Engaging Students in Threat Thinking with the Cyber Security Cinema

Joseph Maguire
School of Computing Science
University of Glasgow
Glasgow, Scotland, United Kingdom
joseph.maguire@glasgow.ac.uk

Rosanne English
Department of Computer and Information Sciences
University of Strathclyde
Glasgow, Scotland, United Kingdom
rosanne.english@strath.ac.uk

Steve Draper
School of Psychology
University of Glasgow
Glasgow, Scotland, United Kingdom
steve.draper@glasgow.ac.uk

ABSTRACT

There are many topics in cyber security that motivate and excite students to learn as well as other topics that do not. The present paper outlines a learning design devised to motivate and engage students with some topics in cyber security using films. Learners are allocated to groups, select a film from a list, identify relevant cyber security concepts that appear in the film and share them with others. The present paper outlines the motivation for the activity, the learning design, feedback from students on an initial execution as well as discussion before offering some concluding thoughts.

KEYWORDS

cyber security, research-led teaching, active learning

ACM Reference Format:
Joseph Maguire, Rosanne English, and Steve Draper. 2023. Engaging Students in Threat Thinking with the Cyber Security Cinema. In *Computing Education Practice (CEP '23), January 6, 2023, Durham, United Kingdom.* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3573260.3573264

1 INTRODUCTION

Films are cultural artefacts that are able to engage and stimulate audiences of all ages. Consequently, films could be used within teaching to engage learners with specific topics and as part of class activities that scaffold learners to recognise and develop valuable skills and knowledge.

Audiences can vary widely in terms of their interpretation of the motivation and actions of characters within films. These differences can lead to stimulating debate between viewers. Similarly, learners could be asked to identify specific concepts in films as examples to other learners, but by doing so as part of a team, learners may come to recognise that others disagree on what is an appropriate example or not. Consequently, learners will need to debate and discuss scenes to come to an understanding or agreement.

This is not dissimilar to processes such as adversarial and threat thinking when teams need to consider the potential risks systems may encounter. An appropriate activity may be to ask learners to identify examples of cyber security concepts in a film, discuss and debate the examples and then share them with the wider class. Consequently, the contributions of this present practice paper are:

- Adaptation of an existing active learning design for use with approximately 400 learners.
- Feedback from learners on the experience of the active learning design.
- Discussion around the challenges and potential improvement to the active learning design.

2 BACKGROUND

The concept of using film as a teaching resource within class has long since been established [10]. In spite of this, a significant challenge has been ensuring learners have equitable access to such resources [9]. However, in recent years, many of the barriers to utilising films within teaching have subsided as video streaming has became more widespread. There are also organisations such as the British Universities and Colleges Film and Video Council that provide valuable resources, such as Box of Broadcasts (BoB) to support educators in incorporating media into their practice [6].

While it may seem reasonable if not obvious for film to form part of arts education, it may not seem relevant to other domains, such as science. Dubeck outlines the design of a higher education course on science for non-science learners centred around cinema [5]. Dubeck reports that despite around half the course time being spent on film screenings, learners demonstrated greater grasp of scientific principles than a typical class of non-science learners enrolled on a traditional course that did not incorporate films [5].

Similarly, Champoux outlines the advantages and disadvantages of using film as part teaching as well as the different use cases [2]. Champoux discusses the experience of using films as part of teaching practice for organisation and management theory. Champoux highlights that film viewers are not passive and have diverse and varied responses. Responses that can be utilised in teaching to develop knowledge and skills.

Given the potential for films, as well as other media, it is unsurprising they have been used in a range of cyber security education and awareness programmes [11]. One body of work which is of particular note is that of Blasco and Quaglia [1]. They outline their attempts to develop film guides for teaching the STRIDE threat thinking framework.

STRIDE is a mnemonic and represents the six common threat categories of Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service and Elevation of Privilege [7]. The expectation is that Software Engineers, or any stakeholder for that matter,

CEP '23, January 6, 2023, Durham, United Kingdom

ACM ISBN 978-1-4503-9821-3/23/01…$15.00
https://doi.org/10.1145/3573260.3573264

can cycle through the categories and consider common threats that a system may encounter and mitigate against them. STRIDE is a valuable framework as it permits a group of stakeholders to discuss and document potential threats from multiple perspectives. The approach from Blasco and Quaglia is interesting as it requires the surfacing of examples from scenes in popular films and collating these into a guide which can then be used by educators to teach STRIDE concepts.

