InfoSec Cinema: Using Films for Information Security Teaching

Jorge Blasco
Information Security Group, Royal Holloway, University of London
Elizabeth A. Quaglia
Information Security Group, Royal Holloway, University of London

Abstract

We present InfoSec Cinema, a film-based teaching activity that uses commercial films to teach information security. We analyse ten films to verify their suitability and build a public and editable database of information security events from films. Our findings show that most films embed enough security events to be used as a teaching tool. This could be used to produce information security teaching activities for a very wide range of audiences. Our experience in running two sessions of InfoSec Cinema was positive. Students were able to identify the most relevant events and even designed mitigations to avoid the problems that were depicted during the film. We also learned that the identification of security events greatly depends on the background and personality of the viewer.

1 Introduction

Today, films are considered an artistic and cultural artefact consumed for leisure, enjoyment and even enlightenment. Independently of their narrative and genre, many films today are based on conflict. Two or more parties clash over opposite goals, and often the roles of attackers and defenders are exchanged as the plot develops. This has similarities with classical information security scenarios, where organisations have to defend from attackers trying to attack their assets.

As teaching techniques develop, it is rather natural to think of films as a new learning vehicle for which enjoyment and engagement are maximised, and therefore consider them as a valuable teaching tool. The idea of using films for this purpose is not new. In [4], authors use film theory to analyse the qualities films have as a communication medium, and discuss how they can be used as a teaching resource in the context of organisational behaviour and management theory. They explore many aspects a film can highlight, and list advantages and disadvantages of this method. Indeed, films are fiction, and as such they may not capture the complexity and diversity of real life. However, they still are a comfortable, engaging and affordable tool, which can be specially suited for *net generation* students [2] and have been used in other areas like healthcare sciences with relative success [8].

In this paper, we propose using commercial films as a teaching resource to learn and foster discussion about information security. Our method is open to any kind of film and can be adapted to different audiences, by focusing either on the type of security events that are of interest or on a particular film. Our goal with this is to produce an engaging activity that teaches and reinforces information security concepts while demonstrating that information security is embedded into everyday behaviours. We have developed an activity, named InfoSec Cinema, where a group of students watches an entire film, but are not provided with pre-selected aspects to analyse. Instead, they are faced with a different task altogether: identify and understand a variety of information security aspects and their evolution over the duration of the film. In this paper, we do not evaluate how accurately a film portrays information security related events, but how the events happening during the film can be used as a teaching resource.

Specifically, our contributions are as follows: (i) We present a new methodology to use films to help teaching information security concepts. (ii) We analyse, create and make public ten *InfoSec film guides*, which consist of a collection of *event cards* describing the security events of a film. Anyone can contribute with new events and films into our database. (iii) We report on the experiences of running two sessions of InfoSec Cinema with two different groups of students (from BSc and MSc degrees respectively).

Section 2 of this paper explains how we transform films into teaching resources and describes our public database of film guides. Section 3 analyses our experiences in running two sessions of InfoSec Cinema and Section 4 presents our conclusions and explains our plans

for future work.

2 Converting Films into Teaching Resources

Using films as teaching material requires a preparatory process that involves the extraction of relevant information from each film and the mapping of events to discussion points to be treated after the film screening. In this section, we explain how to extract information security events from films and organise them so that they can be used for teaching during the subsequent discussion session. We also describe and motivate the kind of information we collect from each of the events. Each of these events could be used in isolation during a lecture, to introduce a more engaging teaching experience, or as part of an entire film screening, where all the events from the same film are later discussed in a moderated session.

2.1 InfoSec Film Guides

An InfoSec film guide helps a facilitator prepare and run a film screening with the additional discussion session. Each guide describes all the information security events that happen during the film. We represent each of these events in what we call *Information Security Event Cards*. A deck of event cards constitutes a film guide. Additionally, a film guide includes a link to the IMDB film page. This gives the facilitator general information about the film and may help them select a film that is suitable for the target audience.

