Human Factors in Cybersecurity - Howto

Sascha Fahl

What should a paper look like?

- Let's look at some calls for papers!
  - SOUPS '19: https://www.usenix.org/conference/soups2019/call-for-papers
  - IEEE Security & Privacy '20: https://www.ieee-security.org/TC/SP2020/cfpapers.html
  - USENIX Security '20: https://www.usenix.org/conference/usenixsecurity20/call-for-papers
  - CCS '19: https://sigsac.org/ccs/CCS2019/index.php/call-for/call-for-papers/
  - NDSS '20: https://www.ndss-symposium.org/ndss2020/call-for-papers/
  - EuroS&P '20: https://www.ieee-security.org/TC/EuroSP2020/cfp.html
- What do they tell us?

Call for papers - SOUPS

We invite authors to submit original papers describing research or experience in all areas of usable privacy and security. We welcome avariety of research methods, including both qualitative and quantitative approaches.

Topics include, but are not limited to:

- innovative security or privacy functionality and design
- field studies of security or privacy technology
- usability evaluations of new or existing security or privacy features
- security testing of new or existing usability features
- studies of administrators or developers and support for security and privacy
- lessons learned from the deployment and use of usable privacy and security features
- reports of replicating previously published studies and experiments
- reports of failed usable privacy/security studies or experiments, with the focus on the lessons learned from such experience

All submissions must relate to both human aspects and security or privacy. Papers on security or privacy that do not address usability or human factors will not be considered. Papers need to describe the purpose and goals of the work, cite related work, show how the work effectively integrates usability or human factors with security or privacy, and clearly indicate the innovative aspects of the work or lessons learned as well as the contribution of the work to the field.

Call for papers - IEEE Security & Privacy '20

Since 1980 in Oakland, the IEEE Symposium on Security and Privacy has been the premier forum for computer security research, presenting the latest developments and bringing together researchers and practitioners. We solicit previously unpublished papers offering novel research contributions in any aspect of security or privacy. Papers may present advances in the theory, design, implementation, analysis, verification, or empirical evaluation and measurement of secure systems.

<long list of topics, similar to SOUPS's>

This topic list is not meant to be exhaustive; S&P is interested in all aspects of computer security and privacy. Papers without a clear application to security or privacy, however, will be considered out of scope and may be rejected without full review.

Human Subjects and Ethical Considerations

Submissions that describe experiments on human subjects, that analyze data derived from human subjects (even anonymized data), or that otherwise may put humans at risk should:

Disclose whether the research received an approval or waiver from each of the authors' institutional ethics review boards (IRB) if applicable.

Discuss steps taken to ensure that participants and others who might have been affected by an experiment were treated ethically and with respect.

The same applies if the submission deals with personal identifiable information (PII) or other kinds of sensitive data. If a paper raises significant ethical and legal concerns, it might be rejected based on these concerns.

How to write a paper?

We mostly steal from here:

`https://cups.cs.cmu.edu/soups/2010/howtosoups.pdf`

Their main points:

- be clear about your hypothesis
- clearly state what your contribution is, your novelty.
- clearly explain your experimental design, the execution, the results.
- disclose limitations in detail
- supplement with meaningful tables and diagrams
- sound statistics!
- sound related work
- let the paper be well-written.

How to review - Guides

Basically:

1. Check that the paper fulfills what was asked for in the Call for papers
2. Check that the paper is novel, making a meaningful contribution and that it is written and presented comprehensively and soundly.
3. Point out missing but crucial related work.
4. Check the experiment/contribution for soundness, validity, sound statistics and sound limitations.

There are guides that you can find online . . . while you don't need to follow them to a fault, they give meaningful insights:

