Do Windows Users Follow the Principle of Least Privilege? Investigating User Account Control Practices

Sara Motiee, Kirstie Hawkey, Konstantin Beznosov

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

ABSTRACT

The principle of least privilege requires that users and their programs be granted the most restrictive set of privileges possible to perform required tasks in order to limit the damages caused by security incidents. Low-privileged user accounts (LUA) and user account control (UAC) in Windows Vista and Windows 7 are two practical implementations of this principle. To be successful, however, users must apply due diligence, use appropriate accounts, and respond correctly to UAC prompts. With a user study and contextual interviews, we investigated the motives, understanding, behaviour, and challenges users face when working with user accounts and the UAC. Our results show that 69% of participants did not apply the UAC approach correctly. All 45 participants used an administrator user account, and 91% were not aware of the benefits of low-privilege user accounts or the risks of high-privilege ones. Their knowledge and experience were limited to the restricted rights of low-privilege accounts. Based on our findings, we offer recommendations to improve the UAC and LUA approaches.

Categories and Subject Descriptors

H.5.2 [**Information Interfaces and Presentation**]: User Interfaces—*Evaluation/Methodology*; D.4.6 [**Software**]: Access Controls—*Invasive Software*

General Terms

Human Factors, Security

Keywords

Usable security, least privilege principle, least privilege user account, user account control

1. INTRODUCTION

To limit damages from security breaches, the "principle of least privilege" [16], or PLP for short, requires that each subject in a system be granted the most restrictive set of privileges possible for performing the task at hand. One practical implementation of PLP in operating systems is a "least-privilege user account" (LUA),[1] which requires users to use accounts with as few privileges as possible for day-to-day work on PCs [17]. To implement this approach, operating system designers have developed various types of user accounts and advise end users to employ low-privilege accounts for their daily tasks [17]. By following this approach, users will be better protected from malware, security attacks, accidental or intentional modifications to system configuration, and unauthorized access to confidential data.

While low-privilege user accounts enhance security, they have not been widely adopted. Indeed, during a Microsoft Financial Analyst Meeting in 2005, it was estimated that 85% of PC users performed their daily tasks using administrator accounts [11]. One reason for the lack of LUA popularity is that many simple tasks (e.g., changing the system time when traveling, installing an application) can only be done from an account with administrative privileges ("*admin account*" for short) [23]. It appears that users often choose the convenience of working with administrative privileges over the reduction in risks associated with security breaches. Even though there is anecdotal evidence suggesting that mainstream operating systems support users poorly in following the PLP, there has been no published empirical data that could inform researchers and practitioners on the actual use of LUA and related mechanisms by users.

The overarching goal of our research is to investigate how well mainstream operating systems for personal computers support users in following the PLP, and what can be done to improve such support. Our particular objectives are to determine (1) how well users are aided by the technology to follow this principle, (2) what challenges they face, (3) what factors motivate their behaviour, and (4) what are the areas of potential failure for current PLP mechanisms.

For the initial study which we report in this paper, we narrowed the scope of our research to Windows Vista and Windows 7. In addition to LUA, Windows Vista introduced user account control (UAC) [23], which was intended to make the use of LUAs more convenient and therefore reduce incentives for violating PLP. 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 adminis-

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

[1]Since LUAs may not necessarily be *least* privileged, we refer to them as "*low*-privilege user accounts".

trative privileges (e.g., when installing software or changing system settings). UAC was revised in Windows 7 to reduce the number of prompts by default and to allow users to customize which prompts they receive. If UAC is disabled,[2] the type of user account determines whether the PLP is followed (in case of a non-admin account) or not (in case of an admin account). However, if UAC is enabled on a user's system, it is not critical what type of user account is in use; as long as the user responds to UAC prompts correctly, the PLP is followed. Given this interdependency between LUA and UAC and the critical role of the two in the support for the PLP, we studied the behaviour of users in employing LUA as well as in responding to UAC prompts.

To this end, we conducted a laboratory study, followed by contextual interviews. We recruited 30 Windows Vista and 15 Windows 7 users in order to observe any changes in their behaviour according to the different UAC implementations on these Windows platforms. None of the demographics of our WV and W7 participants were statistically significantly different, except for the years of experience with the operating system. The participants had a wide range of educational levels (from high school to Masters) and the 16 (out of 45) non-student participants had a variety of occupations. To maintain ecological validity, we asked all participants to perform study tasks on their Windows laptops.

It was perhaps shocking, but not surprising, to find every single participant performing day-to-day activities on own their laptop using an admin account. To better understand the factors affecting the use of LUA approach, we asked the study participants to complete a user account creation task, and we probed their knowledge about LUA. Although most created an appropriate low-privilege user account in the study task, participants were not motivated to employ a low-privilege account for their own daily computer usage. Furthermore, 91% of participants did not understand the security risks of high-privilege accounts or the benefits of low-privilege ones. In addition to a lack of awareness of security risks, prior experience with the inconvenience of low-privilege user accounts in different contexts of prior discouraged participants from using such accounts.

To investigate the use of the UAC approach, we asked participants to complete a set of tasks that raised legitimate and fake UAC prompts to observe their response behaviour. Our results show that at least 68% of participants did not use UAC approach correctly. These were participants who either disabled UAC (20%) or consented[3] to a fake random, i.e., not correlated with their current action, UAC prompt (49%). Interestingly, most of these participants (90%) did not have a correct understanding of the purpose of UAC prompts. On the other hand, those participants who had a partial understanding of UAC did not consent to the fake random prompt. It was not, however, the case for another fake prompt that was triggered as the result of participants' action during installation: all but 2 participants consented to both the fake and real UAC prompts raised during this task. This result suggests that when users initiate an action that might require admin privileges, they do not respond correctly to the subsequent UAC prompts.

Based on our findings, we offer several recommendations. Operating system developers should communicate the purpose and benefits of both UAC and LUA to users through the interface itself, rather than only through the technical documentation from the OS vendor. Furthermore, either users should be made aware of the the distinction between UAC and other security-related mechanisms (e.g., personal firewall, anti-virus software), or UAC should be integrated with the other mechanisms. In addition to the admin account created upon installation of the OS, users should be provided with an initial, default, low-privilege user account and be encouraged to use it for their daily work. However, to ensure users continue following LUA, users must be able to conveniently apply modifications on their PCs from within that low-privilege account. Furthermore, UAC prompts should be raised consistently, in selective and limited situations so that users do not ignore them due to habituation. These prompts should communicate enough information about their purpose and functionality so that users can respond correctly.

In the remainder of the paper, we first discuss related work and background information about the mechanisms of applying PLP in Windows Vista and 7. We then describe the methodology of our study and its results in Sections 3 and 4, respectively. Section 5 provides a discussion of our results, as well as recommendations for applying PLP. We discuss the limitations of our study and outline future work in Section 6 and conclude the paper in Section 7.

