# Towards Investigating User Account Control Practices in Windows Vista

## Sara Motiee, Kirstie Hawkey, Konstantin Beznosov

## Motivation

### Problem

Many users login to their computers using accounts with administrative privileges

Malware can install and run with administrative privileges

### Solution

Apply the Least Privilege Principle

Motivate usage of accounts without administrative privileges (Standard user account in Windows Vista)

## Research Questions

Are users inclined to use administrative accounts or non-administrative accounts? What motivates them to use one or the other?

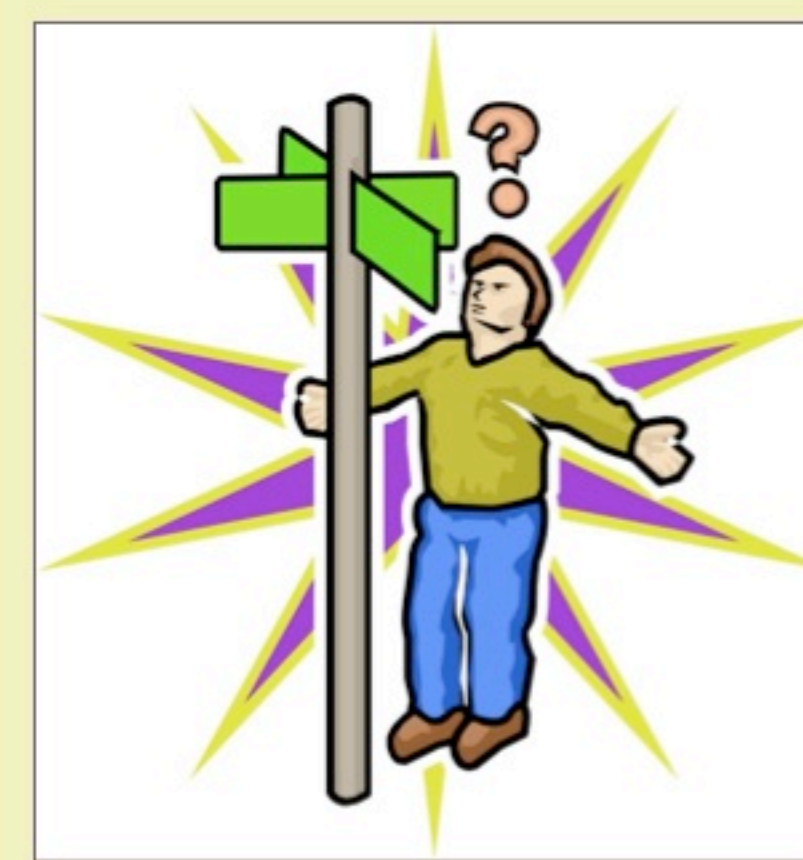What challenges do users face in using non-administrative accounts?
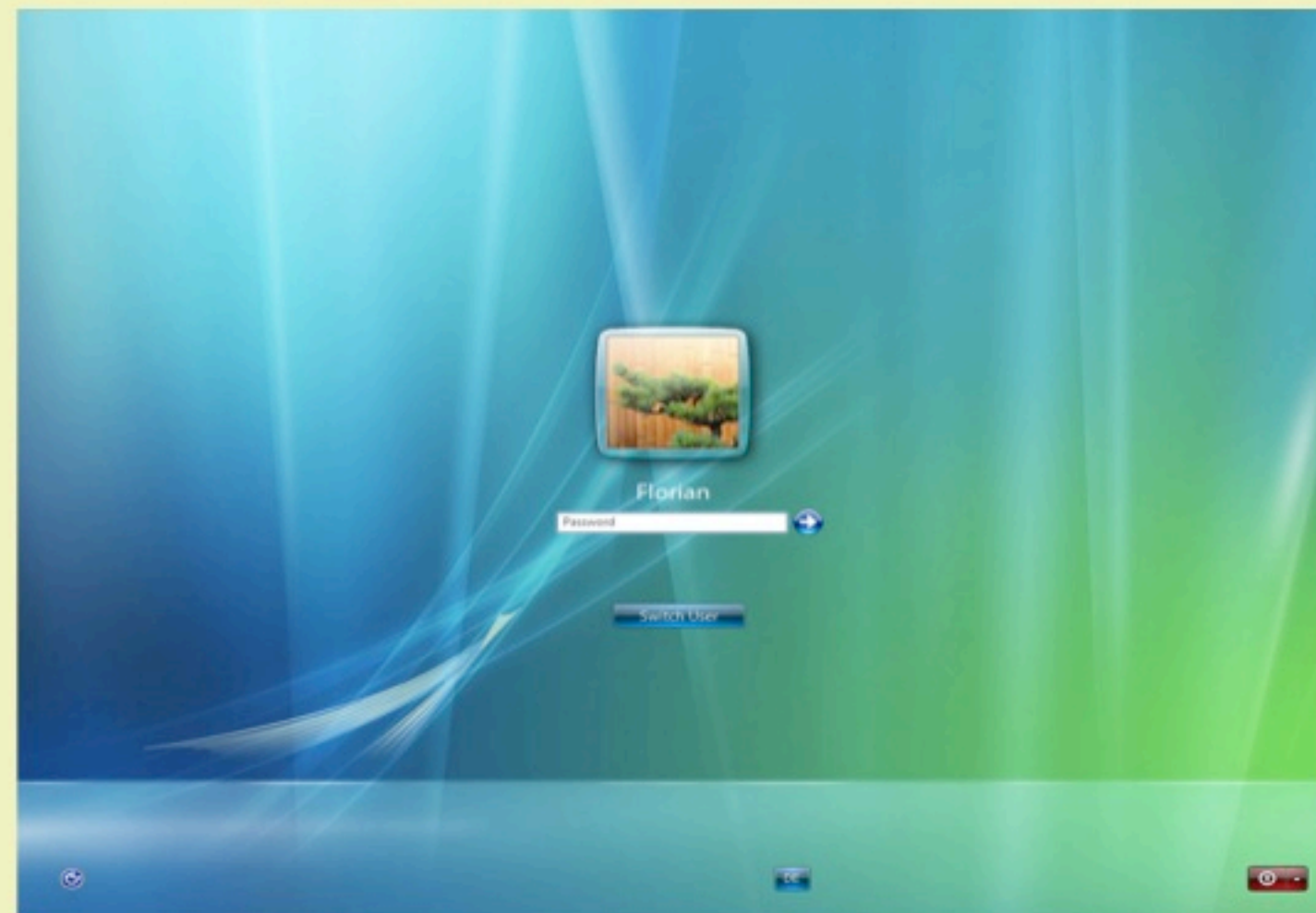
What are the patterns of account usage behaviour and how do they vary depending on the users' knowledge of security?

