An Analysis of the Peer Review Process in Security

CSET 2025

Adam Doupé
https://adamdoupe.com
Arizona State University

About Me

- Involved in research at UCSB as a Master's student in 2008
- Took a brief detour to Microsoft as a Software Developer in 2009
- Came back to UCSB for a PhD in 2010
- Started as Assistant Professor at ASU in 2014

Stats (that I never wanted to calculate)

- Reviewed for ~17 journals
- Served on ~60 PCs (workshops and conferences of all kinds)
- Reviewed ~800 papers
- Track Chair for CCS, Vice Chair for USENIX Security, Associate Chair for IEEE Security and Privacy

Why are we here?

Learn novel things and communicate them

LE

IOVRNAL DES SÇAVANS

Du Lundy V. Ianvier M. DC. LXV.

Par le Sieur DE HEDOVVILLE.

A PARIS,

Chez IEAN CVSSON, ruë S. Iacques, à l'Image de S. Iean Baptiſte.

M. DC. LXV.

AVEC PRIVILEGE DV ROY.

PHILOSOPHICAL

TRANSACTIONS:

GIVING SOME

ACCOMPT

OF THE PRESENT

Undertakings, Studies, and Labours

OF THE

INGENIOUS

IN MANY

CONSIDERABLE PARTS

OF THE

WORLD.

Vol I.

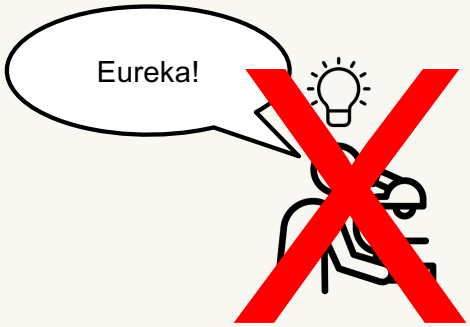
For *Anno* 1665, and 1666.

