution of this paper is twofold. First, we developed specific interventions (idea generation, security talks, mentor feedback and competition style) that aim to allow interested individuals to learn more about security (**RQ**$_1$). Second, based on our evaluation of the aforementioned interventions we developed suggestions for how hackathons can serve as a means to teach interested individuals in the social context of a hackathon (**RQ**$_2$).

## 2 Background

In the following section, we will discuss common design aspects that encourage learning at hackathons (section 2.1) and show the security learning research gaps in prior works on security hackathons (section 2.2). This provides a view into our research contribution.

### 2.1 Hackathon design aspects for learning

Designing hackathons that foster security learning require careful planning to create an environment suitable for informal learning through problem-solving within the hackathon social context [6]. Participants should be able to gain sufficient knowledge about security to explore and contribute to the development of security projects within the tight time constraints of the hackathon [17]. Here, we discuss design aspects that have been found in literature to foster security learning. We will use them as a basis for interventions discussed in section 3.1.

The early part of each hackathon event is typically devoted to **idea generation**. Ideas proposed should be real-world problems that are aligned to the theme of the the event. These ideas form the basis of projects that teams will work on during the event [30]. Idea generation allows participants to involve themselves in self-regulated learning from the investigation of the necessary information, and the pursuit of logical inquiry based on knowledge gained [1]. It is thus crucial for hackathons to start with an open idea generation phase [4] where teams can express and refine ideas.

To encourage security learning by solving security issues, it is necessary to provide participants with both domain-specific knowledge. This can help them to better understand the problem context and develop suitable ideas [30]. **Security talks** at a hackathon can provide participants with an understanding of the security domain and allow them to recognise the need for security within the current advances in information systems. Security talks also provide the opportunity for participants to acquire new information [12] relevant to the security project.

One of most prevalent forms of participant support during a hackathon are mentors which commonly provide on-demand feedback and guidance to teams in need [28,5]. **Mentor feedback** can help teams to scope their projects, provide suggestions about how approach a problem, and help with (technical) problems [20]. Mentorship also allows participants to receive learning-oriented support, especially when mentors perceive their role as that of a traditional (workplace or educational) mentor [24].

Although participation in a hackathon is voluntary, specific incentives can encourage individuals to participate. **Competition style** designs can provide incentives to motivate participants to attempt challenging projects that might even be out of their comfort zone / zone of knowledge [11]. Competition based design promotes active-learning where participants learn something new through problem investigation, reconciling new knowledge gained with experience to solve a given problem [30].

### 2.2 Related work

Hackathons are intense, uninterrupted and *time-bounded* events, typically of 2-5 days, during which people gather together and form *collocated teams*, in attempts to complete a *project* of interest [25,18]. Although studies on security hackathons exist, most reports focus only on describing the hackathon event itself. Kharchenko et al. [15] presented a case study collection of different security hackathons carried out to facilitate university-industry cooperation. However, they did not report on an evaluation of how different hackathon activities contributed to security learning. Similarly, the paper by Starov et al. [29], reports on a hackathon where students were provided comprehensive knowledge in a particular course (i.e, security), then participated in an idea generation and prototype development training. The emphasis of this study was on start-up development and establishing communication between university and industry. The study did not contain an evaluation of hackathon design aspects that foster security learning nor of learning objectives to be achieved by the hackathon. Lastly, Foley et al. [10] discuss findings from a science hackathon for researchers. During this event, researchers were able to explain their ongoing research in cyber-physical systems (CPS) security based on a shared CPS test-bed. But, the paper does not report on an evaluation of the design aspects that foster security learning.

Our work is thus different from prior studies on hackathons because we aim to develop and introduce selected design aspects that foster security learning as *interventions* specific to the context of a case security hackathon. We evaluate the security learning outcomes of participants as a result of the introduced design aspects and then identify means for improving them.

## 3 Empirical method

To answer our two main research questions ($\mathbf{RQ}_1$, $\mathbf{RQ}_2$), we applied an action research approach [21]. This approach appears reasonable because we developed and evaluated interventions from selected design aspects to foster security learning in a hackathon context ($\mathbf{RQ}_1$) with the aim to improve them ($\mathbf{RQ}_2$). In the following we will outline our interventions (section 3.1) before discussing our data collection and analysis approach (sections 3.2 to 3.4) in detail.

### 3.1 Proposed interventions to foster security learning

In this section we discuss the specifics of the interventions we developed to foster security learning at a hackathon. These interventions to be introduced to the security hackathon are based on the design aspects previously discussed in section 2.1.