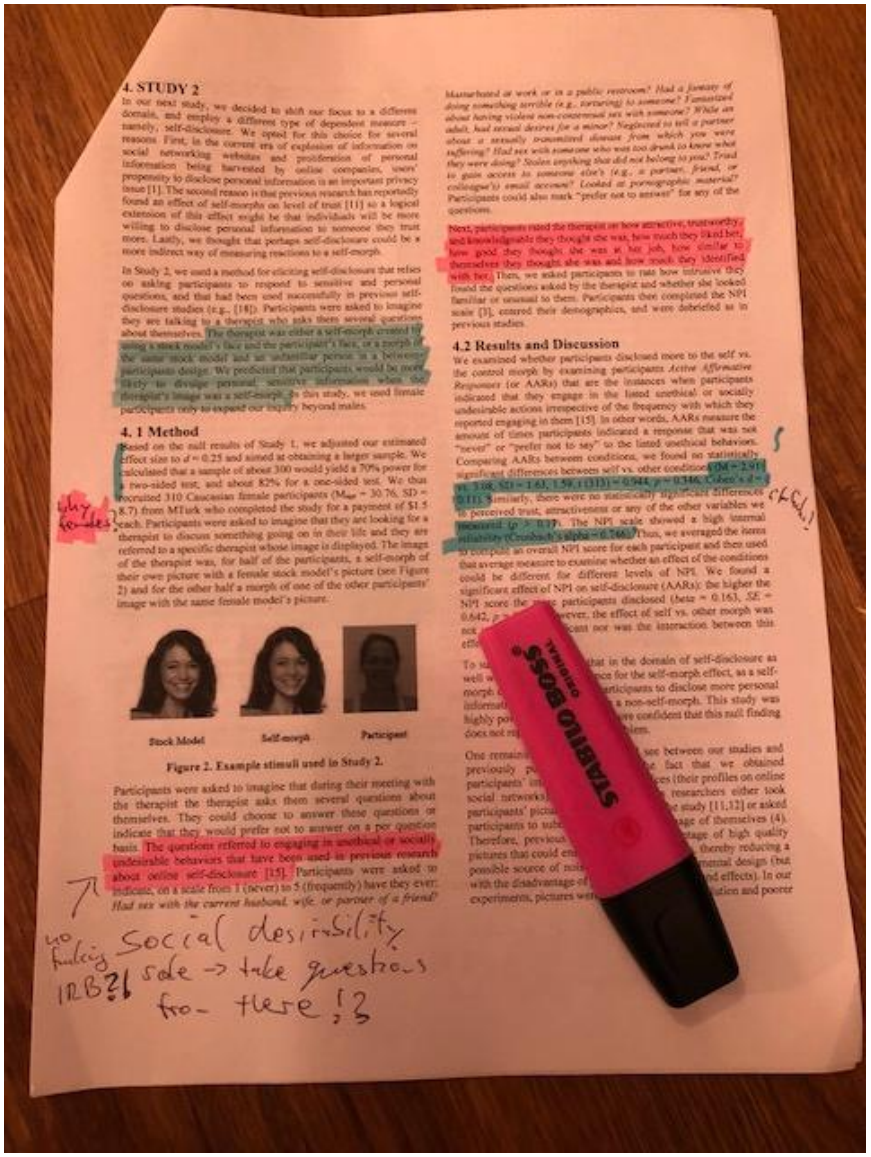
- https://chi2016.acm.org/wp/guide-to-reviewing-papers-and-notes/
- http://www.phd2published.com/2012/05/09/how-to-write-a-peer-review-for-an-academic-journal-six-steps-from-start-to-finish-by-tanya-golash-boza/
- http://violentmetaphors.com/2013/12/13/how-to-become-good-at-peer-review-a-guide-for-young-scientists
- Ihttp://mobilehci.acm.org/2015/download/ExcellenceInReviewsforHCICommunity.pdf

