Interactive Comics as Visual Narratives in Computer Security Education

Leah Zhang-Kennedy
Human-Computer Interaction
Carleton University
Ottawa, Ontario
leah.zhang@carleton.ca

Sonia Chiasson
School of Computer Science
Carleton University
Ottawa, Ontario
chiasson@scs.carleton.ca

Robert Biddle
School of Computer Science
Carleton University
Ottawa, Ontario
robert_biddle@carleton.ca

ABSTRACT

We investigate whether an online interactive comic is effective as a teaching medium to communicate to end-users about password guessing attacks and password security. Users' insecure password decisions make them susceptible to such attacks. Our qualitative analysis reveals that users have misconceptions about what constitutes “good” passwords, largely because they employ a Target mental model of password guessing attacks. We present our educational prototype and evaluate its effectiveness at correcting misconceptions about passwords. We conducted an eye-tracking experiment to evaluate how users learn and interact with such material. Our results suggest that the combination of text and graphical devices encourage learnability and engagement of security topics. Lastly, we present the learning outcomes of the comic prototype based on comparisons of the initial interviews with follow-up interviews. Our evaluation shows promising results indicating that this method helps to enhance understanding and even change user behavior.

1. INTRODUCTION

The average user juggles 7 passwords across 25 accounts [5]. Creating short and easy to remember passwords, reusing passwords, and mixing variations of the same password are common coping strategies [6]. These habits make users vulnerable to three types of online password guessing attacks: brute-force, dictionary, and targeted attacks. While many websites offer password advice, these often do not include reasoning behind why users should follow the advice. We argue that without a reasonable understanding of the risks, users are unprepared to make robust password decisions.

In our earlier work [2], we explored visual strategies to communicate to users about password guessing attacks and built prototypes to test their effectiveness. This approach is inspired by integrated visual-verbal strategies established in education literature [8, 4], and prior work looking at visual strategies to convey security information [7, 11].

In the current paper, we present a two-part follow-up study of our interactive educational comic prototype. Our first contribution is an analysis of users’ mental models of passwords and password guessing attacks. We follow the footsteps of prior work in users’ security mental models [12, 10], with a special emphasis on passwords. Our results show that users’ perception of password guessing attacks is based on a Target Model, leading to a number of implications for password creation, account prioritization, and context of use. Our second contribution is an eye-tracking evaluation of our comic as a tool to teach users about security risks. Lastly, our post-interview results show that our visualization enhances understanding and even changes user behavior.

2. BACKGROUND

In knowledge-based authentication, users are vulnerable to online password guessing attacks when they set up “weak” passwords that can be easily predicted by attackers. Online guessing attacks consist of exhaustive brute-force, dictionary and targeted attacks. Exhaustive brute-force attacks involve guessing every possible password in a theoretical password space. All passwords can eventually be cracked by brute-force, but the size of the search space, time, and processing power makes it unfeasible to crack strong passwords. In dictionary attacks, attackers use pre-compiled or computerized lists of high probability candidate passwords to guess the target password, including slang, and common character substitutions. Targeted attacks are based on the high probability that passwords are composed from personal information which attackers harvest about specific users.

In our previous study [2], we evaluated metaphors for risk communication about password guessing attacks, and designed three infographics [1]. We found that “users as targets” and “password as locks” are promising concepts that can help users understand how attacks work. We next designed a 14-page interactive comic [1] (Figure 1) with original characters, narrative, humour, and interactivity to give users a richer learning experience. To the best of our knowledge, the only exploration of comics in computer security education is Security Cartoon [11] that uses a series of comic strips to improve users’ understanding of various risks. Mainstream comics with security advice include Dilbert [3] and XKCD [9]. Our prototype takes a more comprehensive approach. It teaches users about the threat of password guessing attacks, how the attacks work, and offers practical coping strategies. In our earlier study, participants thought the comic was appealing and engaging. Users especially welcomed advice on creating passwords from a pass-phrase and results showed positive learning outcomes one week later.
3. INTERVIEW AND EYE-TRACKING STUDY

We designed a follow-up experiment to gain a more in-depth understanding of users’ mental models for creating passwords. This study also allowed us to gather eye-tracking measurements on how users read and interact with the comic.

