Poster: Towards a user behavior model in computer security

Poster abstract SOUPS 2011

Hanul Sieger
Quality and Usability Lab
Deutsche Telekom Laboratories
Technische Universität Berlin
Ernst-Reuter-Platz 7, 10587 Berlin
hanul.sieger@telekom.de

Niklas Kirschnick
Quality and Usability Lab
Deutsche Telekom Laboratories
Technische Universität Berlin
Ernst-Reuter-Platz 7, 10587 Berlin
niklas.kirschnick@telekom.de

Sebastian Möller
Quality and Usability Lab
Deutsche Telekom Laboratories
Technische Universität Berlin
Ernst-Reuter-Platz 7, 10587 Berlin
sebastian.moeller@telekom.de

1. INTRODUCTION

The last decade of research in usable security has often shown that programming a system to be both secure *and* usable is a rare occasion. This is caused by a number of factors, most notably

- disalignment between user goals and expectations, and security features;
- security rules enforcement and missing user understanding due to lack of communication and education [7];
- users' rejection of security advice [6];
- continuation of legacy systems not being programmed with security in mind.

Other than in e.g. general GUI interaction, which in most times is an on-going task as long as the user sits at the computer, security features and alerts are usually encountered rarely. Giving login credentials and maybe seeing a spam filter or web certificate alert is often all of security-related interaction during work.

To aid the software architect and programmer to build-in usable security right from the start, a user behavior model, which can be simulated to test security features during development would be useful.

This poster presents recent and on-going work done towards building such a user behavior model. It shows the steps taken to build a model, giving an overview of the iteration process from designing user tests, extracting key factors, building a model, doing a computer simulation of the model, and feeding the results back to all stages for refinement.

2. USER TESTS

Due to the scarce interaction with security features (and the interaction itself often being one mouse-click only), "life-like" user tests or even field tests are too time-consuming to gather enough usable data without enormous efforts.

The goal is to find key factors influencing the user behavior in security-related computer interaction. We gathered some of these factors graphically in what we call a taxonomy (sorting and counting influencing key features and factors) as can be seen in figure 1.

As with a general question in psychology and sociology "What drives people to form decisions and act on them?", we have to answer that in the special situation of people interacting with computer security.

2.1 Focus groups, interviews, surveys

Focus groups, interviews, and surveys generate good qualitative insight into what people prefer (or think to prefer). We did several focus groups and surveys on the topic of security features on mobile phones [2] [8], which delivered user preferences on authentication methods and security levels. Other examples include [9], who interviewed users to characterize types and their different actions regarding computer security aspects (surfing the web, malware).

These results are a good starting point to find key factors and areas to focus on in later user tests.

2.2 Lab tests and micro-worlds

On the other hand focus groups and surveys cannot answer the question in quantitative terms how people actually react, when they have to make a decision on computer security. Some of those questions are: How often do users change settings like security levels or passwords? Do alerts trigger an action? Are alerts really read by users? What amount of time is spent on security-related functions? How is the user's security management affected by news about security breaches, malware etc.?

To gather quantitative data in terms of probabilities usable for our behavior model and its simulation, lab tests are inevitable. A behavior model not only requires rigorous statistics on user preferences, but hard data on decision timings, security setting changes, reactions to alerts etc.

Another approach to get data concerning user behavior is to set up a "micro-world". This is a computer-based scenario, where the user is confronted with an "abstraction" of the real world in order to limit the variables. It delivers good quantitative results and generates lots of data in a very short time, being valuable input towards a user behavior model.

In one test we used a modified version of the popular Tetris game as a micro-world environment to evaluate the tradeoffs between usability and security. The experiment aimed to model the behavior of users who are confronted with security mechanisms upon results found using the micro-world. [1]

