International Journal of Computer Applications (0975 - 8887)
Volume 184 - No.47, February 2023

Security Workers are Users Too: A Novel Framework for Usability

Mrunmayee Khare
Carnegie Mellon University

Rajvardhan Oak
University of California Davis

ABSTRACT

Security workers are critical components of the security lifecycle. Be it researchers, engineers, content moderators, lawyers, privacy champions, all of them play an important role in keeping users and data safe. Most qualitative research in security-related areas has been user-centric; it has focused on identifying pain points and concerns for end users. Usability and perspectives of security workers have been largely ignored. In this paper, we provide a framework that can be used for worker-centric usability studies. Recognizing that security is a multi-faceted issue (ranging from highly technical aspects like cryptography to human-centric aspects like hate speech), we first develop a taxonomy for security workers based on where they lie on this spectrum and classify them into four levels. Because security as an end-to-end task requires coordination across all levels of workers, simply studying or interviewing workers from one level may produce biased results, and lead researchers to suggest solutions that are not practically possible. In order to address this, we present a novel methodology that can be used for effective qualitative research that can help in identifying not only pain points, but also produce actionable insights across multiple levels of security workers.

General Terms

Security Research, Security Usability, Security Framework

Keywords

Worker centric usability research, taxonomy, Cyber security, user perspectives, Worker usability research, Security risks

1. THE WOES OF SECURITY WORKERS

Usability for Security Workers is largely neglected Most research on usability in security focuses on the end user. There has been a strong impetus towards usability testing, qualitative investigations, understanding pain points, and identifying concerns that users have. Needs, perspectives, and usability concerns of workers in security have been largely ignored. As an example, the three premium security conferences: USENIX [1], IEEE S&P [2]and ACM CCS [3] have several accepted papers that discuss user perspectives, expectations on privacy, and experiences in security-related areas, but extremely few that deal with perspectives or issues from a security workers' point of view.

Usability for Users is different than Usability for Workers. This is because improved usability for users translates into quantifiable metrics for the product in terms of user acquisition, engagement, and opinions. Improved usability for security workers, however, has long-term effects that are harder to measure. This lack of focus on worker usability is counter-productive to usability for the end user; identifying pain points can help design better and more understandable mechanisms for threat intelligence and attack detection, which in turn leads to improved experience for users.

Security Workers are not Enemies of Usability. Much of user research in security tends to paint security workers as an enemy indirectly by pointing out flaws in existing systems [9] [14]. This is simply not the case; security workers also have the best interest of the user at heart. The perception arises because security workers must serve the (often conflicting) interests of two parties: the business and the user. While user privacy and usability are important considerations; they also need to bring in revenue for the company that employs them. As a result, they may be perceived to be acting in a way that is not necessarily in the best interest of the end user. In the case of security, a lack of usability often stems not from unwillingness of workers but organizational philosophy and belief of improving security through obscurity [13].

Usability for Workers is Security for Users. While largely ignored, usability is of utmost importance for cyber security workers. After all, workers are tasked with keeping data, systems, and people safe [11]. Improved usability leads to better design, faster investigation, and more effective mitigation. A tool that aggregates data over time periods and automatically produces insightful plots is more useful than a terminal window that allows querying data through SQL commands. Such a tool would lead to security analysts wasting less time on pulling data, errors, and code misses in scripts, and would be able to devote more time to analytical tasks. A tool that highlights potentially offensive words in red would help moderators make faster determinations on toxic content and policy violations. Ultimately, benefit to workers translates to benefit to end-users; the faster and more efficient workers are, the safer they can keep end users.

[1]https://www.usenix.org/conferences
[2]https://www.ieee-security.org/index.html
[3]https://www.sigsac.org/ccs/CCS2022/home.html

2. NOT ALL SECURITY WORKERS ARE EQUAL

Security is a broad area that spans highly technical issues [12] (such as encryption algorithms) to social issues (such as hate speech [6]). Workers working at different levels have different needs and pain points. Here we introduce a taxonomy that classifies security workers based on what part of this spectrum they work on.