Thirteen people from the university community participated in our study. Based on self-reported evaluations, nine participants had low level knowledge about how password-guessing attack work, three have intermediate level knowledge, and one had expert level of knowledge.

This two-part study included questionnaires, semi-structured interviews, and prototype viewing on an eye-tracking computer. To pre-assess current habits and knowledge, participants answered a pre-test questionnaire and a one-on-one semi-structured interview. The questionnaire gave a general assessment of participants’ demographic and current password strengths and coping strategies, while the interview provided an in-depth look at users’ understanding of passwords and guessing attacks. Next, participants viewed the prototype on an eye-tracking computer. The primary purpose of incorporating eye-tracking into our comic study is to evaluate how users read security information in comic format, how they use the interactive elements, and how long they spend on various visual elements.

We watched the eye-tracking videos and observed sequential patterns of visual attention, and took note of the time spent looking at various display elements and spent on each page. Then, we consolidated results by looking for reoccurring visual patterns, and calculated average reading times. The interviews were audio recorded and transcribed verbatim by the experimenter. Open coding was first used to look for emergent themes. We then modified and merged similar themes into high-level categories. Lastly, we looked for cause-effect relationships and synthesized the results.

4. THE “TARGET” MENTAL MODEL

In computer security, users rely on mental models [12] to help them make security decisions. In the analysis of the pre-interviews and questionnaires, we uncovered the presence of a Target mental model and that it impacts users’ perceptions, misconceptions, and understanding of “good passwords”. Users feel that attackers target specific users and that they are not usually likely targets. Users’ understanding of password guessing attacks was mostly restricted to targeted attacks, with little knowledge of dictionary and brute-force attacks. When mentioned, users mistakenly envisioned attackers targeting specific users in brute-force and dictionary attacks. This misunderstanding may strongly influence users’ ability to make the right password choices.

Users are more likely to create stronger passwords for accounts that they consider high value because these are bigger targets. Even the most cautious users reported sometimes practicing unsafe behaviours, such as password reuse. Participants emphasized that they make an extra effort to use strong passwords for accounts that they consider important. Their passwords for these accounts are longer and more elaborate, and are committed to memory. There is consensus that financial information has top priority, followed by primary email accounts. Interestingly, participants who considered Facebook to be a form of email communication said it was important. Those who saw Facebook as a social tool deemed it unimportant. For those who had several email accounts, primary accounts used for formal communication are perceived to contain more sensitive information than secondary accounts used for personal messages. Participants classified “unimportant” accounts as sites that do not request personal information and accounts that are accessed occasionally. These types of accounts include entertainment and gaming sites, and forums. Participants perceive these accounts to contain very little assets and therefore, unlikely targets for hackers.

Users’ definition of a “good” password is a long password with a mix of different types of characters. Users justify passwords such as “P[as)s[0]rd” as strong based on the length and types of characters, and whether it would be easy for humans to guess. Passwords associated with personal information are generally considered to be “bad” because attackers could target them and uncover this information. However, users included only the most obvious personal information like birth date, place of birth, current phone numbers, and information associated with immediate family and close friends. Participants considered outdated information to be personal secrets that are not available to the public, and therefore safe to use as passwords.

Some users created weak passwords because they felt the benefit to attackers from breaking into their accounts is extremely low. The belief that attackers only target wealthy and famous people coincides with Wash’s “big fish” model [12]. In some instances, even high-value accounts are considered less important when they have few assets. For example, a online banking account is perceived as low value if it contains little money. There would be little motivation for users with this mental model to make extra efforts to use strong passwords because they feel they have nothing to lose.