Our **idea generation** intervention consisted of two parts. We conducted a dedicated idea generation event before the main hackathon during which participants could discuss ideas and form teams. The dedicated idea generation event gave participants an opportunity to prepare an idea fully so that the participants (or newly formed team) can focus on the project during the main hackathon. Nonetheless, we also conducted an idea generation session for all participants at the beginning of the main hackathon. This provided another opportunity to facilitate idea generation for both participants of the idea generation events and for participants that only attended the main hackathon. The idea generation session at the main event was set up so that participants from both categories can present their idea proposals and additionally learn from mentor feedback.

We also introduced **security talks** during the main hackathon and during the idea generation events. These covered top security trends in IoT, security risk management, and the general aspects of security learning. The talks were aimed to enable participants learn about basic security concepts and techniques.

They were also aimed to inspire participants to reflect on their ideas and provide them with a foundation to scope and attempt their projects.

**Mentor feedback** was the third intervention we introduced to the hackathon design. Mentors were organised in two ways; mentors assigned to teams based on the team's needs and free-flowing mentors with a broad range of security expertise that provide support for multiple teams. Team interaction with mentors provided participants with the opportunity to gain expert feedback and allowed them to incorporate this feedback into building their security project.

Lastly, in the **competition style** intervention, we gave prizes to teams that were seen to have attempted challenging projects. We set this intervention to motivate participants to learn through security investigations to create unique solutions to security problems.

### 3.2 Setting

In this section, we outline the context and organisation of the hackathon event and related idea generation events we studied. The events were organised as follows:

We first prepared the designed interventions for the hackathon. We then organised idea generation events, bringing together people from diverse backgrounds to generate ideas that aim at tackling security issues. The main hackathon started with an idea generation session which allowed participants who did not attend the dedicated idea generation hackathon event, the opportunity to propose and refine their security ideas based on mentor feedback. Invited security experts delivered planned security talks as additional resources to aid idea generation. Once the idea generation sessions were completed, the participants formed into teams of 5-8 participants per selected idea and mentors were assigned per team.

Team-assigned mentors interacted with their teams providing guidance and feedback concerning the team's security project and team progress. Free-flowing mentors visited teams based on their need. Mentors also provided input during checkpoint sessions were teams gathered to discuss their project progress. Halfway into the hackathon event, an invited security expert presented another security talk on security risk management to provide the participants with more security considerations when building their projects.

At the end of the hackathon, all teams presented their projects and prototypes for evaluation. The hackathon provided live-streamed presentations of the security projects and prototypes to all interested community members. After evaluation, the judges presented incentives in form of prizes to selected winners.

Figure 1 shows the timeline of the hackathon activities, including intervention preparation, idea generation pre-hackathon events and the hackathon event.

### 3.3 Data collection

We selected three teams (denoted as A, B, and C) for our data collection. They were selected was based on their participation in the idea generation pre-

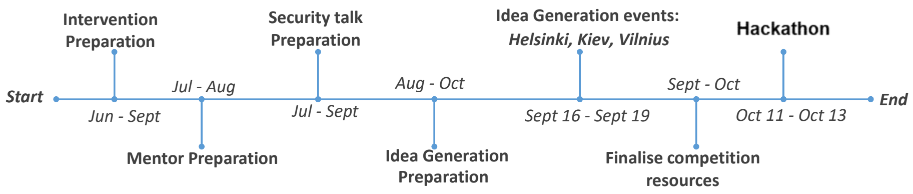

**Fig. 1.** Timeline of the hackathon activities

hackathon events. The selected team characteristics are summarised in table 1. For each team we collected observational data, questionnaires, and post-hackathon interviews. We will elaborate on how each data point contributes to answering our main research questions.

**Table 1.** Team characteristics

| Team | # team members | Interview participants | Selection criteria |
|---|---|---|---|
| A | 6 | A01 (team lead), A02 (lead developer) | No participation in idea generation pre-hackathon event. |
| B | 6 | B01 (team lead), B02 (security expert and developer) | Participation in idea generation pre-hackathon event and continued with the same idea at hackathon. |
| C | 5 | C01 (team lead), C02 (developer) | Participation in idea generation pre-hackathon event but did not continue with same idea at hackathon. |

At the hackathon event, we moved between the teams to observe the participants. The observation method included monitoring at intervals and recording the responses of the participants to the discussed interventions. Reactions such as attentiveness to security talks, positive interactions between teams and mentors reported when discussing with a sample of participants, and perceived satisfaction of participants related to their project indicated reactions to respective interventions. We also recorded other aspects that may contribute to understanding the overall hackathon experience of the participants such as their perception about their teamwork, team process, and their satisfaction with their project. We did not observe all teams throughout the entire duration of the hackathon as we perceived the early, mid and late phases of the hackathon to be most crucial. We use the recorded observations to evaluate if the participants able to achieve learning gains with the introduced interventions as well as other team aspects ($\mathbf{RQ}_1$).

