

Misalignments Between User and Developer Privacy Threat Models

Tianyi Shan, Mary Anne Smart, Jay Jhaveri, Jessalyn Wang, and Kristen Vaccaro
University of California San Diego

1 Introduction

Privacy is a broad concept with no universally agreed-upon definition, and problems can arise when developers and users hold different understandings of the meaning of privacy and of its value [2, 11]. Current approaches in privacy engineering are often limited by failures to account for the complex social interactions that occur between individuals [10]. They primarily focus on protecting user information from external threats such as hacking or unauthorized access, rather than addressing the dynamic nature of relationships over time and the potential for information to be shared within these relationships. For example, domestic and intimate partner violence has historically been overlooked by security and privacy (S&P) researchers [13], only recently receiving more attention by scholars [3, 4, 8, 14–16]. In our work, we aim to uncover similar gaps between the kinds of privacy threats that receive attention from developers and scholars versus the kinds of privacy threats perceived by various users of technology.

2 Methods

We propose to identify these gaps through an interview study based on the framework of privacy threat modeling. This approach prioritizes the proactive identification and mitigation of privacy risks in a system’s design and operation. We believe threat modeling is particularly effective for exploring individuals’ mental models of privacy, developing a more structured and parallel understanding than methods like diagramming [5]. This approach also aligns well with the dynamic and often unpredictable nature of privacy concerns.

2.1 Interview Protocol

While privacy threat modeling offers the opportunity to elicit directly parallel information from different groups, it has historically been a technical approach. Even methods that introduced lower thresholds, like the LINDDUN GO card-based approach, are still targeted at an audience of domain experts and professionals [18]. One challenge is that we aim to interview privacy experts, developers, but also everyday users. These different audiences will bring different kinds of expertise to the interview. But we must also ensure that questions can be answered by all. For example, we have updated the LINDDUN approach with questions like: *Can you think of*

any specific situations where organizations could connect different pieces of information about this person to create a more comprehensive understanding of them? Ongoing pilot interviews aim to ensure that the language in our interview protocol will be as accessible as possible for this diverse set of participants. We also aim to ease participation by streamlining the privacy threat modeling interview to 30 minutes.

2.2 Scenarios

We developed several different scenarios to use in interviews, all of which lend themselves to discussions of social factors such as cultural norms, social hierarchies, and the dynamic evolution of relationships over time.

1. **Photo Sharing.** We have chosen to include this scenario as it may pose threats to group privacy or bystander privacy [1, 19]—aspects that may be overlooked in threat modeling by security experts.
2. **Workplace Monitoring** We chose this scenario, because it deals with an imbalanced power structure that can lead to privacy violations. This complexity is not always addressed by security and privacy experts [9, 12, 17].
3. **Parent-Child Monitoring.** This scenario involves a unique relationship that also contains an imbalance of power. This topic has been studied in the realm of privacy stewardship in families [6, 7], but with little attention to the concerns of experts and developers.

3 Discussion

This project aims to understand whether the privacy engineering approaches may fail to adequately account for the intricate social dynamics among individuals. We make the assumption that security experts’ primary focus is on shielding user information from external threats, such as hacking or unauthorized access, may neglect the ever-changing nature of relationships and the potential for information sharing within these relationships. To address these issues, we’ve constructed a semi-structured interview protocol based on the threat modeling structure and specifically designed scenarios. We plan to conduct interviews with various groups, including users, developers, and security experts, with the aim to comprehend the gaps in understanding and approach among them.

References

- [1] Shane Ahern, Dean Eckles, Nathaniel S Good, Simon King, Mor Naaman, and Rahul Nair. Over-exposed? privacy patterns and considerations in online and mobile photo sharing. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 357–366, 2007.
- [2] Payal Arora. Decolonizing privacy studies. *Television & New Media*, 20(4):366–378, 2019.
- [3] Rahul Chatterjee, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diane Freed, Karen E. C. Levy, Nicola Dell, Damon McCoy, and Thomas Ristenpart. The spyware used in intimate partner violence. *2018 IEEE Symposium on Security and Privacy (SP)*, pages 441–458, 2018.
- [4] Sam Havron, Diana Freed, Rahul Chatterjee, Damon McCoy, Nicola Dell, and Thomas Ristenpart. Clinical computer security for victims of intimate partner violence. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 105–122, Santa Clara, CA, August 2019. USENIX Association.
- [5] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. “My data just goes everywhere”: user mental models of the internet and implications for privacy and security. In *Eleventh Symposium on Usable Privacy and Security (SOUPS 2015)*, pages 39–52. Ottawa, 2015.
- [6] Jess Kropczynski, Reza Ghaiumy Anaraky, Mamtaj Akter, Amy J Godfrey, Heather Lipford, and Pamela J Wisniewski. Examining collaborative support for privacy and security in the broader context of tech caregiving. *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2):1–23, 2021.
- [7] Priya Kumar and Sarita Schoenebeck. The modern day baby book: Enacting good mothering and stewarding privacy on facebook. In *Proceedings of the 18th ACM conference on computer supported cooperative work & social computing*, pages 1302–1312, 2015.
- [8] Karen Levy and Bruce Schneier. Privacy threats in intimate relationships. *Journal of Cybersecurity*, 6(1):tyaa006, 2020.
- [9] Alice Marwick. Privacy without power: What privacy research can learn from surveillance studies. *Surveillance & Society*, 20(4):397–405, 2022.
- [10] Alice E Marwick and Danah Boyd. Networked privacy: How teenagers negotiate context in social media. *New media & society*, 16(7):1051–1067, 2014.
- [11] Deirdre K Mulligan, Colin Koopman, and Nick Doty. Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 374(2083):20160118, 2016.
- [12] Shruti Sannon, Billie Sun, and Dan Cosley. Privacy, surveillance, and power in the gig economy. In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems*, pages 1–15, 2022.
- [13] Julia Slupska. Safe at home: Towards a feminist critique of cybersecurity. *St Antony’s International Review*, 15(1):83–100, 2019.
- [14] Julia Slupska and Angelika Strohmayer. Networks of care: Tech abuse advocates’ digital security practices. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 341–358, Boston, MA, August 2022. USENIX Association.
- [15] Emily Tseng, Rosanna Bellini, Nora McDonald, Matan Danos, Rachel Greenstadt, Damon McCoy, Nicola Dell, and Thomas Ristenpart. The tools and tactics used in intimate partner surveillance: An analysis of online infidelity forums. In *29th USENIX Security Symposium (USENIX Security 20)*, pages 1893–1909. USENIX Association, August 2020.
- [16] Emily Tseng, Diana Freed, Kristen Engel, Thomas Ristenpart, and Nicola Dell. A digital safety dilemma: Analysis of computer-mediated computer security interventions for intimate partner violence during covid-19. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–17, 2021.
- [17] Yanlai Wu, Yao Li, and Xinning Gui. “i am concerned, but...”: Streamers’ privacy concerns and strategies in live streaming information disclosure. *Proceedings of the ACM on Human-Computer Interaction*, 6(CSCW2):1–31, 2022.
- [18] Kim Wuyts, Laurens Sion, and Wouter Joosen. Linddun go: A lightweight approach to privacy threat modeling. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 302–309. IEEE, 2020.
- [19] Dorothy Zhao, Mikako Inaba, and Andrés Monroy-Hernández. Understanding teenage perceptions and configurations of privacy on instagram. *Proceedings of the ACM on Human-Computer Interaction*, 6(CSCW2):1–28, 2022.