How successfully has Windows Vista supported the Least Privilege Principle?

### Initial Scope

- Windows Vista Users
- Home computer users with limited computer security knowledge

### Research Challenges

- The diverse range of users' behavior
- Security is not the primary task of users
- User account usage related behaviors happen occasionally and irregularly

## Methodology

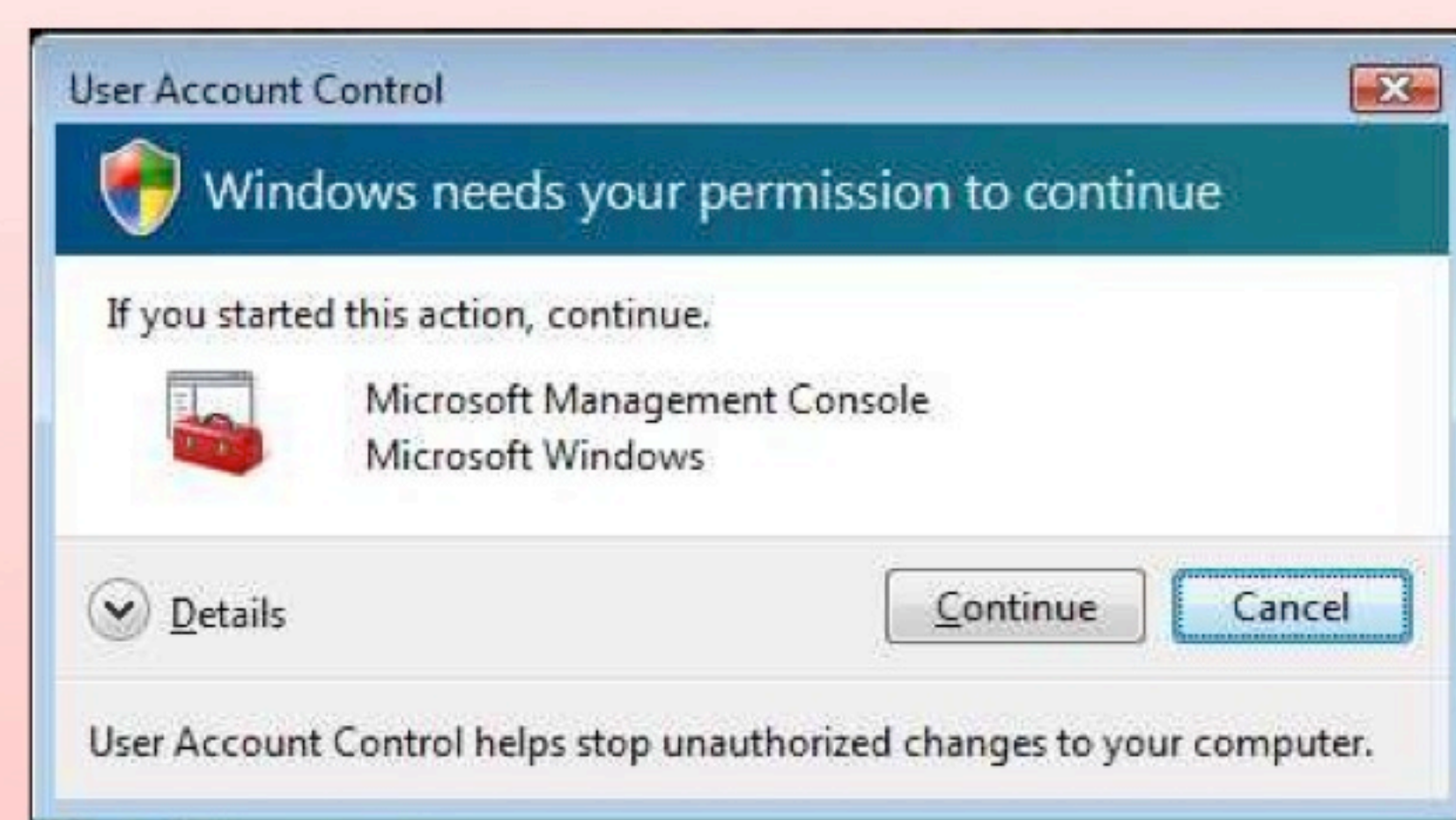### User Study followed by Contextual Interview

