The Effect of Entertainment Media on Mental Models of Computer Security

Kelsey R. Fulton, Rebecca Gelles, Alexandra McKay, Richard Roberts, Yasmin Abdi, and Michelle L. Mazurek, University of Maryland

https://www.usenix.org/conference/soups2019/presentation/fulton

This paper is included in the Proceedings of the Fifteenth Symposium on Usable Privacy and Security.

August 11–13, 2019 • Santa Clara, CA, USA

ISBN 978-1-939133-05-2

Open access to the Proceedings of the Fifteenth Symposium on Usable Privacy and Security is sponsored by USENIX.

The Effect of Entertainment Media on Mental Models of Computer Security

Kelsey R. Fulton, Rebecca Gelles, Alexandra McKay,
Richard Roberts, Yasmin Abdi, and Michelle L. Mazurek
University of Maryland
{kfulton, rgelles, ricro, mmazurek}@cs.umd.edu
{amckay12, yabdi}@terpmail.umd.edu

Abstract

When people inevitably need to make decisions about their computer-security posture, they rely on their mental models of threats and potential targets. Research has demonstrated that these mental models, which are often incomplete or incorrect, are informed in part by fictional portrayals in television and film. Inspired by prior research in public health demonstrating that efforts to ensure accuracy in the portrayal of medical situations has had an overall positive effect on public medical knowledge, we explore the relationship between computer security and fictional television and film. We report on a semi-structured interview study (n=19) investigating what users have learned about computer security from mass media and how they evaluate what is and is not realistic within fictional portrayals. In addition to confirming prior findings that television and film shape users' mental models of security, we identify specific misconceptions that appear to align directly with common fictional tropes. We identify specific proxies that people use to evaluate realism and examine how they influence these misconceptions. We conclude with recommendations for security researchers as well as creators of fictional media when considering how to improve people's understanding of computer-security concepts and behaviors.

1 Introduction

Computer users frequently make security-relevant decisions during password creation, link navigation, messaging platform selection, and other activities. These choices reflect users' mental models about what is risky, what is safe, and how computer systems work. However, many people have limited knowledge of computer security or computers generally; users' mental models are often incomplete or incorrect [2, 27]. Erroneous mental models can lead users to inaccurate conclusions about how to best protect themselves online (e.g., believing that standard text messages are safer than encrypted chat messages) [2].

Prior studies have shown that mass media, including television and film, can influence user mental models of computer security [21–23]. This phenomenon has been observed in other fields as well: The portrayal of medical information in television and film, and its effect on viewers, has been studied extensively, leading to concrete efforts to improve the accuracy of medical information shown to the public. Programs like "Hollywood, Health and Society" provide consultation to the entertainment industry to help ensure that fictional medical storylines are accurate and avoid disseminating harmful disinformation [1]. Research suggests that, overall, mass-media portrayals have imperfect but positive effects on viewers' medical knowledge [12].

In contrast, we are aware of no similar effort to improve accuracy in mass-media depictions of computer security. Depictions of computer security and "hacking" in mass media vary, but are often unrealistic, including confusing jargon, unnecessary visuals of internal computer operations, rapid hacking and counter-hacking, and other tropes [7, 16]. There has been little or no research effort to understand how these portrayals affect users' security beliefs and behaviors. Merely exposing users to the concept of computer security may improve their understanding or awareness. However, inaccurate and exaggerated portrayals could also harm development of healthy mental models.

To investigate this question, we conducted a semi-structured interview study (n=19) to gauge how media portrayals affect people's perceptions of computer security and hackers as well as their resulting mental models. We asked participants broadly about their prior computer security knowledge, experience, and mass media background. We then showed each participant six clips involving computer security from

USENIX Symposium on Usable Privacy and Security (SOUPS) 2019.
August 11–13, 2019, Santa Clara, CA, USA.

television shows and movies, chosen to depict different technological and social dimensions both more and less accurately, asking participants to evaluate the realism of each clip and to explain their reasoning and judgment. In particular, we focused on three main research questions:

RQ1. What do people learn about computer security from mass-media portrayals?

RQ2. How do these learned concepts affect people's overall mental models of computer security and their resulting security behaviors?

RQ3. Why do people learn these particular concepts: for example, why do they find certain portrayals more believable or compelling?

We found that mental models were often affected by incorrect or incomplete information presented in fictional media. While incorrect low-level technical details may not be inherently detrimental, misunderstandings of high-level technical takeaways could cause harm. Media portrayals teach and/or reinforce several common mental models observed in previous work, some of which play a factor in non-optimal security decisions made by users. These include the beliefs that security intrusions are always obvious, that precautions are pointless because hacking is inevitable, and that ordinary users are not important enough to be hacked. Not everything learned from fictional media was negative: participants gained awareness of the danger of phishing and suspicious emails.

We also discovered that participants' trust in fictional depictions — and willingness to incorporate them into their mental models — depends on several key factors. Most participants begin with a default judgment about the average realism of media portrayals (on any topic) and adjust this perception based on cues including their own technical knowledge, their ability to relate depicted events to their own experiences, and the cinematic qualities of the scene. Our results suggest a feedback loop; perceived realism is tied to conformance with pre-existing mental models of security, which may arise in part from prior exposure to fictional media.

We suggest several avenues for improvement. Entertainers should take more responsibility to mitigate the spread of misinformation. Researchers and educators can use our results to better understand the assumptions and decisions that users make when performing security-relevant behaviors and incorporate that knowledge into the design of tools, interventions, and educational content. Perhaps there is room for collaboration toward a common goal of educating users while still keeping them engaged and entertained.

2 Background & related work

Prior work has examined the sources of people's computer-security knowledge. Rader et al. discussed how stories convey security knowledge between individuals, finding this can be an effective medium to change user thought and behavior [20]. In this work, we explore the question of whether stories told in fictional media, rather than person-to-person interaction, also affect knowledge and behavior.

Redmiles et al. investigated why users accept or reject security advice [22], concluding that negative events often motivate users to take advice from fictional and nonfictional stories. In follow-up work, Redmiles et al. found that 67.5% of a broad U.S. sample cited media as a source of security knowledge, and 25% of those participants specifically referenced fictional narratives [21]. Ruoti et al. also found that participants learned about security threats from media [23], and Forget et al. established that many users outsource their decisions to trusted experts, including media [5]. Our work expands on these findings by examining what people learn specifically from fictional television and movies; we explore how perceived realism in fictional media shapes security beliefs.

Other researchers have explored users' mental models of security in detail. Kang et al. used a drawing exercise to elicit mental models of the internet as a whole, finding surprisingly similar security beliefs among users with different levels of technical knowledge [13]. These included beliefs that average users were not of serious interest to hackers, and that security efforts are inherently futile because attackers are too powerful. These beliefs align with those identified by Wash and Rader, who classified several common folk models of attackers as focusing on high-value targets like government officials and wealthy people [27, 28]. Similar mental models were also identified by Abu-Salma et al. in the context of secure messaging applications [2]. This research also identified several misconceptions about the relative security of different communications mechanisms, and about encryption more broadly. Mistaken mental models of encryption were also identified by Wu and Zappala [30]. This broad confirmation of mistaken mental models underscores the importance of understanding where these misconceptions come from.

Prior research has also investigated how mistaken mental models can influence security decision making. Acquisti et al. explored the privacy paradox, in which users express concerns about privacy but do not act to mitigate privacy threats [3]. The authors postulate that this disconnect is due in part to misinformation, as many participants could not correctly identify the likelihood of various privacy abuses. This paper, as well as another by Herley, argues that users trade off the cost of compliance with recommended security behaviors with their perception of the associated reduction in risk [11]. Herley notes that users become habituated to dangers that are oversold or exaggerated. If media suggests that protective behaviors are unnecessarily complicated or onerous, or that threats are so powerful that they cannot be averted, users' willingness to comply may be reduced. Similarly, when media presents exaggerated threats, users' ability to recognize less

dramatic security problems, such as those encountered in real life, may be impaired. We explore these hypotheses further in this work.