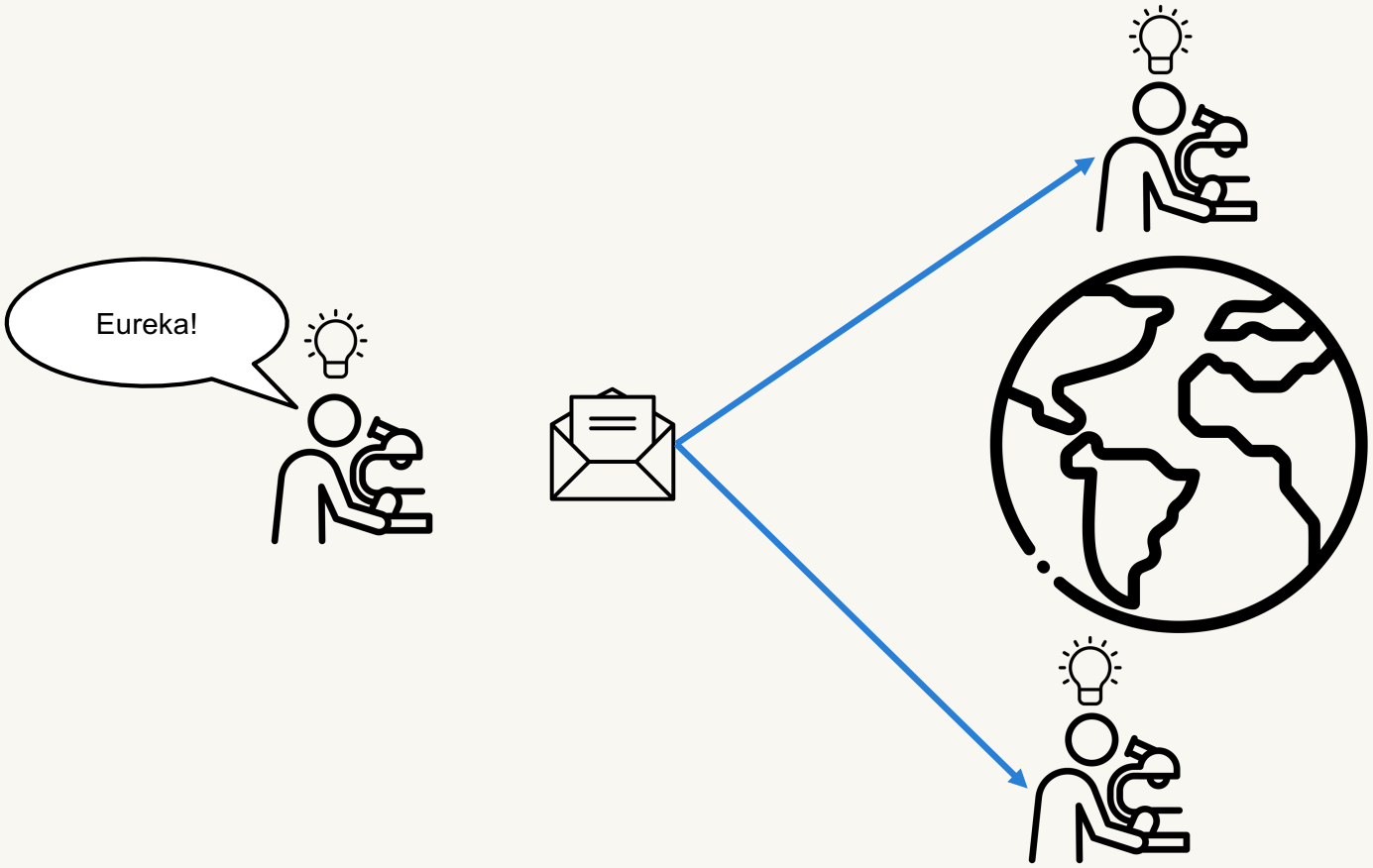
In the *SAVOY*,

Printed by *T. N.* for *John Martyn* at the Bell, a little without *Temple-Bar*, and *James Allestry* in *Duck-Lane*,

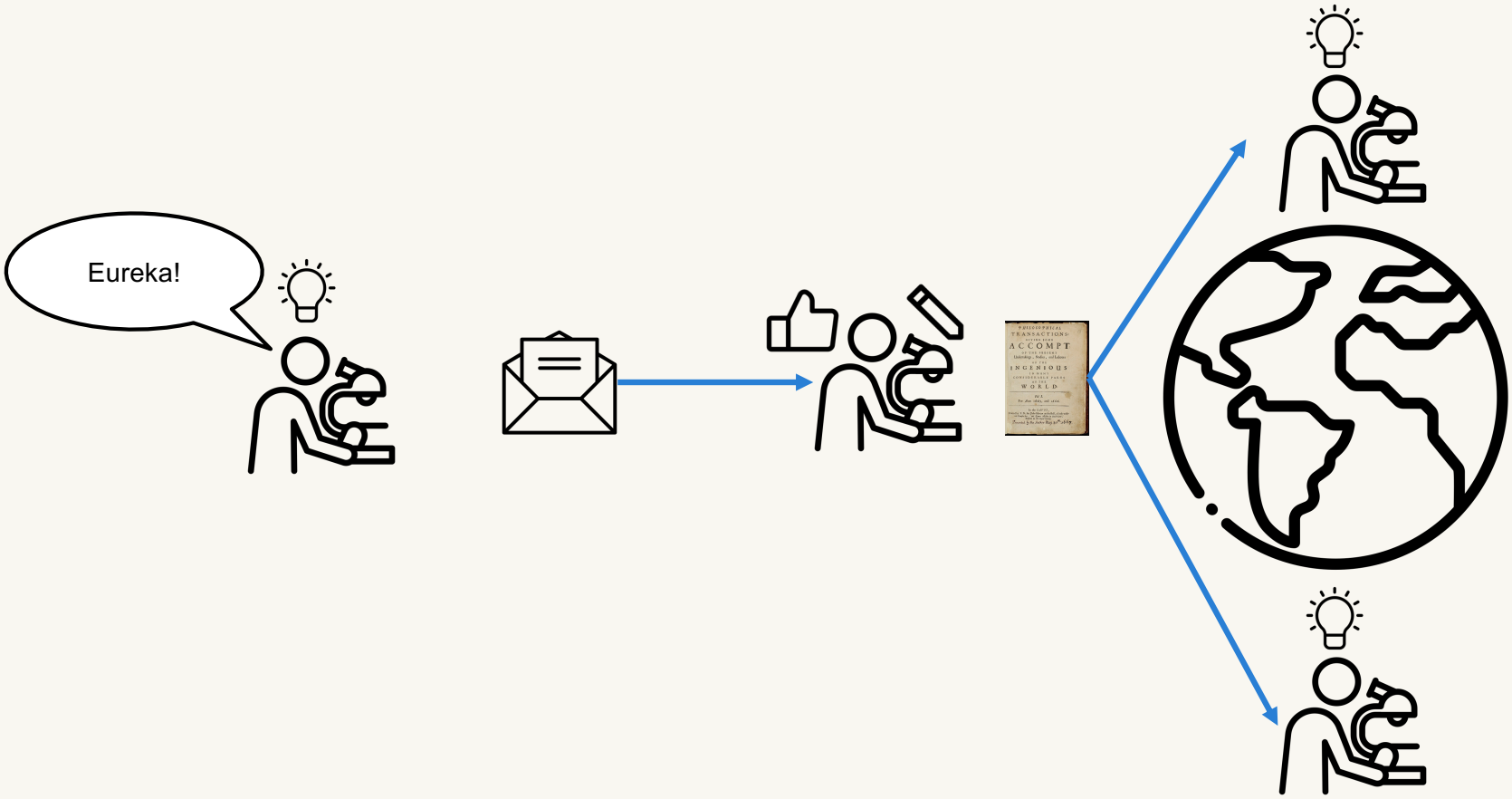
Printers to the *Royal Society*.

