Usable Security and Privacy for Security and Privacy Workers

Mary Ellen Zurko | Massachusetts Institute of Technology Lincoln Laboratory
Julie Haney | National Institute of Standards and Technology

This special issue facilitates a dialog between researchers and practitioners toward informing the development of tools, techniques, and other support mechanisms that are valuable to security and privacy workers, leading to more usable, secure, and privacy-respecting solutions for end users.

Usable security and privacy research considers the human element of security and privacy: people's relationships with, perceptions of, and experiences during their interactions with security- and privacy-related processes, technologies, policies, and training. The ultimate goal of this research is to design systems, products, and services that are usable while also resulting in improved security and privacy outcomes.

Much usable security and privacy research has focused on improving the experience of end users, such as the general public or employees within an organization. However, another group represents an especially important—but often understudied—user population also needing support: the workers who develop, use, manipulate, and otherwise impact security and privacy information and technologies as a significant part of their jobs. Examples of security and privacy workers include but are not limited to the following:

- developers, who design and build software and hardware that manages and protects sensitive information and delivers critical functionality in a secure manner
- security and system administrators, who deploy and manage security-sensitive software, hardware, and cloud-based systems
- privacy engineers and other privacy professionals, who guide the development of new privacy products and features and assess and mitigate privacy risks
- analysts, who collect and analyze security and privacy data
- security and privacy consultants and educators, who provide guidance to individuals and organizations on practicing good security and privacy behaviors and implementing security and privacy technologies.

This special issue of *IEEE Security & Privacy* aims to highlight research of value to security and privacy workers as well as practices and case studies of security and privacy workers of value to researchers and other practitioners. We received 12 submissions to the special issue, with seven selected for publication after a rigorous peer-review process. The selected articles represent a wide breadth of usable security and privacy worker research using a variety of research methods.

Are you one of that broad swath of developers who do not have the time or resources to come up to speed on the details of usable security but see the need to be

Digital Object Identifier 10.1109/MSEC.2022.3221855
Date of current version: 19 January 2023

able to incorporate usable security considerations into your daily job of making tradeoffs for your product? In [A1], Gorski et al. provide a set of usable security principles for developers that can be adopted directly and immediately. The principles are informed by the authors' experience with developers and contain references to more specialized and comprehensive usable security principles, allowing readers with a particular interest in such principles to delve deeper into the topic.

For fans of puns in their titles, the "Building Security In" department of this issue features [A2], an article by Adam Shostack. Continuing the theme of lightweight, adoptable approaches, Shostack provides criteria for evaluating practices that aim at uncovering vulnerabilities, along with some short case studies of lightweight approaches to threat modeling.

In [A3], Weir et al. focus on the challenge of the communication gap between security specialists' advice and how development teams discuss and make decisions about security and privacy issues. The authors use a qualitative approach to produce both *security* and *privacy* definitions as well as themes related to security and privacy decision making from their interviews with senior software professionals from small companies creating health-related devices and services. The article provides an introductory example of qualitative analysis to readers unfamiliar with the methods as well as advice to security advisors on how to communicate with such a target audience.

Engineers of artificial intelligence (AI) and machine learning (ML) systems can be security workers, too! In [A4], Fazelnia et al. propose a framework that characterizes offensive and defensive security tactics, techniques, and tools for AI/ML-enabled systems. The goal of such an effort is to aid AI/ML engineers in incorporating security into the design of their systems from the start.

While software security has gained increased attention over the past few decades, building privacy into systems has been less emphasized, often leaving developers at a loss as to how to practically apply theoretical privacy frameworks. Enter [A5], which provides insights gained through a multiyear research effort to understand developers' challenges in implementing privacy protection within software. It recommends practical solutions for software development platforms and tool providers, organizations, educators, and regulators to better support developers in performing privacy-related tasks.

Further supporting the practical application of privacy concepts, [A6] provides a primer on a privacy definition and model that can aid security and privacy researchers and practitioners in understanding how and when privacy violations occur. Malkin further offers practical recommendations and examples on how contextual integrity can be applied to real-world situations to facilitate more privacy-respecting systems and processes.

Finally, we round out our special issue with [A7], which explores an important but often misunderstood privacy role within organizations. Based on an analysis of data protection laws and guidance, public case studies, and personal experience, the authors provide a rich description of data protection officer tasks, the problems and tensions they face, and their required skills and knowledge. These insights can inform security and privacy workers in their interactions with and support of data protection officers as well as researchers wishing to further investigate this role.