The effect of fictional media on behavior has been explored in other contexts, such as portrayals of medical conditions. Whittier et al. found that those who viewed a storyline about syphilis in a fictional TV show were more likely to report intention to be screened, and to inform others about the risk [29]. The effect is so pronounced that in 1997 the Centers for Disease Control and Prevention launched the "Health, Hollywood, and Society" program, to provide medical information to writers in Hollywood [1]. It is clear that portrayals in fictional media can and do affect people's behavior, both positively and negatively. We apply a similar frame to portrayals of computer security.

3 Method

To understand how fictional TV shows and movies inform viewers' mental models, we conducted semi-structured interviews with people in the Washington, DC area. In this section we detail our recruitment, the content of our interview protocol (including piloting), our clip selection, our data analysis approach, ethical considerations, and limitations of our study.

3.1 Recruitment

To recruit participants, we posted an advertisement to Craigslist in the DC region offering $30 as compensation for participation in an hour-long interview study. Those who wanted to participate were directed to a pre-screening survey. After consenting to the survey, participants entered general demographic information, provided an email address for future contacting, and answered questions about the amount and type of media they consume. From those responses, we selected a sample to invite for interviews, using a modified first-come, first-served approach that also considered demographics. In particular, we selected for diversity of ages, educational backgrounds, and ethnicities, as well as in self-reported frequency of media watching and preferred genres. We also focused on selecting participants with limited technical backgrounds.

We interviewed participants until we stopped hearing substantially new ideas, resulting in a total of 19 participants. This approach was validated when no new codes were created while analyzing any of the final three participants. This sample size aligns with qualitative best practices [8].

3.2 Interview protocol

During September and October 2018, we conducted 19 in-person, semi-structured interviews on the University of Maryland campus. Each session lasted about an hour. Most interviews were conducted by two interviewers; due to scheduling conflicts two interviews were conducted solo. Each interview was audio recorded, with permission.

ID	Gender	Age	Ethn.	Educ.	TV hrs
P1	M	30-39	B	HS	50
P2	F	30-39	B	AD	8
P3	M	30-39	AHP	BD	14
P4	F	40-49	W	BD	15
P5	F	30-39	B	HS	15
P6	F	50-59	B	SC	35
P7	F	18-29	W	BD	10
P8	M	40-49	HL	BD	20
P9	F	50-59	O	PD	2
P10	M	30-39	B	SC	3
P11	M	60-69	B	SC	20
P12	F	30-39	B	MD	5
P13	F	18-29	W	HS	8
P14	F	18-29	B	BD	6
P15	F	18-29	B	BD	3
P16	M	18-29	B	SC	4
P17	F	60-69	W	BD	15
P18	M	50-59	B	HS	6
P19	M	18-29	HL	SC	20

Gender: F - Female, M - Male
Ethnicity: AHP - Asian/Native Hawaiian/Pacific Islander, B - Black/African American, HL - Hispanic/Latino, W - White/Caucasian, O - Other
Education: HS - High school graduate/diploma/equivalent, SC - Some college credit (no degree), AD - Associate's Degree BD - Bachelor's degree, MD - Master's Degree, PD - Professional Degree

Table 1: Participant demographic information including gender, age, ethnicity, educational attainment, and estimated average hours of TV watched per week.

The interview protocol had three phases. Phase one assessed interviewees' familiarity with computer security topics, exposure to security breaches, and pre-existing notions of the portrayal of security in media. First, they participated in a word association exercise. Participants were given the words "cybersecurity," "hacker," and "encryption" and encouraged to define the words or respond with any other related terms that came to mind. Next, participants were asked questions about hackers' goals, capabilities, and limitations. They were then encouraged to talk about a time they or someone they knew had been a victim of hacking, and finally, they were asked to describe times they had seen a depiction of hacking or cyber security portrayed in fictional media. The goal of this phase was to understand participants' mental models before showing them media clips that might influence their answers.

In phase two, participants were shown six scenes from television and movies depicting computer security topics. After each clip, participants were asked if they had any prior exposure to the clip or its source. Next, to assess comprehension, they were asked to summarize the scene. Finally, interviewees were asked to describe which parts of the scene were realistic and unrealistic and why they felt this way. Participants who gave overly general responses were prompted to assess the realism of specific aspects of each scene. The order of the

clips was randomized for each participant to mitigate ordering bias. We describe the six clips we used in Section 3.3.

The final phase dealt with the relative realism of security portrayals in fictional television and movies as a whole. Participants were asked how accurately TV and movies in general portray cybersecurity, hackers, and cryptography. They were then asked if there were any shows or movies that they felt portrayed those topics particularly realistically or unrealistically. Finally, interviewees were encouraged to share any additional thoughts on the subjects discussed in the interview. The full interview protocol is given in Appendix B.

Prior to the 19 main interviews, we conducted a formal pilot with five participants to test our initial interview script and selected media clips. Based on the results, we adjusted our choice of clips since some proved to be difficult to understand out of context. Because the pilot interviews were shorter than initially anticipated, we added a sixth clip (having piloted with five) to increase variety. We also improved some unclear question wording and increased the scope of two questions.

3.3 Clips

We selected six video clips from TV shows and movies, sourced from the research team's background knowledge, discussions with peers and colleagues, and online collections of computer science in media [26]. We carefully selected these clips to cover a broad spectrum of hacking scenarios, tropes, realism, and alignment with "folk models" of hacking identified in prior work [27]; these selection criteria are outlined in Table 2. We summarize the six clips below.

Superman 3. (1983): A man (Richard Pryor) receives his first paycheck at work and is disappointed to learn how much is taken out in taxes. A co-worker points out he's probably making a half cent more, and that in large corporations there are often fractions left over. When pressed, he admits he doesn't know where that money goes, but the computers probably do. Pryor's character then "hacks" into the system to re-route all the half cents into his account. To do this, he types English sentences, like "Override all security," into a black and green terminal. We chose this clip for its portrayal of a financial motivation and for the unrealistic nature of the hacking.

NCIS S2E4, "The Bone Yard." (2004): Members of the NCIS team realize their computer is being hacked when its screen rapidly flashes various windows, images, and code snippets. Two members type on the same keyboard simultaneously to fend off the attacker, but do not succeed as the hacker breaks through "DoD Level 9 Encryption." The computer screen goes dark, and it is revealed that a third team member unplugged the computer to end the attack. This clip was an inspiration for this research project. We chose this clip for its depiction of rapid, real-time hacking and counter-hacking as well as the simple solution to the problem.

Attribute	Superman 3	NCIS	Blackhat	Sneakers	Skyfall	Gumball
Technical Qualities						
Realistic Jargon	○	○	○	●	○	●
Unrealistic Jargon	○	●	○	○	○	○
Realistic Hacker Capabilities	○	○	●	○	○	●
Unrealistic Hacker Capabilities	○	○	○	●	○	○
Unplugging as a Defense	○	●	○	○	◑	○
Simultaneous Hacking/Defending	○	●	○	○	●	○
"Flashy"Hacking Visuals	○	●	○	●	●	○
Hacking is Obvious to Target	○	●	○	○	●	○
Type of Hacking						
Phishing	○	○	●	○	○	○
Breaking Cryptography	○	○	○	●	○	○
Network Intrusion	○	●	○	●	●	●
Privilege Escalation	●	○	○	●	○	○
Nontechnical Qualities						
Played for Drama	○	○	●	●	●	○
Played for Humor	●	●	○	○	○	●
Pre-Internet Setting	●	○	○	●	○	○
Post-Internet Setting	○	●	●	○	●	●
Professional Setting	●	●	●	○	●	○
Cartoon Animation	○	○	○	○	○	●
Who is the Target?						
Individual	○	◑	●	○	○	○
Organization	●	◑	○	●	●	●
Who is Hacking?						
Protagonist	●	●	●	●	●	●
Antagonist	○	●	○	○	●	○
Folk Models Depicted [27]						
Digital Graffiti Artist	○	○	○	●	●	●
Burglar	●	●	●	○	○	○
Target "Big Fish"	●	○	○	●	●	○
Contractor	○	○	●	●	○	○
Hacker's Goal						
Disrupt	○	●	○	○	●	○
Gain Access	○	○	○	●	○	●
Steal	●	○	●	○	○	○

○- not present, ◑- partially present/ambiguous, ●- present

Table 2: Evaluation of each clip based selection criteria.

