Developing a Mental Model for use in the Context of Computer Security

Isaiah Liljestrand
Computer Science and Engineering
New Mexico Tech
USA
Isaiah.liljestrand@student.nmt.edu

Marcelo Gonzales
Computer Science
Colorado School of Mines
USA
magonzal@mymail.mines.edu

Dongwan Shin
Computer Science and Engineering
New Mexico Tech
USA
dongwan.shin@nmt.edu

ABSTRACT

A mental model is a useful tool for describing user's general mental processes that go into certain actions. In this paper, we investigate how to enhance the usability of security applications by considering human factors. Specifically, we study how to better understand and develop the user's mental model in the context of computer security through the use of the reasoned action approach (RAA). RAA explains that a user's behavior is determined by her intention to perform the behavior and the intention is, in turn, a function of attitudes towards the behavior, perceived norms (or social pressure), and perceived behavior control (capacity and relevant skills/abilities). A user study was conducted to test the validity of each of the main components of the model. Our user study concluded that alterations to a computer security application improved by the analysis through the mental model created improved user behavior.

KEYWORDS

Computer security, Usability, Mental Model, Influence

1 INTRODUCTION

One of the common mistakes made when designing computer security applications is that security is assumed to be both important and engaging for users. However, this is clearly not a correct assumption since computer security is almost never the users' primary goal [1]. In addition, computer security is not an easy topic for average users to understand, due to dynamic, complex environments and a lack of motivation. Because of this lack of motivation, understanding, and knowledge, computer security issues that threaten the average user are not properly negated much of the time. In order to counter this, the specific psychological factors that lead to a user's cyber behavior can be used to influence users in a way that decreases the probability of a successful cyber attack against said users.

In this paper, we investigate how to enhance the usability of security applications by considering human factors. Specifically, we study how to better understand and develop the user's mental processing model in the context of computer security through the use of the reasoned action approach (RAA), which explains that a user's behavior is determined by her intention to perform the behavior and the intention is, in turn, a function of attitudes towards the behavior, perceived norms (or social pressure), and perceived behavior control (capacity and relevant skills/abilities). Then we conduct research on how to integrate our model into a security application to enhance its effectiveness and efficiency.

The remainder of this paper is organized as follows: In Section 2, we present background and related work, and our approach to developing a user mental model for use in computer security is presented in Section 3. Section 4 discusses the user study of our research along with a discussion of some findings. Section 5 concludes this paper.

2 BACKGROUND AND RELATED WORK

A mental model describes the thought process associated with a real world action. The mental models being dealt with for our study try to generalize thoughts associated with certain actions and stimuli in order to get a feel for the average case person. An effective mental model takes into account all possible aspects of the thought process in order to accurately assess a person's mental state [2]. This kind of model has been used in many different facets of healthcare and security. Mental models generalize behavior behind certain phenomena and can be used to create different solutions to problems concerning said phenomenon.

2.1 Reasoned Action Approach

The Reasoned Action Approach (RAA) model is widely used as a mental model for human behavior in a broad sense [3], and an important part of its design is to stay very broad and cover the applicable and belief oriented aspects of people's behavior.

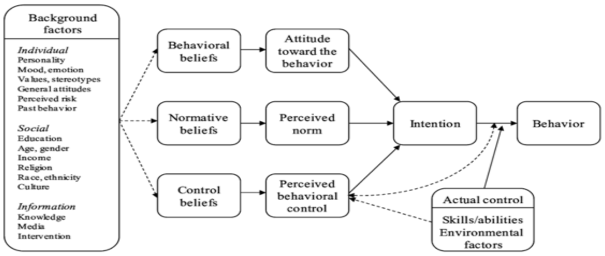

Figure 1. Reasoned Action Approach Model

SAC '19, April 8–12, 2019, Limassol, Cyprus
© 2019 Copyright is held by the owner/author(s).
ACM ISBN 978-1-4503-5933-7/19/04.
https://doi.org/10.1145/3297280.3299748