Presented by the Author May. 30th 1667.

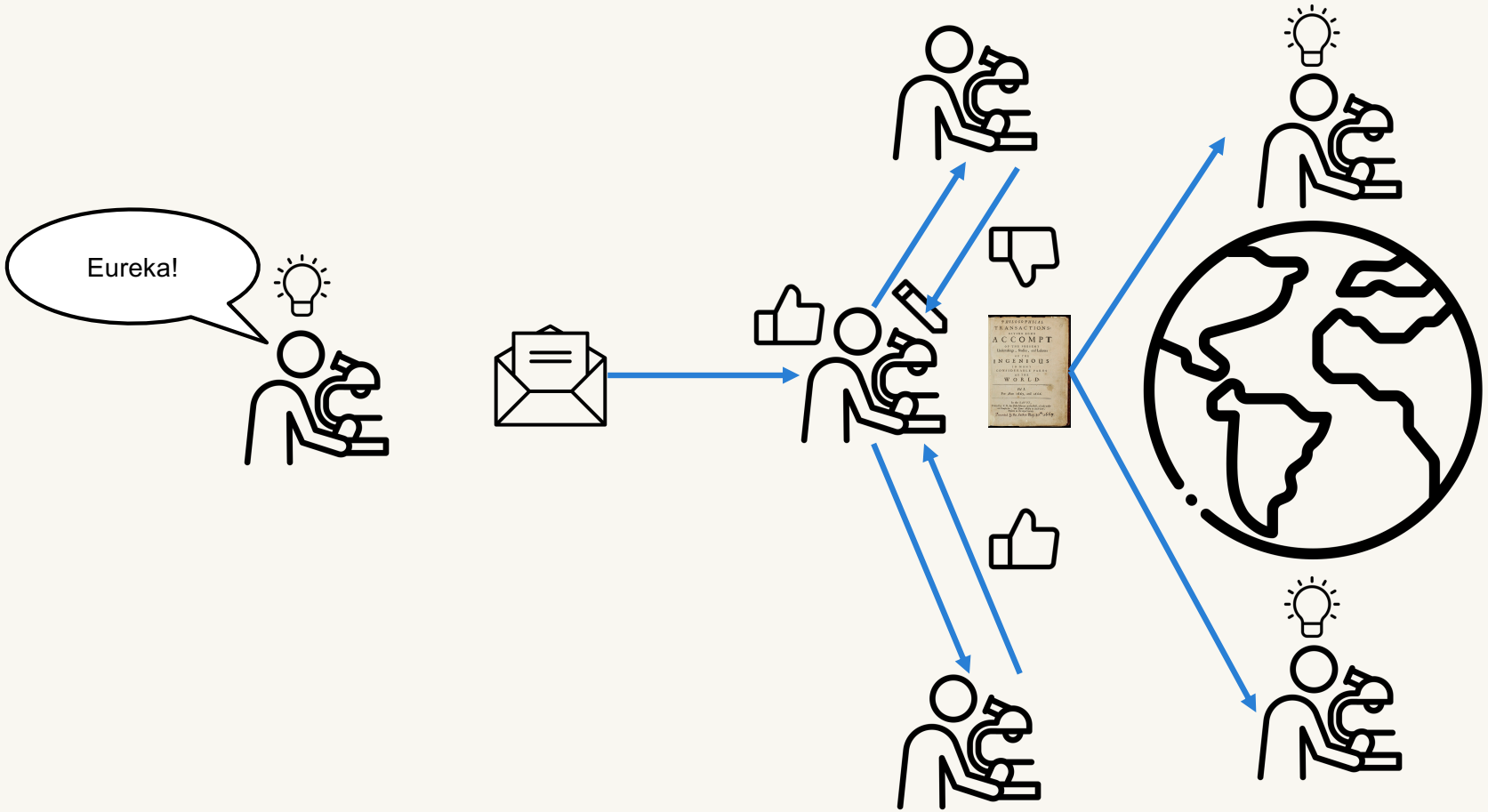

Eureka!


Eureka!

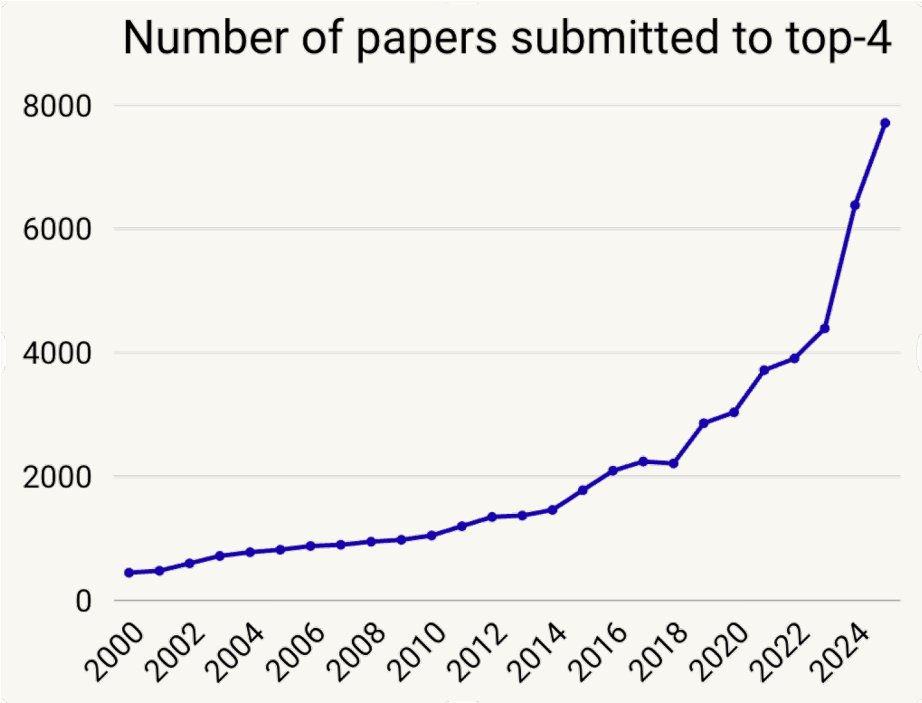
Peer Review



Modern Peer Review



sefcom
security engineering for future computing



https://www.s3.eurecom.fr/~balzarot/security-circus/circus_stats.html
https://github.com/puzhuoliu/Computer-Security-Conference-Acceptance-Rate

