Investigating User Account Control Practices

Sara Motiee
Department of Electrical & Computer Engineering
The University of British Columbia
Vancouver, BC, Canada
motiee@ece.ubc.ca

Kirstie Hawkey
Department of Electrical & Computer Engineering
The University of British Columbia
Vancouver, BC, Canada
hawkey@ece.ubc.ca

Konstantin Beznosov
Department of Electrical & Computer Engineering
The University of British Columbia
Vancouver, BC, Canada
beznosov@ece.ubc.ca

CHI 2010, April 10–15, 2010, Atlanta, Georgia, USA.
ACM 978-1-60558-930-5/10/04.

Abstract
Non-administrator user accounts and the user account control (UAC) approach of Windows Vista are two practical solutions to limit the damage of malware infection. UAC in Windows Vista supports usage of lower privilege accounts; a UAC prompt allows users to raise their privileges when required. We conducted a user study and contextual interviews to understand the motives and challenges participants face when using different user accounts and the UAC approach. Most participants were not aware of or motivated to employ low-privileged accounts. Moreover, most did not understand or carefully consider the prompts.

Keywords
Usable security, Least privilege, User account control

ACM Classification Keywords
H.5.0 Information Interfaces and Presentation:General; D.4.6 Software: Access controls, Invasive Software

General Terms
Human Factors, Security

Introduction
In 2005, it was said that 85% of computer users log in as an administrator [2]. This is convenient for users in terms of performing their daily activities; however, it also means that malware can install and run with administrative privileges. The *principle of least privilege*

Table 1: UAC Prompts Types based on executable's publisher

Publisher	Color
Windows Vista	Blue
Verified (Signed)	Grey
Unverified (Unsigned)	Yellow
Blocked	Red

Table 2: Task descriptions.

#	Description
T1	Download and install an application to play a DVD. We observed participants' decision process for selecting, downloading, and installing an application, including their response to the UAC prompt and other warnings and messages.
T2	Receive a USB key with a text editor installation file from a friend who recommends it. Installation of this application raised an unverified publisher UAC prompt.
T3	Download and install a specific spyware remover application, recommended by a security expert. This application raised a verified publisher UAC prompt.
T4	Create a user account for your brother who wants to use your laptop for tasks such as email, browsing and using Microsoft office.

[4] addresses this issue, requiring that only the most restrictive set of privileges possible for performing authorized tasks is granted. A practical implementation is a *least-privilege user account* (LUA) approach, which advises users to always log on to their systems with non-administrative user accounts [5]. While such accounts enhance security, they inconvenience users as many simple tasks (e.g., changing the system time) can only be done in an administrative account [6].

The goal of Windows Vista's User Account Control (UAC) [6] is for all users, including local administrators, to run with non-administrative privileges. Rather than requiring *standard account* users to switch to an administrator account when attempting a task that requires administrator privileges, a UAC prompt asks for the administrator username and password. Similarly, a *protected administrator* account user gets a UAC prompt to consent to the process elevation. There are four types of UAC prompts, color-coded (Table 1) to inform users of the potential security risk of an action (e.g., installing an application). Microsoft advises users [6] to think carefully when they respond to a prompt and to make everyone – even administrators - use passwords. As an administrator account is created during Vista installation, users are advised [6] to create a standard account after installation for daily use. However, it is not clear whether users apply these guidelines and follow the least privilege principle.

The usability of security warnings in web browsers has been the focus of recent research efforts [1]. For example, 66% of participants in a recent study [8] were fooled by a phishing attack and the security toolbars of their web browsers did not prevent this. However, we are unaware of any related work investigating the usability of least privilege user accounts and UAC prompts. The goal of our research is to study user account control behaviors as well as users' knowledge about this aspect of computer security. Our initial research investigates the approach of Windows Vista, including its least privilege user accounts and UAC approach. Once our future work studying the modified UAC approach in Windows 7 is complete, we will develop usability guidelines for systems that implement the least privilege principle.

User Study

We conducted a lab study, followed by contextual interviews. We designed our study based on Cranor's framework [1]. The framework proposes a question set to analyze the human factors associated with security indicators and identify areas of their potential failure. Our use of multiple methodologies mitigates the biases of any one approach. Conducting the interviews in the context of the study tasks decreases self-report biases. Since security is not the primary user task, evaluation tasks need to be carefully selected. As UAC prompts and user account management happen infrequently, we exposed participants to a set of predefined, controlled tasks. To increase ecological validity, we conducted the study on their personal computers, targeting laptop users that could participate in any public area.

