Poster: Ethics of Computer Security and Privacy Research - Current Status and Trends from a Data Perspective

Kevin Li
Blue Valley Northwest High School
Overland Park, KS, United States
kevinkli405@gmail.com,

Zhaohui Wang
Department of EECS
The University of Kansas
zhwang@ku.edu

Ye Wang
Department of EECS
The University of Kansas
yeah_wong@ku.edu

Bo Luo
Department of EECS
The University of Kansas
bluo@ku.edu

Fengjun Li
Department of EECS
The University of Kansas
fli@ku.edu

ABSTRACT

Ethics is an important criterion for security research. This work presents the current status and trends that security researchers have taken to address ethical concerns in their studies from a data perspective. In particular, we created a dataset of 3,756 papers published in three top-tier conferences between 2010 and 2022, among which 963 papers were identified with ethical concerns. With this dataset, we provided answers to three questions regarding the current practices and trends : (1) What is the landscape of ethical considerations in security research? For example, how many security research projects have raised ethical concerns in their studies, and which research areas are likely to cause ethical risks and concerns? (2) What are the current practices to address these ethical risks? And (3) What are the important factors impacting the ethical awareness of researchers?

CCS CONCEPTS

• **Social and professional topics** → **Codes of ethics**.

KEYWORDS

Computer ethics, Computer security

ACM Reference Format:
Kevin Li, Zhaohui Wang, Ye Wang, Bo Luo, and Fengjun Li. 2023. Poster: Ethics of Computer Security and Privacy Research - Current Status and Trends from a Data Perspective. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (CCS '23), November 26–30, 2023, Copenhagen, Denmark.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3576915.3624378

1 INTRODUCTION

Ethics is an important criterion for security research, as the techniques, methodologies, and outcomes may pose potential ethical risks (e.g., privacy concerns, unknown vulnerabilities). However, compared to other disciplines such as health and biology, ethics guidelines and regulations for security and privacy research have been developed slowly. In 2012, the US Department of Homeland Security published the Menlo Report [1] to provide ethical guidelines for Information and Communications Technologies (ICT) research. Since then, the security research community has started to raise awareness of security ethics. For example, the USENIX Security Conference included an ethics requirement in its call for papers [6] in 2013 for the first time.

However, it is a challenging task to achieve ethical compliance due to several reasons. For example, ethical guidelines for security research are highly abstract, while professional support from researchers' institutions is sometimes limited or missing. The researchers often take an ad hoc approach when analyzing ethical risks or rely on other organizations such as Institutional Review Boards (IRBs) to perform risk assessment for them. There is an increasing need to systematically study ethical concerns in security research and develop useful guidelines. For example, the IEEE Symposium on Security and Privacy in its recent call for papers [5] announced a new research ethics committee (REC) to review papers containing potentially "ethically fraught research" and required researchers to discuss methods and guidelines for responsible disclosure of vulnerabilities and address the ethical considerations of human subjects research.

In this work, we studied the common ethical concerns in security research and the approaches taken by security researchers to address or mitigate them from a data perspective. We have collected a dataset of 3,756 security literature published in three top-tier conferences and analyzed the landscape of the existing ethical considerations in security research, the current mitigation practices, and the factors that impact researchers' ethics awareness.

2 DATA COLLECTION AND ANALYSIS

We collected a dataset of security literature published in three top-tier security conferences and extracted statements expressing how the ethical concerns were addressed by the researchers. Results from analyzing this dataset shed light on the current practices and trends in addressing ethical considerations in security research.

Data Collection: We studied security literature published in three top-tier security conferences: ACM Conference on Computer and Communications Security (CCS), IEEE Symposium on Security and Privacy (S&P), and USENIX Security. Considering the release of

CCS '23, November 26–30, 2023, Copenhagen, Denmark

ACM ISBN 979-8-4007-0050-7/23/11.
https://doi.org/10.1145/3576915.3624378

the Menlo report in 2012 and the first call for papers with explicit ethical requirements in USENIX Security in 2013, we collected papers published in the three conferences between January 2010 and December 2022 to observe the impact of these guidelines.