How to review - Important points

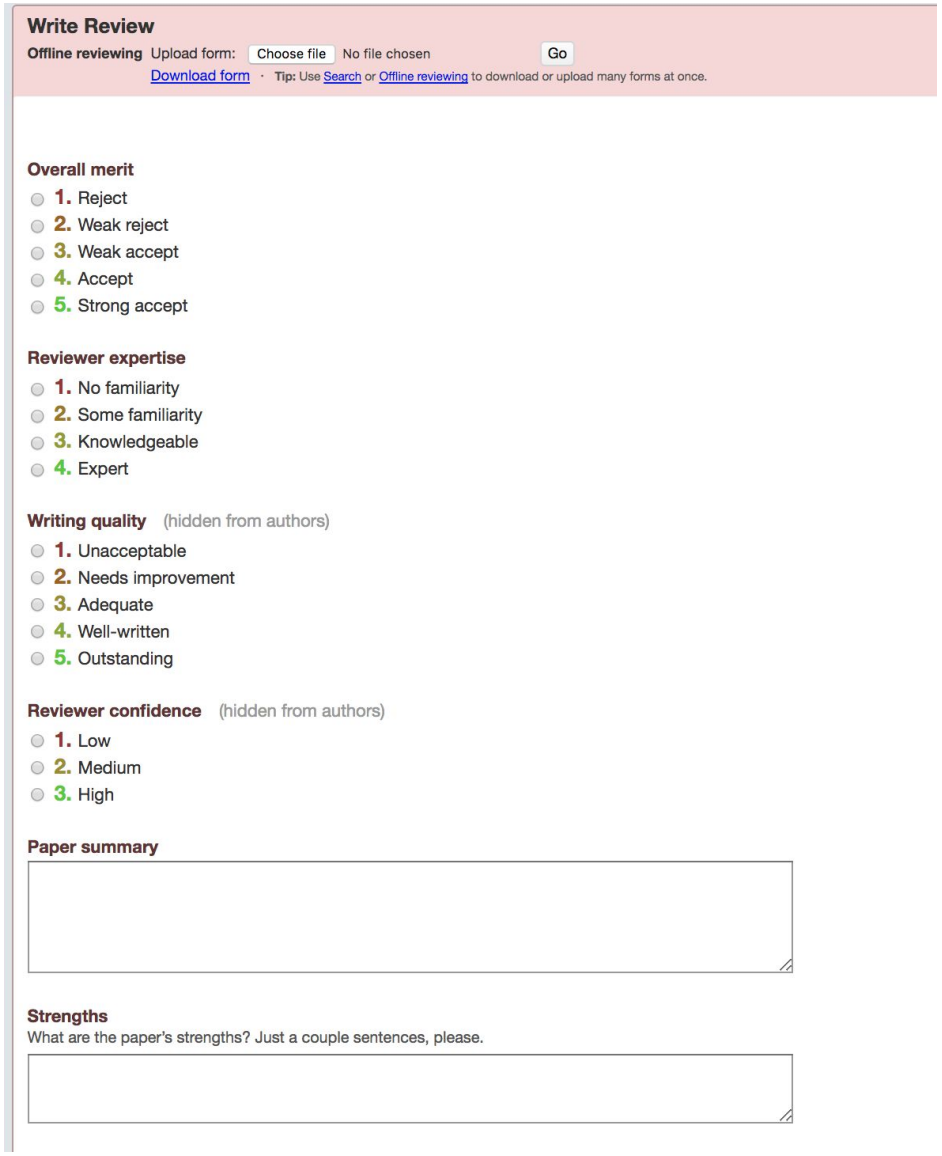
Important points when writing a review:

- Begin with a summary, also address if the contribution is meaningful and novel.
- Point out positive aspects of the paper.
- Point out negative aspects.
- Add other comments for the authors: What should they work on to make their paper better?
- Comments for the PC: Say stuff you might want to discuss with other reviewers but not the authors.
- Give a rating (should it be accepted or not, will you fight for this or not?), also disclose honestly how familiar you are with the topic.
- Stay friendly and constructive in your criticism.
- Print your papers, use colored markers to highlight important points!

How to review



HotCRP Review Form



Write Review

Offline reviewing Upload form: Choose file No file chosen Go

Download form · **Tip:** Use Search or Offline reviewing to download or upload many forms at once.

Overall merit

- 1. Reject
- 2. Weak reject
- 3. Weak accept
- 4. Accept
- 5. Strong accept

Reviewer expertise

- 1. No familiarity
- 2. Some familiarity
- 3. Knowledgeable
- 4. Expert

Writing quality (hidden from authors)

- 1. Unacceptable
- 2. Needs improvement
- 3. Adequate
- 4. Well-written
- 5. Outstanding

Reviewer confidence (hidden from authors)

- 1. Low
- 2. Medium
- 3. High

Paper summary

Strengths

What are the paper's strengths? Just a couple sentences, please.

HotCRP Review Form

Weaknesses
What are the paper's weaknesses? Just a couple sentences, please.

Hints
If you have concrete ideas of how to make the paper stronger, mention them here.

Questions to the authors
Is there anything unclear that you would like to ask the authors in the rebuttal? Mention them here.

Summary of strengths/weaknesses (hidden from authors)
Brief summary of the points for/against the paper.

Comments for PC (hidden from authors)

Real World Example: Email from some PC Chairs

While reviewing, keep in mind:

- Be positive: Rejecting papers is easy and impresses no one.
- Be constructive: Don't be "that reviewer" we all complain about
- Technical vs. philosophical weaknesses: Separating these will aid PC discussion
- Questions for authors: Give R2 paper authors a chance to answer unknowables
- Confidentiality: Continue institutional trust in the process, particularly for vulnerabilities
- Delegation: You are responsible for your reviews and all their content (note below)

Real World Example: Email from some PC Chairs (2)

Let's drive the point home: as a community, we need to be more positive when reviewing. Sure, some papers need to be rejected, but many good papers are rejected on trivial grounds.