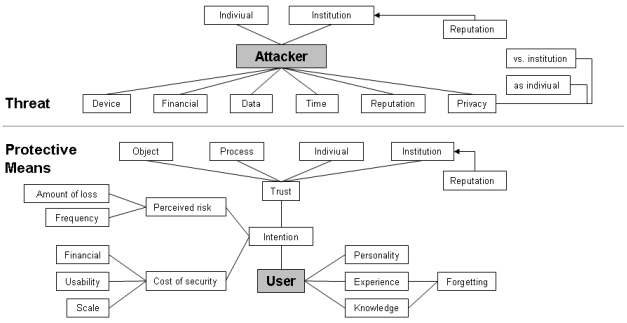

Figure 1: Taxonomy

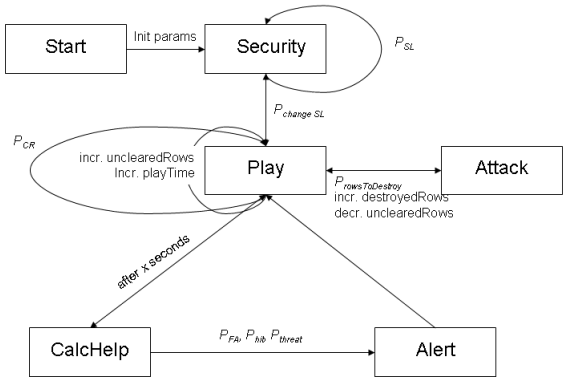

Figure 2: State chart model of the Tetris application used in MeMo.

3. DETERMINING KEY FACTORS AND CONSTRUCTING A TAXONOMY

Figure 1 shows a draft of a security taxonomy showing the user and possible attack vectors, both with possible influencing key factors. The taxonomy was derived from our previous user tests and surveys, literature, and general considerations.

After extracting key factors from previous user tests, those factors are fed into the user behavior model. An iterative circle is then started by using the behavior model for further tests, gaining more insights into the key factors and refining the taxonomy. The key question is how to derive quantitative user tests from insights, e.g. what users think about the "cost of security", which we try to address in the Tetris games test [1].

This taxonomy tries to get as broad an overview as possible, incorporating not only usability-related items, but (at least in the end) all key factors influencing the user's views, decisions, and actions concerning computer security (see also [4] for a security-usability threat model).

4. BEHAVIOR MODEL AND SIMULATION

Figure 2 shows a state chart model of the Tetris application from our simluation software (named "MeMo workbench" – Mental Model [3]) using a mixed probabilistic and rule-driven state machine.

The model maps the results from the tests to probability functions (see P-functions in figure 2) for different action paths. In this example, the model is derived from the Tetris micro-world.

"On the basis of the simulations, user behavior in security-relevant situations can be predicted and user interfaces optimizing intended behavior can be designed". [5]

The behavior model derived from the Tetris test showed good results in predicting the overall trend of the user behavior: "The probabilistic and rule-based simulation approach [...] is apparently able to predict user behavior with respect to three security-relevant variables in a meaningful way. Overall, the frequencies and the range of values observed in the simulation match quite well the ones observed in the experiment." [5].

5. CONCLUSIONS

Despite its initial limitations, the model shows promising results to aid (in a more advanced stage) in the development of computer security solutions. To do so, in the next steps the model has to be expanded to include more states to cover more variables. Using micro-worlds may gain in lots of useful data, but due to the abstraction may not be valid in all real-world scenarios. Thus, the model's underlying functions have to be fed with additional data from other tests to gain more valid predictions from the simulations.

6. REFERENCES

[1] N. Ben-Asher, J. Meyer, Y. Parmet, S. Möller, R. Englert: An experimental microworld for evaluating the tradeoffs between usability and security. *Symposium on Usability, Privacy, and Security (SOUPS) 2010*

[2] N. Ben-Asher, H. Sieger, A. Ben-Oved, N. Kirschnick, J. Meyer, S. Möller: On the need for different authentication methods on mobile phones. *MobileHCI 2011*

[3] K. Engelbrecht, M. Quade, and S. Möller: Analysis of a new simulation approach to dialog system evaluation. Speech Communication, vol. 51, no. 12, pp. 1234-1252, 2009.

[4] R. Kainda, I. Flechais, A.W. Roscoe: Security and Usability: Analysis and Evaluation. *Fifth International Conference on Availability, Reliability and Security, 2010 (ARES 10)*

[5] S. Möller, N. Ben-Asher, K.-P. Engelbrecht, R. Englert, J. Meyer: Modeling the Behavior of Users Who are Confronted with Security Mechanisms, *Computers & Security, Volume 30, Issue 4, June 2011, Pages 242-256*

[6] C. Herley: So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. *NSPW '09, September 8–11, 2009, Oxford, United Kingdom*

[7] A. Adams, M.A. Sasse: Users are not the enemy. *Communications of the ACM, Volume 42 Issue 12, Dec. 1999*

[8] H. Sieger, N. Kirschnick, S. Möller: Poster: User preferences for biometric authentication methods and graded security on mobile phones. *Symposium on Usability, Privacy, and Security (SOUPS) 2010*

[9] R. Wash: Folk Models of Home Computer Security. *Symposium on Usability, Privacy, and Security (SOUPS) 2010*