The User Privacy of Adaptive Assistive Technologies

Foad Hamidi, Kellie Poneres, Aaron Massey, Amy Hurst

Information Systems Department
University of Maryland, Baltimore County (UMBC)
Baltimore, MD, USA
{foadhamidi, kellie5, akmassey, amyhurst} @umbc.edu

1. A HUMAN-CENTERED APPROACH TO ASSISTIVE TECHNOLOGY PRIVACY

Adaptive assistive technologies monitor user activity and dynamically change their functionality and/or appearance to improve system usability [3, 4]. These systems provide a high degree of customizability, the importance of which is well-understood in the area of assistive technology where each user might have unique needs. Increasingly, these adaptive systems are connected to online servers that allow for the remote monitoring of user activity and for user data to be collected, aggregated and utilized to improve overall system functionality and performance.

While this connectivity offers opportunities for system usability improvements, it also opens up the possibility of a range of privacy threats that users inadvertently face when choosing to use these systems. This issue is amplified as the personal data collected by these systems might intersect with sensitive health data. In this context, users are generally not informed about the privacy threats of third-party access to performance data (such as pointing or keyboard input data). Given the prevalence and promise of these systems, we are studying the privacy tradeoffs that users face when choosing to use adaptive systems and ways to keep them informed about these tradeoffs.

We are focusing on older adults who experience variable, mild, or non-impeding difficulties when using a computer pointing device. These difficulties can be caused by health conditions such as Essential Tremors, the early onset of Parkinson's disease or other similar conditions. We focus on this population because individuals with Essential Tremors may be more sensitive towards the disclosure of their evolving health information, and because of the potential adverse effects on employment and access to computers.

To investigate these tradeoffs, we conducted a series of interviews with representative participants using a technology probe in the form of an interactive software prototype (described below) and a threat modeling analysis of adaptive assistive technologies that collect performance data.

1.1.1 PINATA: An Interactive Technology Probe

We developed a functional prototype of an adaptive assistive technology for use as a technology probe [3] to help participants experience using an adaptive system that can provide improvements in usability and accessibility at the cost of collecting personal performance data. *Pointing Interaction Notifications and AdapTAtions* (PINATA) is a software Internet browser extension that monitors users' pointing performance and dynamically adjusts the size and selection area of the on-screen cursor in response to pointing difficulties [4].

1.1.2 Threat Model Analysis

Threat modeling is a process for discovering, classifying, and evaluating the risk of threats from an attacker's point of view. It was originally developed and used for analyzing security threats but has been extended and applied to analyzing privacy concerns as well. We used a LINDDUN threat modeling framework [1] to identify several different types of threats in the context of adaptive assistive technologies, including: Linkability, Identification, Non-repudiation, Detectability, Disclosure of information, Unawareness, and Non-compliance.

1.1.3 Preliminary Results

Participants showed a positive attitude towards assistive technologies that gather their personal data but also had strong preferences for how their data should be used and who should have access to it. They also expressed privacy concerns that can be mapped to every threat category in the LINDUN model. We plan to continue this work to better understand user perceptions and attitudes towards the privacy threats of adaptive assistive systems in the future.

2. ACKNOWLEDGMENTS

This project is funded by a NIDILRR grant #-90DP0061-01-00.

3. REFERENCES

[1] Deng, M., Wuyts, K., Scandariato, R., Preneel, B., and Joosen, W. 2011. A privacy threat analysis framework: supporting the elicitation and fulfillment of privacy requirements. *Requirements Eng*, 16 (1), 3-32

[2] Hutchinson, H., Mackay, W., Westerlund, B., Bederson, B, Druin, A., Plaisant, C, Beaudouin-Lafon, M., Conversy, S., Evans, H., Hansen, H., Roussel, N., and Eiderbäck, B. 2003. Technology Probes: Inspiring Design for and with Families. In *Proc. of* CHI '03, 17–24.

[3] Lavie. T. and Meyer. J. 2010. Benefits and costs of adaptive user interfaces. Int. J. Hum.-Comput. Stud., 68 (8), 508-524.

[4] Martin-Hammond, A., Ali, A., Hornback, C., and Hurst, A. 2015. Understanding design considerations for adaptive user interfaces for accessible pointing with older and younger adults. In *Proc. of* W4A '15. Article 19, 10 pages.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2018. August 12 -- 14, 2018, Baltimore, MD, USA.