We built a Python scraper using BeautifulSoup [3] and Selenium to download PDF files from conference webpages. In total, we collected 3,756 papers (i.e., 872 in IEEE S&P, 1,236 in USENIX Security, and 1,648 in ACM CCS). We subsequently converted them into text files using the Xpdf converter and then identified a set of ethics-related keywords, e.g., "ethic", "IRB", "responsible disclosure", etc., to filter the text with potential ethical statements. This resulted in 963 (25.64% of 3,756) papers. We manually reviewed their ethical statements and confirmed that 819 of them discussed ethical considerations and solutions. We also randomly selected 20 papers from the entire dataset and the manual review confirmed that all the ethical statements were indeed identified by our keyword filter.

Data Analysis. We extracted ethical statements and documented the title, keywords, areas (e.g., ACM CCS concepts), publication time, and venue of the related papers as well as the sessions in which they were presented. Then, we identified 10 general research areas[1] based on our understanding of security literature. We manually categorized 819 papers into 10 topics according to their keywords and session titles. Finally, we extracted the IRB status (i.e., IRB approval or IRB exempted) and the responsible disclosure status of the projects from their ethical statements. This provides useful implications for their ethical risk mitigation approaches.

3 MAIN FINDINGS

The landscape of ethical considerations in security research. We first calculated the number of papers that raised ethical concerns in each venue between 2010 and 2022. Figure 1 shows a consistent upward trajectory in the proportion of these papers (the blue bar) across all three conferences, which indicates an increasing awareness of ethical risks in security research by individual researchers.

Next, we computed the percentage of papers with ethical considerations in each research area. As shown in Figure 2, research in "User", "Authentication", and "Network" topics stands out with high percentages across all three conferences, followed by the "Web" and "Attack" topics. Notably, an average of 80% of the papers classified under usable security and user studies integrated ethical considerations. Conversely, Software, Crypto, and ML topics exhibit smaller percentages (e.g., below 20%) across three conferences. The results indicate that most of the ethical concerns have been raised when the research involves human subjects to ensure voluntary participation and protect them from potential harm. This aligns with the ethical principle of "respect for persons" identified in the Menlo Report and the practices typically involved in an IRB review in the researchers' institutes.

The studies requiring large-scale experiments such as in some "Network" or "Web" security topics, or interacting or tampering with real-world systems such as in some "Authentication" and "Attack" topics also express ethical concerns that need to be addressed or

[1]The topics are *machine learning* (ML), *cryptography and applied cryptography* (Crypto), *network and communications security* (Network), *Internet and web security* (Web), *software security* (Software), *system and application security* (System), *privacy and anonymity* (Privacy), *authentication and access control* (Auth), *attacks, cybercrimes, and forensics* (Attack), and *usable security and user study* (User).

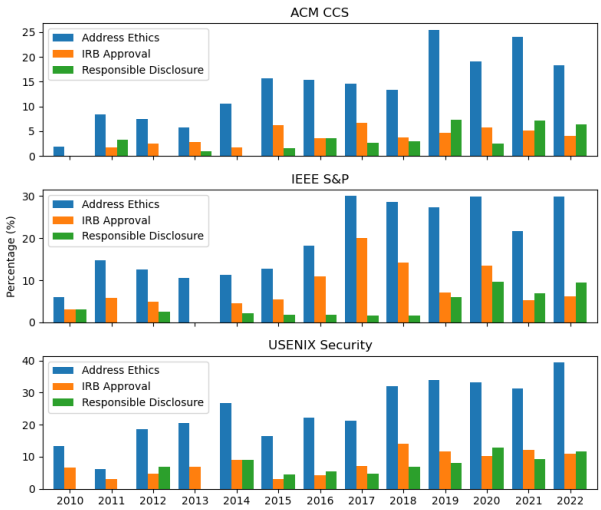

Figure 1: Percentages of papers that addressed ethics, obtained IRB approvals or provided responsible disclosure.

mitigated. Finally, research in "Crypto", "ML", and "System" topics often focus on theoretical designs or are carried out in controlled environments and therefore raise comparably low ethical concerns.