However, a potential adaptation of this teaching practice is to get groups of learners to watch films and identify potential scenes that serve as examples of STRIDE components. The expectation, as Champoux argues, is that learners as viewers will debate and discuss whether a given scene actually does represent an appropriate example or not. The process that the learners go through in the team is a valuable skill as this is what they would need to do in practice when identifying threats with various stakeholders. Consequently, in §4 we outline the adaptation of the teaching practice proposed by Blasco and Quaglia for use directly by learners.

3 CONTEXT

The present practice was employed on a postgraduate cyber security course delivered within a research-led university in the United Kingdom (UK). The cyber security course itself is focused on a number of areas including risk assessment, adversarial behaviours, legislation and fundamental security concepts. The 10-week semester course is offered in the first semester of the academic year and typically has around 350 to 400 enrolled students.

The demographic of the postgraduate course includes students that range from those with limited prior knowledge of Computing Science (CS) and Software Engineering (SE) to students that may have completed an undergraduate degree in CS or SE. The expectation is that all students will have limited to no prior knowledge of cyber security. An important dimension of the postgraduate course and its delivery in the first semester is that the students will have potentially limited knowledge of not only the institution but of the country. The cohort is diverse, comprising students from the UK together with those from several other countries. Consequently, there is potential value in scaffolding interactions amongst students using the activity as a vehicle.

4 LEARNING DESIGN

Learners were issued with an activity sheet and overview video of the activity via the virtual learning environment (VLE) seven days in advance of the teaching session. The activity sheet and overview video outlined the central steps of the non-assessed team activity as well as pointers to necessary resources to complete it.

The first step in the activity was for learners to identify their team. Learners were randomly allocated into teams of six members. Learners were advised to consult the team allocation table on the VLE to identify their team, its members and how to contact them.

The second step in the activity advised learners to arrange a time to meet to select a film and organise a time to watch it. Teams were advised to select one from a list of five. The five films were WarGames, Rogue One, The Lion King, Hackers and Starter for 10. Teams were advised that they should not purchase movies as they could stream them from the Box of Broadcasts (BoB) from The British Universities and Colleges Film and Video Council using their University credentials.

The third step was for learners to familiarise themselves with the STRIDE framework by viewing a short lecture or *lecturette* on the framework. Learners were advised to make notes and to watch the lecturette either alone or as part of the team before watching the film as a team.

The fourth step is for learners to gather in their team and watch one of the films from the list as a team. During the film they should identify appropriate examples of the concepts from the STRIDE framework present in the film. For example, Tampering can be broadly considered as sabotage. A more specific example may be interfering with the integrity of the data. Consequently, an example taken from one of the films would be when the character David in WarGames alters the grade of a classmate without appropriate authorisation. The character is tampering with the grade data and the integrity of the data is now lost.

Learners were advised to identify and discuss examples, of STRIDE concepts, and agree whether they are an appropriate example or not. For example, in the aforementioned example of grade data, teams could debate whether they think that is an appropriate example of Tampering or not.

The fifth step comes when the team agrees a scene from a film is an appropriate example of a concept from STRIDE. Teams were expected to access the VLE and enter the example into a database. For each extracted scene teams were expected to state at which time the scene occurs (Time), its duration (Duration), the threat type example (STRIDE), description of the scene (Scene), the stakeholders involved (Parties) and potential discussion topics for class (Discussion).

The last and sixth step was for teams to attend the class, sit with their teams and be prepared to present some of the examples in the class. In the class, a lecture on threat thinking, adversarial behaviours and STRIDE is presented. During the segment on STRIDE, each element is considered, i.e. Spoofing, Tampering etc. For each element from STRIDE, for example Spoofing, the lecturer uses a random number generator to select a team. The team is then expected to present their example drawn from the film they watched that represents that scene. In the situation where a team cannot present an example, another team is considered. If no example can be drawn from the audience, the lecturer presents a prepared example from one of the films. The class concludes and teams are advised they can access the database on the VLE for STRIDE examples from the films.

5 RESULTS

After the class activity was completed the audience were asked to provide feedback. Given the nature of the activity, the aim of collecting the feedback was to determine whether the activity had any value from the perspective of students and how it could be improved in subsequent iterations. Feedback was sought on each student's perception of the activity: (1) in a single word, (2) what formed this perception, (3) what motivated them to complete the activity (given that it was not assessed), (4) what was positive about the activity (if anything) and lastly (5) how the activity could be improved.