2. BACKGROUND AND RELATED WORK

The aim of our research is to investigate whether users follow the PLP and how well the technology supports them in following this principle. We first present related work on applying this principle. We then provide background about the UAC approach of Windows Vista and 7. As the UAC approach is based on raising warning messages, related work on warning messages is also discussed briefly.

2.1 The principle of least privilege

Different mechanisms have been implemented for applying the PLP. One main category of mechanisms is the user account model offered by various operating systems. There are various types of user accounts with different privileges.

In Unix-style operating systems, the root account has full privileges, while a non-root or basic account has limited privileges. It is considered bad practice to use the root account for daily use, as simple typographical errors in commands can cause major damage to the system [12, 5]. In some Linux distributions (e.g., Ubuntu), there are three user account types: root, admin, and basic. The initial user account created is an admin account that has fewer privileges than root, but can perform most administrative tasks. If a task requires root privileges, the user can use the `sudo` command and enter a password to elevate her privileges. The basic user account has low privileges [13].

In Mac OS X, the root account is disabled and there is a default admin account created during the OS installation or activation. While Apple advises that this account be reserved for making changes to the system and installing system-wide applications [7], it is the only account created during the OS installation and the user has an option of configuring her machine to log into this account automatically (i.e., without entering a password).

Early Microsoft Windows operating systems did not have the concept of different user accounts on the same machine.

[2]UAC prompts can be disabled by the user.

[3]We use the term "*consent*" to indicate that the user consents to privilege elevation asked by UAC prompt.

In NT and later versions of Windows, there are two types of user accounts: *administrator* and *normal* (standard). In Windows 2000, XP Professional, and Server 2003, there is also a "power user" account type that has more permissions than a normal account, but does not have some admin permissions. Microsoft advises users to use low-privilege user accounts for their daily computer use and recommends that admin and power user accounts only be used by trustworthy and knowledgeable users [17]. However, in all versions of Windows, all user accounts are created as admin by default; and users continued to use admin accounts on their systems. Moreover, using non-admin accounts inconvenienced users as many simple tasks (e.g., changing the system time) could only be done with an admin account [23].

Other mechanisms external to the operating system have been developed for applying the PLP. One approach is Sandboxing [9], which provides a tightly-controlled set of resources for a program to run. However, the rules for specifying resources are static and adding privileges to a running program is difficult. Another approach is asking the user to confirm the permissions for an application when it is started or during run time. Some Java Web Start applications follow this approach [6]. Moreover, two packages have been developed for Microsoft Windows for applying the PLP. The first, CapDesk [20], is a distributed file browser and application launcher that was developed to reduce the threat of viruses and trojan horses for everyday users of the Web. It allows users to browse files and open them with the associated application; opening a file in CapDesk first launches a caplet, which only has the authority to edit the file that was double-clicked. A security evaluation found the approach to have merit, but no user evaluation was conducted. The second, Polaris [19] was developed by HP Labs for Windows XP; its design was based on CapDesk. Polaris launches each application without the authority to access any user files. When a user opens a file via double clicking or the file chooser dialog box, Polaris grants the application access to that file. There were plans to install Polaris on consumer PCs that HP ships, but the current status of these plans are unclear.

We are unaware of any study directly evaluating technology support for the PLP; however, there has been some work looking at user account models for shared home computers. Egelman et al. [2] presented and evaluated a new user account model called Family Accounts, which provides a shared family account as well as personal accounts. Switching between accounts happens quickly and does not close running applications. Sharing information is easier using this model and users can switch accounts only when they require personalization or privacy. However, this model does not encourage the use of low-privilege accounts.

2.2 Windows user account control

Based on user account IDs and processes, the design of mainstream operating systems suffers from the limitation that every program has the same privileges as the account under which it has been launched, whether the user wants this or not. This limitation has been exploited by malware performing operations unintended by users. To address this limitation, a user account control (UAC) mechanism was introduced in Windows Vista and revised in Windows 7. It id complementary to LUA; that is, users can employ one, both, or neither of the two. UAC has a goal of allowing all users, including local administrators, to run with non-administrative privileges when administrative privileges are not required. Microsoft has mentioned in [22] that the UAC approach is designed to help prevent malware from installing without the user's knowledge, using "bundling" and social engineering, browser exploits, and network worms.

Task Description	WV	W7
Install a program	✓	✓
Uninstall a program	✓	
Install / uninstall a device driver	✓	✓
Install drivers downloaded from Windows Update or included in the operating system	✓	
Install an ActiveX control	✓	✓
Use the Windows Update console to install updates	✓	
Copy or move files into Program Files or Windows directory	✓	
View/change system-wide settings	✓	
Modify security settings with the Security Policy Editor snap-in	✓	✓
Open or change the Windows Firewall control settings	✓	
Reset the network adapter and perform other network diagnostic tasks	✓	
Configure Remote Desktop access	✓	✓
Configure Parental Controls	✓	
Add or remove a user account	✓	
Change UAC settings	✓	✓
Change a user account type	✓	
Browse another user's directory	✓	
Configure Automatic Updates	✓	
Schedule Automated Tasks	✓	
Backup and restore Files and Settings using Backup and Restore or Windows Easy Transfer	✓	
Running Disk Defragmenter	✓	
Pair Bluetooth devices to the computer	✓	

Table 1: Tasks that trigger a UAC prompt

With UAC, there are only two types of user accounts, protected administrator and standard user account. With a standard user account, users are not allowed to install programs, change system settings, and perform other tasks that require administrative privileges. When a standard user account attempts to perform a task that requires administrative privileges, a UAC prompt asks for the username and password of an administrative account. When a protected administrator attempts to perform a task that requires administrative privileges, she is prompted to consent to the privilege elevation. Windows Vista and 7 have also extended the range of common, low-risk tasks that standard accounts can perform. During the Windows Vista and 7 installation process, the user is prompted for a user account information. By default, an admin account is created. But Microsoft advises users to create a standard account after installation for their daily usage. Moreover, Windows Vista and 7 developers recommend users to think carefully when they respond to a UAC prompt and to make everyone, even administrators, enter passwords; so that they take advantage of UAC features for the security of their system [25].

Label used in the paper	Window Vista		Windows 7		App. Type Whose Action Causes a Prompt
	Backg-nd	Shield	Backg-nd	Shield	
Blocked	Red	Red	Red	Red	Blocked publisher or blocked by Group Policy
Administrative	Blue/Green	Gold	Blue	Blue/Gold	A Windows Vista or 7 administrative application
Verified	Grey	Gold	Blue	Blue	Authenticode signed and trusted by the local comp.
Unverified	Yellow	Red	Yellow	Yellow	(Un)signed but not trusted by the local computer

Table 2: UAC prompts color coding

The underlying UAC approach in Windows Vista and Windows 7 is the same; however, Windows 7 has reduced the number of UAC prompts. The tasks [24, 14, 23] that raise UAC prompts are listed in Table 1. Windows 7, by default, prompts the user when a non-Windows executable asks for privilege elevation [15]. Therefore, when the user changes Windows settings, he is not prompted, but when non-Windows applications (e.g. installing a new software) request administrative changes a UAC prompt appears. We note that omitting the prompts and privilege elevation without asking users are in contrast to the main goal of UAC: preventing silent installation of malware. The effectiveness of this tradeoff has yet to be evaluated.

