Ethics in Security Research: Visions, Reality, and Paths Forward

Yiming Zhang*, Mingxuan Liu*, Mingming Zhang*, Chaoyi Lu*, Haixin Duan*†✉

*Tsinghua University, China †QI-ANXIN Technology Research Institute, China
{zhangyim17, liumx18, zmm18, lcy17}@mails.tsinghua.edu.cn, duanhx@tsinghua.edu.cn

***Abstract*—Ethics has become a prevalent and important criterion for academic research. However, achieving ethical compliance in practice is a highly complex and specialized task. In the field of computer security research, although top-tier conferences all have set out visions for ethical compliance, researchers may encounter practical dilemmas such as the lack of assistance from legal departments and the absence of specific domain guidelines, leading to various realistic obstacles to ethical treatment.**

This paper provides a comprehensive investigation of ethical considerations in computer security research. We first summarize the ethical requirements of top-tier security and network conferences. Then, based on a survey of 6,078 academic papers and an online investigation of 248 researchers mainly from a Chinese security community, we reveal the current status and practical issues of ethical considerations in security research. In particular, given the plight of the lack of authoritative ethical guidance, we offer a series of suggestions on how researchers at institutions without authoritative departments could best mitigate ethical risks. We also raise several open questions, and expect to help seek paths towards better ethical compliance for the security community.

***Index Terms*—Ethical Considerations, Security Research, Institutional Review Board**

1. Introduction

Security research has become an increasingly popular area in both academic and industrial worlds of computer technology. The scale of the security community, including the number of security researchers and projects, is in rapid growth. However, considerable research methodology (e.g., infiltration studies) and outcomes (e.g., the discovery of unknown vulnerabilities) potentially bring harm to both humans and computer systems. As a result, it has been increasingly recognized that security researchers should perform their studies under ethical principles. In recent years, several top-tier security conferences have made explicit ethical requirements in their Call for Papers (CFPs), and failure in adhering to the principles can be grounds for rejection.

In the scope of computer security, it has been difficult to define concrete principles about what research is ethical. There are several well-acknowledged ethical guidelines such as the Belmont Report [16] (published in 1978, for biomedical research) and the Menlo Report [23] (published in 2012, for information and communication technology research). However, the reports only provide outlined guidance (e.g., *beneficence* in the Belmont Report) and leave practical instructions (e.g., how to practically fulfill *beneficence* in network probing experiments) undeveloped. Alternatively, to get assistance in addressing ethical concerns and mitigating risks, researchers may consult specialized departments established by their institution, such as an institutional review board (IRB). However, in practice, many institutions have not yet established such ethical departments, leaving security researchers themselves to make ethical decisions. As a result, security researchers often end up with one question: *how may we address ethical concerns in security research, especially when authoritative departments as IRBs are not available?*

This paper provides a survey on ethical considerations in computer security research. We begin by describing "visions", i.e., the ethical principles expected by major security conferences. Through reviewing historical CFPs, we depict the evolving timeline of ethical requirements. We then investigate the "reality", i.e., how are security researchers understanding ethical principles and addressing ethical concerns. The task is made possible through filtering of 6,078 academic papers published at 5 top-tier conferences, as well as a user study involving 248 researchers. Finally, we make recommendations to "paths forward", on how security researchers should adhere to ethical principles.

Our study suggests a positive outcome: an increasing percentage of published security papers are discussing how their experiments comply with ethical principles. However, only less than 40% of them receive professional guidance, and our user study confirms a shortage in the establishment of such specialized departments. From the results, we also summarise how researchers may address ethical concerns when departments like IRBs are not available, including referring to best practices of previous work, proactively seeking all possible legal advice, designing experiments carefully with experienced experts, and describing ethic-related experimental steps as clearly as possible in the paper. We also raise several open questions, such as the specific ways to establish ethical guidance for fine-grained research fields, and give preliminary discussions.

2. Ethics Required by Security Conferences

From the CFPs, we first summarise the history and development of ethical requirements from academic conferences. To begin with, we consider five top-tier and representative venues from the computer security and network academia: IEEE Security and Privacy (S&P), USENIX Security Symposium, ACM Conference on Computer and

✉ *Corresponding author*

Figure 1. Timeline of ethical requirements made by top-tier conferences.

Communications Security (CCS), ISOC Network and Distributed System Security Symposium (NDSS) and ACM Internet Measurement Conference (IMC). For each conference, we download and manually review their historical CFPs to look for requirements about research ethics.

Figure 1 depicts the timeline of ethical requirements from the 5 top-tier conferences. Starting from its CFP in 2009 [7], ACM IMC is the first conference that explicitly required authors to discuss ethical considerations in their submissions, particularly on how they process privacy data and report vulnerabilities. The remaining four conferences had all made explicit ethical requirements in their CFPs by 2017. According to their latest editions, all five security conferences have decided that failure in properly addressing ethical considerations can be grounds for rejection.