Paper submissions

Challenges PC workload

Quality/quantity of reviews

sefcom
security engineering for future computing

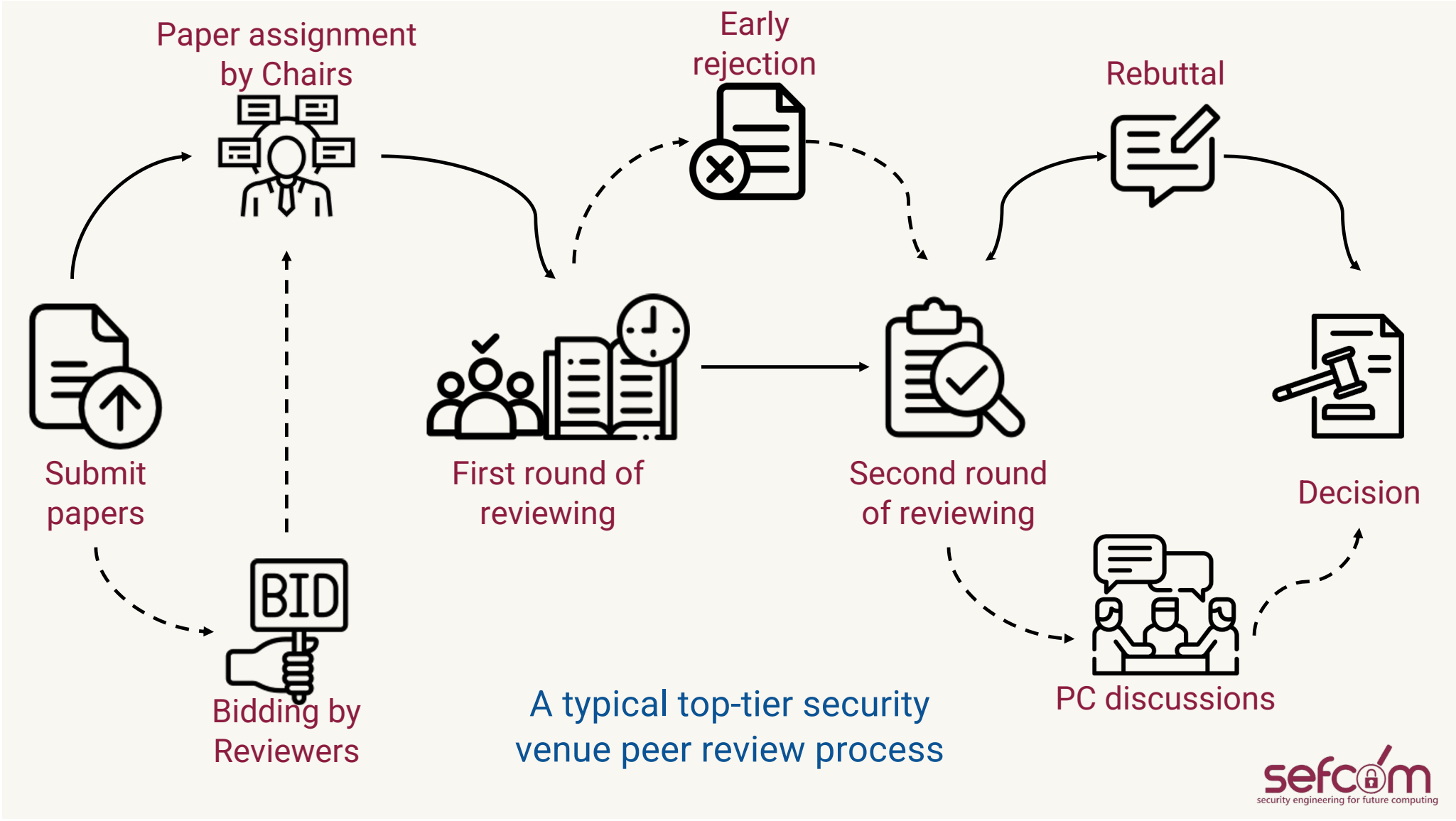
Submit papers

Decision

"Flawed, but like democracy we don't have a better system": The Experts' Insights on the Peer Review Process of Evaluating Security Papers

Ananta Soneji, Faris Bugra Kokulu, Carlos E. Rubio-Medrano, Tiffany Bao, Ruoyu Wang, Yan Shoshitaishvili, and Adam Doupé, "Flawed, but like democracy we don't have a better system": The Experts' Insights on the Peer Review Process of Evaluating Security Papers," in Proceedings of the IEEE Symposium on Security and Privacy, May, 2022.

sefcom
security engineering for future computing


Paper assignment by Chairs
Early rejection
Rebuttal
Submit papers
First round of reviewing
Second round of reviewing
Decision
BID
Bidding by Reviewers
PC discussions
A typical top-tier security venue peer review process
sefcom
security engineering for future computing