After the hackathon event, we conducted a post-hackathon questionnaire using pre-existing instruments [8,9,2] that we adapted to our hackathon study[3]. The questionnaire covered the participants' perception of learning gains from the interventions, learning benefits from completing the security project. We also recorded participants' perception of specific team properties such as size,

[3] Detailed questionnaire information can be found in https://git.io/Jfp55

team familiarity, leadership, skill diversity, product satisfaction and collaboration process. The aim of the questionnaire was to gain additional context related information that might influence the participants' experience during the event.

From the selected teams, we chose 2 participants per team for an interview to discuss the hackathon experience, learning gains at the hackathon, and the hackathon outcome (i.e., security project worked on). These participants were selected because they either held a vital role in the team (i.e., team lead) or by observation, appeared to contribute significantly to the team.

The interviews lasted between 25 and 30 minutes. A sample of questions asked during the interviews include;

1. How was the hackathon from your perspective in the form of: What did you do after you arrived? How did you see the event play out?
2. Did you attend the idea generation pre-hackathon event? What idea did you develop? How else did you prepare for this hackathon?
3. What were the outcomes as a result of learning? [mentors, security talks, team members, working on the project]
4. How do you perceive the outcome of the hackathon? Were you satisfied? How did you see your teamwork?
5. Did you discover new security knowledge during the hackathon? How did you discover this?
6. What about the continuity of your project? Have you use anything learned during the hackathon already? Are you planning to use it in the future?

The data from the post-hackathon interviews allowed us to evaluate how the different interventions related to security learning thus enabling us to develop suggestion on how to improve the proposed interventions ($\mathbf{RQ}_2$).

### 3.4 Analysis procedure

First, we discuss the journeys of each selected team and the impacts of the introduced interventions on each teams based on a combination of observation, questionnaire, and interview results. The questionnaires are used qualitatively as an additional data source to the analysis procedure.

We then compared security learning for the teams using Bloom's taxonomy learning dimensions as a basis [3,19]. Bloom's taxonomy describes levels of learning where each category of *remember*, *understand*, *apply*, *analyze*, *evaluate*, and *create* form the learning dimensions [3,19]. Our application of Bloom's taxonomy is based on data from team observations. A security expert assessed the learning gains for each team. By comparing the teams journeys, we can analyse how the participants encountered and worked with knowledge provided through the interventions.

Lastly, we evaluated how well the interventions worked for the team participants in encouraging perceived security learning using data from the questionnaires and interviews. This also reveals the shortcomings of the introduced interventions in fostering learning, where we suggest improvements to the interventions.

## 4 Findings

This section outlines the journeys of each selected team, the perception of each learning intervention for each team, and the differences between teams in relation to their learning process. Data collected about the perception of learning from interventions are illustrated in figure 2, while table 2 shows data about team properties (of size, team familiarity, leadership, skill diversity, collaboration process, and product satisfaction).

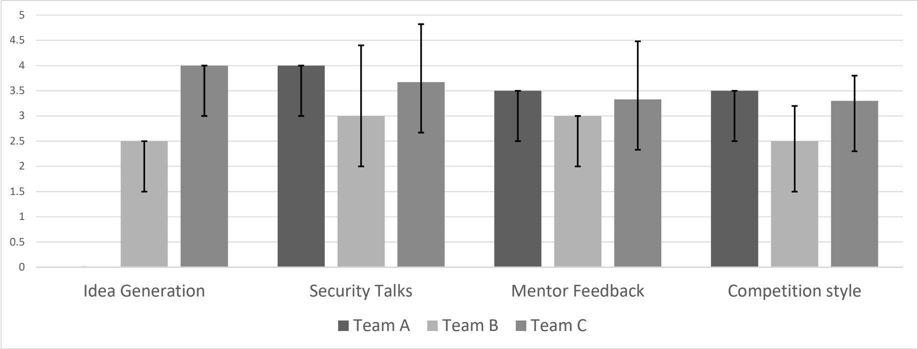

**Fig. 2.** Questionnaire responses by participants after the hackathon about interventions and satisfaction with learning experience. All responses were given on a 5-point scale which were anchored between strongly disagree (1) and strongly agree (5). The bars indicate the mean (m) and standard deviation (SD) for each team.