As shown in Figure 1, all of the environmental and background factors come into play and affect belief systems. The three sections involve individualistic, social, and informational characteristics. These embody all common aspects that have an effect on people's belief systems. Directly to the right of environmental and background factors are the three primary belief systems that affect human behavior. *Behavioral* beliefs outline a person's views towards a behavior. This leads into the *attitude* the person has which is the direct measure of said view towards behavior. The second section, *normative* beliefs, focuses on the social aspects of a person's belief system. This belief affects what the person views as the norm for other's behaviors when faced with the situation being analyzed. Last of all, *control* beliefs cover how much the user believes they are in control of their actions, how strongly they believe in their intended behavior, and other aspects of control. The direct measure of this belief is the person's perception of their control and belief strengths. All of these beliefs and direct measures affect the person's intention on what behavior they want to enact. The variables that affect how capable the person is of executing the behaviors they intend on executing are the person's skills and abilities as well as environmental factors. For example, if someone intends on being very secure in their online activity but is unaware of most threats and do not have the necessary skills to negate threats, they can still rather easily take part in unsafe activities and end up with a virus.

2.3 Protection Motivation Theory

The Protection Motivation Theory (PMT) is a mental model that focuses on the various aspects of fear appeals. This theory splits up fear into two primary sections: threat appraisal, and coping mechanisms [4]. These each split up into the two ways that coping and threat appraisal are measured. Coping is based on the subject's perception of their response efficacy, self-efficacy, and response costs. Coping in general describes the costs associated with dealing with the threat as well as confidence that the given behavior can effectively eliminate the threat. The primary components of a person's understanding that most affect threat appraisal are perceived severity and perceived vulnerability. The more vulnerable to a threat someone is, the more inclined that person is to take actions to negate the effects.

2.4 Fogg's Behavior Model

One of our goals for this study was to gain the ability to effectively influence a user to perform a desired behavior. In order to do this, Fogg's behavior model was considered for our study [5]. This model focuses on three things that affect a person's behavior: motivation, ability, and triggers. For motivation, when applied to a computer security context, the only area of effect that matters is the hope/fear appeal. The other facets of motivation focus more on immediate reward or punishment, or social aspects of motivation. The ability part of the model focuses on a person's ability to perform a certain task. There are six different categories of ability, but for computer security applications only two aspects actually need to be taken into account: *time* and *non-routine*. Last of all, triggers and the timing of triggers are necessary to give a person the nudge they need in order to perform the wanted behavior. Triggers work by exposing a user to a certain stimuli in order to trigger a specific behavior in the user, and triggers only have the capacity to work given certain pre-existing motivation or ability circumstances.

3 OUR APPROACH

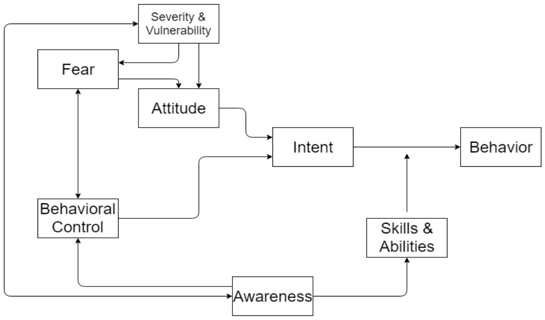

Figure 2. Computer Security Mental Model

As shown in Figure 2, our developed model originally takes off of the structure of the RAA model with PMT aspects integrated in and irrelevant aspects essentially removed. The primary attribute of this model ended up being awareness as it has an impact on every other piece of the model directly or indirectly. Using the knowledge that awareness is the most important aspect of the model, there are three subcategories that awareness ultimately has an effect on.