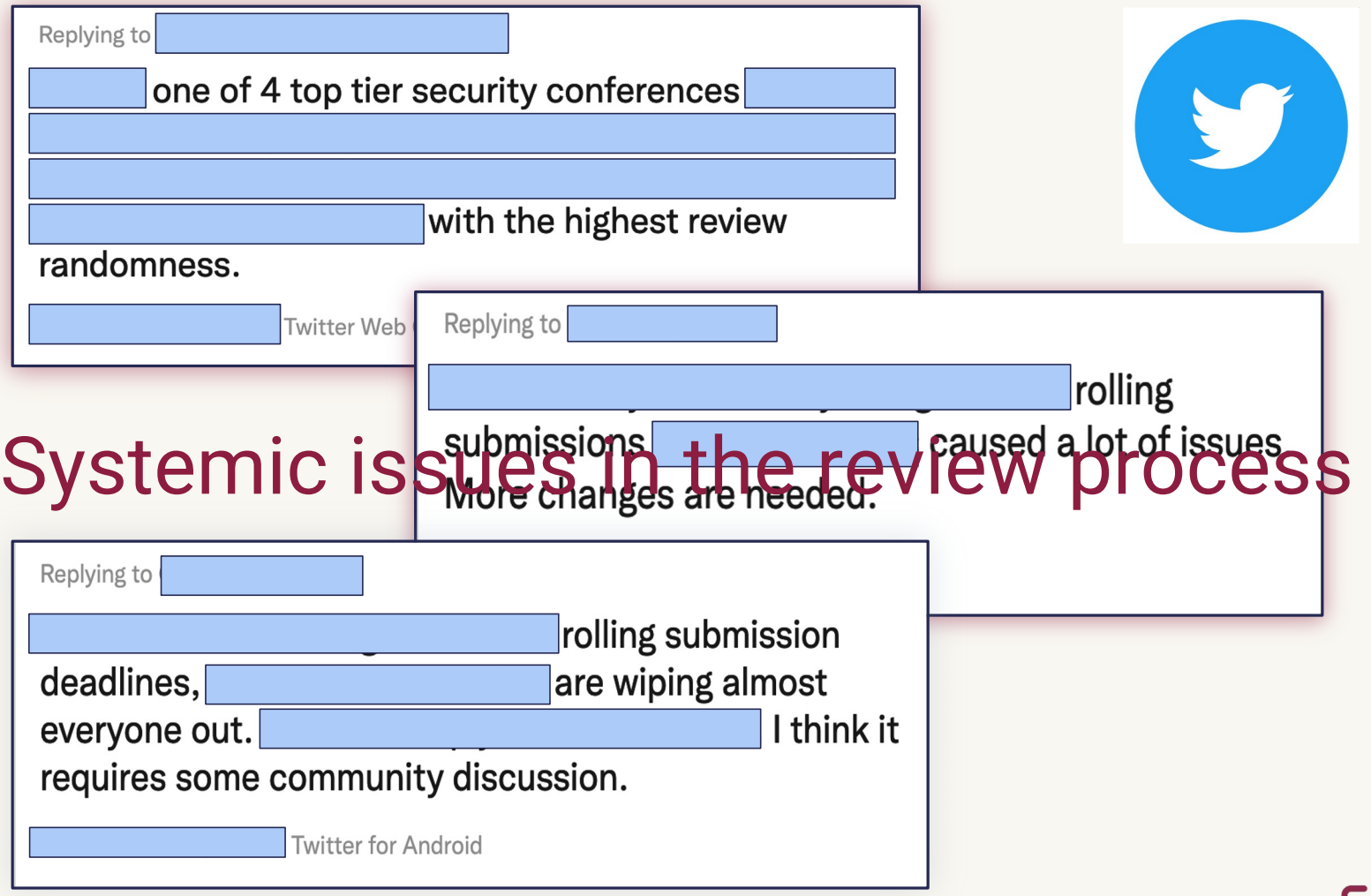
Recruitment Process

~300
PC members

Invited: 70
PC members

Interviewed:
21
PC members
(12 PC chairs)