**Table 2.** Calculated team property data (means, standard deviations, diversity formula, size count) used in qualitative analysis. Mean and standard deviation values are from responses given on a 5-point scale.

| Team property | Team A | Team B | Team C |
|---|---|---|---|
| size* | 6 | 6 | 5 |
| team familiarity | $m = 1.1, SD = 0.25$ | $m = 4, SD = 0.9$ | $m = 1, SD = 0$ |
| leadership | yes | yes | yes |
| skill diversity** | 0.6 | 0.7 | 0.4 |
| collaboration process | $m = 3.8, SD = 0.3$ | $m = 4.5, SD = 0.4$ | $m = 4, SD = 0.3$ |
| product satisfaction | $m = 4, SD = 0.9$ | $m = 2.9, SD = 2.1$ | $m = 3.5, SD = 0.9$ |

*Reported number of participants in a team.

** To estimate skill diversity, we calculated similarities in the reported skills within a team and then determined how different they are (by subtracting the similarity value from one).

### 4.1 Team A

The leader of team A (A01) proposed the idea for the project in the idea generation session at the main hackathon event. A01 derived the idea from "*a security problem from studies*" (A01) of the hackathon and intended to create a tool for enterprises to visualize security aspects. A01 formed a diverse (*0.6*) 6-member team. The team members did not know each other before the hackathon ($m = 1.1, SD = 0.25$). "*Ideation continued during the hackathon because the idea was not properly prepared*" (A01), and completed after discussions in the team and mentor feedback. The idea was refined to "*be targeted at company risk management team to help visualise and communicate security risk scenarios to upper management*" (A01).

At the security talk sessions, team A members reported learning gains from the talks ($m = 4, SD = 0$) and showed an understanding of the security domain while moving forward with the project. A01 highlighted on the "*educating experience about risk management and what is missing in the cybersecurity field*" (A01) presented at the security talks.

During the creation of the final product, A01 highlighted that there was "*support by experienced team members to complete tasks*" for the project. The team leader (A01) fostered learning within the team "*holding everything together, monitoring and identifying the needs of each team members for completing tasks*" (A01). A01 described how teamwork grew and how "*everybody was eager to work and contribute in any way they could*"; "*some team members had no prior experience to security, but they tried to learn and contribute*" (A01). A01 also reported that the team members "*went definitely beyond their current skills*" (A01). The team leader (A01) was involved in "*monitoring and identifying the needs of each team members for completing tasks*", and mentors supported these responsibilities were necessary to adjust scoping of the project. A01 presented updates to the mentors about the project progress, getting feedback from mentors about moving forward to the prototype stage. Talking and interacting with mentors was reported to help the team learn more about security ($m = 3.5, SD = 0.7$).

At the end of the hackathon event, team A presented the security prototype to judges for evaluation. Although team A did not win a prize at the competition, the team members reported, a moderate learning experience from building the final product ($m = 3.3, SD = 0.7$) as an impact of the competition style design. But, there was a moderate agreement on the satisfaction with the product outcome ($m = 4, SD = 0.9$). A01 expressed that there will be no continuation in the project because "*the market value for this type of project*" (A01) was unclear.

### 4.2 Team B

The leader of team B (B01) presented an idea developed at the pre-hackathon event. B01 highlights that attending the idea generation event provided "*a lot of support to [my] idea*". The idea developed was to "*make data security more desirable for startups and give them a badge*" (B01), thereby aiming to improve security learning in startups. B01 presented the idea during the idea pitching session of the hackathon event and received feedback by mentors. After idea generation, B01 reports that team formation was easy. This is because B01 "*was familiar with most of the team because [we] studied together at the university*" (B01) ($m = 4, SD = 0.9$). B01 formed a diverse (*0.7*) 6-member team.

At the security talk sessions, B02 explained that these talks were instrumental as the team "*tried to gather all sorts of information on how to secure systems and gained knowledge*" (B02). Team B members reported security gains from the talks ($m = 3, SD = 1.4$). Team B participants reported learning experiences from the mentor feedback ($m = 3, SD = 0$) as it provided "*an opportunity for [us] to explain our work progress*" (B02). B02 reported that "*different mentors visited multiple times*", and that the mentors "*visited to guide completing tasks*" (B02), but B01 reported that the multiple visits "*disrupted the flow of tasks*"(B01). B01 reported that mentors specifically provided feedback on the scoping of the project, and refinement of project content.

