The Challenges of Understanding Users' Security-related Knowledge, Behaviour, and Motivations

Sara Motiee, Kirstie Hawkey, Konstantin Beznosov
Laboratory for Education and Research in Secure Systems Engineering
Department of Electrical and Computer Engineering
The University of British Columbia
Vancouver, Canada
{motiee,hawkey,beznosov}@ece.ubc.ca

ABSTRACT

In order to improve current security solutions or devise novel ones, it is important to understand users' knowledge, behaviour, motivations and challenges in using a security solution. However, achieving this understanding is challenging because of the limitations of current research methodologies. We have been investigating the experiences of users with two practical implementations of the principle of least privilege (PLP) Windows Vista and Windows 7. PLP requires that users be granted the most restrictive set of privileges possible for performing the task at hand; in other words, they should not use accounts with administrator privileges. By following this principle, users will be better protected from malware, security attacks, accidental or intentional modifications to system configurations, and accidental or intentional unauthorized access to confidential data.

To obtain an understanding of their knowledge, behaviour, motivations and challenges in following PLP, we had participants complete realistic tasks during a lab study that would raise user account control prompts and then performed a contextual interview to probe their behaviours. We faced numerous challenges during our study, including reflecting the realistic behaviour of participants, understanding their knowledge and challenges managing their user accounts and dealing with security warnings, and generalizing our results to a wider community. We discuss how we addressed these challenges, how well our methodological design decisions worked, and the ongoing challenges.

General Terms

Human Factors, Security

Keywords

Usable security, User Study, Methodology, Contextual Interview, Ecological Validity

Symposium on Usable Privacy and Security (SOUPS) 2010, July 14–16, 2010, Redmond, WA USA
.

1. INTRODUCTION

There are numerous security solutions that are not employed by users as their designers intended. To alleviate this problem, designers of these solutions need to better understand users' knowledge about the solution, their behaviors, and motivations in employing the solution and the challenges they face. Such an understanding assists security solution designers to improve the current solution or create a new one. However, understanding users' security-related knowledge, behavior, motivations, and challenges is not trivial.

Users deal with security solutions rarely and infrequently; therefore, observational methods are difficult to employ [2]. Another approach is to use qualitative techniques such as interviews. Interviews can be used to probe users' understanding about a security solution provided that the participant is motivated to actively take part in the interview. However, interviews have limitations for understanding users' behaviour and challenges. It is well known that participants may claim to behave in a particular manner in response to a security mechanism, while following a different approach in reality [3]. Conducting lab experiments to understand users' behaviour and challenges is also difficult. Participants may not be motivated to take a secure action because they feel the study conditions are secure [10, 7] or they may be biased to pay more attention to the security task [11]. Moreover, studies that involve launching real attacks may raise ethical concerns.

We recently faced these challenges when we tried to understand users' knowledge, behaviors, motivations and challenges in following the "principle of least privilege", or PLP for short in Windows Vista and Windows 7 [5]. In this paper, we discuss these challenges and our approach for addressing them. We first describe the objectives of our study (Sections 2) and the challenges we faced (3). We then discuss in Section 4 how we addressed these challenges in our study methodology, before discussing in Section 5 how well our design decisions worked and what challenges are ongoing challenges. We conclude in Section 6.

2. STUDY OBJECTIVES

The "principle of least privilege" [6] requires that each subject in a system be granted the most restrictive set of privileges possible for performing the task at hand. By following this principle, users will be better protected from malware, security attacks, accidental or intentional modifications to system configurations, and accidental or intentional unauthorized access to confidential data.

One practical implementation of PLP in operating systems is a "least-privilege user account" (LUA), which requires users to use accounts with as few privileges as possible for day-to-day work on PCs [8]. While low-privilege user accounts (i.e., non-administrator accounts) enhance security, they have not been popular among users. To alleviate this problem, Windows Vista ad Windows 7 introduced user account control (UAC) [9], which was intended to make the use of LUAs more convenient. With UAC, all users (including local administrators) can work with non-administrative privileges when such privileges are not necessary. A UAC prompt is raised when one of the user's processes requires administrative privileges.