Since the initial and cursory descriptions in the CFP of IMC 2009, ethical requirements by security conferences have been evolving for over ten years and nourishing general principles. Below we summarise three of them that have become practical consensus across security conferences [8], [31], [37], [49]:

- **Human subjects research**. Studies involving human subjects, either directly (e.g., experiment on human subjects) or indirectly (e.g., processing data from human subjects), should state whether they have received approval from the ethical institutional review boards (IRB) of the authors' institutions. Research of this kind should avoid putting humans at risk to the extent possible, and explain how their methodology can protect humans from being affected by the experiments.
- **Protecting private data.** Studies that process personally identifiable information (PII, e.g., human names and network addresses) or other sensitive data should adopt concrete methodology (e.g., proper anonymization) that mitigates risks of data breaches. Research of this kind should also follow policies about data sharing (e.g., by only processing private data on designated machines that are disconnected from the public Internet).
- **Vulnerability disclosure**. Studies that identify software and hardware vulnerabilities pose potential harm to the corresponding users, if the attack methodology is maliciously exploited. As a result, authors are obligated to report the vulnerabilities to vendors and leave sufficient time (generally 45 to 90 days [6], [58]) for the problems to be fixed before publication of their research.

Apart from the general principles, some security conferences also emphasize on particular perspectives of ethical considerations. Submissions to these venues should also fulfill these requirements in order to be accepted. To name a few, IEEE S&P has been requiring authors to state both financial and non-financial competing interests since 2021 [37], [38], and ACM makes ethical regulations for computing professionals that apply to all of its sponsoring conferences [13]. Starting from 2022, ACM IMC is requesting IRB approval/exemption documents for all submissions involving human subjects [8]; if no author's institution has an IRB, the authors are then required to explicitly explain how their work meets the ethical principles outlined by ACM [14].

We also find that a growing group of other security conferences also make similar ethical requirements in their recent CFPs, including IEEE European Symposium on Security and Privacy (EuroS&P) [36], International Symposium on Research in Attacks, Intrusions and Defenses (RAID) [48], the Annual Computer Security Applications Conference (ACSAC) [4] and IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) [34]. Ethical discussions are also increasingly requested in submissions to artificial intelligence (AI) conferences, including the Association for the Advancement of Artificial Intelligence Conference (AAAI) [15], the International Joint Conference on Artificial Intelligence (IJCAI) [32], the Conference on Empirical Methods in Natural Language Processing (EMNLP) [18] and the Conference on Computer Vision and Pattern Recognition (CVPR) [33]. On the other hand, several conferences have not yet made ethical requirements in their latest CFPs, such as the European Symposium on Research in Computer Security (ESORICS) [35]. As a result, submissions to these venues may fall short in ethical considerations.

3. Ethical Solutions in Security Research

According to the CFPs of major conferences, compliance to ethical principles (or even explicit approval from an IRB) is becoming a prerequisite for security research to be accepted. As a result, it becomes urgent and necessary for computer security researchers to determine whether their studies raise ethical concerns, as well as gain knowledge on how to properly address them.

This section sheds light on the status of ethical solutions in security research from two perspectives. We first present an extensive survey on published security literature, to understand how they successfully fulfilled ethical requirements. Further, we perform a user study involving 248 participants, including security researchers with past studies rejected due to ethical concerns or ongoing works involving human subjects, and gather their opinions on compliance with ethical principles. The survey reflects particularly on cases without an IRB, as major interviewees are from China, where such ethical departments are still rare among institutions.

3.1. How are ethical concerns addressed in published security literature?

Our survey focuses on papers published at the same group of top-tier security and network conferences: IEEE

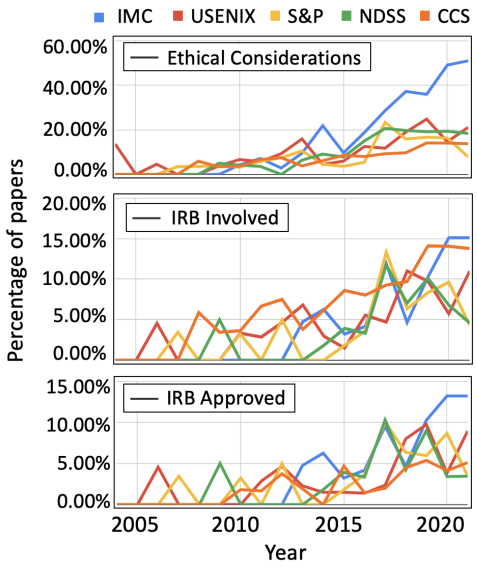

Figure 2. Percentage of papers published at 5 conferences that: discussed ethical considerations, mentioned IRBs and received IRB approvals.

S&P, USENIX Security Symposium, ACM CCS, ISOC NDSS and ACM IMC. We seek answers to the following questions: (1) By what percentage do security research raise ethical concerns? (2) How many of them are supported by specialized ethical/legal departments, like IRBs? (3) How may security researchers address ethical concerns without explicit approval from such departments (e.g., when no author's institution establishes an IRB)?

Paper collection. To begin with, we build a web crawler on top of Chromium [1] and download all papers published at the five venues from Jan 2003 to Dec 2021 (19 years of publication, 6,078 papers in total). We then compile a list of keywords associated with ethics (e.g., "ethic") and search for them in all downloaded papers. This keyword-based filter narrows the scale down to 718 papers (11.8% of 6,078). Finally, all 718 papers are manually reviewed by three of our security researchers, and we exclude works that contain keywords but do not actually involve human subjects (e.g., the word "ethic" only appears in their references). In the end, we confirm that 621 (10.2% of 6,078) papers have raised ethical concerns or discussed ethical considerations. Ethics considerations of our paper collection process are listed in Section 5.2.

