PROJECT PROPOSAL

CSI CYBER GROUP

Kelsey Fulton, Rebecca Gelles, Alex McKay, and Richie Roberts

Wednesday 14th March, 2018

1 Introduction

Computer users make decisions on security based on mental models they have formed that explain if, when, how, and why they are likely to be targeted by computer-based attacks. These models are not formed from complete information; most users are not well-educated about computer security unless it is their primary field of study. This means they have to draw conclusions from the environment around them, and often, they create theories and mental models about computer security that correlate with the input they have received. However, they're models are not guaranteed to match up with reality [1]. If the mental models they have formed are incorrect, they will draw inaccurate conclusions on how to defend themselves from attackers. This can lead to potentially damaging losses as a result of successful attack or potentially unnecessary expenditures of time and money to defend against unlikely threats. Faulty mental models can therefore be quite harmful to users. Prior studies have shown that many users may draw their mental models on computer security from mass media, particularly from television and film, and that these mental models that they have learned may not always be the most accurate [2] [3]. In this paper, we want to examine in depth the question of how media portrayals of computer security affect the mental models of the general population, if they do so at all.

To answer this question, we intend to conduct semi-structured interviews with members of the general population in order to elicit information about the extent, if any, to which their mental models are influenced by television and film, and what influence in particular television and film have had if so. As the area we are trying to evaluate is extremely open-ended, an interview study is the best choice. Our interviews will ask about their opinions on computer security topics independently of film and television initially to learn their immediate impressions. Then, we will gradually incorporate film and television by bringing up famous examples of media and then playing specific clips. This will allow us to view how their baseline mental model has already been (or not been) affected by mass media while also allowing us to see the immediate effect of particular examples of mass media that have more helpful or detrimental portrayals of computer security.

The results of our research will allow us to pinpoint how media can misinform an individual's perception of both the attack model of cyber threats and the steps that can be taken to protect oneself. Inaccuracies in the mental model can encourage foolish or even dangerous behavior, so if these inaccuracies can be demonstrably linked to the media, then steps can be taken to ameliorate this source of confusion. For example, the adoption of ”security consultants” on movie and television sets could be modeled after medical experts who are often called in to help ensure medical situations displayed are feasible, realistic, and responsibly conveyed.

2 Methods

2.1 Data Collection

We plan to collect a diverse group of participants by using Craigslist to recruit from the DC area. We will make a post on Craigslist asking participants to take a short survey that will add them to a field of applicants considered for further interview. Participants will answer a pre-screening survey that will ask basic demographic questions such as: age, race, gender, education level, income, and occupation. From these initial applicants, we will select a population to interview by making our participants as diverse as possible across all the aforementioned demographics. Once we form our population based on the pre-screening, we intend to administer a semi-structured interview to recruited participants. We will conduct these interviews in public spaces in D.C such as rented private rooms in libraries which will help to ameliorate the cost of travel for participants and decrease our no-show rate. We plan to give them a consent form at the beginning to ensure they understand the task and consent to their oral interviews being recorded. Since we will not mention the specific contents of the clips in the form (to avoid priming), we will be sure to choose our clips ethically. No participants will be exposed to profanity or obscenity.

Once the interview begins, it will be broken up into two sections. The first will attempt to identify what the participant's mental model of cyber threats is. We will take care not to correct them if their model is incorrect. Instead, we will simply encourage them to explain who they think executes attacks, who are the victims of attacks, and how attacks are carried out. Following that, we will ask them to describe what or who has helped them formulate this model. They won't have been primed to think about the media, so we will get their organic answers about their sources of information. The next phase of the interview will begin to question them more specifically about the media. We will show them short clips, no longer than four minutes, from television and movies that portray cyber attacks or defenses. With each clip, we will ask the participants if they have seen it before or seen a similar scene. We will then ask them if what they've just seen affects their mental model in any way. Alternatively, based on the previous answers of the participant, we might ask them to point out aspects of the clip they think could or would not happen in real life. For example, if a participant expresses disdain about a portrayal, we will ask them about the inaccuracies instead of asking how it affects their mental model. The data collected will be the audio recordings, which we will analyze after all the interviews are complete. We will not need any significant software or tools to complete our study; we will show the video clips to our participants on our own laptops and will use our cell phones to record the session.