Protocol

After giving consent and completing a background questionnaire, participants installed study software (from a USB key) to record their voice and screen. We also recorded their screen with a video camera, as the recording software did not capture the UAC prompts. The first part of the study investigated whether the UAC approach of Vista has been successful in prohibiting

Table 3: Participants' demographics

Demographics		**N=20**
Gender	Female	7
	Male	13
Student	Yes	17
	No	3
Age (years)	Range	18..50
	Mean	26.75
Education	Computer	1
	Engineering	5
	Other	14

Table 4. Number of participants who generated (G), viewed (V), accepted (A), and cancelled (C) the task (T1-T3) and fake (FC, FT) UAC prompts.

	T1	**T2**	**T3**	**FC**	**FT**
G	17	18	16	18	18
V	17	18	16	17	18
A	17	18	16	9	17
C	0	0	0	8	1

Table 5. Participants' criteria for downloading and installing applications.

Criteria	**N=20**
Reviews and comments	11
Free software	9
Known or trusted web sites	9
Features	5
File size	3

users from installing malicious software unknowingly. We asked participants to perform tasks that would raise UAC prompts on their laptops. To increase ecological validity, we did not provide detailed task instructions; instead, we exposed participants to three task scenarios (T1-T3, Table 2) and asked them to perform their usual steps. They were told that the goal was not task completion and that they could skip a task that they would not normally perform. As they performed these tasks, they were prompted with two fake UAC prompts. The first (FC), named "UpdateCache", was raised by an application installed without participants' notice (wrapped in the screen recorder installer). This unverified UAC prompt appeared 3 minutes after the screen recorder installation finished while participants were busy with downloading and installing applications. It allowed us to observe the response to an unexpected UAC prompt. The second fake prompt (FT) was shown during T2. When the text editor installation file ran, the first unverified UAC prompt was fake with a name similar to the application and the second one (also an unverified UAC prompt) was real. We observed how participants responded to prompts during installation, how many prompts they expected to receive, and whether they paid attention to the application name. Participants were then shown the video of their tasks and interviewed to probe their understanding of UAC in Vista. In particular, they were asked about the criteria they considered when downloading and installing applications, their knowledge of UAC prompts, the prompt's interference with their work, the different prompt types, and their rationale when responding to prompts faced during the study and in normal use.

The second part of the study investigated account usage and participants' knowledge of the least privilege user account approach. We did this second, so as not to prime participants to the purpose of the study during T1-T3. After completing a brief knowledge test about 3 user account types (Standard, Administrator, Guest), they were asked to create a user account (T4, Table 2). We observed their familiarity with user account management and their decision making process for account creation. We then interviewed them, probing their knowledge of account types, the account they use and reason for its usage, rationale for creating the account in T4, their experience with other user account types, and the challenges they face when using them.

Results

To date, we have analyzed the data of 20 diverse participants (Table 3). We created affinity diagrams using a card sorting approach to categorize responses.

UAC Prompts: Knowledge, Actions, and Opinions

Not all participants generated and viewed all the UAC prompts (Table 4). Two participants had disabled them. One, who was very cautious about downloading and installing applications, canceled T1 in the middle and did not start T3. Another, who did not regularly download and install, skipped T1 and T3. When asked about their decision making process during application download and installation, participants mentioned several criteria (Table 5). None mentioned considering the warnings of the operating system or browser.

Only 1 participant knew the term UAC, although all recognized the prompts. Based on participants' explanations of UAC prompts, we categorized them as having a partially correct understanding (PC_UAC) or incorrect understanding (IC_UAC). We also asked about the situations in which prompts appear (Table 6) and

Table 6. Number of participants who know the actions that raise UAC prompts

Group	Actions	N=20
PC_UAC	Install Application	4
	Install Application and Change Settings	4
IC_UAC	Install Application	7
	Incorrect Answers	5

Table 7. Number of participants who understand the difference between UAC prompts types

Understand Difference between UAC Prompts for Verified and Unverified Application		N=20
PC_UAC	Yes	0
	No	8
IC_UAC	Yes (Partially)*	3
	No	9
Understand Difference between UAC Prompts for Windows Vista and other applications		N=20
PC_UAC	Yes (Partially) +	2
	No	6
IC_UAC	Yes (Partially) +	3
	No	9

* Being potentially more dangerous, known or unknown for computer, and being a possible virus.

+ Application related vs setting change

the differences between prompt types (Table 7). The responses highlight the incomplete and often incorrect knowledge that users have of UAC. Eight participants in the PC_UAC group stated they confirm the UAC prompt if they have initiated an action (install or run a program, change settings) that raised the prompt; otherwise, they decide to confirm or cancel the prompt based on the program name. The response of this group to the FC prompt matched with their knowledge and rationale for responding to UAC prompts (all canceled it), although 1 canceled the prompt without reading.