It is important to learn whether users consider UAC prompts carefully or not. If UAC prompts are responded to correctly, the PLP is followed by users. Otherwise, we need to improve the current LUA or UAC approaches or design a new solution for supporting users in following the PLP. Before designing such solutions, we need to understand the perceptions, behavior, motivations, and challenges users face with the LUA and UAC approaches.

3. CHALLENGES

We faced various challenges in conducting our study. We describe these challenges below; and in the next section, we will show how they were addressed in our experimental design.

Understanding realistic behaviour: We were interested in observing the realistic behavior of users when they respond to UAC prompts in various situations. We also wanted to observe users' behaviours when they use different types of user accounts. However, observational methods of normal computer use are not optimal [2], because the activities of interest that raise UAC prompts (e.g., application installation, system configuration) and the act of switching between different user account types happen infrequently during the daily usage of computers. Moreover, self reports of behaviors are inadequate for our research questions because users may not report what they do in reality [3]. We could ask participants to perform these tasks in a lab study; however, they may behave differently in the experimental set up than in reality. For example, they could pay more attention to UAC prompts if they know we are observing their behaviour for responding to these prompts [11] or they may ignore the prompts because they are not concerned about the security of the experimental system that they perform the tasks on[10]. They may also trust the experimenter who gave them the task and assume the requested actions are secure to perform [7].

Simulating an attack: We aimed to observe users' behaviour when they face a UAC prompt raised by malicious software. However, simulating an attack on a users' system may raise ethical issues. Also, conducting study on a lab system and raising the attack on it may suffer from a lack of users' motivation or bias in considering the prompts [10, 11].

Understanding knowledge: To probe the users' perception of UAC and LUA approaches, we decided to interview them. An interview was a better option than a survey or questionnaire because we could probe participants' understanding based on their answers to questions. However, users may not be motivated to answer the interview questions thoroughly and accurately which may lead to unfair judgement about their understanding.

Understanding challenges: One of our study objectives was to understand what kinds of challenges our users face when they employ the UAC and LUA approaches. We had to rely on their reported challenges which they faced in the past, because we could not expose them to all the conditions which they may face during their daily usage of computer. However, users typically can not remember their past experiences accurately [4], which may cause us to obtain an incomplete understanding about their challenges.

Generalizing the results: In order to generalize our study results, we need to study a participant sample that represents the real user population. Recruitment of such a sample is challenging. Windows Vista and Windows 7 are used by millions of users who have different levels of knowledge and background about computer in general and computer security in particular. They also have varying requirements and needs for using a computer. Therefore, the results of the study may vary based on the type of users that have been studied.

Moreover, Windows Vista and Windows 7 are used in multiple contexts, such as in homes, offices, and educational institutions. Security policies and computer usage patterns may differ significantly in each of these contexts. Consequently, the results of the study in one context cannot necessarily be generalized to the other contexts.

Participant recruitment: Recruitment was more challenging than usual because of conditions of our study. We stated in our recruitment advertisement that participants would need to perform a series of downloading and installation tasks on their own laptop. We observed cases where people refused to participate in our study because they were concerned about installing applications on their laptop. Moreover, non-students typically used older laptops, most of which had previous versions of the Widows operating system that did not include the UAC approach.

Studying a new technology: Recruiting participants for Windows 7 was difficult because it does not yet have widespread adoption in the general community. When the study was conducted (January 2010), most of the Windows 7 respondents to our recruitment notices were computer or engineering students who had upgraded their system to this operating system.

Assess computer experience: During our data analysis we needed to investigate how the participants' general knowledge of computers impacts their behaviour. For this purpose, we needed to assess their knowledge and experience. This was a challenging task as no standard procedure exists for such assessment.

4. METHODOLOGY

We attempted to address most of the aforementioned challenges as we designed our study. Since we were interested in understanding the effect of human factors (knowledge and understanding, motivation and intentions, personal variables and capabilities) on the users' behaviour in using LUA and UAC approaches, we considered Cranor's "human in the loop" framework [1], which is designed for analyzing the human factors associated with secure systems. This ensured that our study design provided opportunities to observe and measure the various factors which might impact the behaviour of users when applying the UAC and LUA approaches. In particular, we wanted to observe whether users notice the communication mechanism of the UAC and LUA approaches, whether they comprehend and appropriately apply the UAC and LUA approaches, and whether their personal variables, capabilities, and intentions impact their behaviour.