Both Windows Vista and 7 implement four types of UAC prompts, color coded to inform users of the potential security risk of installing or running an application or applying a change. The prompt type is based on the executable's publisher. Table 2 lists the UAC prompt types (labeled as we refer to them in this paper) and their color schemes in both operating systems; there are some differences.

In addition to enabling and disabling UAC prompts in Windows Vista, users of Windows 7 can choose to receive such prompts only when a non-Windows executable asks for privilege elevation in order to make changes to the computer. They can also choose whether or not the prompts appear on a *secure desktop* in which the screen is dimmed.

When UAC is enabled, the type of user account is not critical for following the PLP. In this case, if the user responds to UAC prompts correctly, she follows the PLP; if she does not respond correctly, the PLP is violated. However, if UAC is disabled, the type of user account determines whether the user follows or violates the PLP. Therefore, it is important to study how users respond to UAC prompts. We also need to study the users' behaviour in using different user accounts to learn what motivates them to use a high or low-privilege account on their systems.

2.3 Security warnings

The UAC approach of Windows Vista and 7 is based on raising security warnings. We are unaware of any related work investigating the effectiveness of warnings that aim to prevent users from installing and running malware on their system. However, prior research investigating the effectiveness of warning messages suggest that these messages should be used as the last solution for reducing a risk [27]. Warnings should communicate the risk and clear instructions for avoiding the risk [18]. Sunshine et al. [21] studied users' behaviour in responding to SSL warnings in web browsers and suggested decreasing the number of warnings and improving their design. Egelman et al. [3] evaluated the effectiveness of active phishing warnings in current web browsers. Of the participants who saw the active warnings, 79% chose to close the phishing web sites. The authors offered recommendations for improving phishing indicators. They suggest a phishing indicator should interrupt the user's primary task, prevent habituation, provide clear choices, alter the look and feel of phishing sites, and fail safely if the user ignores or misunderstand it. Zurko et al. [28] have evaluated the usability of Lotus Notes security alters that aim to prohibit users from running unsigned active content and found that 59% of participants allowed the unsigned content to run. They suggest educating the users or including more information in security-related interfaces.

Wogalter [26] proposed the Communication-Human Information Processing Model (C-HIP) to analyze and identify the reasons that a particular warning is ineffective. In this model, a communication is sent to a human receiver to trigger a behaviour. The behaviour depends on communication impediments, communication processing, and personal variables of the receiver. Cranor [1] enhanced this model to consider the human in the loop in secure systems. Five communication types are defined in the framework: warnings, notices, status indicators, training, and policies. The UAC approach of Windows Vista and 7 is communicated via warnings while LUA is not communicated to users. The use of LUA is only encouraged in online documentation of Microsoft. This framework provides a semantic approach for identifying potential causes for human failure, which we utilized when designing our study and analyzing the results.

3. METHODOLOGY

As we designed our methodology, we referred to Cranor's "human in the loop" framework [1] for analyzing the human factors associated with secure systems. This allowed us to ensure that we observed and considered the various factors that might impact the success of the communication mechanisms of the UAC and LUA approaches (e.g., the prompts in UAC). We aimed to answer the following questions in regards to UAC and LUA:

1. Do users notice the communication mechanism of the UAC and LUA approaches?
2. Do users comprehend and appropriately apply the UAC and LUA approaches?
3. How do users' personal variables, capabilities, and intentions impact their behaviour in employing UAC and LUA approaches?

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 [8]. Security is not usually the primary task or goal of users, therefore, a user study methodology needs to be carefully considered [4]. Because users respond to UAC prompts and manage user accounts infrequently and

Property	WV		W7		Total	
	N = 30	%	N = 15	%	N = 45	%
Gender (F / M)	13 / 17	43.3 / 56.7	6 / 9	40 / 60	19 / 26	42.2 / 57.8
Student (Y / N)	18 / 12	60 / 40	11 / 4	73.3 / 26.7	29 / 16	64.4 / 35.6
Technical background (Y / N)	10 / 20	33.3 / 66.7	8 / 7	53.3 / 46.7	18 / 27	40 / 60
Primary OS - Vista or 7 (Y / N)	27 / 3	90 / 10	12 / 3	80 / 20	39 / 6	86.7 / 13.3
	Mean	Range	Mean	Range	Mean	Range
Age	26.3	18 - 50	23.6	19 - 30	25.4	18 - 50
Daily hours of computer usage	6.9	1 - 15	7.7	3 - 14	7.2	1 - 15
Years of computer experience	11.7	2 - 27	10.5	1 - 23	11.3	1 - 27
Daily hours of WV or W7 usage	5.2	0.3 - 12	5.3	2 - 10	5.2	0.3 - 12
Years of WV or W7 experience	1.5	0.3 - 3	0.3	0.1 - 1	1.1	0.1 - 3

Table 3: Participants' demographics

irregularly, it would be difficult to observe their behaviour during normal computer use. We therefore chose to expose users to a set of predefined and controlled tasks, including those that would raise UAC prompts, so that we could gather observational data about their behaviour. Furthermore, because participants may not be motivated to apply security practices when using study data and equipment, we had them conduct the experimental tasks on their personal computers. This allowed us to observe them in an environment similar to their normal usage context. We targeted laptop users so that sessions could be held at the university.

3.1 Participants

We recruited 30 participants for Windows Vista ("*WV*") and 15 participants for Windows 7 ("*W7*") from both the university and general community. We sent out messages to email lists of several UBC departments, posted messages to Craigslist and Kijiji, and pinned flyers to community bulletin boards. During recruitment, we asked respondents their age, gender, degree, major and occupation to ensure a diverse population for our study. Accordingly, we selectively sampled from the pool of responses in order to achieve breadth in the characteristics of our participants. All participants were paid $10 CAD for their participation. Table 3 shows the demographics of our participants. They had a wide range of educational levels (from high school to Masters) and the 16 non-student participants had a variety of occupations such as teachers, secretaries, managers, and photographers. None of the properties of our WV and W7 participants were statistically significantly different, except for the years of experience with the operating system being studied; the W7 participants were early adopters of Windows 7, which had only been released for a few months at the time of the study.

We also assessed the participants' computer experience by asking them to indicate how difficult they found performing the following six tasks: copying and moving files, installing software, searching on Internet, installing an operating system, administering a network server, and programming. We categorized their computer expertise as low, medium, or high, as shown in Table 4. We also refined our categorization based on their performance during the downloading and installation tasks in the study.