5. INTERACTIVE COMIC PROTOTYPE

As mentioned in Section 2, we developed a 14-page interactive comic [1] that incorporated characters, narrative, metaphors, humour, and interactivity to engage users while learning about password guessing attacks. The prototype (Figure 1) provided users with information about the risks, and gave practical password advice and coping strategies. It uses original artwork drawn by us in Adobe Illustrator and
coded in Flash. The narrative has three original characters. Jack and Nina are agents of computer security who solve computer security crimes and protect users against Hack. As the name implies, Hack’s mysterious character embodies all computer security crimes. Jack and Nina take on the role of mentors to guide users through the lessons. We choose online interactive comic media to communicate security topics to end-users because it has greater potential to reach non-technical users than traditional educational efforts. Comics have the ability to demonstrate complex topics progressively, through the use of narrative and characters. The reading format is lightweight, easy to consume, and does not appear intimidating to read. The media offers an enormous breadth of control to create customized content, through a full range of visual symbols and text-graphics pairings to aid comprehension, as well as rhetorical devices like humour to enhance persuasion.

We explored interactivity as way of giving users additional insights and to enhance engagement. For example, in the “Types of Attacks” section of the comic, users can rollover silhouettes of people to see whose password is vulnerable. At the end of the comic, a “Test your knowledge” game tests users’ ability to identify weak passwords.

6. STUDY RESULTS

We were interested to investigate how users’ attentions are spent, reading times, and ways users process the juxtaposition of text and images in comic format. The results will inform design guidelines for future work in this area.

Path and pattern of fixations: In comics, graphics take up much more space on the page than text. However, our data shows that text attracts attention before graphics. Headings and text blocks get eye fixations first. The only exception is when a graphic takes up most of the real-estate on the page. Interestingly, graphically rendered typographic text attracts the most eye fixation. For example, on page 10 of the comic, the password “abc” is illustrated as personified characters with googly eyes holding hands. On this page, participants spent the most time looking at this graphic. The path of fixation starts with headings, text blocks, and then graphics. After a text block is read, users’ eye moves to the closest surrounding graphic. Images typically get eye fixation for ≤1 second between frames. Sometimes users will look back and forth between text and images, and will re-read small blocks of text after looking at the images. Figure 2 shows a gaze trace for page 6 of the comic.

Participants generally focused more on characters’ faces. Eyes especially drew attention. We noticed that on page 10, the example password “abc” received longer eye fixation than “Ae8%!”. Both typographic images have personified characteristics, but the “abc” graphic included eyes. We did not find the sporadic use of colour affected users’ attention. However, circular objects draw eye fixation, especially when it is highlighted with colour. We did not find any major difference in reading patterns between non-comic readers and participants who read comics for leisure.

Time spent looking at display elements: Participants spent an average of 9 minutes interacting with the comic. Average viewing times between pages varied from 34 seconds to 103 seconds. Three pages were interactive, showing additional examples. Participants spent as much as 60% longer on pages with interactivity. On occasions where the interactive elements reveal cause-effect relationships, participants moused over objects several times to make comparisons. For static examples, participants also spent more time looking at the graphics. For instance, page 11 teaches users how to use the pass-phrase strategy. Participants spent as much as 6 seconds looking at the example “IL3-cp” made from the pass-phrase “I love 3-cheese pizza”, and up to 19 seconds looking at the example “A.MpN8mp” made from the pass-phrase “Aww...my partner Nina 8 my pizza”.

Limitations of the eye-tracking experiment: In our experiment, users gave us their full visual attention to read the comic. We did not find users skimming or skipping content. In fact, some users read certain sections more than once. However, there are several limitations to eye-tracking in the lab environment. The most obvious is that during the calibration stage, users are told that their gaze is being tracked. This might put pressure on users to read the material in whole. In real life, users might not dedicate as much time to reading the comic. When asked about this, users suggested that it would be appropriate to present the comic as a tutorial at the account sign-up stage, or include it in the password advice sections of websites. Participants commented that they would much rather read the information in comic format than from text documents, which is the typical format available to users.

