# Investigating Security-Related Behaviors Among Computer Users With Motor Impairments

John D'Arcy
Computer and Information Science Department
Towson University
001-410-704-4769
jdarcy@towson.edu

Jinjuan Feng
Computer and Information Science Department
Towson University
001-410-704-3463
jfeng@towson.edu

## ABSTRACT
In this paper, we describe a research-in-progress survey study that investigates security-related behaviors, especially password usage practices, among computer users with motor impairments that hinder the use of a keyboard and mouse. We focus on security behaviors in the workplace since they play a crucial role in users' employment opportunities and professional satisfaction. We envision that the study results will provide a better understanding of existing security practices (or lack thereof) among the target population as well as assist users and employers in developing more secure business practices and procedures. The results will also provide insights for future research in improving existing assistive technologies.

## 1. INTRODUCTION
A significant number of people have physical impairments that cause the loss of upper body motor functions [2, 8]. These impairments include spinal cord injuries, which can limit the use of hands or arms, and carpal tunnel syndrome, an injury that causes numbness or total loss of motor functions in the hands or forearms. Amyotrophic Lateral Sclerosis (ALS), arthritis, and brain injuries are also causes of upper body motor impairments [4]. Despite their physical disabilities, motor-impaired individuals continue to gain employment in various industries and across occupational categories [2]. Considering that computer systems now permeate the workplace, a significant challenge for these individuals, and the organizations that employ them, is that motor impairments make it extremely difficult, if not impossible, to operate a computer using the traditional keyboard and mouse input devices. Various alternative input devices are therefore required to assist motor-impaired users. These technologies include speech recognition software, hand or mouth stylus, eye or head controlled interaction software, etc [5].

From an information security perspective, the above assistive technologies pose potential security risks. A fundamental security mechanism in any information system is the ability to authenticate the identity of a system user, and by far the most commonly used method to achieve this is the password [1, 9]. In the case of speech-based input devices, a password authentication procedure requires the user to speak his/her password in order to access the system. This violates the main principle of password security – a password should exist in only the system and the user's mind [3]. In the case of the hand or mouth stylus, the user is limited to entering only one keystroke at a time, and therefore has difficulty entering capitalized letters and special symbols. Information security best practice advocates contend that "strong" passwords should consist of a combination of mixed or special characters, numbers, and upper and lower case letters. Hence, stylus users may be prone to using weak passwords due to the limitations of their input devices.

The preceding examples are representative of the security issues facing motor-impaired computer users. Understanding how both users and employers are dealing with such issues would provide a more complete picture of the current information security threat landscape, and could ultimately lead to solutions that reduce security risks among this user population. A review of relevant literature indicates that there is no research that has investigated security-related behaviors among computer users with physical disabilities. In this study, we attempt to fill this gap.

## 2. RESEARCH OBJECTIVE
We plan to empirically investigate the security practices of computer users with upper body motor impairments (i.e., limited or no use of hands or arms). The research will focus primarily on authentication procedures involving the use of passwords and users' password management practices. Awareness of security risks will also be examined. The intent of the study is to (1) understand the general security practices of the target population, and (2) to document the prevalence of user-related security risks among this population. The next phase of this research program will focus on technical and procedural solutions that can be used to reduce the identified security risks. In summary, we view the current study as a "stepping stone" that will serve as the foundation for a long term research program aimed at providing solutions that enable a usable yet secure computing environment for motor-impaired users.