Solution 1: Seeking for explicit approval from IRBs and other ethical/legal departments. Through manual review, we find that 247 papers (39.8% of 621) attempted to reach to an IRB or similar ethical departments, with an overall approval rate of 83.0% (205 of 247). Among the remaining 42 papers, 35 are exempted because IRBs determine their studies do not involve human subjects; 3 are instead supported by legal departments [17] or ethics officers [30] of the authors' institutions; 4 proceed with their study, claiming that they follow general ethical principles (e.g., the Menlo Report [23]) and best practices established by previous work.

Figure 2 shows the percentage of papers that discussed ethical considerations, reached to and approved by an IRB or similar departments. Note that, the specific name of the department responsible for authoritative review may vary in different institutions. For ease of presenting, we marked all of them as "IRB" in Figure 2. On the positive side, we find that a growing part of papers published at the 5 top-tier conferences are actively taking into account ethical perspectives, which can be a result of increasing requirements made by the CFPs. Particularly, over half of all papers published at ACM IMC 2021 explicitly discussed ethical considerations. However, the ratio of works that received guidance from specified ethical departments (e.g., IRBs) remains limited.

Solution 2: Seeking for compliance with common ethical standards and practical guidelines. Although an increasing number of published papers are discussing ethical considerations, we find that most decisions on compliance with ethical principles are still made by researchers themselves. Without support from an IRB or similar legal departments, security researchers may do the following to mitigate ethical risks (summarised from published papers):

- Seek for legal advice [9], [25], e.g., from lawyers, about sensitive data collection and processing.
- Seek for common ethical principles, e.g., those released by large academic institutions and conferences, as well as local judicial requirements [20], [24], [61].
- Follow general ethical guidelines [41], [42], [46].
- Discuss research methodology with administrators of tested networks [10], or companies [53], [60] that provide technical support.
- Refer to best practices established by previous work [51], [55].
- Follow domain-specific codes of ethics, e.g., [21], [22], [28] with Tor Research Safety Board [3].
- Use anonymized data [44], [50].
- Disclose vulnerabilities in time [52], [59].
- Provide extensive discussion on ethical considerations in submitted papers [11], [12], [45], [56].

Limitations. Our observation was limited to papers that have explicitly mentioned ethics-related terms and may have missed some papers that discussed semantics but failed to match keywords (i.e., false negatives). As we have filtered out false positives by manual review, our estimate of the ethics-mentioned paper may represent a lower bound. Besides, it would be insightful to identify papers where ethical considerations should have been discussed but were not. However, finding such work from thousands of papers is highly challenging and would be left as our future work.

3.2. How do security researchers understand and adhere to ethical principles?

From published security literature we cannot gain a comprehensive view of ethical solutions (e.g., rejected and flawed submissions are overlooked), as well as researchers' understanding of ethical principles. To this end, we design an online survey and perform a user study, particularly involving researchers based in China where IRBs for computer security are rare among institutions. Ethical considerations of the survey are listed in Section 5.2.

Participants of the survey. A total of 248 persons participate in our survey. Among them, 199 (80.2% of 248) are affiliated with universities or research institutes, including 122 (49.2% of 248) professors/lecturers, 63 (25.4% of

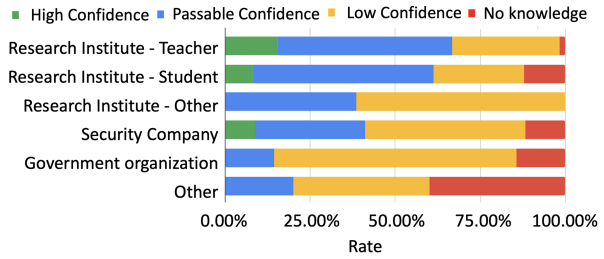

Figure 3. Confidence in understanding common ethical principles.

248) students and 14 (5.6% of 248) research staff. Another 37 (14.9% of 248) are employees of security companies, and the remaining 12 participants (4.8% of 248) come from government agencies and other organizations. From participants who voluntarily inform us about the countries they reside in, we estimate that 92.2% of all 248 interviewees are from China. The full content of the questionnaire has been released in [2]. The main questions and results could be summarised as:

Q1: What is your confidence in understanding common ethical principles of security research? Figure 3 shows the participants' overall confidence in understanding common ethical principles. Participants affiliated with research institutes have a better understanding of ethical principles, and over half of teachers and students show passable or high confidence. However, we find a somehow worrying situation: 6.7% of all participants claim that they do not have any knowledge about ethical principles, including two university teachers and six students committed to security research; among teachers and staff affiliated with research institutes, over 33% of them indicate low confidence or even no knowledge. Although those researchers may have not been exposed to ethics-related projects yet, it is necessary for the security community to help them gain "more confidence" in their fields.

Q2: Is there an IRB or similar department in your institution that reviews security research? How can you receive guidance on compliance with ethical principles? 16.1% of participants indicate their institutions have established IRBs (of any subject), yet only 6.0% respond that their IRBs could provide guidance to security research. Therefore, at least within the security community we surveyed, the range of researchers who could get professional guidance from IRBs is quite limited. We also investigated the channels through which researchers learned ethics-related regulations. The most common way is "self learning" (63.2%), including referring to published studies and learning ethical requirements made by conference CFPs. The second is to be reminded by the supervisors or other collaborated researchers (45.5%). Educations such as courses and lectures (32.5%) and feedback from reviewers (30.7%) are also the main sources of ethics guidance. Only 8.7% of the participants indicated that their ethics compliance guidance came from authoritative legal organisations as IRBs, which further illustrates that authoritative organizations currently play an inadequate role in guiding security experiments practically.