Workers at the Data Level. At the data level, security workers are concerned with the nature of data and the manner in which it is stored. Examples of workers at the data level are software engineers, data engineers and datacenter technicians. The goal of workers at this level is to ensure the confidentiality, integrity, and availability of data. Their focus is on encryption mechanisms, patching hardware vulnerabilities, fault tolerance, backups and complying with standards and regulations for data retention. Security workers at the data level are responsible for securing the data, not the user.

Workers at the Information Level. At the information level, the data turns into usable. content (i.e., information). Examples of workers at the information level include privacy engineers, system admins and database administrators. The goal of workers at this level is to ensure that only authorized individuals have access to data. Their focus is on access control mechanisms, data classification standards and access policies.

Workers at the Application Level. At the application level, information is processed and presented in a form suitable for consumption by end users. An example of this is raw data about Facebook users being transformed into a list of top friend recommendations. Examples of workers at the application level are software engineers, data scientists, designers, and research scientists. The goal of workers at this level is to build systems for application security. Their focus is on building systems for a variety of tasks like malware analysis, supply chain attack detection, hate speech detection and anomaly detection.

Workers at the User Level. At the user level, individuals (the end users of the product) are experiencing the product. Examples of security workers at the user level are content moderators, lawyers working on privacy issues, and law enforcement officers who are investigating digital crimes. The goal of workers at this level is to act in the best interests of the users, protect users from digital crimes (scams, hate speech, fraud, extortion, identity theft) and ensure that users are being treated with respect.

3. SECURITY IS A TEAM ACTIVITY

Solving a particular security problem requires coordinated efforts by workers at all four levels. For example, consider the problem of detecting and removing illegal content from Twitter. Workers at the data level are responsible for storing tweets in data centers; they must be tamper-proof, complying with retention policies and accessible for further analysis. Workers at the information level must ensure that only authorized parties have access to non-public information about tweets (for instance, a marketing intern should not have access to identity verification details for a particular user account, or HR representatives need not have access to tweets with images of suspected child pornography). At the application level, researchers must explore novel methodologies in natural language understanding and machine learning to detect hate speech at a high precision and high recall. Workers at the user level need to manually examine flagged content and annotate hate speech.

This need for coordination across the four levels has important implications for usability research for workers that makes it significantly different than usability research for end users. When considering usability for the end-user, tests are a one-way street; developers and researchers collect user feedback and leverage it to improve user experience. [7] In the case of worker usability, the situation is not quite as straightforward. Usability testing for workers produces action items for other security workers (generally, at a lower level). Resolving these action items may in turn cause unintended consequences for workers at the next level. Continuing our previous example of hate speech detection, researchers at the application level may want unrestricted access to sensitive content to train machine learning models so that it helps them achieve a high precision. This is happening because workers at the information level may be reluctant to grant this access in order to follow the principles of least privilege and other best practices [10]. Even when the core issue is identified, the resolution is not straightforward. If researchers were indeed granted unrestricted access, it might lead to the use of privacy-invasive features and bias in their models; this would cause issues for lawyers and customer service representatives who have to deal with user complaints.

4. A FRAMEWORK FOR WORKER USABILITY RESEARCH

The goal of usability research with security workers is to improve worker experience, identify and address pain points. However, at the same time, we do not want to affect the security functionality. As we saw previously, improving developer experience with unrestricted data access should not come at the cost of end user privacy being invaded or the company facing a lawsuit due to non-compliance with regulations. Research that considers an issue in isolation is of little value since it does not translate to actionable insights. We propose a mixed method framework that combines both qualitative and quantitative approaches to identify pain points and mitigations.The goal of usability research with security workers is to improve worker experience, identify and address pain points. However, at the same time, we do not want to affect the security functionality. As we saw previously, improving developer experience with unrestricted data access should not come at the cost of end user privacy being invaded or the company facing a lawsuit due to non-compliance with regulations. Research that considers an issue in isolation is of little value since it does not translate to actionable insights. [5] We propose a mixed method framework [3] that combines both qualitative and quantitative approaches to identify pain points and mitigations.