Blackhat. (2015): One NSA employee sitting alone at a desk receives an email suggesting he change his password due to his contact with a Joint Task Force. As he downloads a PDF titled "Password Security Guidelines," the scene cuts to two people sitting elsewhere. A man explains to the woman next to him that the PDF the employee has downloaded is actually a keylogger. The scene then cuts between the keyboard on which the employee is typing a new password and the hacker pair's screen, which shows the new password being updated in real time. Both the original and new passwords the NSA employee types are sequences of random letters, special characters, and numbers. The hacker pair successfully log in using the employee's stolen credentials. This scene was chosen for the brevity of the scene and the realism of the hack.

Sneakers. (1992): One group of people watches as a man asks another group to list things that are impossible to access, such as major government agencies. He then demonstrates the ability to decrypt information from these agencies via a "chip" that is the "key to unlock everything." As the man accesses the Federal Reserve, "encrypted" gibberish appears on the screen, which the man "decrypts" into useful and meaningful content. He replicates the feat, within a minute, with the national power grid and air traffic control, to the group's astonishment. He explains he has solved the "impossible" mathematical problems that are the root of encryption and hardwired that solution onto a chip. This technical description is in a sense quite accurate, essentially describing a scenario in which an attacker succeeds in, e.g., factoring large numbers in order to break RSA. (Of course, current real-world attackers generally rely instead on much more commonly available software flaws and human errors.) We chose this clip for its portrayal of encryption and the depiction of an attack that was plausibly realistic, but whose realism came from technical knowledge at a depth such that most casual viewers were unlikely to possess it.

Skyfall. (2012): A field agent and a technical expert attempt to break into a laptop. The laptop is described as a "polymorphic engine" that changes as though "it's fighting back." The field agent notices a keyword among values being flashed on the screen that, when entered, reveals a map of the London Underground. Doors suddenly fly open, and the technician realizes their computer system has been breached. The breach was a result of plugging a malicious laptop directly into their computing infrastructure, which was the reason this scene was selected. It also features very high-quality graphics and a significant amount of plausible-sounding but incorrect technical language.

The Amazing World of Gumball S3E32, "The Safety." (2015): In this cartoon, two characters walk sneakily through an industrial building. When they reach a locked door, the blue creature laments while the pink one says "H-A-C-K hack, press enter" while poking the keyboard. When the door opens, the blue one is shocked, until the pink one launches into an extremely detailed, fast, and fairly realistic diatribe explaining how she did it, which includes references to the VNX array head, decrypting SAS disks, rerouting traffic, and accessing the ESXI server cluster. The scene was selected for its realistic but complex jargon, juxtaposed with the childlike nature of the show and graphics.

3.4 Data analysis

Once interviews were complete, we transcribed the audio recordings as a team. After transcription, two team members independently analyzed the data using iterative open coding, developing the codebook incrementally and resolving disagreements after every three transcripts [24]. The two researchers achieved an overall reliability of Krippendorff's $\alpha = 0.75$ [14], calculated using ReCal2 [6]. This level of agreement is above the commonly recommended thresholds of 0.667 [10] or 0.70 [15]. Finally, the research team worked together in an iterative axial coding process to derive larger themes and theories from the fine-grained open codes.

3.5 Ethics

Both the initial pilot and the larger main study were approved by University of Maryland's Institutional Review Board. We obtained informed consent before the pre-screening survey and again before the interview. One clip we showed contained strong language. We warned each participant about this and reminded them that they could stop the clip or the entire interview if they felt uncomfortable; none did.

3.6 Limitations

As with most qualitative studies, the generalizability of our results is limited by our small sample size. We attempted to mitigate this by recruiting a relatively diverse cohort of participants within the Washington, D.C. area.

We limited our study to television and movies, leaving out other fictional media such as books or podcasts. Similarly, we chose only six clips in order to keep the study short and reduce cognitive burden on interviewees. We sought to choose clips illustrating a variety of ways that cybersecurity is represented in fictional media, but it was not possible to include everything. Nonetheless, we feel that our results provide useful insight across a range of cybersecurity portrayals.

In common with all semi-structured interviews, there is the potential for demand effects, social desirability bias, and satisficing to affect participants' responses. Demand effects, in which participants attempt to provide the answers they believe the interviewer wants to hear, are a particular risk when asking participants to evaluate realism in an area where they may have limited personal knowledge or intuition [18]. To mitigate this, we avoided mentioning the goal of the study directly, and we emphasized to participants that there were no right or wrong answers to our questions.

4 Misconceptions derived from TV and film

Participants explicitly connected their beliefs about computer security to fictional portrayals. Five participants did so even without prompting; for example, when asked about the word "hacker," P2 mentioned "Matthew Broderick in WarGames." When asked where they thought their ideas about computer security originated, three participants named TV and movies; others mentioned media more broadly.

P8, who believes media portrayals are generally accurate, said, "The fact at least two movies have [attempts to steal

Triggering Event	What Users Learn	Influence On User Mindset
Unplugging the computer stops the hacker	It's easy to recover from being hacked	Failure to follow necessary steps to mitigate damage after an attack
Hackers leave call signs or don't hide behavior	If I get hacked, I'll be able to tell	No response to subtle compromises and false assumption of security after missing non-obvious indicators
Hackers can break all encryption simultaneously	Protections are weak and security is futile	Lack of implementation of common-sense security practices out of belief they won't make any difference
Hackers target particular high-value entities	I'm not important so I won't get hacked	Failure to take precautions out of belief they won't be targets; precautions taken against targeted rather than broad attacks
Phishing successfully compromises user accounts*	Suspicious email can lead to being hacked	Greater care taken when evaluating email links and attachments and decreased assumption of security

Table 3: Examples of Mental Models Drawn from Mass Media (*denotes correct mental model)

missing half-cents from paychecks] probably means someone tried to do it, or did do it." But even those who claimed to believe fictional media is inaccurate, such as P14, drew similar conclusions: when asked what encryption is used for, she struggled for an explanation before mentioning "I think about the movie with . . . " and trailing off. Similarly, P7 said media portrays computer security "probably inaccurately" but also said "sometimes when I'm watching movies or TV and someone is doing like equations. . . I'm like 'Is that real or is that made up?' And that makes me think of a lot of the stuff that I don't really question and I'm just like 'Okay that's what it looks like.' Or I just accept those representations." It appears fictional portrayals may be influencing mental models even for people who claim to know better.

These results align well with findings from Redmiles et al. and Ruoti et al. that fictional media can be a major source of security information for users [21, 23]. Further, our results suggest a kind of feedback loop: people learn mental models of security — sometimes from fictional media — and then these models are reaffirmed when they appear in other media later. We highlight below a few ways in which TV and film portrayals seem to have contributed to our participants' security beliefs. These findings are summarized in Table 3.

4.1 Hackers have specific, important targets

When asked about hackers' normal targets, many participants seemed to think hackers only choose important targets, and that targets are always a specific person or entity (rather than, for example, sending a phishing email broadly to many recipients). For example, P18 believes hackers target "very important information, data. The military, law enforcement personnel. . . banks or important corporations, military, intelligence, so they can use it to their advantage." This model was affirmed while watching the Sneakers clip: P18 assumed an attack on "stuff that's been encrypted" would target "intelligence of maybe the Navy or the United States or whatever, banking, stuff like that, it's really huge."

Similarly, P6 commented that she was not important enough to be a target of a hacker: "I'm not a rich person. . . so you know I guess they probably just left me alone." She later connected this belief to the scene in Sneakers, noting that something "that I found realistic was the things that they were breaking the codes to were very high security."