If you are a security or privacy worker, whether you've always known you are or are just discovering you are, we hope you find these articles interesting, useful, and beneficial.

Conducting research with and about security and privacy workers allows for discovering their work practices, challenges, and needs. These insights can inform the development of tools, techniques, and other support mechanisms that are usable and valuable to these workers in the course of their day-to-day work. Better supports for security and privacy work can, in turn, make products and systems more secure, more privacy preserving, and easier to use for the more traditional focus of usable security and privacy research: the general public and organizational employees.

If you are a security or privacy worker, whether you've always known you are or are just discovering you are, we hope you find these articles interesting, useful, and beneficial. As researchers in this area ourselves, we believe that dialog between practitioners and researchers is essential to impactful research. We are editors for this special issue to further that dialog and get research insights in front of the people they're supposed to help. We hope you can make use of this.

We thank the authors who submitted articles to this issue, every single reviewer who guided us in our final selections, and the *IEEE Security & Privacy* editors and staff—especially Sean Peisert (editor-in-chief); Terry Benzel (assistant editor-in-chief); Eric Bodden, Fabio Massacci, and Antonino Sabetta ("Building Security In" department editors); and Dustin Martinez (administrator)—for their guidance and support during the process.

Acknowledgment

Any opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Institute of Standards and Technology or the U.S. Government.

Distribution Statement A. Approved for public release. Distribution is unlimited.

This material is based upon work supported by the U.S. Department of the Air Force under Air Force Contract FA8702-15-D-0001. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the U.S. Department of the Air Force. ■

Appendix: Related Articles

[A1] P. L. Gorski, L. Lo Iacono, and M. Smith, "Eight lightweight usable security principles for developers," *IEEE Security Privacy*, vol. 21, no. 1, pp. 20–26, Jan./Feb. 2023, doi: 10.1109/MSEC.2022.3205484.

[A2] A. Shostack, "Nothing is good enough: Fast and cheap are undervalued as influencers of security tool adoption," *IEEE Security Privacy*, vol. 21, no. 1, pp. 78–83, Jan./Feb. 2023, doi: 10.1109/MSEC.2022.3223551.

[A3] C. Weir, A. Dyson, and D. Prince, "Do you speak cyber? Talking security with developers of health systems and devices," *IEEE Security Privacy*, vol. 21, no. 1, pp. 27–36, Jan./Feb. 2023, doi: 10.1109/MSEC.2022.3221616.

[A4] M. Fazelnia, A. Okutan, and M. Mirakhorli, "Supporting artificial intelligence/machine learning security workers through an adversarial techniques, tools, and common knowledge framework," *IEEE Security Privacy*, vol. 21, no. 1, pp. 37–48, Jan./Feb. 2023, doi: 10.1109/MSEC.2022.3221058.

[A5] M. Tahaei, K. Vaniea, and A. Rashid, "Embedding privacy into design through software developers: Challenges and solutions," *IEEE Security Privacy*, vol. 21, no. 1, pp. 49–57, Jan./Feb. 2023, doi: 10.1109/MSEC.2022.3204364.

[A6] N. Malkin, "Contextual integrity, explained: A more usable privacy definition," *IEEE Security Privacy*, vol. 21, no. 1, pp. 58–65, Jan./Feb. 2023, doi: 10.1109/MSEC.2022.3201585.

[A7] F. Ciclosi and F. Massacci, "The data protection officer: A ubiquitous role that no one really knows," *IEEE Security Privacy*, vol. 21, no. 1, pp. 66–77, Jan./Feb. 2023, doi: 10.1109/MSEC.2022.3222115.

Mary Ellen Zurko is a technical staff member at the Massachusetts Institute of Technology (MIT) Lincoln Laboratory, Lexington, MA 02420 USA. She has worked in product development, early product prototyping, and research and has more than 20 patents. She defined the field of user-centered security in 1996. She was the security architect of one of IBM's earliest clouds. Her research interests include authorization policies, high-assurance virtual machine monitors, code security, the web, and PKI. Zurko received an S.M. in computer science from MIT. Contact her at mez@alum.mit.edu.

Julie Haney is a computer scientist at the National Institute of Standards and Technology, Gaithersburg, MD 20899 USA, where she leads the Usable Cybersecurity program. Previously, she worked as a security practitioner at the U.S. Department of Defense for more than 20 years. Her research interests include the work practices of security professionals and the usability and adoption of security solutions. Haney received a Ph.D. in human-centered computing from the University of Maryland, Baltimore County. Contact her at julie.haney@nist.gov.