## 3. METHODOLOGY
The study utilizes a survey for data collection. The survey development, construction, and administration is taking place in multiple stages following procedures described in [6]. Stage one has been completed, in which we reviewed the information security and assistive technology literatures and constructed a preliminary list of survey items. Stage two will consist of efforts to validate the survey instrument through a pretest and pilot test. The pilot test will be conducted on a convenience sample of graduate students enrolled in the Computer Science and AIT programs at Towson University. Statistical tests [e.g., 7] will be performed to confirm the reliability and validity of the survey, and modifications will be made if necessary. Stage three will consist of the final survey administration. A link to an online version of the survey will be delivered to participants via an email message. Individuals preferring a paper-based survey (due to their physical condition or otherwise) will be asked to provide their contact information, and will then receive a copy of the survey via postal mail. The target sample is a mix (in terms of age, gender,

computing experience, etc.) of motor-impaired computer users located across the United States. Our goal is to collect at least one hundred survey responses in order to conduct a valid statistical analysis. Several national organizations have been contacted and have offered their support in obtaining participants for this study. The final survey responses will be analyzed using various statistical techniques, such as correlation analysis and regression.

## 4. STUDY TIMELINE

We have identified the preliminary survey items and completed the preliminary survey draft. The preliminary survey contains the following sets of questions:

- General computer usage
- Computer password usage
- Attitudes toward password procedures
- Demographic information

The survey has been pilot tested by a sample of graduate students. We are currently pilot testing the survey with industry experts as well as users with upper body motor impairments. These results will be used to finalize the survey instrument. The final survey administration will take place in late June. We anticipate that some early data will be available to be reported at SOUPS 2006. The early results may not bear statistical significance, but will provide insights on the existing security practice of the target population. The security challenges identified may be of particular interest to the SOUPS audience and provoke valuable discussion.

## 5. RESEARCH SIGNIFICANCE

From the technical perspective, we envision that the study will provide a wealth of information on the security practices of motor-impaired computer users, which will enable the identification of security threats within this user population and provide directions for future research in improving existing assistive technologies as well as user interfaces.

From the social and management perspective, this study will help draw attention to the security risks posed by computer users with physical impairments – a severely understudied research area according to the literature. As such, this work extends the scope of both the information security and computer usability research streams. From an applied perspective, the results can be used to improve the security consciousness of motor-impaired users by helping them identify safer computing practices both within the workplace and for home use. The results will also provide employers with a better understanding of the security challenges that motor-impaired computer users present and provide insights into potential solutions that can be implemented to meet the special needs of this user population. These solutions may include increased security training, modified working arrangements, and use of biometric authentication technologies.

## 6. ACKNOWLEDGMENTS

This research is partially supported by a research grant from the Faculty Development and Research Committee at Towson University.

## 7. REFERENCES

[1] 2005 CSI/FBI Computer Crime and Security Survey, available at http://www.gocsi.com. 2005.

[2] National Spinal Cord Injury Statistical Center. The 2005 Annual Statistical Report for the Model Spinal Cord Injury Care Systems, available at http://images.main.uab.edu/spinalcord/pdffiles/facts05.pdf. 2005.

[3] Sasse, M.A., Brostoff, S., and Weirich, D. Transforming the Weakest Link – A Human/Computer Interaction Approach to Usable and Effective Security. *BT Technology Journal* 19, 3 (2001), 122-130.

[4] Sears, A. and Young, M., Physical Disabilities and Computing Technologies: An Analysis of Impairments, in J. Jacko and A. Sears (eds.) *The Human-Computer Interaction Handbook*. Mahwah, NJ: Lawrence Erlbaum and Associates. (2003), 482-503.

[5] Sears, A., Feng, J., Oseitutu, K., and Karat, C.M. Speech-Based Navigation During Dictation: Difficulties, Consequences, and Solutions. *Human Computer Interaction* 18, 3 (2003), 229-257.

[6] Sommer, R., and Sommer, B. A Practical Guide to Behavioral Research: Tools and Techniques. Oxford University Press, (2002).

[7] Straub, D.W., Boudreau, M.C., and Gefen, D. Validation Guidelines for IS Positivist Research. *Communications of the AIS* 13, 24 (2004), 380-427.

[8] U.S. Department of Labor, National Institute for Occupational Safety and Health, available at http://www.osha.gov/SLTC/ergonomics/resources.html. 2006.

[9] Zviran, M., and Haga, W.J. Password Security: An Empirical Study. *Journal of Management Information Systems* 15, 4 (1999), 161-185.