**User Study Goal:** Observe actual users behavior in using user accounts in a specific operating system

**Interview Goal:** Probe users' understanding about user accounts and administrative privileges

**Setting:** Laptop users in a laboratory environment working on their own computer
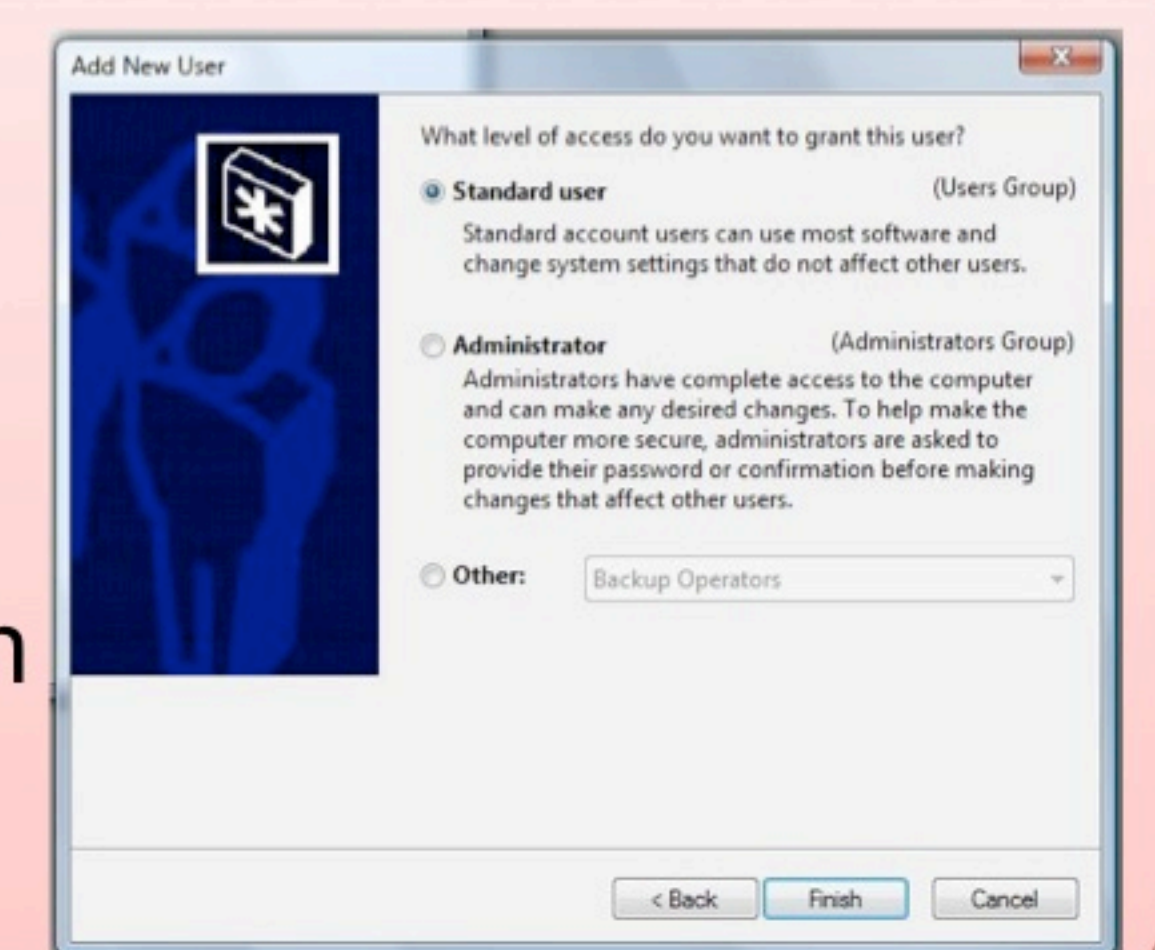
#### Series of tasks such as application installation and changing display settings

- Some tasks raise UAC prompt, some do not.
- A malware installation will be embedded in the task sequence
- Observe users behavior when they face UAC prompts
- Study whether users behave as advised by Windows Vista

#### Interview with technicians who install operating system

- User accounts are created during Windows Vista installation
- Investigate the standards followed in Windows Vista installation

#### Account Creation Task

- Investigate how users interact with account management interfaces
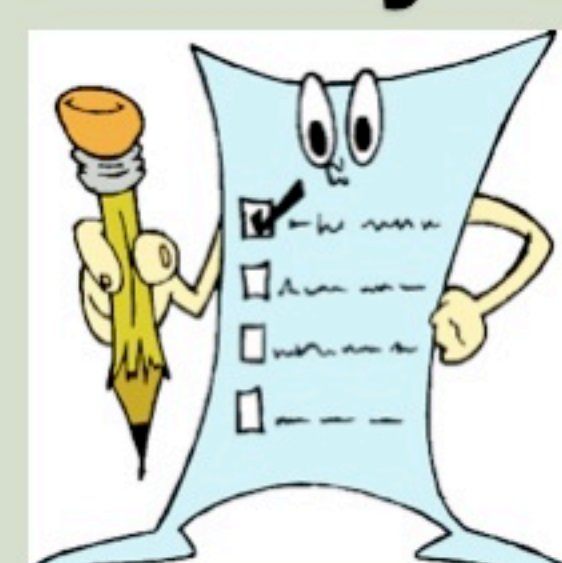- Determine the reasoning which leads users to the use of administrative accounts

#### Post-Study Interview

- Probe users rationale in doing actions during user study
- Determine users understanding of UAC prompts

## Survey

- Obtain overall knowledge about account usage patterns
- Determine usage patterns of non-administrative and administrative accounts

- Explore users' understanding and knowledge of user account types
- Expand scope to other operating systems