Three of the 12 participants in the IC_UAC group stated that they always confirm the UAC prompts without reading and did the same for FC. One said he decides based on his familiarity with the program and another based it on his need for the application; however, the former confirmed FC without reading it and the latter ignored it. The rest (7) said they confirm the prompt if they are doing an action, otherwise cancel it (3) or decide after reading (4). Of these, 1 had disabled UAC prompts, 1 cancelled it, and the remaining 5 allowed the fake cache update. At first glance, this appears to show a mismatch between 5 participants' stated and actual behaviors. However, in 3 cases, because the participants were in the context of downloading and installing, they confirmed without reading. Another participant read the name, but thought his file system was going to be updated. Therefore, we observed only 1 mismatch between self-reported behavior and action.

Of the 18 participants who viewed the FT prompt, only 1 (IC_UAC) did not click "allow". He checked the details of the prompts and, since he got two, canceled the installation. The remaining 17 allowed the installation: 3 were not sure how many prompts they should get and always confirm the prompts; 6 said they did so because they expect to see two or more prompts during installation; 8 said they expected to see one prompt, but allowed the installation. From these 8 participants, 1 believed the second prompt appeared because his click on the first prompt was not received; and 1 thought both prompts were the same.

While half of the 8 PC_UAC participants found them annoying, only one disabled the prompts stating he prefers the risk of getting a virus to getting UAC prompts. The other 7 thought they were beneficial and appreciated giving permission before changes are made to the system and being informed if someone tries to install something on their system. A similar proportion (5/12) of those with incorrect knowledge (IC_UAC) found the UAC prompts annoying: 4 of these did not know what the prompts are for, while 1 said the prompts interfered with the troubleshooting of her computer. Of the 7 who did not find the prompts annoying, 2 just always confirm the prompts and 1 does not get many as he rarely installs anything. The other 4 said prompts are beneficial, but their reasons reveal that they do not understand the main purpose of the prompts. Only 8 participants knew UAC prompts can be disabled: 4 preferred to keep them for protection; 2 disabled them; 1 wanted to disable them, but his father wanted to keep the prompts; 1 had not yet searched for instructions on how to do so. One, who was unaware they could be disabled, was interested to learn how to.

Account Creation: Knowledge, Actions, and Experiences

We observed the types of accounts participants had on their laptops (Table 8); all used administrator accounts.

Table 8. Number of participants with various user account settings on their laptops.

Account Details		**N=20**
Number of Accounts	One	16
	Two	3
	Four	1
Guest Account	Enabled	0
	Disabled	20
Main User Account	Password Protected Administrator	16
	Administrator without Password	2
	Administrator without user name	2

Table 9. Number of participants who knew their account type and the differences between account types.

Knowledge		N=20
Know their Account Type	Yes	10
	No	10
Know Account Type difference	Yes	16
	No	4
Understanding of Account Type Differences		N=16
Administrator can install software & change settings but normal user cannot.		8
Administrator can do everything but normal user rights are limited		8

We asked if they knew their account type (Table 9). Of the 10 who did, we probed their reasoning for using an administrator account: 5 preferred to have full access, 1 was too lazy to switch to a standard account for installation, 1 believed he had to use an administrator account, and 3 did not know why. It is interesting to note that although 4 of these participants were aware of the security risks of using administrative accounts, they prefer to have full access. The other 6 participants had never considered creating another account and were unaware of the security reasons for doing so.

Table 10 shows the results of the account creation task. We asked the 16 participants who created guest or standard accounts their reasons for choosing the account type: 9 believed a guest or standard account is enough for the scenario tasks, 4 did not want anything changed on their system, 2 mentioned both reasons, and 1 said he did not require two administrator on his system. Only 2 had concerns about privacy. We asked participants for a situation in which they would create an administrator account and 11 said they would never do so: of those, 7 could not think of a reason one would be needed, 2 were afraid another administrator may apply incorrect changes to their systems, 1 was afraid his account might be deleted, and 1 thought his system could not have two administrators. The 9 that would create such an account would do so for a person who is trusted (2), needs to install software and knows more than them (4), or a troubleshooting technician (3).

Table 11 shows prior user account experience. Among those 3 who have only ever used administrator accounts, 2 said non-administrative accounts are inconvenient and 1 said, "it is obvious to use the highest account you can." Among those who have used non-administrator accounts, 8 have done so on workplace or school computers. While 5 of them faced difficulty (e.g., cannot install software), 3 were satisfied because of their limited usage of those computers. Two have used non-administrator accounts on their own systems; while one quit using a standard account because of the inability to install, the other preferred to be limited on his Linux system so as not to damage it.