Participants also expected hackers to focus on individual targets rather than random victims. P5, for example, observed that a hacker's target might be "someone that you have a personal grudge against." This mental model was later affirmed when this participant noted that in Blackhat, the targeting of a specific victim personally was "pretty realistic." Participants who believe attacks are targeted specifically rather than at random may choose non-optimal protective behaviors; for example, as Ur et al. demonstrated, users who expect targeted attacks choose passwords differently than than those seek to protect from more general guessing [25].

In general, if people think that only important entities will be attacked and hackers only attack individuals rather than make widespread attacks, they may never worry about protection because they do not view themselves as a potential target. This aligns with Wash's folk model that "hackers are criminals who target big fish" [27].

4.2 Attacks and unsafe situations are obvious

People's ability to correctly recognize evidence of security breaches (or conversely, an unfounded fear that they may be under attack) depends on their idea of what security incidents look like. We found that mental models about what hacking looks like were strongly influenced by portrayals in fictional media, in which hacking is commonly portrayed as a dramatic, active intrusion that triggers anomalous behavior, sometimes including a deliberate "signature" from an attacker. Among our clips, this was most noticeable in NCIS, in which an attack led to obvious pop-up windows and messages, and Skyfall, in which defenders were alerted to an intrusion in real time by the attacker's red-skull call sign.

Participants consistently indicated these attack models were realistic. With Skyfall, some participants said that an attacker might not want to tip off the defenders by displaying a call sign; however, P9 specifically mentioned the skull as a good

indicator that the system was under attack. When describing what she found realistic about the NCIS clip, P14 noted, "Especially in the past getting viruses . . . I can remember that happening with a whole bunch of pop-ups in the screen." The clip affirmed this participant's idea that security problems have obvious indicators. P7 summarized these thoughts well: "I feel like imagery of like being hacked where like all the screens flash and stuff is like what is shown in pop culture a lot of times. . . But in my mind that is like, [an indicator that] hacking is happening." If people are waiting for this kind of obvious indicator to identify a security problem, they are likely never to find it.

4.3 Encryption is fragile and all security measures are futile

Fictional media commonly portrays encryption as quickly and easily broken by sufficiently talented attackers. This is exemplified by our clip from Sneakers, in which a "master chip" can decrypt data from any secure facility quickly and easily. Most participants found this highly plausible. For example, P19 said, "I feel like we are at the point where people could logistically have that much control over air traffic control, federal reserve, etc. and cause a lot of harm, so that doesn't seem like a far stretch." The clip seems to confirm this participant's existing mental model that security measures may be futile: asked about hackers' limitations, he said "There's always new things to be discovered and with the passage of time technology is only going to get better, so I don't see any limitations whatsoever." P23 echoed this idea, saying that hackers "have no limitations." He connected this idea to the Superman 3 clip: "in our day and age, it's like, in a blink of an eye it's like done, you're not protected."

Further, P6 said that after watching the Sneakers clip, "now I understand what encrypted means.. . . And do I think [the master key's] real? Yes. I do think that is realistic. I think that there is a code among all codes to, I mean maybe not work for everything, but work for a majority of things."

These explanations reflect a fundamental lack of faith in encryption with the potential to engender distrust in products or services that advertise security and privacy. While it may indeed be nearly impossible to stop a sufficiently talented, motivated, and resourced attacker, this mentality could prevent people from taking precautions that could stop many other classes of attackers. These media portrayals are one potential explanation for the finding by Abu-Salma et al. that some users believe secure messaging is not worthwhile because encryption can always be broken by technically savvy attackers who understand it [2].

4.4 Unplugging and other solutions

Fictional media often presents simple, facile solutions to complex security problems. Several participants found the NCIS solution — unplugging the computer to end an attack — highly plausible. P16, for example, noted, "The other colleagues came in to help and what solved the situation was pulling the plug. . . . Pull the plug, and it stopped pretty much everything." This affirmed his mental model for solving his own security issues: "There was a time when [hacking] happened, I just pressed the off button really fast to stop it.. . . So the next time I just turned the game off completely. When I turned the whole system off completely, it didn't go down any further. I just turned the whole thing off to stop it."

This sentiment is echoed by P15 who said "But what actually seemed real was when like the dude unplugged it all — cause you know back when I had viruses the first thing I'd do is unplug it and see if it worked again." This kind of straightforward adoption of simple precautions and solutions offered in fictional media, many of which may not be correct, can harm people's efforts to protect themselves.

Also, not one participant mentioned the use of a single standard keyboard by two people simultaneously in the NCIS clip as an unrealistic feature of the scene. While this is a minor detail, not ultimately related to security beliefs and behaviors, it does underscore that viewers take scenes like this one at face value in ways that may be harmful.

4.5 Suspicious emails can be dangerous

Not everything portrayed in fictional media is detrimental to peoples' mental models. Many participants noted that receiving a suspicious email is a proxy for getting hacked. P4 mentioned, "You always hear about viruses that can attach something so that's why you never open attachments unless you know who sent it to you" as a reason why the Blackhat clip seemed realistic. Describing the same clip, P11 said, "I don't know very much about phishing except from just what I've heard or read. But I think that's pretty much the way it works.. . . snatch or steal the information. I'm guessing that that looks legitimate; that looks real." In these cases, the media portrayals aligned with participants' accurate belief that suspicious emails can be a threat vector.

5 Evaluating realism in fictional portrayals of computer security

Our third research question focuses on why users learn these particular concepts about security from fictional media. Users make judgments about realism and importance that determine whether and how these fictional portrayals are incorporated into their overall mental models. Understanding these judgments is compelling because, if we can identify how and why a misconception is formed, we may be better able to prevent it, or even to work within incorrect or incomplete mental models to nonetheless promote better security outcomes. To answer this question, we examined how participants assessed the accuracy of the clips we showed.

Participants exhibited a variety of heuristics for assessing the realism of computer-security incidents and behaviors in fictional media. In particular, most participants started from a default assumption about how likely such media are to be realistic. This default assumption was then mediated by other cues specific to a particular clip or scene. We categorize these additional cues into four major categories:

- *Technical knowledge*, which helps participants who understand some aspects of the depicted events evaluate how realistic they are;
- *Non-technical experience*, in which participants relate the depicted events to their own lives;
- *Plausibility of plot and characters*, in which participants consider whether the motivations and behaviors of characters, together with the broader events of the plot, are reasonable;
- and *Cinematic aspects*, in which visual and audio cues such as set decoration, musical score, and internal consistency affect the participants' evaluations of the scene.

We detail examples from each of these categories, plus default assumptions, in the subsections below.

5.1 Default assumptions about realism

Despite the variability across participants in opinions about the accuracy of the media, we noted that each individual participant's beliefs seemed to default to a particular attitude toward the media's accuracy: accurate, inaccurate, or mixed. When participants lacked sufficient cues to help them decide whether a clip was accurate, or had difficulty understanding the clip, they typically relied on this default opinion. For example, P16 — who said in the final phase of the interview that he found media portrayals generally accurate — also said of the Blackhat clip, "I really didn't get much from it, but I think it falls on the type of realistic thing."

These general views of media accuracy, and the resulting default assumptions about accuracy in individual clips, corresponded to specific opinions about the motivations of the media in presenting computer security information. The eight participants who said the fictional media was presenting a generally accurate picture of computer security tended to believe that one goal of these portrayals is to educate viewers. As P18 noted, "They're [entertainment media] doing a good job I believe, yeah. You learn from it."

Five participants said media generally present computer security unrealistically. Some attributed this to the creators' lack of expertise in the field. This was exemplified by P14: "I'm going to say they're portrayed inaccurately, because I don't think any of the people directing or creating these movies have really experienced being hacked, and I think that's why they're so dramatic and over the top and fast."