2.1.1 Information Security Event Cards

An *Information Security Event Card* is aimed at providing a baseline for discussion while relating information security with the events that happen during the film. Each event card contains the following information:

Time at which the scene occurs and duration This can help the facilitator replay or isolate the scene for its usage during the discussion.

Brief description of the scene This provides a context for the description and discussion of the information security event.

List of fundamental threats For each scene, the facilitator annotates whether it is related to any threat included within the STRIDE framework [11]. The STRIDE framework is extensively used for threat modelling. Although STRIDE is primarily focused on software systems, it expects the analyst to think about attackers, system users, assets and vulnerabilities [10]. The visual nature of a film can help identifying all these aspects: attackers and defenders as characters, assets as physical objects and vulnerabilities as an event or dialogue (to help the narrative). The goal of this information on the event card is to capture the events happening during the scene from an attacker's perspective, so they can be used later by the facilitator to guide the discussion. Although not all threats portrayed on a film have a software component (i.e. threats affecting the physical world), STRIDE can also be used to capture them. For instance, Snow White eats a tampered apple that has a direct effect on her health.

List of ISO 27002 Categories of controls For each scene, the facilitator selects the security controls that are related to the scene's events. This is meant to capture the event from a defender perspective. In some scenes these security controls will be mentioned because they increase the security of one of the characters, and in others they will be mentioned because of failures related to them. We decided to use the Categories of security controls described by ISO/IEC 27002 [1]. This standard provides a very extensive list of security controls that can be easily mapped to areas within information security (e.g. network security, cryptography, etc.). This could help facilitators mapping specific events or films to courses within a programme while keeping the event description general and degree agnostic. For instance, the event described in Figure 1 could be mapped to a Network Security module.

Further Keywords This space is meant to store any additional information that may help to map the scene to a more specific information security topic. Examples of such keywords could be *biometrics*, *social engineering* or any other security keyword that is not explicitly captured by the STRIDE elements or the list of ISO control categories.

List of parties involved For each scene we record how the particular event of the film affects security posture of the characters in relation to each character's goal in the film. This is a quantitative value that can be useful to characterise the security attitudes of the different characters of the film.

Discussion topics The final component of the film card is a list or description of possible discussion topics that could arise from the scene. The goal of this part of the card is to help the facilitator prepare the discussion session.

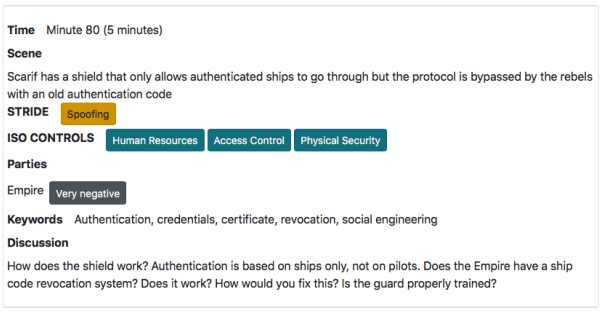

Figure 1: Event card describing the information security aspects of a scene in *Rogue One: a Star Wars Story*.

2.1.2 An Example Event Card

Figure 1 shows an event card representing a security event captured from *Rogue One: A Star Wars Story*. This event describes a scene where a stolen Imperial spaceship has to authenticate to get access to a planet controlled by the Empire. The ship is able to bypass the authentication process using a combination of social engineering and stolen credentials. Because of this, the event card displays spoofing as a STRIDE element and Human Resources, Access Control and Physical Security as the controls that are involved in the attack. The discussion focuses on analysing why the attacks succeeds and also asks the students to design a system that would prevent such an event from happening again.

2.2 Film Analysis

In this section we explain our methodology to extract data and create the InfoSec Film Guides. We also describe and discuss the results obtained after producing the film guides for a selection of ten films.