Q3: Are there ethical considerations associated with your ongoing/past security research? How do they come to your attention? Do you have difficulties addressing them? We also investigated whether their conducted or ongoing research projects involved with ethical issues. 16.1% of participants explicitly stated that they were involved, and a high percentage (39.5%) of participants encountered confusion in identifying whether their projects have ethical risks. In particular, 13 researchers reported that there might be ethical issues in their research projects, but were not sure how to mitigate corresponding risks. In addition, 43 researchers reported that their work had been ethically challenged by reviewers; 3 even say that it is still unclear to them how their experiment could be improved to mitigate ethical risks (or whether certain experimental procedures are high-sensitive ones that should be deleted). We also investigated the ways they identified ethics-sensitive parts of their research projects. The results showed that the vast majority (53.6%) relied on the researchers' individual judgement rather than certification from external professional organizations as IRBs (21.4%). It suggests that the current treatment of ethicality by researchers could be highly subjective, which may create opportunities for unconscious ethical violations.

Q4: What are your recommendations to addressing ethical considerations in security research? Participants also shared their suggestions on how to build a more ethical-compliant security community. First and foremost, is the urge for research institutions to establish professional communities as IRBs for supervision, and make strict policies to ensure any research project that may involve ethical issues for review to mitigate the risks. At the same time, the academic security community should also make effort to establish ethical guidelines for specific areas (e.g., by setting up area-specific working groups and publishing practical examples as the Tor community [3]). Furthermore, we need to enhance the training and education of researchers through lectures, training classes and courses to raise their attention on ethical compliance and help them to form the habit of thinking proactively of ethical issues. In addition, researchers need to describe the detailed experimental steps and explain the handling of ethically sensitive parts in their paper. It could both alleviate the potential confusion of reviewers, and also provide a reference for other researchers in follow-up or similar future work.

4. Recommendations

Based on the survey for authoritative reports and previous work, we draw the following takeaways to help newcomers better consider and achieve ethical compliance. In this section, we offer recommendations on: (1) where to learn ethical requirements, (2) how to design ethical experiments when authoritative ethical departments are not available, and (3) how to present a proper discussion on ethical considerations in the paper.

4.1. Understand Ethical Requirements

1. Learning from authoritative principles and guidelines. Ethical norms are necessary for a wide range of research fields. Several authoritative documents and community precedents have so far become the consensus in academia and have been adopted as basic principles. Therefore, we can learn from legal or authoritative documents to carefully design experiments, especially for human-involving projects.

General ethical principles. The Belmont Report is an aggregate of fundamental principles [16], providing guidelines for the ethical protection of human subjects in biological or medical experiments. This report identified three core principles: *respect for persons*, *beneficence*, and *justice*. These principles have been adopted as ethical norms in various research fields. Another authoritative reference is the Menlo Report [23], which is a guiding report on ethical principles specifically on information and communications technologies. Inheriting from the Belmont Report, this report added a fourth principle, *respect for law and public interest*. Among the security papers we surveyed in Section 3.1, we found 7 and 11 cited and discussed Belmont Report and Menlo Report respectively.

Domain-specific guidelines or best practices. Several research communities in specific domains have also proposed guidelines or the best practices in their fields. For example, *network measurement studies* often involve sensitive data, which might leak privacy information or expose user behaviors. Partridge et al. have discussed the sound ethical considerations for all network measurement papers [40]. Besides, network measurements are usually conducted based on the *public dataset*. Allman et al. discussed how to share and use network measurement data, and provided some basic suggestions [5], especially in a privacy-concerning way.

2. Consulting authoritative organizations. In principle, studies on human subjects should be reviewed and approved by ethical review boards or equivalent agencies. However, some institutions may lack such committees. As an alternative, researchers can seek advice from authoritative organizations and conduct experiments in coordination with them.

Legal department. Researchers could consult law enforcement agencies or law departments of universities and to ensure that their experiments could adhere to domestic or local laws (e.g., General Data Protection Regulation (GDPR) in EU law [57]). Besides, they should also comply with the agreements or policies provided by the relevant organizations, like collaborating companies and third-party providers.

Professional departments or experts. If the research topics are not legally sensitive, it might be acceptable to consult other professional departments. First, *research communities* of several domains have specialized consulting agencies and guidelines. For example, measurements on Tor networks should follow the safety guidelines published by the Tor research safety board [3], which are followed by existing studies [21], [22], [27], [28]. Second, an *ethics feedback panel* is a feasible option that can provide suggestions for practice-based researchers, as was done by [39]. Notice that such panels could also be official legal committees that can provide professional approvals. Last, or at least, we can also consult *experts in the same field*, like the dean of the department, senior colleagues and network administrators [10], [26].

3. Learning from university courses. Ethics courses should ideally be set up as compulsory by the universities. Several leading universities (e.g., UC Berkeley, Harvard University) in the world have already set up ethics courses or regarded them as entrance education. Besides, ethical principles in university teaching have been discussed for years since 1996 [29]. It is necessary for university students to get educated on ethics before starting any scientific and humanistic studies.

4. Obtaining advice from peer-reviewers. As conference programs become increasingly concerned with ethics, peer reviewers are required to pay critical attention to ethical discussion sections of papers. As such, authors may seek advice from their reviewers or shepherds if they could not provide sufficient evidence to prove the experiments and data are ethical. They can either adjust their approaches based on the reviewers' professional suggestions, or provide more detailed explanations of their efforts to reduce potential risks. In addition, releasing data processing scripts, implementation codes or models is another possible way to receive peer suggestions, while it is out of voluntary.