The novelty of our proposed approach lies in the participant selection methodology; we leverage the taxonomy developed in the previous section to select participants from multiple groups, and obtain diverse perspectives that cover a broad range of issues relating to the problem.

Formalize your Problem and Identify the Target. As a first step, you should clearly define what the problem you want to solve is and determine the class of security workers it focuses on [4]. Based on these two factors, identify where they fall in the security worker taxonomy we introduced. Do you want to improve usability or identify pain points for content moderators (user level), data scientists (application level), network administrators (information level), or data engineers (data level).

Sample Participants from Three Levels. Once you have identified the level your primary target workers fall in, begin your recruitment. Traditional user research guidelines would recommend sampling participants randomly but uniformly to minimize extraneous factors so that your research draws upon perspectives from participants as similar as possible. That would mean simply recruiting workers from the level you identified in the problem space under consideration. While this will still enable you to understand worker perspectives, it would not consider the root causes behind issues or pain points, and possible fallouts if those issues were to be resolved. In order to have your research produce solutions and actionable insights, you need to recruit participants from three levels – your target level, and the ones before and after it. Participants must be treated with respect, following the principles of ethical research as laid down by the Menlo Report [1].

Research Instruments. Usability studies use several research instruments like surveys, interviews, user studies and focus groups. The methods chosen depend on the nature of the study and the underlying hypothesis. Our aim here is not to instruct on the various forms of usability study but to focus on the participants instead. Research instruments must be chosen appropriately depending on the nature of the study, but they should be applied to participants at three levels as described previously [2]. While analyzing the collected data (interview transcripts,survey responses, etc) treat each group of participants separately at first. Qualitative responses received as part of the interviews should be analyzed using open coding [8]. Codes must be identified for each level of security workers independently. It is a good idea for independent sets of researchers to work on coding each level so that any bias can be avoided. Irrespective of the survey instruments employed, conducting a focus group at the end with participants at all the three levels will help in identifying and discussing conflicting and overlapping themes and perspectives.

5. UNDERSTANDING CHALLENGES IN DETECTING MISINFORMATION: A USER STUDY

We will now discuss an example user study where we will demonstrate how our framework can be applied and the advantages it brings to the table.

Goal. Misinformation is a pressing problem on social media, and identifying misleading content is the need of the hour. Even with advances in machine learning and artificial intelligence, the detection mechanisms are still lacking in precision and recall. The goal of this study is to examine the challenges and obstacles in detecting misinformation on social media through the perspectives of data scientists and identify the reasons for the not-so-good performance of machine learning techniques in detecting misinformation.

Participants. The target group here is data scientists, meaning workers at the application level. Following the guidelines outlined in the previous section, we need to select participants from two other levels: the information level and the user level. We would naturally recruit data scientists working with misinformation detection models (our target group). From the information level, we would recruit system administrators analysts, and privacy engineers who work with the relevant information (such as user data, content metadata). At the user level, we would recruit content moderators who make decisions on posts reported as misinformation and lawyers that deal with the legal ramifications of content posting and removal.

Research Methodology. As discussed earlier, research instruments should be chosen based on the nature of the problem being studied. There are multiple techniques that could be applied here. A discourse on research methodology is not the focus here. Our study will begin with a set of semi-structured interviews with participants across the three levels. Beginning with the target group of application-level workers, we will identify the pain points and possible resolutions. Then, we will leverage the pain points and discuss the reasons for their existence in our interviews with workers at the information level. We will also leverage the consequences of having the pain points resolved and identify the effects it will cause during interviews with workers at the user level. After identifying key themes, we could conduct a survey to 'scale up' and validate our results. Finally, a focus group with all three – data scientists, system administrators or privacy engineers, and content moderators and lawyers could help identify conflicting themes and potentially reach a resolution that causes minimal harm to all the three levels.