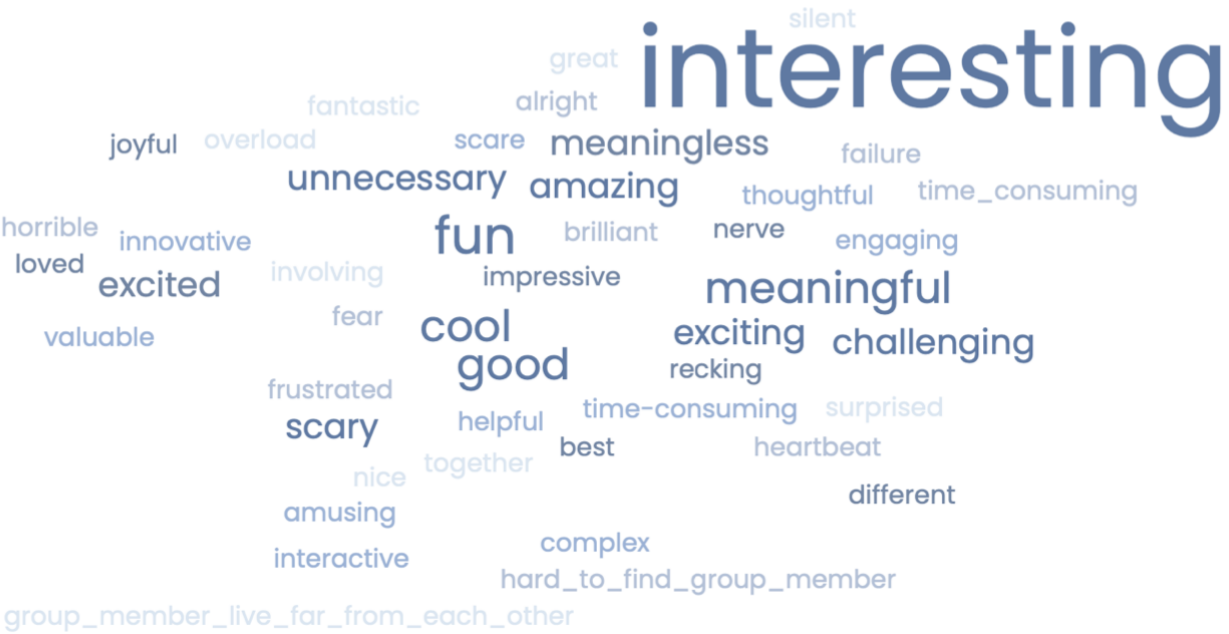

Figure 1: A word cloud generated from student responses when asked to describe the activity in a single word.

Figure 1 illustrates a word cloud generated from 45 student responses when asked to describe their perception of the activity in a single word. The general feedback was positive, the majority of students who responded felt the activity was at least engaging and interesting with comments such as "*valuable*", "*interesting*", "*engaging*" and even "*joyful*". However, there were also comments such as "*scary*" and "*unnecessary*". Follow-on questions asked students asked for feedback as to why they had formed this perception. For students that submitted words such scary, the perception seemed to be best summarised by Participant 10 or P10 with "*getting picked*" as it was "*hard getting in contact with group*". A response that suggests the student was nervous as they had not completed the activity, mainly because they had not been able to connect with their allocated team. In regards to comments such as unnecessary, P19 reflected the sentiment of most students with the feedback "*grades*", probably referring to the fact the activity was not assessed in any way and was merely an activity to prepare for the class.

Exploring this more, students were specifically asked what motivated them to complete the activity given it was not assessed. Responses were given by 42 students. P22 represented many responses with the comment "*being asked to answer questions randomly in class*". The concern with potentially being asked to provide an example in class clearly motivated some teams to engage with the activity. However, there were also many responses that stated they wanted to learn about the concepts considered. For example, P29 reflected the majority of such sentiment with *"I wanted to better understand STRIDE and I wanted to watch WarGames"*.

Learners were also asked to provide feedback on what was positive about the activity, which resulted in 40 responses. While there were some comments from learners which stated "*nothing*" or represented that sentiment, most of the feedback provided was positive. P16 represented the majority sentiment with "*getting to know more classmates and improve understanding of cyber security knowledge*". Similar feedback included "*make friends and learn knowledge*" and "*make friends with other classmates*". P19 provided a comment that at least reflected the intention of the activity with "*it actually makes you feel more connected with the people as well as you came to know different perspectives*". P9 stated "*it was good enough to be a worthwhile event*" reflecting that the activity had some value.

The last element of feedback sought from the class was how the activity could be improved. P12 reflected the majority of responses with "*feels hard to contact other classmate before the class*". There was also the sense that shorter content may be more valuable than long-form films, P11 stated "*try to shorten the content, from movies to short films*" and P7 stated "*some new movies*".

6 LIMITATIONS

The primary limitation of the presented work is reliance on open-text feedback collected from students during class to gain insight into student perception of the activity. The data is not used to assess effectiveness of the approach. Having said that, sharing feedback as well as lessons learned is a contribution that prompts other computing educators to consider aspects of introducing the present activity or any others.