Discussion

Because least privilege user accounts and Vista's UAC approach rely on users making security decisions, users should be supported in performing security functions. Our analyses, grounded in the human in the loop framework [1], reveal the ineffectiveness of the communication mechanisms of these approaches in conveying the correct security actions to users.

Although most participants (80%) exhibited some knowledge about user account types and created an appropriate non-administrative account for the task, all used an administrative account for their main account. A failure in communication left many participants unaware of the benefits of using low privilege accounts or the risks of high-privilege ones.

When UAC prompts are triggered, they often fail to communicate the risk and appropriate action. As with other security warnings[1], little notice is taken of them due to their frequency, the inability of users to comprehend the prompts, and lack of instructions in them. We found that knowledge does play a role, but did not guarantee safe actions. The UAC approach of Windows Vista was not effective in prohibiting silent installation of malware for the 60% of participants with an incorrect understanding about these prompts. When

Table 10. Number of participants who created different user account types in T4

User Account Creation		N=20
Familiarity with the procedure	Yes	13
	No	3
	Partially	4
Created Account Type	Standard	11
	Administrator	1
	Guest	5
	Not done	3

Table 11. Participants' experience is user account creation and non-administrative account usage

User Account Creation		N=20
Not done		10
Administrator	Home PC	4*
	Work PC	2
Guest (For family members)	Home PC	2
Non-Administrator	Home PC	1+
	Work PC	1
Non-Administrator Usage		N=20
Do Not Know		6
Not Used		3
Yes	Home PC	2#
	Work PC	8
	Other	1

+ 1 created during OS installation
* Created on Linux
# One is used on Linux

these participants are in the context of doing an action (download, run and install application or change settings), they confirm the prompts without reading them. It is encouraging that those participants who exhibited at least partial knowledge of UAC did not allow the fake cache update prompt. However, regardless of their understanding, 95% of participants allowed the potential malware installation that was bundled with a legitimate application. Education that focuses on encouraging users to read the prompts and be aware of their frequency and differences (85% were unaware of the different prompt types) may be helpful.

Both least privilege user accounts and UAC are examples of conflicts between security goals and the users' goals. Even those participants that were aware of the security risks associated with ignoring prompts or using administrator accounts often did not take the safe action. Their past experience with low-privilege accounts or UAC prompts influenced their attitude and beliefs about these security mechanisms.

Conclusion and Future Work

Our user study and interviews with 20 participants reveal reasons why the principle of least privilege is often not followed. Participants were not motivated to use lower privilege standard user accounts and most did not understand the UAC approach. As they did not carefully consider the raised prompts, most allowed the actions of the fake prompts raised during the study.

We are currently developing a survey to obtain statistics about user account control practices of all operating systems users. Comparing the results of the survey with user study findings will allow us to see which aspects of our study can be generalized to a larger population. Furthermore, we will extend our study to Windows 7 users to observe how recent modifications to UAC, which reduces the number of UAC prompts, have impacted user behaviors. By default, it prompts the user when a non-Windows executable asks for privilege elevation [3], but when a user changes Windows settings, he is not prompted. It is unclear how many users will modify the default settings, the extent to which this approach will reduce prompts, and whether it will encourage users to more carefully consider the prompts that they do see and to employ the least privilege principle in their account selection.

References

[1] Cranor, F. L. A framework for reasoning about the human in the loop. In *UPSEC '08* (2008).

[2] Poole, W. Financial Analyst Meeting, Senior Vice President, Windows Client, July 2005. http://www.microsoft.com/msft/speech/FY05/PooleFAM2005.mspx.

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

[4] Saltzer, J. and Schroeder, M. The protection of information in computer systems. Proc. of the IEEE, 63(9), 1278-1308, Sept. 1975.

[5] Steven A., Applying the Principle of Least Privilege to User Accounts on Windows XP, Microsoft TechNet Library, January 18, 2006.

[6] Some guidelines for securing your windows vista pc, 2007. http://download.microsoft.com/download/0/e/9/0e922c03-8537-482f-b57c-aa385b3dee20/Security_Best_Practice_Guidance_for_Consumers.doc

[7] Understanding and Configuring User Account Control in Windows Vista http://technet.microsoft.com/en-us/library/cc709628(WS.10).aspx

[8] Wu, M., Miller, R., and Garfinkel, S. Do Security Toolbars Actually Prevent Phishing Attacks? Proc. of CHI 2006, 601-610, April 2006.