Expert. Level	WV		W7		Total	
	N=30	%	N=15	%	N=45	%
Low	7	23	2	13	9	20
Medium	16	53.3	8	53.3	24	53.3
High	7	23.3	5	33.3	12	26.7

Table 4: Participants' computer expertise

3.2 User Study Protocol

We used the same protocol for WV and W7 participants. After signing the consent form, each participant completed the background questionnaire, which had questions about their computer usage pattern, such as usage hours, experience, and used operating systems. Then participants installed software (provided on a USB disk) to record their voice and capture their laptop's screen. We also recorded their screen using a video camera, as the recording software did not capture the UAC prompts raised on the dimmed screen. We observed participants as they were completing the tasks and asked them to think aloud. There were two main parts to the study. The first was designed to investigate the knowledge, behaviour and motivations of participants in using UAC approach. The objective of the second part was to learn about participants' account usage behaviour and their knowledge about the LUA approach. We did this last, so as not to prime participants on the purpose of the study during the first part. At the end of the study, participants uninstalled all the applications that they installed on their laptop during the study.

Part 1: Examination of UAC practices

We asked participants to perform three tasks on their laptops. These tasks were designed to raise two different types of UAC prompts (Verified and Unverified). To increase the ecological validity of the study, we did not provide detailed instructions for performing the tasks. Instead, we presented participants with three hypothetical task scenarios and asked them to perform the same steps that they would normally take. They were told that task completion was not the goal and that they could refuse doing the task if they did not perform such an activity during their normal computer usage. The tasks were as follows:

1. T1: Getting an application for playing a DVD. We presented participants with different options (such as downloading free software, buying software online or from a store, getting application from a friend) and asked what approach they usually took. If they usually downloaded and installed software, they were asked

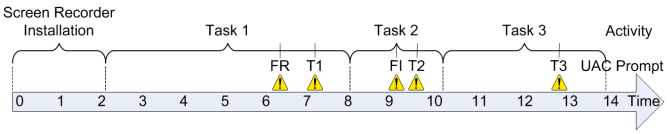

Figure 1: Typical timeline of user study tasks and corresponding UAC prompts

to perform the same steps in the study session. We observed their decision process for downloading and installing an application, including their response to the UAC prompts and other warnings and messages.

2. T2: Receiving the installation file of a text editor application on a USB disk from a friend who recommended installing the application. Participants were asked whether they installed the application in such a situation. If they responded "yes", they were requested to install the application as they would in a similar real life situation. Installation of this application raised an Unverified UAC prompt.

3. T3: Downloading and installing a specific spyware remover application, recommended by a security expert. This installation triggered a Verified UAC prompt.

While performing these tasks, participants were prompted with two additional fake UAC prompts. The first was raised by an application installed without their notice (wrapped in the screen recorder installer). The application raised an Unverified UAC prompt named "UpdateCache" three minutes after the screen recorder installation finished; we explicitly chose a name that was unrelated to their tasks. Since this prompt was not correlated with the participants' actions, we call it the "Fake Random" prompt (FR for short). Participants faced the FR prompt while they were doing one of the study tasks. While Figure 1 shows a typical timeline of UAC prompts during the user study, the interleaving of FR with the other UAC prompts raised depends on the speed with which tasks were completed. We observed participants' response to this unexpected UAC prompt.

The second fake prompt was shown during the installation of the text editor. When the installation file ran, the first Unverified UAC prompt was a fake one with a name similar to the application and the second prompt was the real one (also an Unverified UAC prompt). Since this fake prompt was correlated with the installation task, we call it the "Fake Installation" (FI) prompt. We observed participants' response prompts that appear during installation.

After performing the tasks, we replayed to each participant the video capture of their screen and interviewed them about their understanding of the tasks and their rationale for the actions they took. In particular, they were asked about their knowledge of the UAC prompt, its interference with their computer usage, its different types, their rationale for responding to these prompts, and their reasoning for responding to fake prompts. Since the interview was conducted in the context of user study tasks, its ecological validity increased while self report issues decreased.

Part 2: Examination of LUA practices

Participants were first asked about the differences between admin and standard user accounts. They were then presented with a scenario in which they were asked 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. By giving them this task, we observed their familiarity with user account management and their decision making processes for account creation. We then probed each participant about their rationale for creating the account in the user study task, the account they used and their reasons for its usage, their experience with other user account types, and the challenges they face when using them. For WV participants, we also asked them about the UAC prompt they faced before creating the account to determine whether they were aware of the difference between it and those they received during the first part of study. This prompt was not raised when the default UAC settings were used in W7. As all W7 participants used the default settings, none received this prompt and we did not ask them about it.

3.3 Analysis

To analyze the data, we used a card sorting approach [10]. Participants' responses to the interview questions were written on index cards. The index cards for each question were then sorted into multiple piles so that cards representing similar responses were in the same pile. We associated a theme with each pile, that represented participants' knowledge, behaviour, and motives based on the corresponding question. The sorting and naming of the piles was done iteratively to find participants' behavioural patterns.

4. RESULTS

In the following two sections we present results from the first (UAC practices) and second (LUA practices) parts of user study, respectively.

4.1 UAC Practices

In this section, we report our participants' knowledge and opinion about UAC prompts, their responses to UAC prompts during the user study, as well as their reported rationale for responding to these prompts during their normal computer usage. We contrast their actual behaviour to their reported rationales to determine any mismatches and the underlying reasons for their behaviours.

When comparing the responses and behaviours of WV and W7 participants, we used the χ^2 test; when its assumptions were not met (i.e., cells had an expected count <5), we used the Fisher's exact test. Since in most cases, there was no statistically significant difference between WV and W7 participants, we report the overall behaviour of all 45 participants unless such a difference exists.

We found that at least 69% of our participants did not employ the UAC approach correctly. These were participants who disabled UAC (20%) or consented to FR (49%). The latter did not have a correct understanding of the purpose of UAC prompts. All but two consented to both the fake (FI) and real prompts triggered during the second installation task; when they initiated an action, they were unlikely to respond to the subsequent prompts correctly.

4.1.1 Knowledge of UAC prompts

The responses of our participants to interview questions indicated that none fully understood the UAC approach. Table 5 shows the knowledge our participants had about different aspects of UAC: knowing the terminology; recog-

Knowledge type		WV		W7		Total	
		N=30	%	N=15	%	N=45	%
Terminology		1	3	5	33	6	13
Recognition		29	96	15	100	44	97
Partial Understanding	Getting user's permission	4	13	3	20	7	15
	User initiated operation	4	13	3	20	7	15
Difference between Verified and Unverified prompts		3	10	3	20	6	13
Difference between administrative and other prompts		6	20	N/A	N/A	6	20
Operations raising prompt	Installing application	4	13	5	33	9	20
	Installing application and changing settings	4	13	0	0	4	8
	Privilege elevation	0	0	1	6	1	2
	Installation plus incorrect answers	11	36	4	26	15	33
	Did not know why raised	11	36	5	33	16	35

Table 5: Participants' knowledge about UAC prompts.

Reason For Disabling	Total	
	PartiallyCorrect	Incorrect
All prompts ask the same thing	3	1
Interference with computer troubleshooting	2	0
Did not know the reason, as another family member disabled	0	2
Getting "Java Update" prompt during each startup	1	0

Table 6: Number of participants who disabled UAC prompts and their reasons

nizing the prompts; partially understanding the purpose of UAC prompts; understanding the difference between Verified, Unverified and Administrative prompts; and knowing the operations that trigger prompts. All participants recognized the UAC prompts, except for one WV participant whose family member had disabled UAC during her laptop setup. The only significant difference between WV and W7 participants was that more W7 participants knew the term UAC ($p = 0.012$, Fisher's exact test).