4.2. Adhere to Ethical Principles

All ethical principles and legal guidelines should be taken into consideration at the outset of experiment designs. Based on published papers in the field of computer security, we have outlined the following recommendations, including but not limited to:

Controlled experiments. Researchers should primarily consider experiments in controlled environments, e.g., in private networks or simulators, rather than real-world networks to minimise potential negative impact at best. When such controlled environment is not inadequate, researchers should also attempt to conduct experiments in a "controlled" manner, e.g., attacking their own web service accounts or scanning networks at an acceptable rate.

Adequate informed consent. All participants must actively and explicitly consent to the processing of their data. Researchers are required to provide valid consent for their studies based on existing guidelines like [19], [47].

Mindful data collection. When collecting or exploring any dataset, researchers should always pay attention to the handling of sensitive data, like secret data of organizations or personally identifiable information. It would be feasible to ensure data anonymity (e.g., avoiding collecting, encrypting or removing sensitive data) and get permission from owners or administrators. If the experiment is built on public data, attention should also be paid to the requirements imposed by the publisher.

Reliable data storage and processing. Another key issue is how to handle and retain the collected data. Researchers themselves may have already gotten permission for the use of data, while others might not. To this end, strict access controls must be in place to ensure that only authorized individuals have access to the data, or that the data is processed under the supervision of experienced experts.

Secure data destruction. Destruction of (sensitive) data should also be an essential part of the whole data processing cycle, for which best practices and legal requirements have already been proposed [43]. Researchers should carefully follow the requirements, and securely dispose and destruct sensitive data both in electronic forms and paper files upon completion of the research project [54].

Responsible disclosure and mitigation. While discovering vulnerabilities, researchers need to consider how to fix or mitigate the issues to avoid large-scale threats. They could propose solutions or report issues to relevant parties

like vulnerability disclosure programs, security response centers, or research communities.

4.3. Provide Extensive Discussion in Papers

A well-organized discussion section on ethical considerations is necessary to evaluate the work or to alert follow-up researchers to potential risks. Here, we summarize the main writing points learned from previous work.
Point out the risks. Authors need to sort out which processes and operational steps of the experiment may involve ethical risks. The direct, indirect, and potential risks should be considered as comprehensively as possible when designing experiments. It is also important to explain why such risks are unavoidable and how the benefits (e.g., contributions) and the risks have been balanced.
Discuss whether the experiments have achieved ethical compliance. Authors should state whether their experiments comply with the ethical requirements or guidelines in authoritative documents and laws, and explain what they have done for achieving these. It is also possible to cite and refer to the published papers or the best practices in the same field.
Refine details like respect for people and protection of privacy. For example, demonstrate whether and in what manner user consent is provided by showing screenshots or quotes; and whether data is anonymized and stored under strict access controls.
Obtain professional guidance or approval from authoritative departments. Guidance from authoritative departments or experts could help to reduce ethical risks as much as possible. Meanwhile, review and approval from authoritative departments, such as IRBs or other similar departments, is a strong proof of ethical compliance.

5. Discussion

5.1. Open Questions

Based on the observations in paper survey and online investigation, we consider that there are still several open questions requiring a concerted effort of the security community on ethics, including but not limited to:

1. How to establish consensus standards and specific guidance on ethics for sub-fields of security research and make them easily accessible to researchers? As far as we know, although there are several authoritative consensuses on ethics such as the Belmont Report [16] and Menlo Report [23], their requirements are quite abstract, leaving a big gap from the practice of security research experiments. It has been suggested in the online survey that we could develop fine-grained ethical standards by establishing working groups with experts and legal advisors in various research fields, which may be a good solution but need to be well organised by the security community. In addition, establishing open platforms such as the Wikipedia of security research for all the members to maintain and share ethical compliance references and guidelines may also be a feasible approach.

2. Is it fair to ask researchers at institutions without sound ethical support to completely avoid conducting any research projects that may raise ethical issues? Some participants in the online survey suggested that researchers without authoritative ethical guidance should avoid any ethic-sensitive project at all. However, given the complexities of different technical and economic background of research institutions, such a requirement may be opinionated and would leave a significant number of researchers in straitened circumstances. Certainly, in the absence of professional guidance, researchers should try to avoid conducting ethical risky projects, but the balance is quite hard to control.

3. Can the security community provide more technical assistance to researchers who need guidance on ethical compliance? Although there is a strong call for research institutions to establish professional IRBs or other legal communities for supervision, it is obvious that the process would take a long time. Before legal support is widely available in research institutions, it would be helpful if the security community could provide some public legal assistance (e.g., in the form of paid consultation). Even if such services could not offer ethical compliance proof with legal validity, they at least afford specific guidance on the experiments, creating opportunities for researchers to perform more ethics-compliant security research projects.

4. How to make authoritative departments as IRBs more useful in ethical guidance for security researchers? Even for the existed authorities such as IRBs, their current role in ethical guidance for security researchers is hardly satisfactory. In our survey, 15 (6.0%) of the 40 (16.1%) participants from institutions with IRBs indicated that the authority was unable to provide practical assistance. Improving the professionalism and functionality of such authorities should be considered as an important task for the security community.