- **Skills & Abilities**

The limitations on someone's ability to affect their behavior are purely based on that person's skills and abilities. This is only half of the puzzle because someone who has proper motivation to affect their behavior can fail to do so because of a lack of adequate ability. On the other hand, someone who has the necessary skills and abilities to behave in the best manner possible but lacks the intent to do so will also fall short and fail to effectively behave in an ideal manner.

- **Behavioral Control**

Behavioral Control is the mechanism through which people have an effect on their intent. The two aspects of behavioral control that come from the PMT model are perceived response efficacy and perceived self-efficacy. These two aspects of PMT make up the coping section. Through the perception of one's abilities to protect themselves and perception of effectiveness of various behaviors, users develop methods of coping with threats. This part of the PMT model is mirrored by a section in the RAA model in the form of control beliefs and perceived behavioral control. For the sake of keeping the pieces of this model coherent, the behavioral control beliefs were not included. This was done because rather than being a more direct component of someone's behavior, control beliefs describe more abstract characteristics or a person's mental process.

- **Severity & Vulnerability, Fear, and Attitude**

The third section of our model is the largest as it involves three aspects. The primary feature of this is attitude. Attitude affects how favorably or unfavorably a behavior is viewed. Attitude takes into account expected outcomes of said behavior and judges the positive and negative aspects of the outcome. This leaves people with a disposition for or against various behaviors that strengthens or weakens intent to enact specific behaviors. Severity & Vulnerability describe a person's perception of a threat's severity as well as their perception of how vulnerable they are to that threat. This is a very important part of the model as it derives more directly from knowledge than most. While this part of the model is not describing a person's actual knowledge of a threat, their perception of a threat is highly influenced by their understanding of threats. This is primarily derived from the PMT approach for its effectiveness in threat and risk appraisal. Risk appraisal is extremely important when dealing with threats and therefore is a very important part of the model [6]. Last of all, as a consistent motivator, fear is a very important aspect of this model. Fear motivates through attitude as well as behavioral control [7]. With respect to computer security, it affects attitude by modifying a person's value system in favor of more secure behaviors. Behavioral control is affected by fear and vice-versa due to self-efficacy being a large part of behavioral control. When a person has high self-efficacy they will tend to not be affected by fear as much and vice versa. Due to the nature of fear however, an influx of fear tends to lower people's self-efficacy that motivates people to take more secure actions and raise their self-efficacy. Threat appraisal in this model is split up between behavioral control and attitude since perceived severity and vulnerability as well as fear have an effect on both behavioral control as well as attitude.

The only part of our model that does not originate from the RAA or PMT models is *awareness*. It had been decided that awareness is a huge part of computer security decision-making because of the lack of general knowledge about computer security information for the majority of the public.

4 USER STUDY

A user study was designed and conducted to test the feasibility of our model. Specifically, our user study was focused on testing how effectively our mental model when applied to a security application works and help to improve its usability.

4.1 Security Application and its Analysis

SSLight was used as a security application in order to test our developed mental model [8]. It is a Google Chrome extension[1] that attempts to prevent Secure Socket Layer (SSL) based man-in-the-middle (MITM) attacks by alerting the user to the lack of a secure connection between a web server and a Google Chrome. This was done with a traffic light analogy, as shown below.

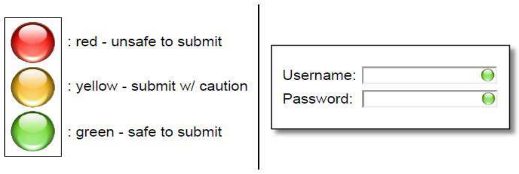

Figure 3. Visual security cues to prevent SSL-based semantic attacks

The light appears within the login or sign up input field of any website. A green light indicates a secure connection, a red light indicates an insecure connection, and a yellow light indicates that the user should proceed with caution. SSLight is already a computer security application aimed at fixing a security problem from the perspective of human factors, and this makes it an excellent example for testing our mental model.