During the creation of the final product, the team perceived their collaboration process to be efficient ($m = 4.5, SD = 0.4$). B01 mentioned that a "*blackboard equipment for documenting the team's process and ideas, allowing [us] to see the big picture*" (B01), thereby aiding collaboration between members of the team and between the team and visiting mentors. On the impact of competition style of the hackathon on team B, there was a moderate learning experience($m = 2.5, SD = 0.7$) from accomplishing the task of building security content for the prototype.

Towards the end of the hackathon event, Team B pitched their project and presented the prototype for evaluation. Team B won a prize for a unique product developed and its perceived usefulness to the security community. Interestingly, there was a moderate satisfaction with the outcome of the project ($m = 2.9, SD = 2.1$). B01 raised an issue with a team member leaving the team unexpectedly halfway through the hackathon with the resources already gathered by the team. Continuation of the project following the competition style intervention was encouraged by the incentive prize awarded to the team project. Although B01 reported that the team intends to continue with the project, we learned from both B01 and B02 that the provided incentive might not be useful to its continuation.

### 4.3 Team C

The team lead (C01) pitched an idea during the idea generation session of the hackathon event. Although C01 attended the idea generation pre-hackathon event, the idea pitched at the main hackathon event was different from the one C01 worked on during the pre-hackathon event. C01 pitched the idea to "*create a binary betting platform for smart contracts*"(C01) on a blockchain platform. However, mentors provided feedback that the presented idea did not readily provide a project addressing current security issues and asked C01 to think more about potential security aspects of that idea. C01 formed a less diverse (*0.4*) 5-member team, consisting mainly of developers interested in developing a blockchain-based project.

Once team formation was complete, the participants in team C continued idea refinement with the mentor feedback. C02 stated that the initial idea "*didn't seem like a good idea for a security hackathon, so [we] needed to connect it to a security topic*" (C02). Thus, a new idea was formed based on blockchain, where the team decided on "*an availability insurance smart contract for service providers*" (C02). The team leader (C01) provided progress reports on development to the mentors, who contributed feedback on how to enhance the proposed security prototype. The participants of team C reported learning experience from the provided mentor feedback ($m = 3.33, SD = 1.15$). Although there were no individual reports from the participants of team C about learning experiences from the security talk sessions, questionnaires responses from team C participants report learning gains from the security talk intervention ($m = 3.67, SD = 1.15$).

The participants in team C report security learning experience by working on project tasks ($m = 3.3, SD = 0.5$) such as researching the security aspects of the prototype. The team perceived their collaboration process to be efficient ($m = 4, SD = 0.3$). C02 highlighted that this was due to the team's high interest in development using blockchain. Towards the end of the event, Team C pitched the final prototype for evaluation. After evaluation, Team C did not win a prize at the event and reported satisfaction with the outcome of the project ($m = 3.5, SD = 0.9$). C02 mentioned that there were no intentions of the participants to continue with the project idea.

### 4.4 Team comparison

In this section, we compare the learning gains between the teams A, B and C based on the knowledge of the team's activity, and other observations at the hackathon (see section 3.1). Figure 3 shows the learning gains based on Blooms taxonomy. According to our findings, team B showed the most learning gains followed by team A then team C. In the following, we discuss how the teams were observed to use the different interventions in order to achieve learning gains.

Team A was showed the ability to recognise relevant security knowledge and to provide specific security information gained through the security talks. The study participants (A01, A02) were able to recall the security risk management concepts discussed in the security talks, and discussed about these concepts in relation to their security project. Team B also showed the ability to remember security knowledge from the security talks intervention. B01 presented the security idea of a platform that encourages data security, related to security issues raised in the security talks. Team C participants talked about the availability security aspects of blockchain, recalling knowledge from security talk sessions. Teams A, B, and C thus attained the **remember** process category.

Teams A and B showed the ability not only to remember and recall but interpret and explain security concepts. Team A showed an understanding of security issues from the security talks. This understanding is evident in the generation of a security-relevant idea and discussions with mentors on security issues and their impact in a security risk-aware business environment. Team B showed an understanding of security concepts, evident in the generation of a security-relevant project for the start-up environment. Thus the teams' A and B attained the **understand** process category.