Based on our participants' explanations about the purpose of UAC prompts, we categorized them as having a partially correct understanding (PartiallyCorrect) or incorrect understanding (Incorrect). We classified 30% of participants (third row of table 5) in the PartiallyCorrect group; they perceived UAC as a mechanism for getting users' permission before applying any change to the system or ensuring that the user has started the operation.

Most participants did not understand the difference between various UAC prompts types. Only 13% of participants perceived the Unverified prompt as being potentially more dangerous, a possible virus, or an unknown application for the computer. Only 20% of WV participants associated the administrative prompt with an administrative task, Windows related operations, or a configuration change prompt versus application related prompt. As all W7 participants used the default settings for UAC, they did not receive the administrative prompt.

4.1.2 Response to UAC prompts

Some participants did not receive all the potentially raised UAC prompts in the study. Nine participants (WV:6, WV:3) had previously disabled UAC on their laptop. Furthermore, not all participants completed all of the user study tasks. One, who was very cautious about downloading and installing, canceled T1 in the middle and did not start T3. Another, who did not regularly download and install applications, did not do T1 and T3. One other participant

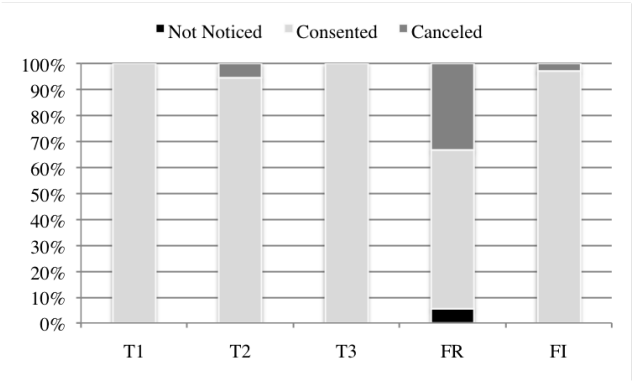

Figure 2: Percentage of generated prompts that were not noticed, consented to, and canceled

needed the name of the application to download, so she did not do T1. One, who had disabled UAC did not do T2 because she only installed software that she had heard of before. Three did not do T3 because they were concerned about the compatibility of the spyware remover with their anti-virus software. There were also two participants that did not respond to a prompt which was raised. These participants did not notice the generated FR prompt. When a UAC prompt is not triggered as the result of user's action, it is minimized in the task bar and may not be noticed.

Figure 2 shows from the prompts that were generated in the study, what portion were not noticed, consented to, or canceled. Since all participants used admin account on their laptop and did not change the default settings of UAC, they did not require to provide admin credentials on the prompts.

As mentioned before, 9 participants had disabled UAC. Table 6 indicates their reasons for doing so. We asked the remaining participants their rationales for responding to UAC

Reported Rationale	N=34			
	PartiallyCorrect		Incorrect	
	Consented	Canceled	Consented	Canceled
I always confirm without reading	0	0	10	0
If I initiated action raising prompt, I confirm it; otherwise I decide after reading	0	10	3	1
If I initiated action raising prompt, I confirm it; otherwise I cancel	0	0	5	0
I read & decide based on familiarity with the program	0	0	3	0
I read and decide based on the relevance of prompt with my current action	0	1	0	0
I always cancel Unverified prompts & confirm others	0	0	0	1

Table 7: Reported rationale for responding to UAC prompts and response to FR

prompts during their daily usage of computers. Below we contrast participants' reported rationales and their actual responses to the fake prompts of the user study.

Fake Random prompt (FR)

Of those who received FR, 61% (49% of all participants) consented to this fake prompt. Six percent did not notice it, as they were interacting with another application when the prompt was raised, and 33% canceled the prompt. Table 7 lists the participants' response to FR and their claimed rationale for responding to UAC prompts during daily computer usage. The response of all PartiallyCorrect participants matched their reported rationale for responding to UAC; they all canceled FR, although one canceled the prompt without reading it.

Only two Incorrect participants canceled FR; the rest confirmed it. The participants who stated they always confirm UAC prompts behaved as they reported. However, there was a mismatch between the behaviours and claims of those who said they read or cancel prompts that are not triggered as the result of their actions. Most of these participants (except one) consented to FR because they were in the context of downloading, installing and running an application; they did not recognize that the random prompt was not a result of their current actions. Also, those who claimed they read the prompt and decided their action based on their familiarity with the program, consented to FR. These participants also thought the fake prompt was related to the application they were downloading and did not read it closely.

Fake Installation prompt (FI)

The second fake prompt was FI which was raised during the installation of the text editor application. When the installation file ran, the first UAC prompt was a fake one with a name similar to the application and the second prompt was the real one. Of the 35 participants who viewed the FI prompt (9 disabled UAC and one system did not generate the FI), only 2 participants did not consent. One checked the details of the prompts and, since he got two, canceled the installation; he had stated that he consented to all the prompts. The other did not allow FI since he always cancels Unverified prompts. Therefore, most participants did not respond correctly to the UAC prompts when they initiated an action that triggered prompts.

We asked the participants who consented to FI how many prompts they expect to receive when installing an application. As shown in Table 8, 3 did not know how many prompts they should get and consented to FI to continue the installation, and 9 consented to FI since they expected to receive 2 or more prompts during single installation. Although 21 participants expected to receive one prompt, they consented to two consecutive prompts; their reasons for confirming FI are shown in Table 9.

	WV	W7	Total
Did not know	2	1	3
One prompt	12	9	21
Two or more prompts	8	1	9

Table 8: Participants' expectations of the number of prompts to be raised when installing an application

Reason For Confirming	WV	W7	Total
Did not know	6	2	8
Continue the installation	2	6	8
Do not notice the difference between two prompts	3	0	3
The first click was not received by computer	1	0	1
Always confirm	0	1	1

Table 9: Participants' reasons for confirming FI

4.1.3 Opinion about UAC prompts

We asked participants whether they found UAC annoying, and whether they would disable it or not (Table 10). Most PartiallyCorrect participants did not find UAC annoying. They appreciated giving permission before changes were made to the system and being informed if someone tries to install something on their system. Only 21% preferred to disable UAC; they were confident that their expertise, their use of security software, and their performance of regular back-ups kept their systems secure.