2.2.1 Methodology

We ensured that all films were watched at least twice by a member of the research team. During the first viewing, we would familiarize with the plot to reduce distractions during the next viewings. During the second and consequent viewings we would stop the film whenever a relevant event was found and would fill in the corresponding information security event card. The identification of security events was driven by the categories described in Section 2.1.1 and the team's experience in the field (as academics in information security).

We emphasize that the identification and interpretation of events during the film may have elements of subjectivity that we cannot control. Therefore, with this methodology, we are aiming at extracting relevant events that could be used during a teaching session. In fact, as we saw during our screenings with students, different people may have different views or opinions about the same event. This shows that personal circumstances, background and other factors may affect the awareness against certain events. This is discussed in more detail in Section 3.3.

2.2.2 Film Selection

Our initial collection is composed of ten InfoSec Film Guides. Instead of targeting films with a specific tech flavour, we decided to select top grossing films in terms of boxoffice (adjusted to inflation) [1]. Our motivation for this decision is two-fold: top grossing films are likely to have been watched by, and potentially impacted, a larger number of people; and considering a variety of film genres, rather than just one, can help highlight how often, perhaps surprisingly, information security events can populate our lives.

From the top 60 in above list, we selected 10 films that run under two hours, since this is the standard length of a class (Table 1). Our selection also tries to capture a variety of topics, genres and release dates.

Short title	Year	IMBD Id
Snow White	1937	tt0029583
101 Dalmatians	1961	tt0055254
Mary Poppins	1964	tt0058331
The Exorcist	1973	tt0070047
Jaws	1975	tt0073195
E.T.	1982	tt0083866
Jurassic Park	1993	tt0107290
The Lion King	1994	tt0110357
Avengers Assemble	2012	tt0848228
Rogue One	2016	tt3748528

Table 1: List of films analysed in this paper.

2.2.3 Results

Figure 2 shows each STRIDE-related event identified during each film. For most films we identified events related to STRIDE elements embedded through the whole duration of the film. In most cases, these events are originated from characters as they try to achieve their goals. For instance, in *Rogue One* most of the attacks are originated from Rebels trying to steal the first Death Star plans. In *Snow White*, they are initiated by The Queen while trying to be the "fairest" in the land, and in *Jurassic Park* they are instigated by a disgruntled employee, Nedry, trying to steal dinosaur embryos.

[1] http://www.boxofficemojo.com/alltime/adjusted.htm

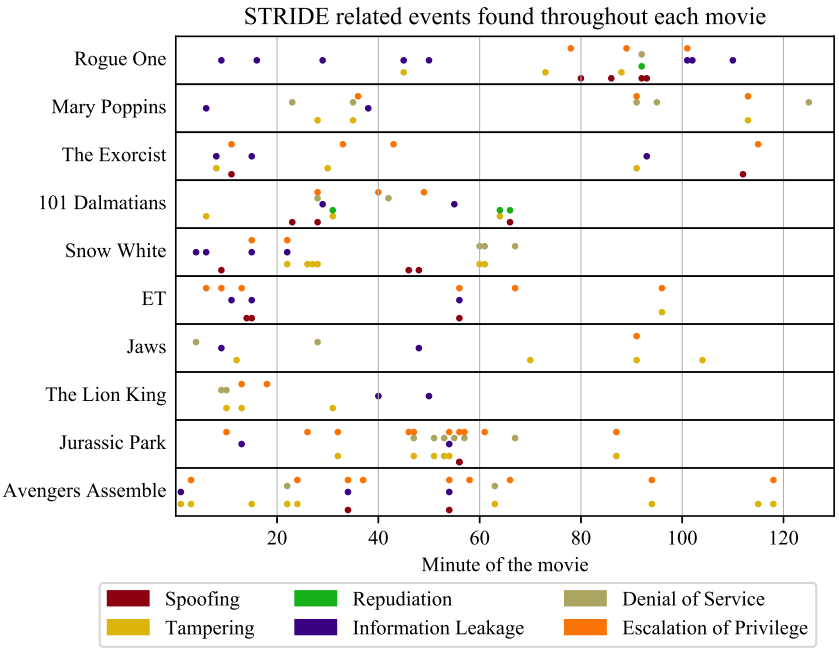

Figure 2: STRIDE-related events identified in the films.

