Codebook

Category Name	Category Description	Codes
RESPONSIBILITY AS A REVIEWER	Statements that capture the primary responsibilities of security reviewers mentioned by the participants.	- provide enough / quality / constructive feedback - make sure accepted papers are of quality - not letting bad science in - identify good papers - make sure accepted papers are of sound technique - make sure accepted papers are of interest - check the paper for its contributions - check if the paper contributes to / advances the fundamental knowledge / science / the state-of-the-art - check the paper for fit to conference - help PC chairs to reach a conclusion - check if the paper would have impact - check for validity - let good ideas spread - help the PC to shape the best program - check if claims are backed up - check for novelty - being honest in assessment - check for correctness / accuracy - being fair in assessment - check for new / interesting /practical / difficult problem - evaluation of method - evaluation of result / verification - check for helpfulness to community - check for citations - fair representation and advocation for a paper - checking the writing / presentation of the paper
CHARACTERISTICS OF HIGH-QUALITY REVIEWS	Statements that describe how the participants characterize a high-quality review.	- taking a clear position - providing evidence to support the position - listing out both strengths and weaknesses - providing different and useful POV (reviewers) - providing evidence to support the claims - providing reason/(s) to support the claims - constructive and actionable - polite and respectful - recommending to submit elsewhere (negative) - asking questions - providing different and useful POV (authors) - honest - portray understanding of paper (summary) - detailed - avoiding subjective remarks - finding strengths before weaknesses - clearly written - understandable to the reader - open-minded - separating technical criticism from philosophical criticism - extracting out key criticisms - extracting language / typographical errors - a non-trivial restatement of what the paper is - specific statements on why the paper is good - reinforce and reward good characteristics of the paper - N/A

Category Name	Category Description	Codes
PRECAUTIONS WHILE WRITING REVIEWS	Statements that showcase the precautions taken by participants while writing reviews for security papers.	- no precautions - polite and respectful (non-aggressive / avoid harsh and snarky comments) - neutral - clear - supporting the claim - professional - non-emotional - being constructive / providing suggestions - avoid conflict of interest - positive - prevent self-deanonymization - friendly - encouraging - carefully written - honest - avoid shallow reviews - objective - avoid patronizing of authors - proofreading the reviews - writing a review one wouldn't mind receiving - trying to be in a positive mood - N/A
RED FLAGS TO AVOID – FOR AUTHORS –	Statements that reference an understanding of red flags that the participants mention avoiding while writing security papers.	- over-claiming / in-correct claims - bad writing - not explaining / discussing the results - incomprehensible writing - unclear problem statement/ motivation - non-thorough literature review - not having solid comparison with the state-of-the-art - incorrectly building the expectation - reinventing a known problem - not doing / describing experiments thoroughly - not linking results with claims - having bad / colloquial language - rushing papers - ineffective communication - incremental papers - resubmitting without making changes - having bad grammar - incomprehensible results - incomprehensible graphs/tables/figures - not mentioning the attack model - not clearly outlining contributions - evaluation mistakes - improper / insufficient / shoddy experiments - not mentioning a takeaway message - lacking proper execution - not mentioning / unclear limitations - not treating literature fairly / not objective comparison with literature - misleading title - writing inconsistencies with multiple authors - trivial advancement - not explaining the methodology - technical mistakes - not mentioning the research questions - mistakes in the methodology

Category Name	Category Description	Codes
RED FLAGS TO AVOID – FOR AUTHORS – (CONT.)	Statements that reference an understanding of red flags that the participants mention avoiding while writing security papers.	- plagiarism - lacking ethical considerations in human studies - not motivating certain choices - not pointing out conceptual ideas - mistakes in formulas / algorithms - raw data without explanation - useless and uninteresting papers - not having a convincing security argument - lacking real world applicability - traditional research problem - not showing competency in the topic - not being aware of the related work - not having clear security application - out of scope for a security venue - not backing up the claims - unnecessary obfuscation - hiding details of reproducibility
RECOMMENDATIONS TO LEVERAGE – FOR AUTHORS –	Statements that reference an understanding of recommendations that the participants mention suggest for writing high-quality security papers.	- properly articulated problem statement - novelty - having a good research problem - having a well-written paper - well presented paper - ensuring repeatability / reproducibility - convincing / comprehensive evaluation - clear methodology - interesting and original ideas - applicability - correctness - providing motivation for the problem - having a good / catchy title - having appropriate title - providing proofs of the work - having a strong impact - having takeaways - well organized - showing benefit over the state-of-the-art - explaining the metrics - clear / comprehensive dataset - clear results - analyzing the results - having informative title - doing appropriate / comprehensive experiments - deployable work - qualitative comparison with the literature - good figures - describing the assumptions - clear technical body - explaining data / numbers - having technical depth - evaluation matching the claims - addressing reviewers' doubts in advance - clear and precise contributions - justifying the choices made - great results over writing - new topic over well-written papers - having simulation or experimentation - proper grammar and typo check