Others instead believed entertainment media were intentionally hiding information about computer security from viewers. These participants were unlikely to trust the portrayals we showed and likely to believe that all forms of security are futile (Section 4.3). For example, P6 said "I think it's [fictional media] probably inaccurate because we all know the government don't allow you to show everything that goes on. . . and they're not going to put realistic things for everyone to view." As mentioned above, P6 also found the portrayal of a master encryption key in Sneakers realistic.

Finally, six participants assumed that fictional portrayals were a mix of realistic and not, resulting from the creator's choice to trade off presenting security information accurately and providing a compelling plot. Accurate portrayals were seen as too boring to sell well. P7 describes this feeling: "I think it would be hard to portray the actual process so it would keep the flashy appeal to mass audiences that those movies target, because I imagine it's something that slowly develops over a long period of time and there's a lot of trial and error. And it's not just use a button and flashy things happen. It's like I imagine it would be more subtle."

Redmiles et al. note that uptake of security advice is commonly mediated by trust in the advice giver rather than evaluation of the advice content [21]. This reinforces our finding that people's default trust in fictional media will affect the way they process and absorb fictional depictions.

Participants' reliance on these default assumptions of accuracy, however, was mediated by a variety of cues and proxies that signal realism in a particular clip, as described in the following sections.

5.2 Technical knowledge

Participants frequently tried to use their pre-existing technical knowledge as a basis for discriminating between realistic and unrealistic depictions of computer security. However, participants often did not have enough technical knowledge to fully evaluate a clip, falling back instead on various proxies:

Jargon typically implies technical realism. Many characters in the selected clips demonstrate technical expertise by reeling off litanies of technical terms, and participants often responded to these unfamiliar terms by assuming the clips must be realistic. In particular, 12 participants assumed that if they don't understand what is being said, the person speaking must be knowledgeable, and thus their words and actions must be plausible. This was the case for P1, who referenced the jargon in the Gumball scene: "What she said was realistic . . . it's like a foreign language to my ears, like when it's a doctor and you have no knowledge of what they talk about." P10 agreed, saying "Some of the words she was saying, like proxy and all that, I was like oh my gosh she knew her stuff. Yeah that was realistic." But not every participant was so quick to trust explanations filled with obscure technical terms. P11, for example, believed jargon might indicate an unrealistic attempt to sound technical without real accuracy, noting that

"It may have been someone pulling a lot of technical terms and throwing them into a paragraph."

If it's too fast or easy, it's not realistic. Another common heuristic used by interviewees was to assess whether the level of difficulty portrayed in the scene seemed appropriate for the task, with 12 participants noting that surprisingly fast or easy tasks seemed unrealistic. P14, for example, commented on how easily the defenders in Skyfall noticed they were being hacked: "Even like once the hacker hacks you, I don't think it would be as easily identifiable." P12 drew a similar conclusion about the defenders in NCIS: "How sudden and fast it seems like, and the fact that she knew it was happening." Participants' tendencies to assume that computer security defense must be difficult and advanced, and be surprised when it seems too simple, may be related to findings by previous researchers that users find computer security advice advanced and intimidating, and feel helpless to take appropriate action to protect themselves [13, 22].

5.3 Non-technical background

Participants also used their non-technical background and experience, including the relatability of characters in a scene, to inform their realism judgments.

If it matches a negative personal experience, it's realistic. Eleven participants assessed realism by connecting on-screen events to a previous negative experience in their own life. This often led them to believe a scenario was more likely to be accurate. For example, in response to Blackhat, P13 said, "He used a keylogger to find out his password from a email and a download, which I believe is totally possible. I had a weird thing where my stepdad put a keylogger on my computer to see if I had a Facebook. So I know that this is possible." These findings fit with previous research identifying negative personal experiences as one important source of security mental models [21, 22].

Relatable events are realistic. When participants did not have relevant personal experience to draw from, they often used the relatability of a clip — whether or not they could imagine having the same events happen to them or behaving as the on-screen characters did — as a proxy for realism. In response to the phishing attack in Blackhat, P8 said "I probably would've fallen victim to it too. Anybody else would, it seems like a credible thing referencing an email the way it did." This was echoed by P9, who said of the NCIS clip: "It was almost like a rash, you couldn't do anything to stop the itching or the burning, it was moving so fast. That's the part I could identify with." This aligns with Redmiles et al.'s finding that negative experiences depicted in media can serve as a learning tool for security behavior when the characters are relatable [22], as well as Moyer-Gusé's theory that character identification can increase retention and behavior change with respect to educational entertainment more broadly [17].

5.4 Compliance with existing folk models

Many participants judged the overall realism of a clip in part by the extent to which it seemed to plausibly reflect their existing, non-technical beliefs about how the world works and how hackers behave. As discussed above, this can create a feedback effect whereby sufficiently common tropes influence users' beliefs and their judgments about subsequent media.

Motivation for hacking matters. Eleven participants noted that the attacker's motivation informed their overall evaluation. Watching Superman 3, multiple participants suggested that the main character's motivation to steal residual money from the pay system because he was disgruntled about the size of his paycheck was realistic. P19, for example, noted that "a lot of people feel like they are unpaid for the work that they do. I can relate: with various jobs, I felt like I was underpaid, and a lot of people feel the same way at their jobs."

Participants similarly believed that real-world hackers are motivated by the desire to flaunt their talent; thus, attackers trying to prove their talent or intelligence was taken as a signal of realism in a clip. P8, for example, found the Gumball clip believable because "She was showing off, and she enjoyed showing off. . . . If you're good at it there's inclination to want to be very good at it, to show 'em who you are." This mirrors Wash's folk model of hackers as "graffiti artists," motivated to attack to show off [27].

Relatedly, participants were skeptical of on-screen hackers' motivations when they did not believe the tradeoff between the cost and benefit for the hacker added up. P14 expressed mixed feelings about the realism of Superman 3: "Yes, as an individual you want to try and get your money, but no, because when it comes to the government the risks are so high that I don't think the cost-benefit is worth it."

High-value targets imply realism. As discussed in Section 4 above, our participants tend to believe that hackers exclusively target specific, high-value victims. This fed back into a belief that government targets and targets with high monetary value made a scene more realistic (n=5). In reference to the primarily governmental targets in Sneakers, P6 observed, "Well, the only other thing that I found realistic was the things that they were breaking. The codes were very high security." This, too, mirrors a mental model identified by Wash, that "hackers are criminals who target big fish" [27].

Violating hacker stereotypes is not realistic. Instead of focusing on the target, five participants zeroed in on the hacker, using their perceptions and stereotypes about who hackers are to evaluate the validity of the plot. When the portrayed hackers didn't match their expectations, they found the entire scene less plausible. For example, when asked about Gumball, P5

stated, "I don't think someone that age could do that." P8 said that Blackhat was unrealistic in part because of "how good the actor [Chris Hemsworth] looks, I guess." Here Wash's folk models play out in a more general way, with participants questioning characters who fail to fit into any of the hacker mental models they have available [27].

Existence of consequences helps determine realism. Participants also used the consequences for hackers to inform their overall evaluation. For example, two participants noted that the clips often included acts that were against the law, and that they therefore expected the attackers to be punished. P2 stated, "I think that when someone is hacking into government stuff or agencies, I feel like the authority will be alerted or someone or something will be alerted, and they will take action. I feel like in the clips they don't show, like, police or government taking any action, or someone alerting them that someone is hacking into their system," and that made the entire clip seem unrealistic.

In contrast, when authorities did intervene, some participants felt that this increased the realism. In reference to the NCIS clip, where the defenders actually are the authorities, P1 said that the clip was realistic because "the outcome of the show — they caught the guy, you know, how the whole thing played out." While this was not a common observation, some participants did use this as a proxy for realism.

Hacking is plausible. More broadly, participants considered whether the events of the plot were plausible, extrapolating from their beliefs about how the real world works. Fifteen participants, for example, mentioned that at least one clip was realistic in part because hacking does happen often in real life. In reference to Skyfall, P10 said that "companies do get hacked. That's how it's real." Occasionally, the likelihood of hacking in general was the only tangible thing participants could connect with reality, as demonstrated when P12 answered that the only realistic thing about the NCIS clip was "that it happens, people do get hacked."