We employed a laboratory study, followed by a contextual interview. This multi-method approach allowed us to mitigate the biases of any one approach and increase the methodological strengths [4].

Our study consisted of two sections. In the first section, we examined how participants respond to UAC prompts by asking them to perform a series of downloading and installation tasks that raise UAC prompts. We then conducted a semi-structured interview to understand participants' knowledge, motivations and challenges in responding to these prompts. In the second section, we investigated how participants employ different user account types. We first tested their knowledge about the differences between user account types and then asked them to create a user account for a user with a specific usage scenario. We then conducted another semi-structured interview to learn participants' motivations and challenges in using different user accounts. We were aware that testing participants' knowledge about user accounts in the beginning may bias them in user account creation task. However, we needed to do it first because there is a short description about the administrator and standard user account in the user interface for account creation in Windows Vista and Windows 7. We did not want our participants to read this first and increase their level of knowledge about user accounts. Further details of our study protocol is available in [5]. Below, we explain how our design decisions addressed the aforementioned challenges.

Understanding realistic behavior: As mentioned in Section 3, we could not use observational methods to understand the natural behavior of users; we therefore chose to expose users to a set of predefined and controlled tasks so that we could gather observational data about their behaviours. However, we tried to reflect the realistic behaviour of participants in the study by making the following design decisions.

1. Performing the lab study on the participants' personal computer: To increase participants' motivation for performing the tasks as they do in their daily usage of computer, we had them conduct the experimental tasks on their personal computers. Therefore, they were responsible for taking care of the security of their systems.

2. No detailed instructions: We did not provide detailed instructions for performing the study tasks. Instead, we exposed participants to task scenarios and asked them to perform the same steps that they normally would. They were told that the goal was not task completion and that we were interested in their normal behavior.

3. Letting the user decide: We instructed to participants that they could refuse to do each user study task if they did not perform such an activity in their daily computer usage or they did not feel comfortable doing the task. Therefore, it was participants' decision to perform or refuse the tasks. When they refused to do a task, they could proceed to the next task in the study.

Such design decisions allowed us to observe fairly realistic behavior of participants in an environment similar to their normal usage and consequently increased the ecological validity of study. We targeted laptop users so that they could participate in the study at the university.

In order to understand our participants' behavior in responding to UAC prompts, we asked them to do three downloading and installation tasks that raised UAC prompts. The tasks were designed so that the relationship of study tasks and UAC prompts was not obvious to participants. Therefore, they should not have been biased to pay extra attention to UAC prompts during the study. We told participants in the beginning that the purpose of study is learning their behavior in doing some typical tasks (installation and downloading) on the computer. A summary of tasks is described below. We observed users as they completed the tasks and asked them to think aloud.

- Task 1: Getting an application for playing a DVD. We presented participants with different options (such as downloading free software, buying software online or from store, getting application from a friend) and asked what approach they usually took. If they typically download and install software, they were asked to perform the same steps in the study session.

- Task 2: Receiving the installation file of a text editor application on a USB from a friend who recommended installing the application. Participants were asked whether they would install such an application; and if yes, they were requested to do the same procedure.

- Task 3: Downloading and installing a specific spyware remover application, recommended by a security expert.

There is evidence that our decisions were effective as some participants refused to perform some tasks because they had concerns such as decreasing the performance of their system, inconsistency of installed application with their current application, and no familiarity with the applications that were asked to be installed.

However, in order to understand participants' behavior in using low privilege user accounts, we had to rely on their self reported behaviours because none used such an account on their laptop. However, many did report previously experiencing low privilege accounts in public places, school, or work place computers.

Simulating an attack: In addition to observing the behavior of participants when faced with legitimate UAC prompts, we wanted to observe how they behave when they are faced with a UAC prompt which is raised by malicious software that intends to apply some changes in their system without their notice.