We also noted that several patterns recur during the films. For instance, events that involve tampering followed by denial of service appear in 8 out of the 10 films. This may have to do with film writers using similar narrative constructs to get characters to achieve their goals. In this case, most of the tampering attempts had as a final goal a denial of service attack.

Table 2 (upper part) shows the number of times each STRIDE component appeared within an event for each film. It is clear that some STRIDE components were more present than others during our film analysis. For instance, events related to tampering and escalation of privilege account for more than 50% of the events while there were only 4 events that are related to repudiation. This specific threat is predominant in *101 Dalmatians*, as Cruella tries several times to cover the thieves' errors that would incriminate her of stealing the puppies.

Figure 3 shows the same data as Figure 2 but for events related to ISO/IEC 27002 Control categories. Controls are also well distributed across film duration, as they generally appear along a STRIDE event and most of the STRIDE events affect or try to avoid a security control. In this case, patterns are less noticeable, partially, because, in most cases, we identified more than two control categories related to the same scene.

The bottom part of Table 2 shows the number of times each control category was identified within a scene for each film. The number of events related to controls is, for most films, higher than for STRIDE related events. This is mainly because controls are embedded in many scenes without them being attacked. This happens in two ways: when the scene portraits a control that is increasing the security posture of a character (or group), or when the controls are not implemented correctly. The first case can be seen, for instance, when the computer systems are used to activate the *Jurassic Park* control room locks again. An example of the second case is when, in the Dwarfs lock the door of their vault, but leave its key hanging besides that same door. As it happened with the STRIDE components, some control categories are much more frequent than others. Cryptography, Supplier Relations and Compliance events appear in very few films while Access Control, Operations Security and Physical Security appear in almost all films. We believe that this pattern will appear in other non-IT focused films.

Both the number of event cards and the distribution of STRIDE components and ISO controls can be useful to decide whether or not to use a specific film for a viewing session. In our case, films like *E.T.*, *Jaws* or *The Lion King* have a very limited number of events and wouldn't be very useful for a full film screening. However, films like *Rogue One*, *101 Dalmatians*, *Snow White* and *Jurassic Park* include a good number of quite heterogeneous events and would be suitable for a full film screening. In fact, these films can help students realise that information security is not an isolated issue and should be addressed holistically. The final decision of what kind of film to select for a specific screening will depend on the audi-

	Rogue One	Mary Poppins	The Exorcist	101 Dalmatians	Snow White	ET	Jaws	The Lion King	Jurassic Park	Avengers Assemble	Total (%)
STRIDE											
Spoofing	4	0	2	3	3	3	0	0	2	2	**19(12%)**
Tampering	3	3	3	3	6	1	4	3	6	9	**41(26%)**
Repudiation	1	0	0	3	0	0	0	0	0	0	**4(2%)**
Information Leakage	8	2	3	2	4	3	2	2	2	3	**31(19%)**
Denial of Service	1	5	0	2	3	0	2	2	6	2	**23(14%)**
Escalation of Privilege	3	3	4	3	2	6	1	2	10	9	**43(27%)**
STRIDE Event Cards*	**17**	**10**	**10**	**12**	**13**	**9**	**8**	**7**	**18**	**14**	-
Control Categories											
Policies	1	2	0	1	1	1	0	1	3	1	**11(3%)**
Organization	3	1	0	0	3	1	0	1	3	1	**13(4%)**
Human Resources	7	3	4	2	8	0	0	0	12	0	**36(11%)**
Asset Management	3	3	0	1	0	0	2	1	4	7	**21(6%)**
Access Control	7	4	3	5	7	3	0	2	11	9	**51(15%)**
Cryptography	1	0	1	0	1	0	0	0	0	1	**4(1%)**
Physical Security	8	5	4	5	5	6	4	2	8	5	**52(16%)**
Operations Security	3	3	6	5	7	2	1	1	12	4	**44(13%)**
Communications Security	2	0	4	3	2	1	1	1	0	2	**16(5%)**
System acquisition, develop. and maint.	1	0	2	0	1	0	0	0	13	0	**17(5%)**
Supplier Relations	0	0	1	0	5	0	0	0	0	0	**6(2%)**
Incident Management	4	1	3	6	5	1	3	0	8	2	**33(11%)**
Business Continuity	0	1	0	1	2	0	2	0	8	0	**14(5%)**
Compliance	0	0	1	0	2	1	1	0	3	0	**8(3%)**
Control Event Cards*	**19**	**11**	**12**	**15**	**18**	**8**	**7**	**5**	**30**	**15**	-