Learning Outcomes: Participants returned one week later for a short follow-up interview. We asked them whether they changed their passwords. We compared participants’ responses based on their self-evaluated password strength. Our results show that 4 out of 5 participants with weak passwords changed them at home after the initial learning session. All 4 participants used the pass-phrase strategy to create their new passwords. 8 participants, who self-assessed their passwords as strong or moderately strong, did not change their passwords. These respondents felt that they were already maintaining good passwords for high-value accounts, and were not motivated to change other passwords.
85% of our study participants said they would use the pass-phrase strategy in the future. Please see Figure 3 for a result summary. To assess information retention, we asked participants to recall and describe how password guessing attacks work. All participants were able to identify and describe brute-force, dictionary, and targeted attacks.

7. DISCUSSION

Users commented that learning about password guessing attacks brought the risks to the forefront and that this prompted them to ask critical questions like “am I vulnerable?” Even though some people did not change their passwords within the period of a week, they credited the experience for making them aware of the risks. Interestingly, two participants shared information they learned with their family and friends. One participant reportedly helped her teenage son change his password using advice from the study.

Participants found the comic to be visually appealing and enjoyable to read. Based on the feedback we received, the most memorable section of the comic was the advice on pass-phrases. Participants thought the advice could easily be incorporated into securing their own passwords. Additionally, participants praised the section that taught them about the attacks work. Participants thought it was useful to be able to differentiate the different types of attacks, and to understand how to combat each one.

During the interview, all participants were able to recall the three types of online guessing attacks. Our follow-up results for targeted attacks were similarly positive. For brute-force attacks, participants grasped that long and complex passwords take more time to crack. Participants were particularly surprised and impressed by how quickly computers can be used to guess short passwords. The fact that a single character added to a password can make guessing it exponentially harder has motivated users to make their passwords longer. Participants correctly identified dictionary attacks, which use a library of dictionary words, and even understood that passwords using letter substitutions, slang, and alternative languages were also vulnerable to this attack. However, some users still considered the use of dictionary words acceptable if they were combined with unrelated words, or if they were particularly long.

8. CONCLUSIONS

We found that prior to interacting with our visualization, users’ ability and motivation to create strong passwords was limited by the presence of a “Target” model mindset. When users believe most attacks are aimed at specific targets, they seem to minimize their vulnerability based on the rationale that ordinary people with ordinary assets are unlikely victims. As a result, there is little motivation to protect accounts that users do not consider important.

Participants who viewed our comic prototype were able to successfully describe brute-force, dictionary, and targeted attacks one week later. We believe that understanding how the attacks work enabled participants to correct misconceptions about “good” password practices. Further, we believe the pass-phrase strategy provided practical and actionable advice to help users create memorable, strong passwords. In fact, our results found that 80% of users with weak initial passwords changed their passwords within days of interacting with the comic.

Our eye-tracking results provided insight on how security information is read when presented in comic format. The data we collected showed that users often refer to accompanying graphics to help them understand textual information. When interactivity was incorporated, users spent more time “seeking” new information. We believe these results confirm that comics are a promising method of deploying security-related education material.

9. ACKNOWLEDGEMENTS

This project has been funded by the Office of the Privacy Commissioner of Canada (OPC); the views expressed herein are those of the authors and do not necessarily reflect those of the OPC. S. Chiasson acknowledges funding from NSERC for her Canada Research Chair in Human Oriented Computer Security. This work was partially funded by the NSERC ISSNet Strategic Network and the GRAND Networks of Centres of Excellence.

10. REFERENCES

[10] F. Raja, K. Hawley, S. Hsu, K. Wang, and K. Beznosov. A brick wall, a locked door, and a
bandit: a physical security metaphor for firewall
warnings. In *SOUPS: Symp. on Usable Privacy and


*Proceedings of the 6th Symposium on Usable Privacy