Teams A and B were able to apply the security knowledge gained during the idea generation sessions, following mentor feedback and in the process of building a unique security project. Team A (A01) was able to incorporate feedback from mentors to focus on resources to visualise and communicate security risk scenarios. Team B (B01) was able to apply mentor feedback in defining the security aspects within the life-cycle of target start-ups. Team B also showed the application of security knowledge gained by research on the security aspects within start-up life cycles. Team C participants, in interviews, did not readily show the application of gained security knowledge in its process and blockchain based product. Thus, teams A and B attained the **apply** process.

Teams A, B, and C were given the chance to present their developed security prototypes. However, only team B was able to show how the security knowledge gained through interventions related to the overall purpose and structure of their project. Team B respondents presented an analysis of how the introduction of each intervention affected each task, sub-task or process in the development of the final prototype. The team B achieved the **analyse** process.

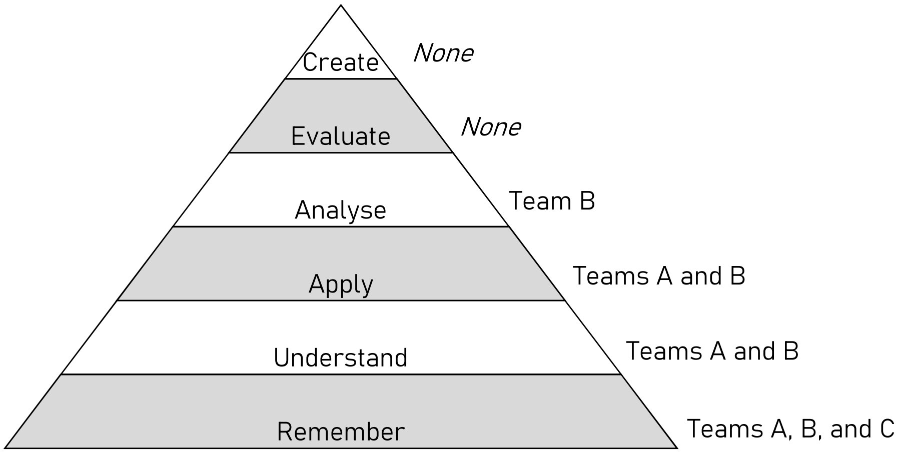

**Fig. 3.** Team learning comparison

## 5 Discussion

In this section, we evaluate how the teams A, B, and C benefited from the different proposed interventions. Relating those with the previously discussed differences related to the teams' learning gains allows us to develop improvements for the interventions thus answering $\mathbf{RQ}_2$.

### 5.1 Evaluation of interventions

Our findings indicate that Team B benefited the most from the **idea generation** intervention as it was instrumental in creating the security project, and as a result, winning the competition. Of all three teams, team B was able to take the most advantage of this intervention, and having more time to work on their idea, resulted in a more mature security idea they could work on during the main hackathon. Team B reported that this was possible because the team lead (B01) attended the idea generation sessions at the pre-hackathon event and began developing their project idea already then. Although C01 attended the idea generation sessions at the pre-hackathon event, C01 ended up working on a new idea during the main hackathon. Also, none of the participants of team A attended the pre-hackathon event. As such, these teams had fewer chances in involving in as much security learning from idea generation as team B.

Teams A and B benefited most from **security talks** while team C showed little to no benefit according to our findings. This could be because the security talks provided were mainly related to teams A and B's security projects. A01 reported that the security talk on security risk management was relevant to their security risk visualisation project. B01 reported that the security talk on start-up security learning provided the required security knowledge relevant to the team's project. C01 reported that the security talks were not particularly relevant to their blockchain project but were only useful to provide general security knowledge. It thus appears important that talks need to be tailored towards team needs in order to be perceived as useful.

Our findings also indicate that Team B benefited most from the **mentor feedback** intervention in achieving security learning as opposed to other teams. This could be because of the high amount of interaction with diverse mentors. B02 reported that different mentors visited the team at multiple times to provide an expert perspective on work progress. However, B01 said that mentoring became disruptive to the team process because of multiple visits. Teams A and C, showed little benefit from this intervention and did not report as much interaction with diverse mentors as with team B. A01 reported mentor interaction in idea generation and in supporting the completion of set tasks for the security project, while C01 only reported mentor interaction related to idea generation. Thus, reducing the teams' chances of involving in as much security learning as team B. It appears crucial that we should organise mentoring appropriately to ensure an adequate amount of mentor interaction.