5.2. Ethical Considerations of This Study

The user study in Section 3.2 is aimed at helping researchers better achieve ethical compliance without ethics review committees. It is supported and approved by the security research community together with senior experts in this field. Our institution does not require IRB review for online survey studies. Nonetheless, we do our best to mitigate ethical risks of the user study itself. Specifically, all participants were enrolled voluntarily and received information about the study purpose and how data would be used, in order to ensure informed and affirmative consent. We carefully designed insensitive questions, and did not collect and retain personally identifiable information (e.g., human names). Besides, we have provided an "open questions" option to receive participants' concerns, suggestions, or complaints about the interview and the research topic. The full questionnaire and the consent information has been released in [2].

In addition, the survey in Section 3.1 only focused on the published security papers, which was conducted based on public data. The data was collected with a limited rate under the campus network through our student accounts of the school library, which has received permission from the campus network administrator. The collected papers are stored in the internal servers and only the authorized researchers can access them. The paper files will not be

shared with the public considering the intellectual property rights and copyright of the relevant authors and the original publishers. Besides, the dataset is only used for research rather than profit or commercial purposes.

6. Conclusion

Ethical compliance has been increasingly concerned by the security research community in recent years. However, the lack of authoritative ethical assistance and concrete guidelines poses various challenges for researchers to fully comply with ethical requirements. This paper provides a comprehensive survey of ethical considerations in security research, including the "visions", i.e., the principal ethical requirements of top-tier security and network conferences, the "reality", i.e., the current researchers' treatment of ethical risks and the practical issues they encountered, and the "paths forward", i.e., suggestions toward better ethical compliance for the security community.

Acknowledgement

We thank the anonymous reviewers for their valuable comments to improve this paper. We also greatly appreciate all participants of the online survey. This work was supported in part by the National Natural Science Foundation of China (U1836213, U19B2034).

References

[1] The chromium projects. https://www.chromium.org/chromium-projects/, 2022.

[2] Survey: Ethics in Security Research. https://github.com/Cypher-Z/Survey-Ethics-in-Security-Research, 2022.

[3] Tor Project Research Safety Board. https://research.torproject.org/safetyboard/, 2022.

[4] Annual Computer Security Applications Conference (ACSAC). Call for papers for acsac 2021. https://www.acsac.org/2021/submissions/papers/, 2021.

[5] Mark Allman and Vern Paxson. Issues and etiquette concerning use of shared measurement data. In *Proceedings of the 7th ACM SIGCOMM Conference on Internet Measurement*, IMC '07, page 135–140, New York, NY, USA, 2007. Association for Computing Machinery.

[6] CERT/CC. Vulnerability disclosure policy. https://vuls.cert.org/confluence/display/Wiki/Vulnerability+Disclosure+Policy, 2019.

[7] Internet Measurement Conference. Call for papers for imc 2009. https://conferences.sigcomm.org/imc/2009/cfp.html, 2009.

[8] Internet Measurement Conference. Call for papers for imc 2022. https://conferences.sigcomm.org/imc/2022/cfp/, 2022.

[9] Zainul Abi Din, Hari Venugopalan, Jaime Park, Andy Li, Weisu Yin, HaoHui Mai, Yong Jae Lee, Steven Liu, and Samuel T. King. Boxer: Preventing fraud by scanning credit cards. In *29th USENIX Security Symposium (USENIX Security 20)*, pages 1571–1588. USENIX Association, August 2020.

[10] Zakir Durumeric, Eric Wustrow, and J. Alex Halderman. ZMap: Fast internet-wide scanning and its security applications. In *22nd USENIX Security Symposium (USENIX Security 13)*, pages 605–620, Washington, D.C., August 2013. USENIX Association.

[11] Kathrin Elmenhorst, Bertram Schütz, Nils Aschenbruck, and Simone Basso. Web censorship measurements of http/3 over quic. In *Proceedings of the 21st ACM Internet Measurement Conference*, IMC '21, page 276–282, New York, NY, USA, 2021. Association for Computing Machinery.

[12] Birhanu Eshete, Abeer Alhuzali, Maliheh Monshizadeh, Phillip A. Porras, Venkat N. Venkatakrishnan, and Vinod Yegneswaran. Ekhunter: A counter-offensive toolkit for exploit kit infiltration. In *22nd Annual Network and Distributed System Security Symposium, NDSS 2015, San Diego, California, USA, February 8-11, 2015*. The Internet Society, 2015.

[13] The Association for Computing Machinery. Acm code of ethics and professional conduct. https://www.acm.org/code-of-ethics, 2018.

[14] The Association for Computing Machinery. Acm publications policy on research involving human participants and subjects. https://www.acm.org/publications/policies/research-involving-human-participants-and-subjects, August 15, 2021.

[15] Association for the Advancement of Artificial Intelligence (AAAI). Aaai code or professinal ethics and conduct. https://www.aaai.org/Conferences/code-of-ethics-and-conduct.php, 2019.

[16] United States. National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. *The Belmont report: ethical principles and guidelines for the protection of human subjects of research*. Department of Health, Education and Welfare, 1979.

[17] Xiao Han, Nizar Kheir, and Davide Balzarotti. Phisheye: Live monitoring of sandboxed phishing kits. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, page 1402–1413, New York, NY, USA, 2016. Association for Computing Machinery.

[18] Empirical Methods in Natural Language Processing (EMNLP). Call for papers for emnlp 2021. https://2021.emnlp.org/call-for-papers, 2021.

[19] IRB in University of Michigan. Informed consent guidelines & templates. https://research-compliance.umich.edu/informed-consent-guidelines, accessed on Mar 28, 2022.