For this purpose, while participants performed the tasks, they were prompted with two fake UAC prompts. The first one was raised by an application installed without participants' notice (wrapped in the screen recorder installer which participants installed on their system in the beginning of their study to record their screen). The application raised a UAC prompt named "UpdateCache" three minutes after the screen recorder installation finished. Participants faced this prompt while busy with downloading and installing applications. The second fake prompt was shown during installation of the text editor. When the installation file ran, the first UAC prompt raised was a fake one with a name similar to the application; the second prompt was the real one.

Our simulated attack did not raise any ethical issues and it did not have any impact on participants' system. Since it was raised on the participants' system, they were motivated to respond to any unusual incident as they would normally do when using their computer. As the purpose of study was not obvious to them, we do not believe that they were biased to pay extra attention to security incidents.

Understanding knowledge: We examined participants knowledge of UAC prompts by conducting a semi-structured contextual interview after they finished performing the first three tasks of study. We showed them the video capture of their actions with respect to UAC prompts during the task and asked them questions about the purpose of UAC prompts, the actions that raise these prompts, and the differences between the various types of UAC prompts. Since the interview was conducted in the context of the user study tasks, participants could more easily understand the questions and convey their answers by referring to examples they faced in the study tasks. However, some participants were not motivated to answer the questions in detail. We also asked participants how they typically respond to UAC prompts during the daily usage of computer and contrasted their claim with their actual behavior in the study. This was an effective means of examining participants' understanding about UAC prompts and validating their claims; consequently, it decreased the biases of self reported data.

In order to examine participants' knowledge of the LUA approach, we asked them to create a user account for their "brother" who wanted to use their laptop for some tasks such as email, browsing, and using Microsoft Office. This allowed up to observe their familiarity with user account management. We also asked them about their reasoning for choosing the account type to examine their understanding about the LUA approach and conducted a semi-structured interview about the differences between user account types,

Understanding challenges: The study tasks did not adequately inform us about the challenges that participants faced in using LUA and UAC approaches. Therefore, we asked participants about these challenges during the interviews. Since the interviews were conducted in the context of user study tasks, participants could more easily remember their experiences with UAC prompts and different types of user accounts. However, a complete recall is not possible.

Generalizing results and participant recruitment: It is not feasible to recruit a participant sample that represents the real user population. However, we did aim for diversity and tried to recruit both male and female participants from different age groups with various educational and professional backgrounds. For this purpose, we sent out messages to email lists of several departments of UBC, posted messages to Craigslist and Kijiji, and attached flyers to community bulletin boards. During participant recruitment, we asked respondents their age, gender, degree, major, and occupation to ensure a diverse population for our study. We narrowed our study scope to personal computers that are managed by users. Therefore, we did not study people at their work places since such users are usually forced to follow company security policies on their computers.

Assess computer experience: To assess participants' computer experience, we asked them to indicate how difficult they find performing the following six tasks: copying and moving files, installing software, searching on the Internet, installing an operating system, administering a network server, and programming. We also refined our assessment based on participants' performance during the study tasks. Therefore, the final assessment was not solely based on participants' self reported capabilities. However, a more accurate assessment would require more detailed questions about the computer knowledge and experience of participants.

5. DISCUSSION

In this section we highlight the design decisions that we believe were particularly successful in our study. Such design approaches can be followed in similar studies that intend to understand users' behaviour, knowledge, motivations and challenges in using a security mechanism. We also acknowledge the challenges that we could not mitigate completely.

5.1 Successful design decisions

Making participants responsible for their actions: To increase participants' motivation for performing tasks as they do in normal computer usage, we had them conduct the tasks on their own computer and let them decide whether to perform or refuse the task. If participants perceive that their actions in the study may impact their long term and real conditions, they should have increased motivation to perform their normal security behaviours during the study tasks. The motivations should match those that participants have when performing similar tasks during their normal computer usage.

Avoiding detailed instructions to participants: To observe participants' natural behaviors, we avoided giving them detailed instructions for performing the tasks. The participant should have the authority to perform the tasks as she usually does rather than getting caught up in following the steps of user study tasks.