Table 2: Number of times each STRIDE component or control category is related to a scene during each film. A scene can be related to more than one STRIDE component and/or control category.

ence and the kind of events the facilitator wants to focus on. To help them make this decision we have developed a film database that is described in the next section.

2.3 InfoSec Cinema Database

The InfoSec Cinema Database (`https://guizos.github.io/infosec-cinema`) displays the InfoSec Film Guides for the ten films that were analysed for this work. Initially, the website shows all the films in a collapsible list of event cards. An example of event card can be seen in Figure 1. The website also has a form that allows to filter all the events per keyword, STRIDE component or security control category. In this way, a facilitator can look for specific kinds of events or keywords. This feature can be used by a facilitator to extract particular events related to a particular security concept, so they can be shown during a regular lecture on that topic. The keyword filter searches within the description of the scene, the extra keywords and the proposed discussion topics. At the moment our database only performs `OR` operations with the different filters.

The website, hosted on Github, uses *HTML*, javascript and the *JSON* InfoSec Film Guides to generate the page and allow user queries. Using Github as a hosting platform has two main benefits. First, our film guides are freely available in both human (*HTML*) and computer-readable (*JSON*) formats. Second, it allows anyone with a Github account to contribute to the database without requiring to implement any server logic. Contributors just need to create a pull request in `https://github.com/guizos/infosec-cinema`. A film guide update will just require a pull request over a single *JSON* file. Adding a film to the database requires the contributor to create a pull request with a new *JSON* file and an update to the `list.json` file.

The website also includes a link to the presentation used to run our InfoSec Cinema for *Rogue One*. This presentation is based on the contents of its corresponding InfoSec Film Guide.

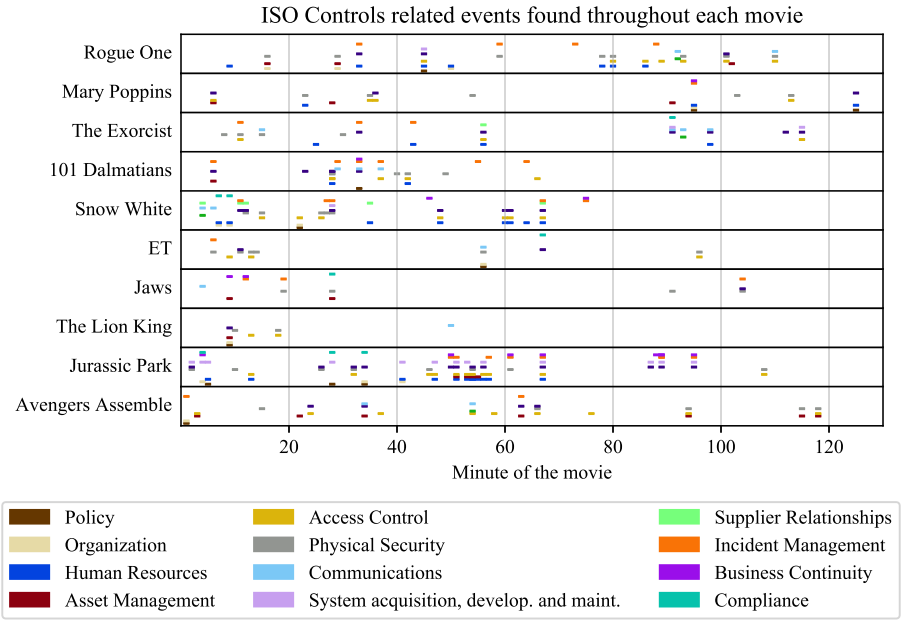

Figure 3: ISO Control categories related events identified in the films.