Besides, we have observed spikes and fluctuations in Figure 1, even in recent years. This can be in part attributed to topic-specific ethical concerns and the variation of topic distributions in the conferences over the year. In Figure 3, we visualized the topic distributions of the papers published each year in three conferences, respectively. The topic distributions vary significantly in all three conferences. For example, IEEE S&P published more papers on "User", "Web", and "Crypto" topics than in past years, while ACM CCS published more "Privacy" papers and fewer "Crypto" papers in 2021. It is also interesting to see that the first spike of machine learning security papers occurred in 2016. Since then, research in this area has demonstrated continuous growth. Meanwhile, topic distributions across the three conferences also vary. For example, IEEE S&P and USENIX Security have published more papers on the "System" topic, whereas research in cryptography and its applications has been an important part of ACM CCS. However, the proportion of system papers in USENIX Security varies over the year, ranging from 9.4% to 54.5%.

The topic distribution difference across the conferences and over the years has shown a non-negligible impact on the number of papers with ethical statements published in security conferences. For example, the rate of ethical considerations at IEEE S&P experienced a sudden decline in 2021, which could be attributed to the absence of papers related to User studies in that year.

Finally, it is worth noting that our observations shed light on the landscape of ethical concerns recognized and considered important by researchers in three venues. The percentages in the topics may change if data from other conferences is included in the study.

Current practices for mitigating ethical risks: Many researchers look towards the Menlo Report as a high-level guideline for conducting research ethically. Among the 819 papers with ethical statements, 21 (2.6%) of them explicitly mentioned the Menlo Report when discussing their ethical considerations, while many others

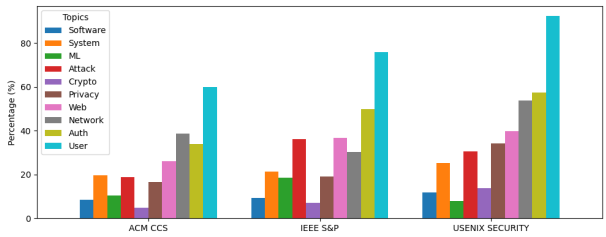

Figure 2: Percentages of paper with ethical considerations in ten security research topics.

indirectly followed the core principles of the Menlo Report, i.e., *respect for persons*, *beneficence*, *justice*, and *respect for law and public interest*. In particular, 25 papers mentioned that they obtained informed consent from their participants by the *respect for persons* principle, while 8 papers evaluate the benefits of their research along with the associated risks following the *beneficence* principle. A few papers mentioned the steps they took to ensure that all their participants were treated equally, indicating consideration of *justice*. 15 papers about privacy research discussed their compliance with the EU's General Data Protection Regulation (GDPR), showing *respect for law and public interest*. Interestingly, the papers mentioning the Menlo Report, whether directly or indirectly, all fell under the area of usable security and user study. This indicates a wide use of the Menlo Report to guide ethical designs of security research involving human subjects.

We also observed that obtaining IRB approval stood out as a significant approach for addressing ethical concerns, as illustrated by the orange bars in Figure 1. Ethics statements in 331 (40.4% of 819) papers explicitly mentioned practices of applying for approvals from institutions' IRB committees or similar organizations. Among them, 258 (77.9%) papers received IRB approval, while the rest either obtained IRB exemption or decided IRB approval was not required. On one hand, the increasing use of IRB review to assess and address ethical considerations in security research shows researchers' awareness and willingness to mitigate ethical risks. On the other hand, we want to point out that the ethics guidelines provided by university IRB policies are mainly directed toward medical research. As a result, they can provide useful guidance to experiments and studies involving human subjects but are still limited in ethics-related regulations for security research.