Analysis. By having participants across three levels as opposed to only our target group, we will be able to examine diverse perspectives and derive conclusions more well-rounded than that which we would have in a traditional user study. Interviews with our target group will help identify the obstacles to better misinformation detection systems. This could be lack of specific kinds of data, such as user features at a very fine-grained level due to which reaching a higher precision is not possible. Having access to this data would potentially result in better systems, but interviews with privacy engineers at the information level might indicate that having such fine-grained information could be a violation of certain privacy regulations. Similarly, interviews with lawyers working at the user level may reveal that making decisions based on certain data may open up the platform to lawsuits in certain regions. Focus groups could foster an open discussion, where data scientists and privacy engineers could discuss the privacy-utility tradeoffs, as well as potential solutions like machine learning on encrypted data or differential privacy.

6. CONCLUSION

Most usability research in security has focused on users and not workers. Although workers have been largely neglected when it comes to usability, the issue is an important one because improved usability for workers can translate directly to improved security and experiences for end-users. Solving a security problem requires a coordinated effort by a multitude of security workers; each of whom have their own pain points and usability issues. Often times, security workers are responsible for pain points and issues for other security workers. Resolving these pain points is not straightforward – making things simpler for workers at one level can have unintended consequences for those at the other levels. We present a taxonomy of security workers based on whether they work for security at the data, information, application, or user level. To conduct a meaningful study, researchers should carefully determine where their target subjects fall in the security worker spectrum. We present a research methodology where researchers can sample participants from the target audience and two adjoining levels to collect diverse perspectives and understand the big picture.

7. REFERENCES

[1] Michael Bailey, David Dittrich, Erin Kenneally, and Doug Maughan. The menlo report. *IEEE Security & Privacy*, 10(2):71–75, 2012.

[2] Peter Birmingham and David Wilkinson. *Using research instruments: A guide for researchers*. Routledge, 2003.

[3] S Gerber Alan and P Green Donald. Field experiments and natural experiments, 2008.

[4] Marc Hassenzahl and Noam Tractinsky. User experience-a research agenda. *Behaviour & information technology*, 25(2):91–97, 2006.

[5] Kasper Hornbæk. Current practice in measuring usability: Challenges to usability studies and research. *International journal of human-computer studies*, 64(2):79–102, 2006.

[6] Shagun Jhaver, Sucheta Ghoshal, Amy Bruckman, and Eric Gilbert. Online harassment and content moderation: The case of blocklists. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 25(2):1–33, 2018.

[7] Paul C Jorgensen. *Software testing: a craftsman's approach*. Auerbach Publications, 2013.

[8] Shahedul Huq Khandkar. Open coding. *University of Calgary*, 23:2009, 2009.

[9] Tony Romm. Facebook ads push misinformation about hiv prevention drugs, lgbt activists say,'harming public health'. *The Washington Post*, pages NA–NA, 2019.

[10] Fred B Schneider. Least privilege and more [computer security]. *IEEE Security & Privacy*, 1(5):55–59, 2003.

[11] Filipo Sharevski, Adam Trowbridge, and Jessica Westbrook. Novel approach for cybersecurity workforce development: A course in secure design. In *2018 IEEE integrated STEM education conference (ISEC)*, pages 175–180. IEEE, 2018.

[12] William Stallings. *Network and internetwork security: principles and practice*. Prentice-Hall, Inc., 1995.

[13] Dafydd Stuttard. Security & obscurity. *Network Security*, 2005(7):10–12, 2005.

[14] Joshua Uyheng and Kathleen M Carley. Characterizing bot networks on twitter: An empirical analysis of contentious issues in the asia-pacific. In *Social, Cultural, and Behavioral Modeling: 12th International Conference, SBP-BRiMS 2019, Washington, DC, USA, July 9–12, 2019, Proceedings 12*, pages 153–162. Springer, 2019.