3 Running InfoSec Cinema

An InfoSec Cinema Session comprises a film screening and a discussion. Instead of focusing the discussion on the technical aspects of film-making such as scriptwriting, an InfoSec Cinema discussion focuses on the information security events that appear during the film. In this section, we explain how to prepare and run an InfoSec cinema session. In addition, we also describe and analyse the data that we captured from running two InfoSec Cinema sessions screening *Rogue One: A Star Wars Story*.

3.1 Preliminaries

The first step to prepare an InfoSec film screening is to read (or create) the corresponding InfoSec Film Guide. In our case, we also decided to prepare a supporting presentation. This includes a subset of the events that were captured from the film (*Rogue One*). For each event slide we include the time within the film and description of the scene. Each event slide also gives some hints and asks questions to facilitate and guide the discussion. This can help the facilitator moderate and guide the students through the different events that happen during the film.

Before running any film screening it is very important to verify that it complies with the relevant copyright legislation. In the UK, copyright legislation is contained in the the Copyright Designs and Patents Act 1988 (CDPA 1988) [3]. This legislation includes a series of exceptions, including a provision for education and teaching. Specifically, Section 34(2) of the CDPA 1988 [5] states: *"The playing [...] of a [...] film [...] before [...] an audience at an educational establishment for the purposes of instruction is not a playing [...] of the work in public for the purposes of infringement of copyright."* where audience refers to people directly connected with the activities of the establishment for the purposes of instruction.

We consider that our screenings fall under this exception. They were teaching activities part of a BSc and an MSc programme. We recommend anyone to consult relevant legislation before running a session.

3.2 Sessions Details

We ran two sessions of InfoSec Cinema. The first session was run for a group of 7 students with no technical background enrolled in a Security Management module from our BSc in Management. The second session was run with 12 students from our MSc in Information Security.

In addition to the film screening and the subsequent discussion, we gave each student a sheet to log all the information security events they identified during the film. Each entry in the event log included a field to write a short description of the scene and another one for security keywords. Event logs are different from the event cards (Section 2.1.1). They include information that can be captured in a few seconds without stopping the film. The purpose of the event logs was two-fold: students would be able to keep a log of the events to help them during the discussion, and this would allow us to analyse

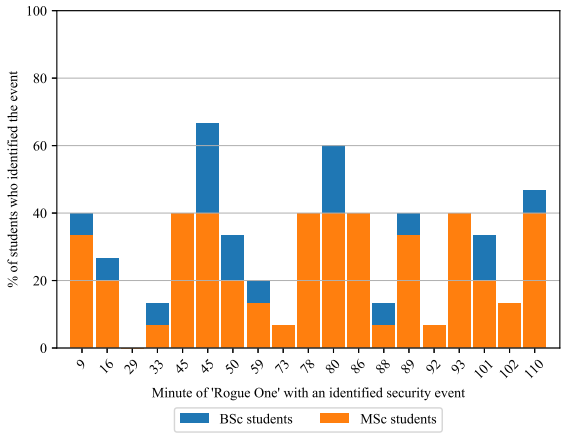

Figure 4: Security events that were identified by the students during the screening.

the kind of events they were able to identify during the screening. This last motivation required us to get clearance from our Ethical Review Board. Before the screening began we gave each student an information sheet describing the purpose of the data collection and informed consent form. We advised students that they had no obligation to participate on the data collection and that they could withdraw at any time, without any consequence on their participation on the film screening or discussion.