On the other hand, more than half of the Incorrect participants, found the prompts annoying and preferred to disable them. They gave several reasons, such as having an awareness about their own actions, having a lack of awareness about the purpose of prompts, interference with troubleshooting of their PC, UAC having the same functionality as anti-virus, the time consuming activity of responding to prompts, and a preference for automating the UAC functionality by operating system. The rest of the Incorrect participants did not complain about UAC because they treated it as a part of the procedure of doing an action (e.g. installation or configuration), or they believed the prompts are

		WV		W7		Total	
		N=30	%	N=15	%	N=45	%
Annoying	PartiallyCorrect	2	25	2	33	4	28
	Incorrect	13	59	6	66	19	61
	All	15	50	8	53	23	51
Prefer to Disable	PartiallyCorrect	1	12	2	33	3	21
	Incorrect	11	50	5	55	16	51
	All	12	40	7	46	19	42

Table 10: Number of participants who found UAC annoying and preferred to disable it

User Account Details		N=45
Number of user accounts	One	39
	Two	5
	Four	1
Guest Account	Enabled	0
	Disabled	45
Main user account	Password protected admin	36
	Admin without password	9

Table 11: Number of participants with various user account settings on their laptops

Non-admin account usage		N=45
Did not know		12
Not used		5
Only used on home computer		5
Used Guest	Public computer	10
Used Standard	Family computer	4
	Work computer	7
	School	2

Table 12: Participants' experience with using non-admin accounts (not on their current personal computer)

beneficial because of protection they offer through monitoring the correctness of their actions. However, these participants did not take advantage of this security mechanism as all allowed the fake prompts.

4.1.4 Difference Between Windows Versions

We asked the 14 W7 participants who had experienced Windows Vista UAC prompts about the difference between UAC prompts in Windows Vista and 7. Of the 5 PartiallyCorrect participants, 4 noticed the decrease in the number of prompts and 1 other appreciated the ability to tune the settings. The Incorrect participants did not recognize any change, thought the number of prompts had increased, or did not remember the prompts in Windows Vista. Four participants had disabled UAC in Windows Vista; 3 of them did the same in Windows 7, and 1 changed the settings so that the screen was not dimmed.

4.2 LUA Practices

In this section we present participants' knowledge about the types of user accounts, their rationales for using various account types on their system, their prior experience with user account creation, the result of the user account creation task, their experiences with using low-privilege user accounts, and the challenges they face in using such accounts. The results reported in this section include both Windows Vista and Windows 7 participants.

All of our participants used an admin account, and most were not aware of the security risk of high-privilege user accounts or the benefits of low-privilege ones. Many created a standard account in the user study task, understanding the sufficiency of such account for daily tasks and having concerns about the unwanted changes that can be made by an admin account. However, none were motivated enough to use a standard account for their own daily usage.

4.2.1 Knowledge about user account types

Our participants' knowledge about the differences between user account types was limited to the capabilities and rights of each account type. Most did not show any understanding of the security risks and benefits.

When we asked participants about the difference between admin and non-admin accounts, thirteen did not know the difference; the others mentioned various differences such as admin being able to modify the system (26), manage other users' rights (9), and have more control on the computer (6). Moreover, two said that if an application is installed by the admin account, non admin accounts cannot access it.

We also asked whether participants were aware of any security risk associated with using an admin account; most (36) were not aware of any risk. Of the rest, 5 were aware of the possibility of applying inappropriate changes by themselves when using admin accounts; and 4 were aware of the feasibility of unwanted and unknown changes by a malicious user. However, both groups preferred to use an admin account for convenience, choosing to keep their system secure by performing regular backups and using security software.

4.2.2 User account usage experience

Most participants did not have any experience with a non-admin account on their own computer, however, most had experienced them in public and workplace settings. Table 11 shows the current user account settings on participants' laptops. All participants used the default admin account, whether or not they installed the OS themselves. We probed the 32 participants who knew their account type for their reasoning for using an admin account. Three participants did not why(3); the others mentioned different reasons, such as having complete access to change everything (17), being unaware of any benefits of using an account of another type(10), owning the computer (6), being the only user of computer (5), having a need to log on and log off if using a non-admin account (5), admin being the default option (3), and being unaware of non-admin accounts (1).

We also asked participants about the type of user accounts

User Account Creation		N=45
Familiarity with the procedure	Familiar	36
	Unfamiliar	4
	Partially familiar	5
Created user account type	Standard	32
	Guest	8
	Admin	1
	Not done	4

Table 13: Number of participants who created different user account types in the user study task

they have used on their own previous home computers. Except for five participants, all used admin accounts or did not remember their account type. Two of these five participants were Linux users who used a non-admin user account to avoid applying wrong and accidental changes on their systems. Two others quit using non-admin accounts due to the inability to install applications. The fifth was a developer who created a standard account to test developed software.

Most participants did not use a non-admin account on their own computer. However, they have used it on public or workplace computers (Table 12). These participants either complained about the inability to install software (8) or were satisfied because they used the account for only a few tasks (8). Some (3) of those who used a non admin account in the workplace preferred to have fewer privileges so that IT-admin can control things; however, they preferred to use an admin account on their home computer.

4.2.3 User account creation task

Most participants appropriately created a low-privilege (standard) user account in the user study task, understanding that daily computer activities do not require any high-privilege user account (19) and that a low-privilege account can not apply unauthorized changes on their system (21). Also, some (15) were aware that a high-privilege user account should be used by knowledgeable and trusted people for administrative tasks, and some (12) knew that a high-privilege user account may apply undesired modifications to their system. Despite such understandings, none of our participants used a non-admin account on their own laptops.

Table 13 shows the results of the user account creation task. Our participants mentioned various reasons for choosing the account type such as guest or standard accounts being sufficient for browsing the Internet and using email and Microsoft office (19), avoiding any application installation or unwanted changes on their systems (17), avoiding giving the same level of control as their own to somebody else (4), using the default option (2), preserving their privacy (5), not needing more than one admin account (2), and not being able to create a second admin account (1).

We asked participants about the situations in which they would create an admin account. Nine did not know whether they would ever do so. Fifteen indicated that they would create such an account for a person who is trusted (4), needs to install software or perform an administrative task (6), or has an appropriate level of knowledge (4). Sixteen participants would not create an admin account for anybody because of concerns about incorrect changes to their systems (3), fears that their account might be deleted (3), having control on their computers themselves (6), and being concerned about the competence of the new user (1). Two thought that their system could not have two admin accounts; and one preferred to share his account instead of creating a new one.

User Account Type	System	User	N
Not Done	-	-	21
Provide details for admin in start up	Home computer	Personal	7
Admin	Home computer	Family member	3
	Work computer	Colleague	3
Non-admin	Home computer	Family member	5
	Home computer	Personal	3
	Work computer	Colleague	2
	Work computer	Personal	1
Guest	Home computer	Family	3

Table 14: Prior user account creation experience

4.2.4 Prior user account creation experience

We asked participants about their prior experience with user account creation (Table 14). Half the participants had such an experience, and all but one applied a correct rationale when selecting the user account type. This participant created an admin account because he was unaware of the non-admin account type. Six participants had created admin accounts for family members or colleagues. This was either to share the computer (5) or due to their lack of awareness of non-admin accounts (1).