What makes a good review?

- Constructive criticism.
- Clear explanations of what is missing.
- Knowledge about the topic or disclosure of not being knowledgeable.

What makes a bad review?

- Unprofessional roughness.
- Uninformed rejection, e.g. someone is uninterested in user studies and says that the paper is crap because user studies are crap.
- Lack of explanation of the acceptance / rejection rating.

A review we've received

"The idea behind this paper is really good, and I'm happy that someone is looking at the effects of research methodology on user behaviors."

- Novelty: Check
- Contribution: Check

"However, I think that the authors make a crucial mistake in their definition of "consistency". The problem is twofold:

<explanation of two points>"

- Constructive criticism: Check

"To conclude, I'm not sure if the effects the authors claim to have found are indeed due to methodological differences, or rather due to chance (point 1) or contextual differences (point 2)."

- Usefulness? Questionable.
- Results? Questionable

“Finally, I want to point the authors to their use of casual language (“way more”), contractions (“don’t”), mixed english (“generalized” and “behaviour”), and some missing references to Sections of the paper.”

- Helps polish the paper - good comment. It’s such a pain writing papers with different people!

A review we've received

"DEF CON has under~100 speaking slots this year, cutting our overall quantity and that means~4 out of 5 submissions are going to be rejected. Some, for no decent real reason, "Competition forthese slots are hard". It is infuriating, but completely common forme to reject a talk that has majority or all yes votes."

What's a meta review?

- A meta-review is based on original reviews.
- Highlights the main points (positive and negative) of the original reviews.
- Can also include a meta-reviewer's own perspectives and commentary on a paper.
- A good meta-review also discusses what and why other reviewers' comments were weighted more heavily.
- Typically meta-reviews quote/paraphrase key comments from each original review.

A meta-review we've received

- Your Assessment of this Paper's Contribution to HCI
  - "This paper examines how users deal with security warnings (TLS) in a Web browser using three techniques (telemetry, laboratory study, and online study). It then compares the results to examine whether the findings of lab or online study are consistent with those from telemetry. The goal of the comparison is to comment on the ecological validity of using laboratory/online studies to study how users deal with warnings. The notable strength of the comparison is that the *same* users are being compared across conditions (because of how the method was set up)."
- Overall Rating
  - "1.5 . . . Between reject and possibly reject "
- Expertise
  - "4 (Expert)"

"Even though the numeric scores of reviewers are somewhat spread due to a 2.5 from a non-expert reviewers, the text of the reviews as well as the subsequent discussion (not directly accessible to the authors) indicates a clear consensus among reviewers regarding the assessment of this paper."

- Summary: Consensus

On the positive side, reviewers find that the paper tackles an important and interesting topic and the specific research question being examined as well as the basic underlying approach taken to study are promising. (R1: The idea behind this paper is really good; R2: I really understand the intensive work done for this paper; R3: The topic of this paper is very exciting. The authors have formulated a great research question in this area. R3 further commends the authors for the basic underlying approach that allowed comparing the behavior of the same people across conditions in a non-priming way (R3: The approach taken is also remarkable.) and R2 is impressed by the attention to the technical details of traffic capture and analysis (R2: technical solutions to measure these actions were explained in detail. The procedure of filtering out requests that are not triggered by the users' browsing is impressive.)

- Positive aspects summarized, paraphrasing.

“Unfortunately, all reviewers have identified a fundamental flaw in the study design and execution. Specifically, reviewers point out that the notion of "consistency," on which all of the results and the subsequent conclusions are dependent, is incorrectly defined. - R1: the authors make a crucial mistake in their definition of"consistency." - R2: the authors defined the "consistent" and"inconsistent" behaviors. The authors did not explain the reasonings of setting up these criteria. In my opinion, the definition is somewhat biased. - R3: The conclusion of the paper seems to hinge on the “consistent behavior” definition, which I find dubiousand not adequately justified. Please see the individual reviews for further detail and explanation regarding this problem. ”

- Negative aspects summarized, paraphrasing, referral to individual reviews.

In future work on this problem, the authors could perhaps consider approaches that could capture all network traffic from a user's computer. (That being said, I recognize that this is not trivial to achieve.)

- Suggestions for future work / improving the paper.

Overall, the authors are to be commended for taking on an important research problem. Despite the promise of the underlying idea, their initial exploration is (rather unfortunately) fundamentally flawed, making this paper unsuitable for acceptance. I would like to stress that all of us would like to see this question tackled and I strongly encourage the authors to design and carry out a new study that takes the suggestions of these reviews into account.