Repeated tropes are more realistic. Another indicator of realism for participants was the popularity of plot points across the entertainment industry. Discussing Superman 3, two participants said they had previously seen other depictions of a disgruntled employee collecting fractions of cents shaved off of other employees' paychecks. Similarly, P10 was initially unsure about the realism of hacking of power grids in Sneakers, because he "never heard about it in real life happening, like someone taking over the city lights or whatever," but eventually concluded that the scene was realistic because he had "seen it in plenty of movies." This fits well with our overall finding that fictional tropes help to develop mental models, which are then reinforced by repeated exposure. It also aligns well with findings by Redmiles et al. that participants are more likely to trust information they are given based on "how widespread the advice was on various media outlets" [22].

5.5 Cinematic aspects

Finally, participants often cited aspects of the clips that were intrinsic to the medium of fictional television and film as a proxy for determining realism.

Visual and audio cues affect realism. One influential cue was the visual quality of a scene, which 17 participants pointed to when determining what was realistic and what was fantasy. Participants were split on whether overt demonstrations of so-called "Hollywood Hacking" — a common set of visual indicators that signify to an audience that hacking is occurring within the context of the movie, such as the red-skull calling card in the Skyfall clip — were realistic or not. Auditory effects also played a role. P8 noted of the Sneakers clip, "It reminded me actually of [Skyfall] because of the music escalating and being very overt and very dramatic and trying to move the plot along." For this participant, the dramatization made the scene feel less realistic.

Physical and temporal setting have to fit. Participants often used the set and setting of a scene to determine how realistic the scene was. Several participants called into question physical aspects of scenes that were incongruous with the rest of the environment, resulting in an overall judgment that a clip was unrealistic. In Skyfall, for example, a hacking attempt is portrayed as successful by showing several glass containers on the floor of an office building opening on their own. According to P16, "What looked less realistic was the tops coming out of the floors, I don't know what that was." P12 said, "I think it was kinda funny how they had showed the underside of the keyboard literally logging the keys," in response to the Blackhat clip, where the camera focuses on a seemingly unrelated portion of the scene for dramatic effect.

Temporal settings raised similar concerns. Two of our clips are decades old (Superman 3, Sneakers); three participants had a difficult time balancing whether they thought a task was realistic in the present, compared to in the time period the clip was portraying. According to P13, "I have no idea if that's realistic or not, because that is super old, so maybe it's realistic, he maybe could have done it, but . . . I don't know what the super low-level security would be at that time."

Character behavior must be realistic. The general behavior of characters, both targets and hackers, also impacted perceptions of realism, both positively and negatively. For example, P9 cited "the emotion, his reaction that he'd been duped," in Skyfall when judging it as a realistic scene, because the character responded as she would have expected. Similarly, in the NCIS clip, P3 pointed out that "the team supporting each other" seemed real. Interestingly, other participants used the same logic to judge the same scene as less realistic. For example, P11 thought the NCIS clip was unrealistic because "everybody just seemed too casual about it. A guy is eating a sandwich and saying what's going on, is this a video game?"

Portrayals on screen need to match explanations. "Show, don't tell" is a common piece of advice for writing, but this advice is not always followed. In the Gumball clip, the main character claims that she went through a lengthy process in order to hack into and open a door, but is only shown typing in four letters. While this discrepancy seems intentional, for comedic effect, three participants latched onto it to explain why they felt her actions were unrealistic. P15 commented: "I think what was kind of realistic was how she described in depth how she hacked it, you know, it just sounds complex and like there are probably some things they have to do to hack the system. But the unrealistic, you know, is that H-A-C-K hack." P6 explicitly noted that "She named so many things that she did and she only pushed 3 or 4 buttons. I mean, the only thing I saw her do was open the door." In the real world, a hacker or security professional could certainly kick off a large series of complex steps by issuing a single command, e.g. to run a script. However, without showing that laborious process, viewers are left to wonder how the simple action they saw relates to the complicated process that was discussed.

Incongruity reduces realism. Apparent randomness, or the generally incongruous nature of various elements in the clips we tested, also affected perceived realism. For example, seven participants expressed doubt about the realism of the Gumball clip just because it was a cartoon. P1 noted that the clip is not believable because "it's a cartoon." P18 agreed that "I don't think animation can be real," and P16 commented that "it's a cartoon, so you know, this is for kids." The technical jargon in this clip was so incongruous with the childlike nature of the visual elements that people perceived it as unrealistic, even though it was in some respects the most technically realistic scene showed during the interview. Even mundane plot elements that seemed out of place affected participants' interpretation of the clips. For example, P12 thought the conversation that led to the hacking in Superman 3 seemed forced, saying "I don't know why that coworker would randomly tell him about that."

6 Discussion

Our interviews demonstrate that users draw conclusions about what is (not) realistic about computer security in fictional media using a variety of heuristics, most of which are either entirely non-technical or only partially grounded in technical understanding. Further, many users believe that these media portrayals are either mostly, or at least partially, accurate: eight participants believed portrayals were generally accurate, six believed they were mixed, and only five concluded they were primarily inaccurate. This has important implications for users' mental models, as we know from previous studies that fictional media is one important factor in establishing these models for security behaviors [21, 23]. If the mechanisms users apply when deciding which information to adopt from fictional media are mostly divorced from even approximate technical correctness, and this media frequently presents unrealistic depictions, then users will be left with inaccurate and potentially harmful mental models.

Indeed, we see this play out in our study. Several clips were chosen because of their inaccuracies. Despite this, participants often failed to identify obviously unrealistic behavior. For example, it was common for participants to watch the Sneakers clip and conclude that widespread breaking of encryption is plausible and perhaps even occurs commonly in reality. While there are many existing vulnerabilities that place existing systems at risk, the belief that nothing can be safe, inculcated in part by television and film, can have negative consequences for users. This echoes work by Wash and Rader that found that users who believe that there is no way to make something secure often conclude that efforts to defend themselves and use good security behaviors are pointless [28]. Similar results, in the context of encrypted messaging, were observed by Abu-Salma et al. [2]. Even in cases of more benign errors, such as when two defenders in the NCIS clip worked together on the same keyboard to frantically defend against a hacker in real time, participants' consistent failure to notice the inaccuracy may be cause for alarm. Despite occasional success at pointing out other unrealistic aspects of the scene, the overall willingness to credit a scene with such an obvious inaccuracy, with one participant even noting the defenders working together as realistic, raises concern about the effect of inaccurate media on viewers.

The need for collaboration. Our findings point to the need for collaboration between the entertainment industry and the computer-security community. The entertainment industry has strong institutional knowledge in maintaining viewer engagement, but often seems to lack either the technical knowledge or the desire to depict security reasonably realistically, in a way that improves people's ability to make good security-relevant decisions. The academic security community, in contrast, has desirable lessons to teach users, but lacks a wide-scale platform to do so. One possibility for future work is to explore how to improve depictions of computer security in fictional media and evaluate how these improvements might affect users' understanding and decision making. We are particularly interested in the parallel to the field of medicine: In this field, the American Medical Association has issued guidance cracking down on pseudoscience and inaccuracies in the media, and medical advisors have been hired for films and television [4, 19]. Studies assessing the impact of these interventions on viewers have demonstrated positive impact almost three times as often as negative [12]. We are intrigued by the possibility that analogous interventions related to computer security could have a similar positive impact on viewers' knowledge and behavior.

To this end, we propose a Cybersecurity in Entertainment Task Force to mediate between the entertainment industry and the security community. Additionally, we encourage television and film productions that intend to portray computer security or hacking on-screen to hire technology advisors. These suggestions parallel the science and medical advisors many productions already hire, as well as the work done by the Hollywood, Health, and Society organization, which has worked with 91 TV shows to provide consultants and accurate medical information [1]. Further, there is good evidence that accurate portrayals of hacking can indeed be entertaining. For example, the television show Mr. Robot, which has been lauded for its accurate depictions of computer security, has also enjoyed critical acclaim [9, 31].