Another common approach to mitigate potential risks caused by a security study to individuals, systems, organizations, and society is responsible disclosure, which reveals the discovered vulnerabilities to relevant parties and proposes mitigation suggestions. We found that 206 (25.2% of 819) papers mentioned responsible disclosure practices before publication. As shown in Figure 1 (i.e., the green bar), there have been significant increases in responsible disclosure in all three conferences over the years.

Factors impacting researcher awareness: Our data shows that the percentage of papers surged, particularly when comparing the first two years to the recent two years, with an increase of 3-4 times, which shows an increase of ethical awareness in the security research community. However, there is no clear clue to relate it to the release of ethical guidelines, such as the Menlo Report, which may be attributed to two reasons: the slow start effect and the lack of detailed guidance in applying abstract principles.

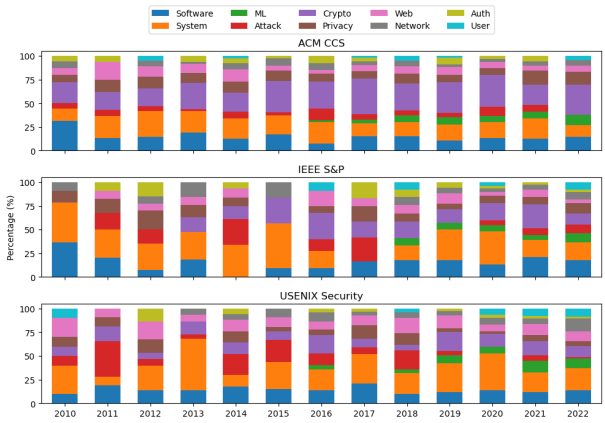

Figure 3: Topic percentage in different conferences and years.

However, our results showed that conference guidelines had a substantial impact on boosting ethical awareness. When conferences introduced guidelines concerning ethical considerations, there was a noticeable surge in the percentage of papers addressing ethics (spikes in Figure 1). For instance, the USENIX Security Conference, IEEE S&P, and ACM CCS first included a statement emphasizing ethical considerations in their call for papers (CFP) in 2013 [6], 2017 [4], and 2018 [2], respectively. While USENIX Security and CCS experienced a delayed response in the following year, the CFP of IEEE S&P prompted a more immediate increase in the same year. The subsequent decline following these spikes indicates that ethical considerations were not fully matured at the moment. As a result, the authors were inclined to adhere to new requirements by including ethical considerations and removed some non-essential concerns after reevaluation in the subsequent year.

4 CONCLUSION

From 2010 to 2022, there has been an upward trend in the number of papers with ethical concerns at top-tier security conferences, indicating an increasing awareness of the potential risks that security researchers should mitigate. Our results show that research in usable security, user studies, authentication, network and Web security, attacks, and privacy topics have raised more ethical concerns than studies related to cryptography and its applications or the security of machine learning models, software, and computer systems. Besides, we observed an increasing number of papers seeking IRB approval and performing responsible disclosures. The risk assessment and mitigation approaches taken by the researchers are highly influenced by the explicit guidelines of the security conferences.

REFERENCES

[1] Michael Bailey, David Dittrich, Erin Kenneally, and Doug Maughan. 2012. The menlo report. *IEEE Security & Privacy* 10, 2 (2012), 71–75.
[2] ACM CCS. 2018. ACM CCS 2018 Call for papers. https://www.sigsac.org/ccs/CCS2018/papers/
[3] Leonard Richardson. 2007. Beautiful soup documentation.
[4] IEEE S&P. 2017. 38th IEEE Symposium on Security and Privacy Call for papers. https://www.ieee-security.org/TC/SP2017/cfpapers.html
[5] IEEE S&P. 2023. 44th IEEE Symposium on Security and Privacy Call for papers. https://sp2023.ieee-security.org/cfpapers.html
[6] USENIX. 2012. 22nd USENIX Security Symposium Call for papers. https://www.usenix.org/conference/usenixsecurity13/call-for-papers