Contrasting participants self reported claims with their behavior: To decrease the effect of self report, we contrasted participants' self reported claims with their behavior during the study and investigated the reasons for any mismatch. Such contrasting provided valuable insights about our participants' behavior and their understanding about security mechanisms.

Putting the user in the context: Our contextual interview helped participants to understand the questions and recall their past experiences more effectively. When possible, a contextual interview can serve better than an interview for understanding participants' behavior, knowledge, motivations, and challenges.

Using semi-structured interview: We probed participants' differently based on their responses to interview questions. Understanding their knowledge, motivations, and challenges can be achieved more effectively through the use of semi-structured interviews than with structured ones as interesting responses can be followed up. However, some structure in our interview was required because we were interested in specific issues (participants' knowledge, motivations, behaviour and challenges) about UAC and LUA approaches.

5.2 Ongoing challenges

We had to rely on participants' self reports during various points of study, which sometimes led to incomplete or inaccurate data. For example, our understanding about the challenges users face in using LUA and UAC approaches are not complete because participants could not accurately remember their previous experiences outside of the study environment. Also, our assessment of participants' computer knowledge and expertise was mostly based on self report, but some participants may not have had a correct understanding of their expertise or may not have reported it accurately.

Another ongoing challenge that we could not address completely was recruiting a representative participant sample. As mentioned in Section 3, because of the specific characteristics of our study, achieving this goal was more challenging.

6. CONCLUSION

Conducting a lab study to understand users' knowledge, behavior, motivations, and challenges in using a security system is not trivial. Researchers should employ careful consideration to reflect the natural behavior of participants and mitigate the shortcomings of self report, bias, and lack of motivation. We suggest that making participants responsible for their actions, avoiding giving detailed instructions for performing the tasks, contrasting participants' behavior with their reported claims, and using semi-structured contextual interviews will help mitigate some of the limitations of lab studies.

7. REFERENCES

[1] L. F. Cranor. A framework for reasoning about the human in the loop. In *UPSEC'08: Proceedings of the 1st Conference on Usability, Psychology, and Security*, pages 1–15, Berkeley, CA, USA, 2008. USENIX Association.

[2] S. Egelman, J. King, R. C. Miller, N. Ragouzis, and E. Shehan. Security user studies: methodologies and best practices. In *CHI Extended Abstracts*, pages 2833–2836. ACM, 2007.

[3] J. Gideon, L. Cranor, S. Egelman, and A. Acquisti. Power strips, prophylactics, and privacy, oh my! pages 133–144. ACM Press New York, NY, USA, 2006.

[4] J. E. McGrath. Methodology matters: doing research in the behavioral and social sciences. *Human-computer interaction: toward the year 2000*, pages 152–169, 1995. Morgan Kaufmann Publishers Inc.

[5] S. Motiee, K. Hawkey, and K. Beznosov. Do windows users follow the principle of least privilege? investigating user account control practices. In *Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS) (to appear)*, pages 1–13, New York, NY, USA, July 14-16 2010.

[6] J. Saltzer and M. Schroeder. The protection of information in computer systems. *Proceedings of the IEEE*, 63(9):1278–1308, Sept. 1975.

[7] A. Sotirakopoulos, K. Hawkey, and K. Beznosov. "i did it because i trusted you": Challenges with the study environment biasing participant behaviours. In *SOUPS Usable Security Experiment Reports (USER) Workshop*, 2010.

[8] A. Steven. Applying the principle of least privilege to user accounts on Windows XP. Microsoft TechNet Library, http://technet.microsoft.com/en-us/library/bb456992.aspx, 2006.

[9] Understanding and configuring user account control in Windows Vista. http://technet.microsoft.com/en-us/library/cc709628(WS.10).aspx, 2007.

[10] T. Whalen and K. M. Inkpen. Gathering evidence: use of visual security cues in web browsers. In *Graphics Interface*, pages 137–144. Canadian Human-Computer Communications Society, 2005.

[11] M. Wu, R. C. Miller, and S. L. Garfinkel. Do security toolbars actually prevent phishing attacks? In *Proceedings of the SIGCHI conference on Human Factors in computing systems(CHI '06)*, pages 601–610, New York, NY, USA, 2006. ACM.