Entertaining responsibly. Although it is unclear whether users are learning from fictional media or fictional media is reinforcing their already existent mental models (or both), it is clear that media portrayals include known technical fallacies. Some of these inaccuracies matter more than others in terms of what viewers ultimately take away from scenes. If what viewers learn from an inaccurate scene is that two hackers can use one keyboard in an emergency, or that it only takes a moment to break into a secure headquarters, their own security behaviors are unlikely to be negatively affected. However, if they instead learn that all encryption is broken, that hacking is always obvious and easy to identify, or that the best way to respond to a breach is to restart your computer, they may make bad security decisions. By choosing which forms of inaccuracy to portray, creators of entertainment can still create exaggerated scenes filled with fast-paced action and sensationalism, while avoiding imparting particularly problematic misconceptions to their viewers. Further, our results identify heuristics that convey not only realism, but lack of realism. When presenting potentially harmfully inaccurate information, the media could provide cues not to take it seriously, mitigating the harm done. Further, even when it is not possible to convey all details accurately, ensuring that depictions of computer security are at least reasonable at a high level would still be a strong improvement.

Guidance for researchers and educators. Security researchers and educators, of course, may not be in a position to change the habits of entertainment producers. Our findings, however, also provide insight to help researchers and educators cope with misinformation disseminated in fictional media. Educators, researchers, and designers who better understand common tropes, and the misconceptions they lead to, can address these tropes directly in security tools, informational messages, and other guidance by pointing out explicitly what users may misunderstand. Alternatively, interventions could try to work within existing tropes by adapting advice, tools, or interfaces to fit existing mental models. Further, researchers and practitioners can take advantage of these tropes to lend realism and seriousness to their own informational messages and examples. Designing security interventions that will be perceived as realistic and relatable could help users understand and adopt better threat models and behaviors.

The media is not a monolith. In this paper, we explored fictional U.S. television and film about computer security. Future work could examine how cybersecurity is portrayed in other regions, in non-fiction and news, or in other types of fictional media, like books or podcasts. It might be particularly interesting to consider whether the specific media properties that users consume directly affect the mental models they end up with; however, untangling this possibility from other factors that might inform a user's mental model may prove challenging. A related question concerns genre in fictional media: do certain genres tend toward portrayals that do a better or worse job of developing accurate mental models in users, or do users who primarily watch particular genres develop more realistic mental models?

7 Conclusion

In this paper, we interviewed 19 participants about their mental models of computer security, hacking, and encryption, and how those mental models were influenced by portrayals of these concepts in fictional media. To focus on the role of media in forming mental models, we showed interviewees six clips from television series and films depicting computer-security topics. We asked participants what they considered realistic and why, in these individual clips and in fictional-media depictions of computer security as a whole.

We find that people incorporate fictional portrayals into their mental models of computer security, with sometimes unfortunate effects. Participants typically used proxies, many of which were non-technical, to evaluate the accuracy of particular depictions of computer security. Further, these models — in part drawn from popular depictions — can be self-reinforcing, as additional exposure to common tropes serves to confirm participants' pre-existing beliefs.

We therefore conclude that media portrayals of computer security contribute to the development of incomplete and inaccurate mental models. So long as this remains true, common fictional tropes must be taken into account when seeking to improve security education. To address this challenge, we propose a closer partnership between the computer-security field and the entertainment industry, we suggest approaches for the entertainment industry to provide entertainment while avoiding inculcating misconceptions, and we recommend that security researchers and educators take the effects of fictional portrayals into account when trying to teach users about security concepts and behaviors.

References

[1] History: HH&S by the numbers. https://hollywoodhealthandsociety.org/about-us/history-hhs-numbers.

[2] R. Abu-Salma, M. A. Sasse, J. Bonneau, A. Danilova, A. Naiakshina, and M. Smith. Obstacles to the adoption of secure communication tools. In *2017 IEEE Symposium on Security and Privacy*, pages 137–153, May 2017.

[3] Alessandro Acquisti and Jens Grossklags. Privacy and rationality in individual decision making. 3(1):26–33, 2005.

[4] Julia Belluz. The American Medical Association is finally taking a stand on quacks like Dr. Oz. https://www.vox.com/2015/6/13/8773695/AMA-dr-oz#, Jun 2015.

[5] Alain Forget, Sarah Pearman, Jeremy Thomas, Alessandro Acquisti, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, Marian Harbach, and Rahul Telang. Do or do not, there is no try: user engagement may not improve security outcomes. In *2016 Symposium on Usable Privacy and Security*, pages 97–111, 2016.

[6] Deen G Freelon. ReCal: Intercoder reliability calculation as a web service. *International Journal of Internet Science*, 5(1):20–33, 2010.

[7] Damian Gordon. Forty years of movie hacking: considering the potential implications of the popular media representation of computer hackers from 1968 to 2008. *International Journal of Internet Technology and Secured Transactions*, 2(1/2):59–87, 2010.

[8] Greg Guest, Arwen Bunce, and Laura Johnson. How many interviews are enough? an experiment with data saturation and variability. *Field Methods*, 18(1):59–82, 2006.

[9] Aisha Harris. The fourth season of 'Mr. Robot' will be its last. https://www.nytimes.com/2018/08/29/arts/television/mr-robot-last-season.html, Aug 2018.

[10] Andrew F Hayes and Klaus Krippendorff. Answering the call for a standard reliability measure for coding data. *Communication Methods and Measures*, 1(1):77–89, 2007.

[11] Cormac Herley. So long, and no thanks for the externalities: the rational rejection of security advice by users. In *2009 Workshop on New Security Paradigms Workshop*, pages 133–144. ACM, 2009.

[12] Beth L. Hoffman, Ariel Shensa, Charles Wessel, Robert Hoffman, and Brian A. Primack. Exposure to fictional medical television and health: a systematic review. *Health Education Research*, 32(2):107–123, 2017. http://dx.doi.org/10.1093/her/cyx034.

[13] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. "My data just goes everywhere:" user mental models of the internet and implications for privacy and security. In *2015 Symposium on Usable Privacy and Security*, pages 39–52. USENIX Association Berkeley, CA, 2015.

[14] Klaus Krippendorff. Reliability in content analysis : Some common misconceptions and recommendations. 2015.

[15] Matthew Lombard, Jennifer Snyder-Duch, and Cheryl Campanella Bracken. Content analysis in mass communication: Assessment and reporting of intercoder reliability. *Human Communication Research*, 28(4):587–604, 2002.

[16] Johnny Long. Secrets of the hollywood hacker! In *DefCon 14*, 2006.

[17] E. Moyer-Gusé. Toward a theory of entertainment persuasion: Explaining the persuasive effects of entertainment-education messages. *Communication Theory*, 18(3):407–425, 2008. http://dx.doi.org/10.1111/J.1468-2885.2008.00328.X.

[18] Delroy L. Paulhus. Chapter 2 - Measurement and control of response bias. In John P. Robinson, Phillip R. Shaver, and Lawrence S. Wrightsman, editors, *Measures of Personality and Social Psychological Attitudes*, pages 17 – 59. Academic Press, 1991. http://www.sciencedirect.com/science/article/pii/B978012590241050006X.

[19] McKenna Princing. I was a medical advisor for Grey's Anatomy. Here's what i learned. https://rightasrain.uwmedicine.org/well/stories/i-was-medical-advisor-greys-anatomy-heres-what-i-le
2018.

[20] Emilee Rader, Rick Wash, and Brandon Brooks. Stories as informal lessons about security. In *2012 Symposium on Usable Privacy and Security*, page 6. ACM, 2012.

[21] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. How i learned to be secure: a census-representative survey of security advice sources and behavior. In *2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 666–677. ACM, 2016.