Five participants created non-admin accounts on their own home computer for family members for various reasons such as preserving their privacy, avoiding unwanted changes, and the limited requirements of their family. Two created non-admin accounts on their office computers so that colleague could perform a few tasks (e.g., printing). One participant, a developer, created a standard account to test some software. Only three participants had created non-admin accounts for their own usage. While one quit using a non-admin account due to the inability to install programs, the others (Linux users) still used it.

5. DISCUSSION

Because the UAC approach and low-privilege user accounts rely on users making security decisions, users should be supported in making such decisions. Our analysis and discussion reveal how effective the UAC and LUA approaches were in communicating security-related actions to participants, and whether participants were able to comprehend these communications and respond to them correctly. We also discuss how participants' personal variables and motivation influenced their behaviours in using these security mechanisms. Finally, we discuss how well the PLP is followed by participants using the LUA and UAC approaches.

5.1 User Account Control

We found that at least 69% of participants did not employ the UAC approach correctly because 20% disabled the UAC prompts, while using admin accounts, and 49% consented to a fake random prompt.

Communication delivery

The UAC approach is communicated to users by prompts. To be successful in communication delivery, users should notice UAC prompts and pay attention to them in order to process the prompts. UAC prompts were effective in capturing our participants' attention as all but two participants noticed the prompts raised during the user study. However, many participants did not carefully consider the UAC prompts and respond to them correctly when they were in the context of installing or running an application, especially when they had initiated the action themselves.

Comprehension and application

The majority (77%) of participants had an incorrect understanding of the purpose of the prompts. This incorrect understanding left their laptops vulnerable to security breaches, as all of these participants (except the one who canceled and the two who did not notice the prompt) consented to the fake random prompt. Although some of these participants did give a partially correct rationale for responding to UAC prompts, they failed to apply the rationale when responding to the prompts during the user study. When these participants were in the context of performing an action (e.g., downloading, running, and installing an application; changing settings), they consented to the prompts. In contrast, those participants who exhibited at least a partial knowledge of UAC, had developed a correct response rationale and demonstrated it by canceling the fake random prompt during the study.

Therefore, understanding a security mechanism can lead users to apply it successfully. We found that there is a strong correlation between "partial understanding of UAC" and "safe response to the fake random prompt" ($p < .001$, Fisher's exact test).

Personal variables and motivations

Our participants' computer expertise impacted their understanding of UAC and their responses to its prompts. Those who did not confirm the fake random prompt had a high (58%) or medium (42%) level of computer expertise. We found that knowledge does play a role, but it still does not guarantee safe actions as 22% of participants with a high level of expertise consented to the fake random prompt.

We also found that understanding a security mechanism impacts users' motivation for applying that mechanism. Most of the PartiallyCorrect participants (79%) preferred to keep the prompts enabled while more than half of the Incorrect participants preferred to disable them.

Some other factors also impacted our participants' motivation for paying attention to UAC prompts. For example, the attitude of Windows 7 participants was impacted by their prior experience in Windows Vista as participants who disabled UAC in Vista followed the same approach in Windows 7. Also, users should not perceive that security mechanisms overlap with each other, otherwise they start to ignore one of them; some participants ignored UAC because they believed their anti-virus software can keep them informed about security risks. Moreover, although some Incorrect participants believed that UAC may keep their system safe, they consented to the fake random prompt.

5.2 Low-privilege User Account

None of our participants used a low-privilege user account on their Windows laptops. This shows that the LUA approach has not been effective in supporting users to follow the PLP.

Communication delivery

The low-privilege user account approach is not communicated to users. The use of LUA is only advised in the online documentation of Microsoft. Our results reveal that 91% of participants were unaware of this principle of computer security, and all used admin accounts on their systems. A failure in communication left many participants unaware of the benefits of using low-privilege accounts or the risks of high-privilege ones. Our participants' understanding of a low-privilege user account was limited to its restrictions in modifying and managing computer systems, and they perceived using a high-privilege account as a convenient way of working with their computer.

Comprehension and application

Most participants had a partial understanding of the differences between admin and non-admin accounts; 71% mentioned this understanding, and 87% demonstrated it by creating an appropriate user account in the user study task and providing a reasonable rationale for choosing the account type. Even though 42% understood that a low-privilege account is sufficient for most daily tasks, they did not apply this understanding to their own computer usage. Also, while 60% were aware that a high-privilege account allows them to make critical changes to the computer and should be used by trusted users for admin tasks, they could not transfer this knowledge to the potential for malware to compromise their system and perform critical changes on it.

Personal variables and intentions

Only four participants explicitly demonstrated an understanding of the security risks associated with using admin accounts. Three were participants with a high level of computer expertise and one had a medium level. However, they still preferred using admin accounts because of the ability to modify their systems easily. They were not motivated to consider using a low-privilege user account to avoid such security risks; instead, they relied on their expertise or use of security software.

Not surprisingly, we found that our participants' prior experience with low-privilege user accounts in different contexts appeared to impact their knowledge about these user accounts and their motivation to use them on their personal computers. Although 62% had prior experience with using low-privilege accounts, all but two of these participants (who were also Linux users) were not sufficiently motivated to use such accounts on their Windows PCs.

5.3 Principle of least privilege

Prior to the UAC implementation in Windows, users had to use LUA to follow the PLP. However, with the introduction of UAC, if users keep UAC enabled and respond to the prompts correctly, regardless of the type of their user account, they will follow the PLP. If they disable UAC, the type of their user account determines whether they follow or violate the PLP.

Our study shows how well the PLP was followed by our participants:

1. Violated: At least 69% violated the PLP. These are participants who either had disabled UAC and used an admin account (20%) or who consented to the fake random prompt (49%). We chose to use the response rate to the fake random prompt (instead of the fake installation prompt) to determine whether participants respond to UAC correctly in order to be more conservative. A higher bound would be 93% in violation because 73% of all participants (94% of those participants who received both fake installation and real prompt) consented to both the fake and real installation prompt.

2. Followed: Only 27% followed the PLP because they canceled the fake random prompt.

3. Can not be judged: 4% did not notice and respond to fake random prompt.

5.4 Recommendations

Based on the findings of our study, we offer the following recommendations to operating system developers for improving the UAC and LUA mechanisms.

Educational prompt – The UAC prompt should communicate its purpose and functionality to users so that they can respond to prompts correctly. Understanding a security mechanism motivates users to appreciate its benefits and to apply the correct response rationale in various situations.

Selective occurrence – The UAC prompt should include an appropriate level of intelligence to minimize its occurrence for requesting confirmation of actions initiated by the user. Otherwise, users start to ignore the prompts because of habituation.

Integrated solution – Users perceive UAC as an redundant solution because they believe their anti-virus or personal firewall provide the same security functionality. Users may reap a a greater benefit from security solutions if their functionalities are integrated so that misconceptions in security coverage do not arise.

Risk communication – The risks of high-privilege user accounts and the benefits of low-privilege ones should be conveyed to users; otherwise, users will not be motivated to follow the principle of least privilege by using low-privilege accounts for daily tasks.

Convenient usage – Using low-privilege user accounts should be convenient for users as they perform legitimate and informed actions on their PCs. Otherwise, they may quit using low-privilege accounts after facing restrictions.