Category Name	Category Description	Codes
RECOMMENDATIONS TO LEVERAGE – FOR AUTHORS – (CONT.)	Statements that reference an understanding of recommendations that the participants mention suggest for writing high-quality security papers.	- authors taking care about writing - explanatory captions - explaining the trade-offs - quality over presentation - novelty over presentation - impact over presentation - building effective system - internal consistency - methodological validity - meaningful results over generalizability - surprising and insightful techniques - mentioning biases and limitations - advancing science - execution over contribution - execution over novelty - contributions supported by experimental evidence - ”wow” moment - title reflecting novelty - cover variety of datasets - experiments supporting the claims - providing broader insight - generating follow-up research - falsifiable and verifiable science - having top down writing / presentation approach - having a high-level figure - following established norms for evaluation - utility - clear statement for solution - case study to contextualize the problem - defining the threat model - formulation of research questions - describing experiments to answer each research question - providing backup for conclusions drawn - contextualize the field in related work section
DELEGATION PROCESS	Statements expressing the participants' purpose of delegation, approach, and opinions on the delegation process in security conferences.	- increase confidence level - expert opinion - feedback and second opinion - reduce reviewing load - time constraints - development and training of students - being fair - setting the criteria for delegation - delegating to external experts - delegating to PhD students, postdocs - advantages / disadvantages of delegating to junior researchers/PhD - trusting the reviews - supervising before submitting - write your own review; discuss and debate - follow conference guidelines - delegation as a balanced act - PC doing nothing and getting credit - pushback from PC when delegation denied - giving recognition to external reviewers/delegates - need for more delegates - difficult to manage review quality with delegation - large PC over delegation - delegation: as a common practice

Category Name	Category Description	Codes
DELEGATION PROCESS (CONT.)	Please refer to the above description.	- mixed feelings towards delegation - Sentiment (negative=−1, positive=1)
SYSTEMATIC ISSUES WITH THE REVIEW PROCESS	Statements expressing the participants' complaints with the current reviewing model of security conferences and suggestions to improve the current state. Also include, statements expressing general comments and opinions on the current reviewing model of security conferences.	- from reading paper to writing reviews - scheduling the reviewing process - "number of hours" spent - variability / non-variability in review time - papers that take more time - papers that take less time - getting non-core paper is rare - getting a broad range of papers - familiar with the subject area - picking papers that are difficult to review - some PC do not follow rules - negative in scoring - randomness - evaluation metrics are not universal - scalability challenges and redundancy issues - double-blind and peer-review - need for expansion of PC? - need for across-community communication - need for accountability - bias for / against certain areas - way more submissions - lack of good match and need for balanced PC - favor-ism - quota for accepted papers - reviewers are on multiple PC - focusing on attack is killing innovation - unfair reviews and fair / unfair resubmission - how advocating for paper can make / break a paper - need for objectivity from both sides - usefulness of shepherding - usefulness of reviewing history - usefulness of rebuttals - pressure on PC chair - pros and cons of old model - suggestions - help from PC - negative remarks - positive comments - Sentiment (negative=−1, positive=1)
IMPACTS OF ROLLING SUBMISSIONS ON REVIEWERS	Statements where the participants describe how the revised model with rolling submissions impacts the reviewers of security conferences.	- spread out load - affecting review quality - difficult to manage - continuous load - exhausting - has the reviewing load really decreased? - growing pain - mixed comments
IMPACTS OF ROLLING SUBMISSIONS ON AUTHORS	Statements where the participants describe how the revised model with rolling submissions impacts the authors of security papers.	- procrastination - increased efforts - learning from early submissions - increased flexibility - other positive comments
REVIEWERS' COMMENTS ON ROLLING SUBMISSIONS	Statements expressing the participants' opinions on the new change of multiple rolling deadlines to security reviewing process.	- conversation with authors is possible - resubmission with rolling model - disrupts timeline of research

Category Name	Category Description	Codes
REVIEWERS' COMMENTS ON ROLLING SUBMISSIONS (CONT.)	Statements expressing the participants' opinions on the new change of multiple rolling deadlines to security reviewing process.	- need for better coordination among conferences for deadlines - positive comments on the revision option - comments on "number of deadlines" - acceptance based on rounds - neutral towards - negative comments on rolling submissions - positive / encouraging comments on rolling submissions - Sentiment (negative=-1, positive=1)