3.3 Analysis of Event Logs

Overall, 15 students signed the consent form. From these, only 3 had previously watched the film. In the following, we analyse the events they were able to identify and the keywords they used to describe them.

3.3.1 Identification of Security Events

The students identified a total of 86 events. Figure 4 depicts the percentage of students who identified events that were already included in our film guide.

The majority of students ($\geq$60%) identified the same two events in minutes 45 and 80. These correspond to the most important events from the information security perspective. The first scene shows a disgruntled employee describing a vulnerability he introduced in the first Death Star. The second one depicts an authentication process between a spaceship and a planetary shield.

The events happening during minutes 29, 33, 73, 88, 92 and 102 were identified by less than 20% of students. Four of these had to do with security events that had a positive effect on the Empire. This makes us believe that the viewer might be biased towards negative events that affect the malicious party on the film. The other two security events were embedded in action-packed scenes, which leads us to think that action scenes may hinder the identification of information security events.

Students also identified several events that were not part of the film guide. One example was a scene where the rebels used binoculars to gather information from an Imperial base. Another example that was identified by several students was the reprogramming of the K250 Imperial robot. We didn't identify this as a security event as the reprogramming doesn't actually happen during the film, it is only mentioned by the characters. It is important to remark that the purpose of the film guides is not to be a 100% accurate compilation of all the events of the film. Nevertheless, these two examples show that there is bias when identifying security events and their perception depends on the background, personality and other circumstances. In fact, the MSc students identified more events than the BSc students. This is in accordance with other studies which show that security behaviours depend on personality traits and the same training and policies may produce different results on different employees [7, 6]. We foresee that using a similar experiment (i.e. film screening with security logs) could be used to identify this bias and develop more tailored information security training programmes.

3.3.2 Used Security Keywords

Figure 5 shows a visual representation of the 150 most frequently mentioned keywords across all student's logs. We use a *word cloud* as it provides a very quick and visual representation of the most frequent words in the student logs. We generated the word cloud with the *word_cloud* Python implementation from Andreas Mueller [9]. This algorithm takes a text as input, in our case the student log keywords joined together, and generates an image based on each word frequency. The algorithm removes pronouns, prepositions and other common words. Once the frequency of each word has been normalised, the most frequent one is drawn, with a previously defined maximum font size. The rest of the words are drawn reducing the font size by a factor of $r_s \cdot freq_{ratio}$ where $r_s = 0.3$ and $freq_{ratio}$ is the ratio between the normalised frequencies of the word being drawn and previously drawn word.

Most of the words included in the world cloud are directly related to information security with few exceptions like *Empire*, *droid* or *K250* which reference the film plot. *Data* and *access* are the most frequent words found in the student logs (21 times each). This is somehow expected as the film plot evolves around characters trying to get access to a very sensitive documents (the first Death Star plans). *Authentication* is the third most frequent word, appearing 16 times. This happens because the film con-

Figure 5: Wordcloud with the keywords used by the students to describe the security events found.

tains several authentication scenes, including the one in minute 80 which was identified by 60% of the students. Words like *Physical* and *risk* appear 11 and 10 times respectively. Many of the events that happen during the film have a physical security component (8 in our film guide) and risk is explicitly mentioned by the K250 robot several times during the film (referencing the chances the main characters have to survive certain events).

3.4 Discussion Session and Student Feedback

After the screening, each group held a one-hour discussion session which finished with the students filling in a feedback form. Each discussion started with a question about the students' impressions. In both occasions, several students highlighted that they were not expecting to find so many relevant events during the film and that this changed their way of thinking about information security as an isolated issue. One student even went further and wrote the following in the feedback form: *"This activity can train people in a way of thinking which is very applicable to real-life circumstances"*.