[22] Elissa M Redmiles, Amelia R Malone, and Michelle L Mazurek. I think they're trying to tell me something: Advice sources and selection for digital security. In *2016 IEEE Symposium on Security and Privacy*, pages 272–288. IEEE, 2016.

[23] Scott Ruoti, Tyler Monson, Justin Wu, Daniel Zappala, and Kent Seamons. Weighing context and trade-offs: How suburban adults selected their online security posture. In *2017 Symposium on Usable Privacy and Security*, pages 211–228. USENIX Association, 2017.

[24] Anselm Strauss, Juliet Corbin, et al. *Basics of qualitative research*, volume 15. Newbury Park, CA: Sage, 1990.

[25] Blase Ur, Jonathan Bees, Sean M Segreti, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Do users' perceptions of password security match reality? In *2016 CHI Conference on Human Factors in Computing Systems*, pages 3748–3760. ACM, 2016.

[26] Reddit: /r/itsaunixsystem/. https://www.reddit.com/r/itsaunixsystem/, 2018.

[27] Rick Wash. Folk models of home computer security. In *2010 Symposium on Usable Privacy and Security*, page 11. ACM, 2010.

[28] Rick Wash and Emilee J Rader. Too much knowledge? security beliefs and protective behaviors among united states internet users. In *2015 Symposium on Usable Privacy and Security*, pages 309–325, 2015.

[29] David Knapp Whittier, May G Kennedy, Janet S St. Lawrence, Salvatore Seeley, and Vicki Beck. Embedding health messages into entertainment television: Effect on gay men's response to a syphilis outbreak. *Journal of Health Communication*, 10(3):251–259, 2005.

[30] Justin Wu and Daniel Zappala. When is a tree really a truck? exploring mental models of encryption. In *2018 Symposium on Usable Privacy and Security*. USENIX Association, 2018.

[31] Kim Zetter. How the real hackers behind Mr. Robot get it so right. https://www.wired.com/2016/07/real-hackers-behind-mr-robot-get-right/, Jul 2016.

A Recruitment survey

Please specify the gender with which you most closely identify.

- Male
- Female
- Other
- Prefer not to answer

Please specify your age.

- 18-29
- 30-39
- 40-49
- 50-59
- 60-69
- Over 70

Please specify your ethnicity.

- White
- Hispanic or Latino
- Black or African American
- American Indian or Alaska Native
- Asian, Native Hawaiian, or Pacific Islander
- Other

Please specify the highest degree or level of school you have completed

- Some high school credit, no diploma or equivalent
- High school graduate, diploma or the equivalent (for example: GED)
- Some college credit, no degree
- Trade/technical/vocational training
- Associate degree
- Bachelor's degree
- Master's degree
- Professional degree
- Doctorate degree

If you are currently a student or have completed a college degree, please specify your field(s) of study (e.g. Biology, Computer Science, etc).

- Text field

Please select the response option that best describes your current employment status.

- Working for payment or profit
- Unemployed
- Looking after home/family
- A student
- Retired
- Unable to work due to permanent sickness or disability
- Other [text field]

If you are currently working for payment, please specify your current job title.

- Text field

Please write in the number of hours you typically spend on each of the following activities in the specified time range:

- recreational TV: ___ hours /week
- newspaper: ___ hours /week
- podcasts: ___ hours /week
- social media: ___ hours /day
- movies: ___ hours /month
- TV news: ___ hours /week
- magazines: ___ hours /week

Which genres do you enjoy consuming media in (select as many as you want):

- action
- comedy
- romantic
- documentary
- horror
- drama
- kids
- adventure
- sci fi
- fantasy
- other
- thriller/spy films

Please enter your email address so the we can contact you for the interview, if you are selected.

Your contact information will only be used to invite you to participate in the study. After the study, all records of your contact information will be destroyed unless you indicated above that you agree to be contacted regarding future studies.

- Text field

B Interview protocol

Introduction

- Hello. My name is [name] and this is [name]. Today we will be conducting a study to learn about what you may heard about cyber security threats.
- First, let's quickly go over how the study will work. We will break the session into three parts: questions about how you perceive cyber threats, the presentation of some short audio visual clips, and questions about your reaction to those clips. I expect the study will take approximately one hour. This is not a quiz or test of your knowledge; in fact there are no correct answers. We only want to learn about what you have heard about cyber security threats.
- Describe everything in the consent form.
- Although I do not expect this to occur, if you become uncomfortable at any time during the study please let me know. Do you have any questions at this point?
- Give the subject the consent form. I have this consent form here. It tells you whom to contact if you want to report any objections. I'll give you two copies - one is for you to keep, and the other is for you to sign.
- Ppint out places the subject needs to sign; point out the section where it states they will be auditorily recorded.

Phrase association and mental models

- To begin I'm going to ask you for any associations you have with some buzzwords. What comes to your mind when you hear:
  - Cybersecurity
  - Hacker
  - Encryption
- Now I'm going to ask some specific questions about your beliefs with regard to cyber security topics. Remember there are no wrong answers; I'm curious about your perceptions.
  - Can you describe to me what a hacker's goals are in general?
  - What makes someone an easy target for a hacker?
  - Can you describe to me who a hacker's intended target normally is?
  - What are some ways that users and businesses implement cyber security?
  - What, if any, limitations to hackers have? What mechanisms do they hackers utilize?
  - What is encryption used for?
  - How do you think people become involved with the hacking community?
  - What are some ways people can defend themselves against hackers?
- Where do you think those ideas come from? That is, what influences your perception of those ideas and phrases?

Personal experiences

- Now let's talk about your experiences with these topics. Have you or someone you know been hacked?
  - How did that happen/ What do you think happened?
  - What alerted you/them to the fact that their security had been breached?
  - What steps did you/they take to remedy the issue?

Prior media exposure

- Have you ever seen any depictions of the terms or ideas we've been discussing in fictional media? In a fictional TV show or in a movie? For example of a hacker?
  - Where?
  - How recent is/was it?
- Can you name any specific fictional TV shows or movies that have such depictions?
  - Can you think of any specific examples of a scene about [term] that you saw recently? Can you explain what was depicted?

Clip presentation and reactions

- Now we're going to move to the second section of the interview. I am going to show a series of short clips from various fictional movies and T.V shows, and then ask some questions about what you've seen immediately after each one. Before we begin, do you have any questions about what we've discussed so far?
- Play a clip, with the video in full screen mode.
  - Have you seen this show/movie before?
    - If so, have you seen this specific scene or clip?
  - Can you give me an overview of what you think is happening in the scene?
  - Scenes from fictional TV/movies often have some aspects that are realistic and some that are less realistic. What did you think was realistic about this scene?
    - Why do you find that aspect realistic?
  - What did you think was unrealistic about this scene?
    - Why do you find that aspect unrealistic?
- Repeat this same process with five additional clips.

Post-clip responses

- We're now beginning the final stage of the interview. I'm going to ask some questions about media portrayals in general. But first, do you have any questions about what we've covered so far?
- Do you feel the media, specifically fictional TV and movies, portrays cybersecurity, hackers, and encryption accurately, and why?
- Can you think of any fictional TV shows/movies that portray the topics we've discussed today realistically?
- Conversely, can you think of any fictional TV shows/movies that portray the topics we've discussed today unrealistically?

Closing

- That brings us to the conclusion of this interview! Do you have any final thoughts or questions?
- Thank you so much for your time. Here is your compensation and the consent form for your records.
- Give participant compensation and have them sign a receipt that they were paid. Also give them the unsigned consent form for their records.

Clips shown

- Skyfall: https://www.youtube.com/watch?v=aApTVqeGJMw
- Superman 3: https://www.youtube.com/watch?v=iLw9OBV7HYA
- Sneakers: https://www.youtube.com/watch?v=F5bAa6gFvLs
- NCIS: https://www.youtube.com/watch?v=u8qgehH3kEQ
- The Amazing World of Gumball: https://www.youtube.com/watch?v=-rQPdWwv3k8
- Blackhat: https://www.youtube.com/watch?v=7HWfwLBqSQ4