7 DISCUSSION

Chi et al. described careful experiments on learners collaborating while viewing learning material [3]. Their learners viewed in pairs,

with a worksheet, and used a pause button to halt the video when they wished to discuss something. Comparing that paper with the present activity suggests several points and prompts many questions. A simple one to start with could be whether groups should have six or only two members? For the present activity, six gives much more flexibility before the groups and the structure of the exercise becomes well understood. An alternative adjustment could be if groups were allocated early in the course, and had experience of collaborating on simpler tasks (one per week perhaps) before this one.

As Figure 1 suggests, the activity gained student approval as promoting getting to know more classmates. This is a familiar idea, and has been called a "social ILO (Intended Learning Objective)" i.e. a goal of the learning design which is not defined in terms of content knowledge but of creating social relationships which in turn tend to lead to better learning outcomes [4, 8]. The data also showed that learners wanted to learn content and an important consideration here is whether films are useful here.

Films force learners to watch 2 hours when probably only a few minutes are fragments with direct relevance to STRIDE concepts. In a lecture probably it would take less than 5 minutes to explain how a STRIDE concept appeared in the plot of the movie. Consequently, the activity, on the surface, could be perceived as a *massive* waste of time from the perspective of students wishing to learn this particular concept, despite having value in other ways that could support learning.

There is also the structure and delivery of expecting learners to engage in constructing groups, consume content, prepare for an activity outside of contact hours without the motivation of assessment. This is an expectation that can be difficult for some learners to meet, such as those with other responsibilities like care giving or employment.

Having said that, the activity does provide an opportunity for learners to hone skills such as communication and collaboration which they can utilise later, but it raises the issue of whether educators should consider aspects relevant to learners outside primary contact hours or whether they should operate in a vacuum focused only on the present course.

8 CONCLUSION

The present account also represents replication of previously disseminated teaching practice deployed in a different context. Overall the practice appears to have been appreciated by many students, though the non-assessed aspect appeared to dissuade some students from participating and the 'on-the-spot' element appeared to induce anxiety for others. As such, the activity could benefit from further revision to ensure optimal engagement. The practice itself raises many questions, especially around execution and general aims that act as contribution that many educators would want to ask themselves when they introduce a novel activity.

REFERENCES

[1] Jorge Blasco and Elizabeth A Quaglia. 2018. {InfoSec} Cinema: Using Films for Information Security Teaching. In *2018 USENIX Workshop on Advances in Security Education (ASE 18)*.

[2] Joseph E Champoux. 1999. Film as a teaching resource. *Journal of management inquiry* 8, 2 (1999), 206–217.

[3] Michelene TH Chi, Marguerite Roy, and Robert GM Hausmann. 2008. Observing tutorial dialogues collaboratively: Insights about human tutoring effectiveness from vicarious learning. *Cognitive science* 32, 2 (2008), 301–341. https://doi.org/10.1080/03640210701863396

[4] Quintin Cutts, Matthew Barr, Mireilla Bikanga Ada, Peter Donaldson, Steve Draper, Jack Parkinson, Jeremy Singer, and Lovisa Sundin. 2019. Experience Report: Thinkathon - Countering an 'i Got It Working' Mentality with Pencil-and-Paper Exercises. *ACM Inroads* 10, 4 (nov 2019), 66–73. https://doi.org/10.1145/3368563

[5] Leroy W Dubeck. 1981. Science and Science Fiction Films. *Journal of College Science Teaching* 11, 2 (1981), 111–13.

[6] Vicki Holmes, Wilma Clark, Paul Burt, and Bart Rienties. 2013. Engaging teachers (and students) with media streaming technology: the case of Box of Broadcasts. In *Increasing student engagement and retention using mobile applications: Smartphones, Skype and texting technologies*. Emerald Group Publishing Limited.

[7] Michael Howard and Steve Lipner. 2006. *The security development lifecycle*. Vol. 8. Microsoft Press Redmond.

[8] Joseph Maguire, Rosanne English, and Steve Draper. 2019. Data protection and privacy regulations as an inter-active-constructive practice. In *Proceedings of the 3rd Conference on Computing Education Practice*. 1–4.

[9] Don D Smith. 1973. Teaching introductory sociology by film. *Teaching Sociology* 1, 1 (1973), 48–61.

[10] Hart Wegner. 1977. Teaching with Film. (1977).

[11] Leah Zhang-Kennedy and Sonia Chiasson. 2021. A systematic review of multimedia tools for cybersecurity awareness and education. *ACM Computing Surveys (CSUR)* 54, 1 (2021), 1–39.