Default settings – Although Microsoft advises users to create a non-admin account, the initial and only account created during OS installation is an admin account. In addition to this account, a low-privilege account should be created; users should be encouraged to use it for daily work.

6. LIMITATIONS AND FUTURE WORK

The goal of our research is to study the users' understanding, behaviour, and challenges in applying the PLP, which targets every end-user of computer systems. However, it is difficult to study a participant sample that represents the real user population. Participant recruitment was more challenging than usual. Some respondents to our recruitment notice were concerned about installing applications on their laptop; and middle-age people tended to use older laptops, which often had previous versions of the Windows operating system. Recruiting participants for Windows 7 was particularly difficult because it was not yet widespread in the general community; most respondents were computer science or engineering students who had upgraded their system to this operating system.

Currently our data is limited to Windows Vista and 7 participants. For future work, we aim to extend our study to other operating system users. To study a larger number of participants, we intend to conduct a survey to obtain information about users' knowledge and usage patterns of user accounts. While the number of user studies is limited, surveys can provide a large number of responses. Moreover, one part of the survey will be dedicated to UAC prompts including the users' understanding and rational for responding to these prompts. Running the user study helped us to design better survey questions. We will administer the survey to users of all operating systems. Comparing the results of the survey with the user study findings will help us to determine which aspects of our findings might be generalizable to a larger population.

We did not study people at their workplaces; because, in addition to the difficulty of recruiting people at their workplaces, their workplace user accounts are usually low-privilege due to the computer security policies of organizations. We are mostly interested in users' behaviour when they are not forced to follow any imposed policy.

7. CONCLUSION

Our user study and interviews with 30 Windows Vista and 15 Windows 7 participants provides a rich description of the practices of users in applying the principle of least privilege. Our analysis revealed the reasons why this privilege is often not followed by users. We studied users' motives, understanding, behaviour, and the challenges they face when they use two implementations of this principle: UAC and low-privilege user account. We found that 69% of our participants did not employ the UAC approach correctly as they either disabled it or consented to any UAC prompt that arose when they were in the context of doing an action, especially when they initiated an action themselves. Most participants had an incorrect understanding of UAC and responded to prompts incorrectly.

All our participants used an admin account on their laptop. Although 71% had a partial understanding of the limitations and rights of each user account type, 91% of participants were not aware of the security risks of high-privilege accounts or the security benefits of low-privilege ones. Also, while 62% had experienced a low-privilege user account, they were not motivated to use it on their own laptops because of the limitations they had faced using these accounts.

To improve the UAC and LUA approaches, we recommend conveying the purpose and benefits of them to users, raising UAC prompts in fewer situations, integrating UAC functionality with other security software, providing users with default low-privilege accounts, and making the use of low-privilege account convenient in order to ensure that users continue to use them.

8. ACKNOWLEDGEMENTS

We thank the members of the Laboratory for Education and Research in Secure Systems Engineering (LERSSE), at-

tendees of the ISSNet workshop, Cormac Herley, and anonymous reviewers who supplied valuable feedback on the research and this paper. This research has been supported in part by the Canadian NSERC ISSNet Internetworked Systems Security Network Program.

9. 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, A. B. Brush, and K. M. Inkpen. Family accounts: a new paradigm for user accounts within the home environment. In *CSCW '08: Proceedings of the 2008 ACM Conference on Computer Supported Cooperative Work*, pages 669–678, New York, NY, USA, 2008. ACM.

[3] S. Egelman, L. F. Cranor, and J. Hong. You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In *CHI '08: Proc. of the SIGCHI conf. on Human factors in Computing Systems*, pages 1065–1074, New York, NY, USA, 2008. ACM.

[4] 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.

[5] Gnu/linux post-installation checklist. http://www.linux.org/docs/ldp/howto/Post-Installation-Checklist/steps.html.

[6] S. Kim. Java web start: Developing and distributing Java applications for the client side. White paper, IBM Corp. Armonk, NY, September 2001. http://www.ibm.com/developerworks/java/library/j-webstart.

[7] An introduction to Mac OS X security. http://developer.apple.com/internet/security/securityintro.html, August 2004.

[8] 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.

[9] G. McGraw and E. W. Felten. *Securing Java: Getting down to business with mobile code*. John Wiley & Sons, 2 edition, 1999.

[10] J. Nielsen. Card sorting to discover the users' model of the information space. http://www.useit.com/papers/sun/cardsort.html, 1995.

[11] W. Poole. Financial Analyst Meeting. http://www.microsoft.com/msft/speech/FY05/PooleFAM2005.mspx, July 2005.

[12] Root definition. The Linux Information Project, http://www.linfo.org/root.html, October 2007.

[13] Rootsudo. Ubuntu Documentation, https://help.ubuntu.com/community/RootSudo, February 2010.

[14] C. A. Rusen. Windows 7 vs Windows Vista: the UAC Benchmark. http://www.7tutorials.com/windows-7-vs-windows-vista-uac-benchmark, August 2009.

[15] M. Russinovich. Inside Windows 7 User Account Control. TechNet Magazine, July 2009.

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

[17] 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.

[18] D. W. Stewart and I. M. Martin. Intended and unintended consequences of warning messages: A review and synthesis of empirical research. *Journal of Public Policy and Marketing*, 13(1):1–19, 1994.

[19] M. Stiegler, A. H. Karp, K.-P. Yee, T. Close, and M. S. Miller. Polaris: virus-safe computing for Windows XP. *Commun. ACM*, 49(9):83–88, 2006.

[20] M. Stiegler and M. Miller. A capability-based client: The DarpaBrowser. Technical report, Focused Research Topic 5. Combex, Inc., Meadowbrook, PA, June 2002.

[21] J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, and L. F. Cranor. Crying Wolf: An empirical study of SSL warning effectiveness. In *Proceedings of 18th USENIX Security Symposium*, pages 399–432, 2009.

[22] How Windows Vista helps protect computers from malware. TechNet Library, http://technet.microsoft.com/en-us/library/cc507865.aspx, September 2006.

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

[24] What's new in user account control. TechNet Library, http://technet.microsoft.com/en-us/library/dd446675(WS.10).aspx, June 2009.

[25] Some guidelines for securing your Windows Vista PC. http://download.microsoft.com, Security_Best_Practice_Guidance_for_Consumers.doc, 2007.

[26] M. Wogalter. Communication-Human Information Processing (C-HIP) Model. In *Handbook of Warnings*, pages 51–61. Lawrence Erlbaum Associates, 2006.

[27] M. Wogalter. Purpose and scope of warnings. In *Handbook of Warnings*, pages 3–9. Lawrence Erlbaum Associates, 2006.

[28] M. E. Zurko, C. Kaufman, K. Spanbauer, and C. Bassett. Did you ever have to make up your mind? what notes users do when faced with a security decision. In *ACSAC '02: Proceedings of the 18th Annual Computer Security Applications Conference*, pages 371–381, Washington, DC, USA, 2002. IEEE Computer Society.