Related to the **competition style** intervention, Team B benefited the most. B01 reported that the intervention encouraged rapid knowledge gathering and application of the security knowledge to product creation, thus winning a prize at the hackathon. The perceived benefit could also be as a result of culminating factors including idea generation, team formation, and team properties such as team familiarity, collaboration, satisfaction and leadership, all within the competition constraints. Teams A and C showed little benefit from this intervention. A01 reported that they did not win a prize because too much time was spent on idea generation, causing a race with time to complete the security project adequately. C02 also reported difficulties faced in idea generation.

### 5.2 Suggestions for improvement

Based on our analysis we developed the following suggestion to improve the four main interventions introduced in section 3.1 thus answering $\mathbf{RQ}_2$.

Based on our findings, we would suggest supporting teams in **idea generation** to develop ideas before the main event and continue coaching them related to this idea throughout. Changing an idea does not appear to be feasible. For **security talks**, three suggestions can be proposed for future iterations based on our findings. First, the content of the security talks can be more domain-generic. Another option is to appropriately scope the ideas generated at the hackathon to the context of the hackathon. Finally, we develop the security talks only after idea generation is completed, so that the talks are more domain-specific and have maximum effect of offering adequate security knowledge to participants. Based on our findings, we suggest that the **mentor feedback** intervention be handled with excellent coordination not to disrupt the team process. We suggest that a designated member of the team (most likely the team leader) with knowledge of the team's process, stand in between the mentors and the team when necessary, to handle explanations of the teams progress, and what the team needs in mentoring to prevent multiple disruptions.

### 5.3 Limitations

The aim of our study was to develop and evaluate specific interventions that can foster security learning during a hackathon. While it appeared reasonable to conduct an action research study [21] there are certain limitations associated with this particular study design. We developed specific interventions and studied three teams that participated in a hackathon over a limited period of time that had specific backgrounds and goals for attending the hackathon. Despite selecting teams thoroughly it is not possible to generalize findings beyond our study context since studying a different setting with different teams, during a different hackathon working on different projects might yield different results. Moreover the researchers conducting the study were involved in the planning of the hackathon which can affect the reported findings despite our best efforts to refrain from interfering during the hackathon itself. We also abstained from making causal claims instead providing a rich description of the observed behavior and reported perceptions of teams based on which we discuss differences in how they reacted to the different proposed interventions.

## 6 Concluding remarks

In this paper, we reported on findings from an action research study of three teams at a security hackathon. The study aimed to propose and evaluate how specific interventions – namely idea generation, security talks, mentor feedback and a competition-style event – can foster security learning. Our findings indicate that these interventions foster informal learning about security in the social context of a hackathon. Our results also point to suggestions for improvement. These include organising idea generation as a separate event before the hackathon, preparing security talks focused on topics relevant to the hackathon projects, and coordinating mentor feedback to increase mentor-participant interaction.

## References

1. Akcay, B.: Problem-based learning in science education. Journal of Turkish Science Education **6**(1), 28–38 (2009)
2. Bhattacherjee, A.: Understanding information systems continuance: an expectation-confirmation model. MIS quarterly pp. 351–370 (2001)
3. Bloom, B.S., et al.: Taxonomy of educational objectives. vol. 1: Cognitive domain. New York: McKay pp. 20–24 (1956)
4. Böhmer, A.I., Beckmann, A., Lindemann, U.: Open innovation ecosystem-makerspaces within an agile innovation process. In: ISPIM Innovation Summit (2015)
5. Byrne, J.R., O'Sullivan, K., Sullivan, K.: An iot and wearable technology hackathon for promoting careers in computer science. IEEE Transactions on Education **60**(1), 50–58 (2017)
6. Case*, J., Marshall, D.: Between deep and surface: procedural approaches to learning in engineering education contexts. Studies in higher education **29**(5), 605–615 (2004)
7. Davenport, T.H.: Analytics 3.0. Harvard business review **91**(12), 64–72 (2013)
8. van Eemeren, F.H., Garssen, B.: Scrutinizing argumentation in practice, vol. 9. John Benjamins Publishing Company (2015)
9. Filippova, A., Trainer, E., Herbsleb, J.D.: From diversity by numbers to diversity as process: supporting inclusiveness in software development teams with brainstorming. In: 2017 IEEE/ACM 39th International Conference on Software Engineering (ICSE). pp. 152–163. IEEE (2017)
10. Foley, S.N., Autrel, F., Bourget, E., Cledel, T., Grunenwald, S., Rubio Hernan, J., Kabil, A., Larsen, R., Rooney, V.M., Vanhulst, K.: Science hackathons for cyberphysical system security research: Putting cps testbed platforms to good use. In: Proceedings of the 2018 Workshop on Cyber-Physical Systems Security and PrivaCy. pp. 102–107. ACM (2018)
11. Grimes, J., Seng, J.: Robotics competition: Providing structure, flexibility, and an extensive learning experience. In: 2008 38th Annual Frontiers in Education Conference. pp. F4C–9. IEEE (2008)
12. Horton, M.P.A., Jordan, S., Weiner, S., Lande, M.: Project-based learning among engineering students during short-form hackathon events. In: ASEE Annual Conference and Exposition, Conference Proceedings. vol. 2018 (2018)
13. Hung, M.: Leading the iot, gartner insights on how to lead in a connected world. Gartner Research pp. 1–29 (2017)
14. Juell-Skielse, G., Hjalmarsson, A., Johannesson, P., Rudmark, D.: Is the public motivated to engage in open data innovation? In: International Conference on Electronic Government. pp. 277–288. Springer (2014)