After the initial question the discussion advanced by analysing different scenes of the film. As none of the scenes were identified by all the students, every time a new scene was discussed, the student starting the discussion would have to justify why they had identified that scene as a security event. The group of MSc students discussed the spaceship authentication scene (minute 80) in much more detail than the other group. They even tried to design a scheme to avoid the weakness of the Imperial system. Their proposals took into account the need of authenticating the crew and the cargo in addition to the only-vehicle authentication that is used by the Empire. This shows how a relevant scene can foster discussion and even encourage students to apply the knowledge learnt during a course in an applied scenario. The group of BSc students focused more on the insider problem. This was a natural discussion for them as they came from a Management background. They discussed possible indicators to identify risk coming from insiders behaviours and talked about mechanisms to avoid some insiders having too much control over a critical activity.

In general terms, the student's feedback was positive, describing the activity as a *"fresh new approach to an example and great way to conduct the last lecture"* or *"a great approach with interesting examples."*. Some students provided constructive critical feedback. One student mentioned that *"A film cannot portrait all information security events known in the real world"*. Two other students complained about the film duration, stating that instead of a film screening, specific scenes could be selected and shown during a lecture. We acknowledge that this is a possibility and for many audiences it may be preferable over a full film screening.

4 Conclusions

In this paper we propose the usage of films as information security teaching resources. We propose an activity, InfoSec Cinema, consisting of a film screening and a subsequent discussion session of approximately one hour of duration. InfoSec Cinema does not focus on hacking films. Instead, we propose to extract information security behaviours and events from mainstream films.

We analysed the suitability of ten top-grossing films for their usage in InfoSec Cinema. Our results show that most films, independently of their genre, display several information security events and behaviours across the entire duration of the film. Some films would not be suitable for a full-length screening because of their limited number of events. The film analysis are publicly available on a website so other facilitators can search for specific kinds of events or keywords and prepare more engaging lectures or their own cinema sessions. We plan to expand our film database with new films but we also invite others to make their own contributions.

We report on the experiences of running two InfoSec Cinema sessions screening *"Rogue One: A Star Wars Story"*. Most of the students were able to identify the two main events which also took most of the discussion time. Our screenings also showed that students, and even facilitators, are sometimes biased towards specific kinds of events. We plan to use this fact to develop a similar activity solely focused on identifying this bias.

Considering the different age classification and genres of our film set, we believe that this activity could also attract more diverse audiences into information security. Our future plans include running similar events College-wide and preparing an activity tailored for School groups by isolating scenes from child-friendly films.

References

[1] 27, I. J. S. ISO/IEC 27002:2013 information technology-security techniques-code of practice for information security controls, 2013.

[2] BERK, R. A. Multimedia teaching with video clips: Tv, movies, youtube, and mtvu in the college classroom. *International Journal of Technology in Teaching & Learning 5*, 1 (2009).

[3] CARTY, H., AND HODKINSON, K. Copyright, designs and patents act 1988. *The Modern Law Review 52*, 3 (1989), 369–379.

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

[5] CROWN, T. Copyright, designs and patents act 1988 (c. 48), 2003.

[6] FURNELL, S., AND RAJENDRAN, A. Understanding the influences on information security behaviour. *Computer Fraud & Security 2012*, 3 (2012), 12 – 15.

[7] GABRIEL, T., AND FURNELL, S. Selecting security champions. *Computer Fraud & Security 2011*, 8 (2011), 8 – 12.

[8] MEMBRIVES, M. D., ISERN, M. T. I., AND MATHEU, M. C. L. Literature review: Use of commercial films as a teaching resource for health sciences students. *Nurse Education Today 36* (2016), 264 – 267.

[9] MULLER, A. Wordcloud. `https://github.com/amueller/word_cloud`. Accessed on May 2018., 2018.

[10] SHOSTACK, A. Experiences threat modeling at microsoft. In *Modeling Security Workshop. Dept. of Computing, Lancaster University, UK* (2008).

[11] SHOSTACK, A. *Threat modeling: Designing for security*. John Wiley & Sons, 2014.