[20] Suman Jana, David Molnar, Alexander Moshchuk, Alan Dunn, Benjamin Livshits, Helen J. Wang, and Eyal Ofek. Enabling Fine-Grained permissions for augmented reality applications with recognizers. In *22nd USENIX Security Symposium (USENIX Security 13)*, pages 415–430, Washington, D.C., August 2013. USENIX Association.

[21] Rob Jansen and Aaron Johnson. Safely measuring tor. In Edgar R. Weippl, Stefan Katzenbeisser, Christopher Kruegel, Andrew C. Myers, and Shai Halevi, editors, *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, October 24-28, 2016*, pages 1553–1567. ACM, 2016.

[22] Rob Jansen, Matthew Traudt, and Nicholas Hopper. Privacy-preserving dynamic learning of tor network traffic. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, CCS '18, page 1944–1961, New York, NY, USA, 2018. Association for Computing Machinery.

[23] Erin Kenneally and David Dittrich. The menlo report: Ethical principles guiding information and communication technology research. *Available at SSRN 2445102*, 2012.

[24] Katharina Krombholz, Karoline Busse, Katharina Pfeffer, Matthew Smith, and Emanuel von Zezschwitz. "if https were secure, i wouldn't need 2fa" - end user and administrator mental models of https. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 246–263, 2019.

[25] Chaoyi Lu, Baojun Liu, Yiming Zhang, Zhou Li, Fenglu Zhang, Haixin Duan, Ying Liu, Joann Qiongna Chen, Jinjin Liang, Zaifeng Zhang, Shuang Hao, and Min Yang. From WHOIS to WHOWAS: A large-scale measurement study of domain registration privacy under the GDPR. In *28th Annual Network and Distributed System Security Symposium, NDSS 2021, virtually, February 21-25, 2021*. The Internet Society, 2021.

[26] Max Maass, Alina Stöver, Henning Pridöhl, Sebastian Bretthauer, Dominik Herrmann, Matthias Hollick, and Indra Spiecker. Effective notification campaigns on the web: A matter of trust, framing, and support. In *30th USENIX Security Symposium (USENIX Security 21)*, pages 2489–2506. USENIX Association, August 2021.

[27] Akshaya Mani and Micah Sherr. Historε: Differentially private and robust statistics collection for tor. In *NDSS*, 2017.

[28] Akshaya Mani, T. Wilson-Brown, Rob Jansen, Aaron Johnson, and Micah Sherr. Understanding tor usage with privacy-preserving measurement. In *Proceedings of the Internet Measurement Conference 2018, IMC 2018, Boston, MA, USA, October 31 - November 02, 2018*, pages 175–187. ACM, 2018.

[29] Harry Murray et al. Ethical principles in university teaching. 1996.

[30] Alena Naiakshina, Anastasia Danilova, Christian Tiefenau, Marco Herzog, Sergej Dechand, and Matthew Smith. Why do developers get password storage wrong? a qualitative usability study. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, CCS '17, page 311–328, New York, NY, USA, 2017. Association for Computing Machinery.

[31] The Network and Distributed System Security (NDSS). Call for papers for ndss 2022. https://www.ndss-symposium.org/ndss2022/call-for-papers/, 2022.

[32] International Joint Conference on Artificial Intelligence (IJCAI). Call for papers for ijcai 2022. https://ijcai-22.org/calls-papers/, 2022.

[33] Conference on Computer Vision and Pattern Recognition (CVPR). Call for papers for cvpr 2022. https://cvpr2022.thecvf.com/sites/default/files/2021-06/CFP_CVPR2022.pdf, 2022.

[34] Annual IEEE/IFIP International Conference on Dependable Systems and Network (DSN). Call for papers for dsn 2022. https://dsn2022.github.io/cfpapers.html, 2022.

[35] European Symposium on Research in Computer Security (ESORICS). Call for papers for esorics 2022. https://esorics2022.compute.dtu.dk/cfp.html, 2022.

[36] IEEE European Symposium on Security and Privacy (S&P). Call for papers for euros&p 2022. https://www.ieee-security.org/TC/EuroSP2022/cfp.html, 2022.

[37] IEEE Symposium on Security and Privacy (S&P). Call for papers for s&p 2021. https://www.ieee-security.org/TC/SP2021/cfpapers.html, 2021.

[38] IEEE Symposium on Security and Privacy (S&P). Financial conflicts policy for s&p 2021. https://www.ieee-security.org/TC/SP2021/financial-con.html, 2021.

[39] Andriy Panchenko, Fabian Lanze, Andreas Zinnen, Martin Henze, Jan Pennekamp, Klaus Wehrle, and Thomas Engel. Website fingerprinting at internet scale. 02 2016.

[40] Craig Partridge and Mark Allman. Ethical considerations in network measurement papers. *Communications of the ACM*, 59(10):58–64, 2016.

[41] Paul Pearce, Ben Jones, Frank Li, Roya Ensafi, Nick Feamster, Nick Weaver, and Vern Paxson. Global measurement of DNS manipulation. In *26th USENIX Security Symposium (USENIX Security 17)*, pages 307–323, Vancouver, BC, August 2017. USENIX Association.

[42] Victor Le Pochat, Tom van Goethem, Samaneh Tajalizadehkhoob, Maciej Korczynski, and Wouter Joosen. Tranco: A research-oriented top sites ranking hardened against manipulation. In *26th Annual Network and Distributed System Security Symposium, NDSS 2019, San Diego, California, USA, February 24-27, 2019*. The Internet Society, 2019.