The strengths and weaknesses of the security application were analyzed with respect to our mental model to better understand what aspects of the user's thought process were touched on more and which ones were lacking. As a result, it was understood that the two aspects of the model that the current solution was hitting on effectively were behavioral control and fear. Unfortunately however, it lacked in its ability to affect the user's skills and abilities, severity and vulnerability, and some of the overall aspects of awareness. The improvements to the solution are aimed at improving the user's skills and abilities, increasing their perceived severity of the threat as well as their vulnerability to it, and overall awareness of the situation.

After analyzing the original solution with respect to Fogg's persuasion approach, it was decided that the original solution and the initial ideas to improve the application lacked strong enough triggers. Since this solution was meant to appeal to people with a large variety in ability and motivation, a strong trigger is necessary to greatly affect decision-making behavior in a more broad population. SSLight was improved upon in such a way that the first time an insecure connection is happened upon, an overlay appears with an arrow pointing at the icon bar. Along with the arrow, a text box appears, telling the user that the connection is insecure and that they can click on the SSLight icon in order to learn more. If they click anywhere other than the icon, the overlay disappears, however if they do click on the icon an educational video plays. This video[2] includes a visual depiction of an SSL based MITM attack and a visual explanation of what SSLight does to counteract them. An important bit of information involved in the video is what actions the user can take to prevent their personal information from being stolen.

4.2 Hypotheses

The user study was conducted in order to test if the improvements to the existing solution made a difference in the end user behavior. However, the more important underlying reason for testing is measuring whether the individual components of the mental model each affect behavior. Due to the nature of the model, the overarching hypothesis for this study is about awareness, since awareness affects behavior control, perceived severity and vulnerability, and skills & abilities.

4.3 Experimental Design

There were two surveys taken by two separate groups, using Amazon Mechanical Turk and Survey Monkey. The control group was given the explanation of the scenario as they had the original version of SSLight. The other group of test subjects was given the explanation of the scenario as they had the improved version of SSLight. Test subjects first read a brief paragraph explaining what SSLight is by giving them the same amount of information that a user would have if they downloaded SSLight and read the description. The group with the improved version of SSLight was also given a display of what happens when the user clicks on the icon in the scenario of an insecure connection. The video shown in the improved version of SSLight was also embedded in the survey. From here the subjects were asked to answer a total of ten survey questions regarding their demographic backgrounds, skills and abilities, severity and vulnerability, fear, and behavior control.

4.4 Results

[1] https://chrome.google.com/webstore/detail/sslight/pclfifcfbjajkiemajjagohjminbkbjk?utm_source=chrome-ntp-icon

[2] https://youtu.be/UZ9VT189jhQ

The survey was conducted with 20 test subjects in each group. Overall, there were 4 test subjects that had answers that did not make sense or that took the survey twice. Three of these test subjects were in the group with the original version of SSLight, and one in the group that referenced the improved version of SSLight. This resulted in 17 legitimate data points for each question in the original SSLight group, and 19 in the improved SSLight group. From all of these data points there was a legitimate change in answers between the groups that does support all three hypotheses.

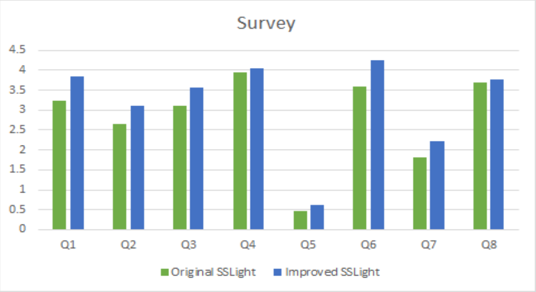

Figure 4. Graphs displaying the questions and relative answer values

Figure 4 represent how much the average user agreed with the questions posed about the hypotheses. Note that the results of two questions on demographics (Q9 and Q10) were excluded from the graph. Strongly agree is rated as a 5, strongly disagree is rated as a 1 with each other answer being scaled between the two. As is shown in Figure 4, in every question there is more agreement with the questions in the group that used the improved SSLight. This trend, along with the significance of almost all of the differences between questions leads to the conclusion that the changes made to SSLight did have a significant impact on user behavior. The two aspects of the model that did not seem to be significantly affected were the response efficacy part of behavioral control and the severity and vulnerability affect on attitude. In order to formally measure the differences, a t-test was used to measure the significance of the differences between each distribution.