15. Kharchenko, V., Sklyar, V., Brezhnev, E., Boyarchuk, A., Starov, O., Phillips, C.: University-industry cooperation in cyber security domain: Multi-model approach tools and cases. In: Proceedings of the University-Industry Interaction Conference: Challenges and Solutions for Fostering Entrepreneurial Universities and Collaborative Innovation. pp. 265–283 (2016)
16. Kienzler, H., Fontanesi, C.: Learning through inquiry: A global health hackathon. Teaching in Higher Education **22**(2), 129–142 (2017)
17. Kollwitz, C., Dinter, B.: What the hack?–towards a taxonomy of hackathons. In: International Conference on Business Process Management. pp. 354–369. Springer (2019)
18. Komssi, M., Pichlis, D., Raatikainen, M., Kindström, K., Järvinen, J.: What are hackathons for? IEEE Software **32**(5), 60–67 (2015)
19. Krathwohl, D.R., Anderson, L.W.: A taxonomy for learning, teaching, and assessing: A revision of Bloom's taxonomy of educational objectives. Longman (2009)
20. Lara, M., Lockwood, K.: Hackathons as community-based learning: a case study. TechTrends **60**(5), 486–495 (2016)
21. Lewin, K.: Action research and minority problems. Journal of social issues **2**(4), 34–46 (1946)
22. Medina Angarita, M.A., Nolte, A.: Does it matter why we hack?–exploring the impact of goal alignment in hackathons. In: Proceedings of 17th European Conference on Computer-Supported Cooperative Work. European Society for Socially Embedded Technologies (EUSSET) (2019)
23. Morgan, S.: Humans On The Internet Will Triple From 2015 To 2022 And Hit 6 Billion. Cybersecurity Ventures. https://cybersecurityventures.com/how-many-internet-users-will-the-world-have-in-2022-and-in-2030/ **July** (2019)
24. Nolte, A., Hayden, L.B., Herbsleb, J.D.: How to support newcomers in scientific hackathons - an action research study on expert mentoring. Proceedings of the ACM on Human-Computer Interaction **4**(CSCW1), Article 25 (May 2020), 23 pages (2020)
25. Nolte, A., Pe-Than, E.P.P., Filippova, A., Bird, C., Scallen, S., Herbsleb, J.D.: You hacked and now what?:-exploring outcomes of a corporate hackathon. Proceedings of the ACM on Human-Computer Interaction **2**(CSCW), 129 (2018)
26. Pe-Than, E.P.P., Nolte, A., Filippova, A., Bird, C., Scallen, S., Herbsleb, J.D.: Designing corporate hackathons with a purpose: The future of software development. IEEE Software **36**(1), 15–22 (2018)
27. Porras, J., Knutas, A., Ikonen, J., Happonen, A., Khakurel, J., Herala, A.: Code camps and hackathons in education-literature review and lessons learned. In: Proceedings of the 52nd Hawaii International Conference on System Sciences (2019)
28. Soltani, P.M., Pessi, K., Ahlin, K., Wernered, I.: Hackathon: A method for digital innovative success: A comparative descriptive study. In: Proceedings of the 8th European Conference on IS Management and Evaluation. pp. 367–373 (2014)
29. Starov, O., Kharchenko, V., Sklyar, V., Phillips, C.: Hacking the innovations with university-industry hackathons. In: Academic Proceedings 2015 University-Industry Interaction Conference UIIC'2015. pp. 47–61 (2015)
30. Stoyanov, S., Kirschner, P.: Effect of problem solving support and cognitive styles on idea generation: Implications for technology-enhanced learning. Journal of Research on Technology in Education **40**(1), 49–63 (2007)