[43] Privacy Technical Assistance Center (PTAC). Best practices for data destruction. https://studentprivacy.ed.gov/sites/default/files/resource_document/file/BestPracticesforDataDestruction%282019-3-26%29.pdf, accessed on Apr 19, 2022.

[44] Sazzadur Rahaman, Gang Wang, and Danfeng (Daphne) Yao. Security certification in payment card industry: Testbeds, measurements, and recommendations. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, CCS '19, page 481–498, New York, NY, USA, 2019. Association for Computing Machinery.

[45] Reethika Ramesh, Ram Sundara Raman, Matthew Bernhard, Victor Ongkowijaya, Leonid Evdokimov, Anne Edmundson, Steven Sprecher, Muhammad Ikram, and Roya Ensafi. Decentralized control: A case study of russia. In *27th Annual Network and Distributed System Security Symposium, NDSS 2020, San Diego, California, USA, February 23-26, 2020*. The Internet Society, 2020.

[46] Abbas Razaghpanah, Rishab Nithyanand, Narseo Vallina-Rodriguez, Srikanth Sundaresan, Mark Allman, Christian Kreibich, and Phillipa Gill. Apps, trackers, privacy, and regulators: A global study of the mobile tracking ecosystem. In *25th Annual Network and Distributed System Security Symposium, NDSS 2018, San Diego, California, USA, February 18-21, 2018*. The Internet Society, 2018.

[47] User research community in the U.K. Getting informed consent for user research. https://www.gov.uk/service-manual/user-research/getting-users-consent-for-research, 2018.

[48] Intrusions Research in Attacks and Defenses (RAID). Call for papers for raid 2022. https://raid2022.cs.ucy.ac.cy/call.html, 2022.

[49] Usenix Security. Call for papers for usenix 2021. https://www.usenix.org/conference/usenixsecurity21/call-for-papers, 2021.

[50] Camelia Simoiu, Ali Zand, Kurt Thomas, and Elie Bursztein. Who is targeted by email-based phishing and malware? measuring factors that differentiate risk. In *Proceedings of the ACM Internet Measurement Conference*, IMC '20, page 567–576, New York, NY, USA, 2020. Association for Computing Machinery.

[51] Drew Springall, Zakir Durumeric, and J. Alex Halderman. Measuring the security harm of tls crypto shortcuts. In *Proceedings of the 2016 Internet Measurement Conference*, IMC '16, page 33–47, New York, NY, USA, 2016. Association for Computing Machinery.

[52] Marius Steffens and Ben Stock. *PMForce: Systematically Analyzing PostMessage Handlers at Scale*, page 493–505. Association for Computing Machinery, New York, NY, USA, 2020.

[53] Kurt Thomas, Damon McCoy, Chris Grier, Alek Kolcz, and Vern Paxson. Trafficking fraudulent accounts: The role of the underground market in twitter spam and abuse. In *22nd USENIX Security Symposium (USENIX Security 13)*, pages 195–210, Washington, D.C., August 2013. USENIX Association.

[54] John Carroll University. Procedures for sensitive data destruction. https://jcu.edu/its/about/policy/procedures-sensitive-data-destruction.

[55] Benjamin VanderSloot, Johanna Amann, Matthew Bernhard, Zakir Durumeric, Michael Bailey, and J. Alex Halderman. Towards a complete view of the certificate ecosystem. In *Proceedings of the 2016 Internet Measurement Conference*, IMC '16, page 543–549, New York, NY, USA, 2016. Association for Computing Machinery.

[56] Thomas Vissers, Timothy Barron, Tom Van Goethem, Wouter Joosen, and Nick Nikiforakis. The wolf of name street: Hijacking domains through their nameservers. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, CCS '17, page 957–970, New York, NY, USA, 2017. Association for Computing Machinery.

[57] Paul Voigt and Axel Von dem Bussche. The eu general data protection regulation (gdpr). *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, 10(3152676):10–5555, 2017.

[58] Project Zero. Vulnerability disclosure FAQ. https://googleprojectzero.blogspot.com/p/vulnerability-disclosure-faq.html, 2019.

[59] Mingming Zhang, Xiaofeng Zheng, Kaiwen Shen, Ziqiao Kong, Chaoyi Lu, Yu Wang, Haixin Duan, Shuang Hao, Baojun Liu, and Min Yang. Talking with familiar strangers: An empirical study on HTTPS context confusion attacks. In Jay Ligatti, Xinming Ou, Jonathan Katz, and Giovanni Vigna, editors, *CCS '20: 2020 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event, USA, November 9-13, 2020*, pages 1939–1952. ACM, 2020.

[60] Yiming Zhang, Baojun Liu, Chaoyi Lu, Zhou Li, Haixin Duan, Shuang Hao, Mingxuan Liu, Ying Liu, Dong Wang, and Qiang Li. *Lies in the Air: Characterizing Fake-Base-Station Spam Ecosystem in China*, page 521–534. Association for Computing Machinery, New York, NY, USA, 2020.

[61] Zesen Zhang, Alexander Marder, Ricky Mok, Bradley Huffaker, Matthew Luckie, K C Claffy, and Aaron Schulman. Inferring regional access network topologies: Methods and applications. In *Proceedings of the 21st ACM Internet Measurement Conference*, IMC '21, page 720–738, New York, NY, USA, 2021. Association for Computing Machinery.