- *Hypothesis 1: The skills & abilities gathered about computer security have a direct effect in changing behavior*

The first two questions (Q1 and Q2) asked about people's skills and abilities and how this affects behavior. The first question asked about how the person felt about their skills and abilities to defend against man in the middle attacks. The second question however asked how confident they would be in their abilities to prevent the man-in-the-middle attack in this scenario. The t-test for the first question produced results that show a difference with 90% confidence while the second produced results closer to a 65% confidence interval. The first question was more directly related to the skills and abilities of the subject and stated in a more broad sense so the fact that this is the stronger result is promising.

- *Hypothesis 2: Response efficacy and self-efficacy are both increased once the user learns information about computer security; this leads to a change in behavior*

Q3 involving behavioral control asked about the subject's confidence while Q4 asked about their response efficacy. The t-test results for the first question fell just short of an 80% confidence interval. The second question however had a t-test of inconsequential difference.

- *Hypothesis 3: An increase in the knowledge of severity and vulnerability and higher fear can lead to a more favorable attitude towards computer security actions*

Q5 dealt with perceived severity and vulnerability. It did not have a significant enough t-value to be considered substantial. While it cannot be considered substantial, the value was promising for somewhere around 60-70% confidence. Q6 dealt with the user's fear response and what effect this had on behavior. This is the only question that produced results within a 95% confidence interval. This is not surprising since fear is a commonly used and generally very effective motivator in computer security. Last of all, Q8 asked whether severity and vulnerability have an effect on attitude. This question produced the least significant results of this survey.

5 CONCLUSION

In this paper we studied how to better understand and develop a user mental model in the context of computer security, and a user study was conducted to test the validity of each of the main components of the model. The results of our user study showed that the proposed mental model was effective and each of the primary components of the mental model were shown to change user behavior. There were a few components that did not reap very promising results, though, and we believe that these components need to be tested more thoroughly with various security applications and with a larger population. There is a great potential for use of our model in a variety of computer security applications to improve threat negation rates. Hence, our immediate future work will focus on expanding the scope of and testing the effectiveness of our mental model to a broader spectrum of security applications such as for phishing.

ACKNOWLEDGMENTS

This work was partially supported by the grant from the National Science Foundation (NSF-CNS-1757945).

REFERENCES

[1] M. Zurko. 2005. User-centered Security: Stepping up to the Grand Challenge. In the proceedings of 21st Annual Computer Security Applications Conference.

[2] Jansen, J. and van Schaik, P. 2017. Comparing three models to explain precautionary online behavioural intentions. Information and Computer Security, 25(2), pp.165-180.

[3] Fishbein, M. & Ajzen, I. 2010. Predicting and changing behavior: The Reasoned Action Approach. New York: Taylor & Francis.

[4] Rogers, R. W. 1975. A Protection Motivation Theory of Fear Appeals and Attitude Change. Journal of Psychology, 91:93-114.

[5] BJ Fogg 2009. A Behaviour Model for Persuasive Design. In Proceedings of Persuasive 2009, Claremont, California, USA.

[6] Camp, L. 2009. Mental models of privacy and security. IEEE Technology and Society Magazine, 28(3), pp.37-46.

[7] Johnston and Warkentin. 2010. Fear Appeals and Information Security Behaviors: An Empirical Study. MIS Quarterly, 34(3), p.549.

[8] D. Shin, R. Lopes. 2011. An Empirical Study of Visual Security Cues to Prevent the SSLstripping Attack. In Proceedings of the 27th Annual Computer Security Applications Conference (ACSAC).