Matching Mental Models: Visual Narratives for Communicating Risks to Non-Expert Users

Tonya Stroman

Overview

Risky user behavior is a threat to system security. Current approaches to understanding and addressing this threat do not offer a definitive solution that can guarantee a congruous relationship between emerging technologies and evolving user attitudes and experiences. As the correlation between a users‘ system activity and the users‘ offline security increases, new ways of improving user understanding of the relationship between user actions and system security need to be considered and evaluated. We suggest that a different approach to computer risk communication, matching mental models of non-expert users through interactive visual narrative, may alleviate the problem. Supporting this concept, we conducted a conceptual user test of a risk-communicating interactive visual narrative. We found that providing risk related information in this format consistently changed user behavior from risk-ignoring to risk-avoiding. This suggests that interactive visual narratives , as a better risk communication method, can change user behavior and, consequently, help maintain system security.

Mental Models

Our investigation of mental models of security risk is grounded in previous card sorting mental models studies designed to understand the difference between expert and non-expert users. These card sorting experiments; were designed to address the following questions:

• Do the mental models implicit in the security literature correlate with the mental models of experts or non-experts?

•To what degree do the mental models of experts correlate with the mental models of non-experts users?

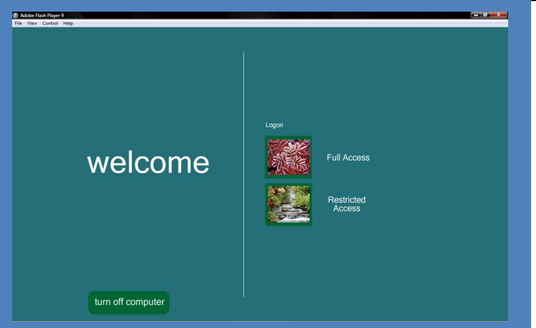
•How sensitive is the correlation between experts' and non-experts‘ mental models to the definition of expertise?

The card sorting experiment revealed how mental models of computer risk relate to:

- criminal risk
- physical security
- warfare
- economic failure
- medical risk

The results suggested that experts and non-experts have distinct mental models for many security risks. These results implied that individual mental models of security are strongly a function of their level of expertise.

Notably, non-experts categorized computer security risk as physical risk significantly more often than did experts.



Visual Narrative Test

The next step in our risk communication research agenda was therefore to generate narratives that reflected non-expert's mental models of security and determine if these were effective in altering behaviors. Bringing these experiments together we developed a narrative that described the risks of being an administrative user using the model of personal space and crime. This approach communicates system behavior and consequences of interaction with the system in a manner which is familiar and natural to people, in narrative form. Additionally, It‘s not just about making a risk known and understood, it is also about making the risk important enough to the user that it provokes behavioral change.

First, we devised a narrative metaphor based on the physical mental model of security risk of the non-expert user. This narrative offered two choices in selecting a rental unit. The descriptions of the two choices were roughly as follows.

1. You can stay in the fully furnished, fine apartment. However, if anyone steals from that apartment you are liable for the loss. And, because the apartment has so many wonderful things, including a hot tub, an expensive sound system, and a state-of-the-art computer, it is a likely target.

2. You can stay in the minimally adequate, adjacent apartment. You can still access the fine apartment. But you have to call the landlady to let you in, and call her again when you are finished to lock the fine apartment. In this case, your own possessions are unlikely to be stolen. If something is stolen from the fine apartment you are not liable.

For the test, we created the narrative metaphor, which represented system file access privilege, as a stand alone Flash movie file with content from the Sims 2 machinima engine. We tested 6 students, 3 female and 3 male, between the ages of 18 and 23. We gave all participants a pre-test questionnaire. All scored at the novice (non-expert) level of knowledge of computer systems; level was determined by the perceived level of knowledge indicated by the participant and responses to the pretest questionnaire.

We recruited subjects by simply inquiring of people in the lobby of an office building. We asked them to read a narrative that required that they sign in to the computer at the beginning of the test. The goal was that the user not particularly focus on the sign in process, but rather on the task to be completed, reading the narrative.

1. For the first task, we allowed each participant to “login” by choosing the ‘full access’ or ‘restricted access’ login option.

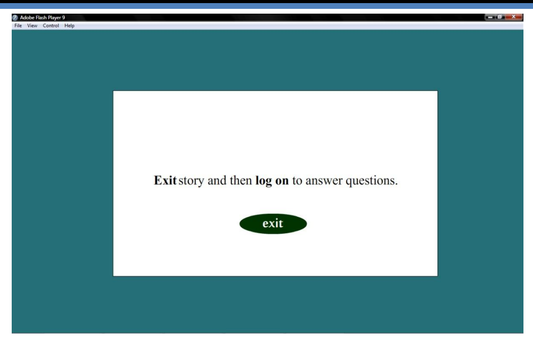
2. Due to potential usability issues with the labels ‘administrator’ and ‘guest‘, we used labels that described the concept we wanted to explain through the narrative.

3. We then allowed the participant to read through the narrative as slowly as needed.

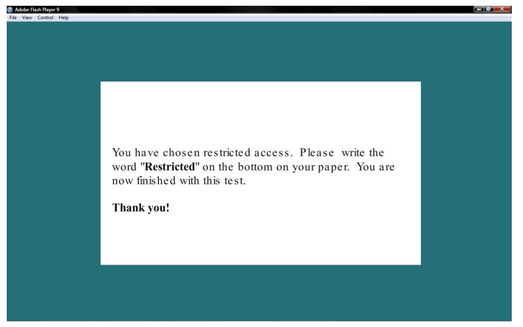
4. The last screen of the narrative instructed the participant to login again to complete some final questions.

5. In reality, we wanted to see if the narrative changed the participants choice of login option.

Behavioral Change



In the six instances where the task was completed without the narrative movie, all individuals chose ‘full’ access upon logging in. In contrast, after watching the narrative movie, users selected to use ‘restricted’ access accounts to complete their assigned task. So while this is too qualitative to provide statistical evidence of the efficacy of risk communication based on mental models, it illustrates the potential of the approach. More quantifiable experiments are in process.



Discussion

In conclusion, poor communication of computer risk contributes to user conceptual understanding of technology and, ultimately, system insecurity. If users do not understand the way a system works, they will never be able to understand how their behavior affects the stability of the system. Many of the approaches, which are meant to improve risk communication, poorly address the human side of the communication expectations. Of course, making the information easy to grasp is very important. However, it is just as important to make the information compelling. If the information does not inspire behavioral change, security does not improve. So, the solution to this problem requires much more than just accurate information about risk, it also requires an understanding of the complexity of human nature. Although there was observable behavioral change in the participants of our test, these results point to a need for further studies with a larger number of participants. Verifying a quantitatively significant, positive correlation between mental model matching, narrative exposure, and behavioral change is the next step. Once this relationship is established, we will be able to provide strong evidence that physical-model visual narrative communication is a highly effective, user-centered method of security risk communication.