- Summary of the reviews, final rating (reject), reiteration that the contribution is novel and important, but the experiment needs a better setup, taking suggestions from the review into account.

What's a rebuttal?

Authors see preliminary reviews and can respond with a rebuttal.The rebuttal offers authors an opportunity to rebut factual errors in reviews, or to answer questions asked by reviewers. (CHI'16)

How to write a rebuttal

- A rebuttal usually is limited to 500 words.
- The intention of a rebuttal is not to bring up new content.
- Authors of a paper are given the opportunity to respond to reviews:
  - Answer specific questions asked by reviewers.
  - Point reviewers to factual errors.
- Usually, a short, succinct rebuttal is better than an exhaustive,prose-format rebuttal.
- When writing a rebuttal be as objective and fair as possible, even if reviewers might not always be.

Rebuttal example

Reviewer 1: Although there has been a serious attempt in this work to contact developers of vulnerable apps, 14 interviews is not an adequate statistical sample. . . . I believe you could have had a much more solid part on the behavioral study by making a more extensive survey, and by providing details on the questions used and perhaps some graphical results.

Rebuttal example

Response: To the best of our knowledge these 14 qualitative interviews are the first study of app developers who failed to implement correct SSL validation. While conducting (end) user studies is relatively straightforward (e.g. think of Amazon Mechanical Turk), conducting developer studies is much more difficult. The aim of these interviews was to find the root causes behind implementing broken SSL in apps and not to find out what app developers do in general when it comes to SSL. To evaluate the actual SSL practices, we evaluated the actual implementations of 13,500 apps, as detailed in the paper, which has the additional benefit of not being subject to self-reporting and interview biases. Due to space constraints, we did not put more interview details into the paper, but we can gladly make room for more details in the study section or the appendix if the reviewers feel that this is necessary.

Rebuttal example

Reviewer 1: I strongly agree with the approach of adding as many security-related features as possible to the OS, substituting the custom code development option with custom configuration options for developers. . . . In addition, although the proposed framework limits the security concerns raised by careless developers, it does not address the problem of incorrect library implementations and does not provide a generic architecture to enable addition of new features in the future, when new issues arise.

Rebuttal example

Response: Moving the SSL related features to the OS gives us the chance to fix incorrect library implementations and adding new features (such as certificate transparency or fixes for bugs in the SSL protocol) by triggering one central OS update instead of having to fix thousands and thousands of apps.

Rebuttal example

Reviewer 3: This paper needs to be published (and then publicised). Did any of the developers that were interviewed mention losing customers because they didn't want to disable certificate checking, or did they all bow to customer pressure?

Rebuttal example

Response: We focused the interviews on app developers who failed when it came to implementing SSL. Hence, no developer mentioned losing customers because of refusing to disable certificate checking. Instead, two app distributors reported that they canceled contracts with app developers that turned off certificate validation for their apps and threatened the apps' users in this way.

Lightning talk

For the PC meeting – 5 minutes!

The goal of lightning talks is to articulate a topic in a quick, insightful, and clear manner. These concise and efficient talks are intended to grab the attention of the audience, convey key information, and allow for several presenters to share their ideas in a brief period of time.[1]

- short summary
- highlight important points
- briefly discuss positive / negative aspects
- conclude if the paper should be accepted or not, and why

[1] https://en.wikipedia.org/wiki/Lightning_talk

Paper presentation

For the conference – 15 minutes presentation plus 5 minutes for the reviews.

You're the author. Present your work in 15 minutes.

- Cover problem area, hypothesis, methodology, results, limitations for 15 minutes.
- Unlike at a real conference: Revisit reviews and what you could have done better according to them; if they were helpful or not (5 minutes).
- Like a real conference: Answer questions concerning the paper's content.

Presentation pitfalls

- Do not bore your audience!
- Do not throw them into cold water - explain a few critical fundamentals (e.g. provide technical/statistics background).
- Do not lose yourself in details, make your point clear.
- But also don’t be funny to the point of being ridiculous -you’re at a conference.
- Don’t discredit your work by having crappy misaligned powerpoint slides.

- Use the links we pasted into this presentation!
- Come to us for help / in case of questions.
- Use overleaf (overleaf.com) to use latex without having to install anything and its beamer slides for an effortless presentation theme (you can still customize).
- If you want to use PowerPoint, please take care that your design and alignment doesn’t suck.
- Google Slides is another great way to design slides.