2.2 Data Analysis

Our data analysis will be primarily qualitative rather than quantitative. We will use the audio recordings from our interviews to code participant responses. This may take a two-stage approach. In the first stage, we will come up with categories to code responses based on brief analysis of the recordings and broad themes encountered. In the second stage, we will code every response into one or potentially multiple categories. To ensure coding quality, team members will come up with labels independently in the first stage, and then they will work to select a core group of labels as a team. In the second stage, we will have multiple analysts from our team code each response and use Cohen's Kappa to ensure high agreement between coding choices. If the agreement is not satisfactory, we will discuss reasons behind individual coding choices, work together to come to consensus, and recode.

3 Anticipated Challenges and Limitations

Since this is an interview study, there are certain challenges inherent in the study format. One of these is that we will have to code the data after we collect it since it is qualitative data. None of our group members have experience with data coding, so we expect to draw from the expertise of our instructors and technical resources in learning how to tackle this problem. Another problem in interview studies is recruiting participants. Participants need to be willing to sit down in some location (or over Skype, but that may not work for our study because of the media aspect) for a significant period of their time and talk to us which is much more of a commitment than an online survey. This also makes it harder to find a representative sample for our study, since we have fewer potential participants to draw from. This, along with the fact our sample size is likely quite small and all from the same geographic area, will be a limitation on the external validity of our study. While this is a limitation, we consider it an acceptable one since this study is best run as an interview study and changing its methodology to increase the number of participants would not lead to useful data. Instead, we view this study as a pilot study, which could be run with more participants in the future.

A final challenge that is more specific to our topic is ensuring that our participants are likely have some experience with the media we are considering as a potential influence of mental models without priming them to consider that media. There are numerous potential media clips that exist related to computer security topics; due to the scope of our study and our own knowledge of media, we can only consider a subset of these. That means that the subset we consider is not guaranteed to overlap with the subset our interview subjects have seen. We considered pre-screening interview subjects to ensure they had seen one of the clips we are including as options, but we ultimately rejected that idea since it would prime the participants to be considering those particular movies or television shows when they participated in the study.

There are two major topics that are beyond the scope of our study. Our study will only cover media representations of computer security in film and television; it will not cover any other form of media like print, audio, or graphic. We made this decision because we concluded that television and film generally had more universal audiences than other forms of media, and there were generally fewer niche audiences: we believed we were more likely to be able to find media that a significant portion of the population had engaged with in those areas. Our study also only attempts to answer the question of whether the media can affect a person's mental model in a potentially detrimental way; it does not engage with the question of whether there is a way to repair faulty and inaccurate mental models, or whether the media has any role to play in doing so. While we may be able to speculate on the answer to these questions, we are not engaging in actual research to answer them.

4 Proposed Budget

For this study, we anticipate compensating interviewees 30 dollars for their time with us. This is consistent with past research efforts out of UMD and is a high enough amount that people will have an incentive to spend the hour long interview with us. We also keep this cost down by traveling to D.C to conduct our interviews and using the free facilities of a library. We hope to conduct five interviews, which would put our participant payment budget at 150 dollars.

References

[1] Walsh, R. "Folk Models of Computer Security." In SOUPS, 2010.

[2] Redmiles, E. M., Kross, S., and Mazurek, M. L. “How I Learned to be Secure: a Census-Representative Survey of Security Advice Sources and Behavior.” In Proceedings of ACM CCS, 2016.

[3] Redmiles, E. M., Malone, A. R., and Mazurek, M. L. “How I learned to be secure: Advice sources and selection in digital security.” In IEEE S&P, 2016.