sefcom
security engineering for future computing



Systemic issues in the review process

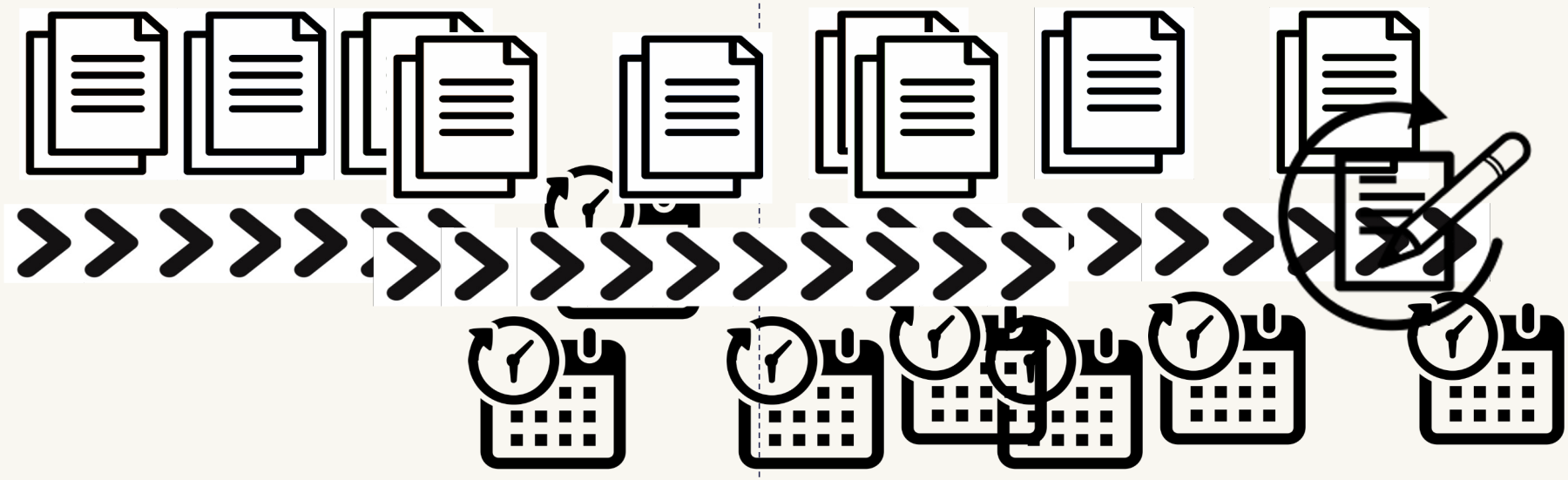
sefcom
security engineering for future computing

Randomness of reviews

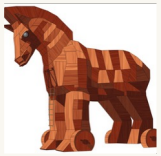
> If we can be more accurate in our reviews, then yeah, it (gaming the system) is a horrible thing to do. But, we are not; it works. And so, somebody whose job depends on getting these papers in, why would you blame them for doing something that works.

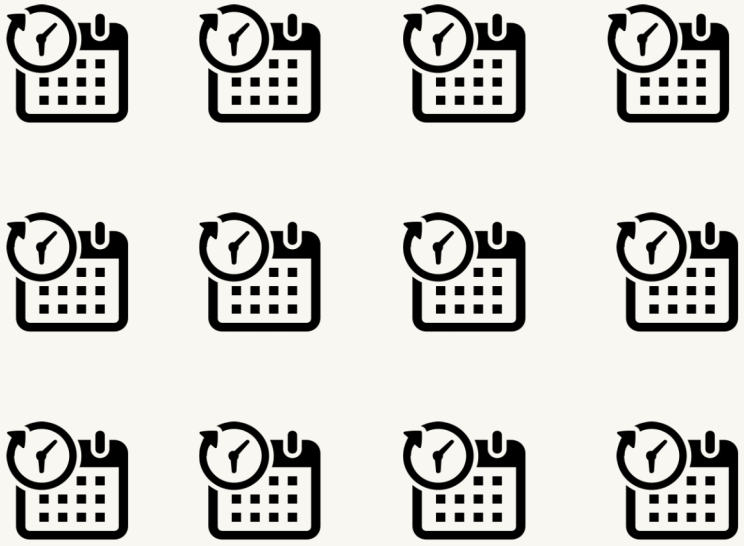
- P7, Chair Participant

Rolling submission deadlines



IEEE S&P





2012 2020-22 2020

Accept
Minor Revise
Major Revise
Reject & Resubmit
Reject

Accept
Minor Revise
Major Revise
Reject

Accept
Major Revise
Reject

sefcom
security engineering for future computing

Reviewer sentiments on the revised model

- Review more fairly
- Increased review quality
- Possibility of dialogue
- Writing more constructive reviews (P10)

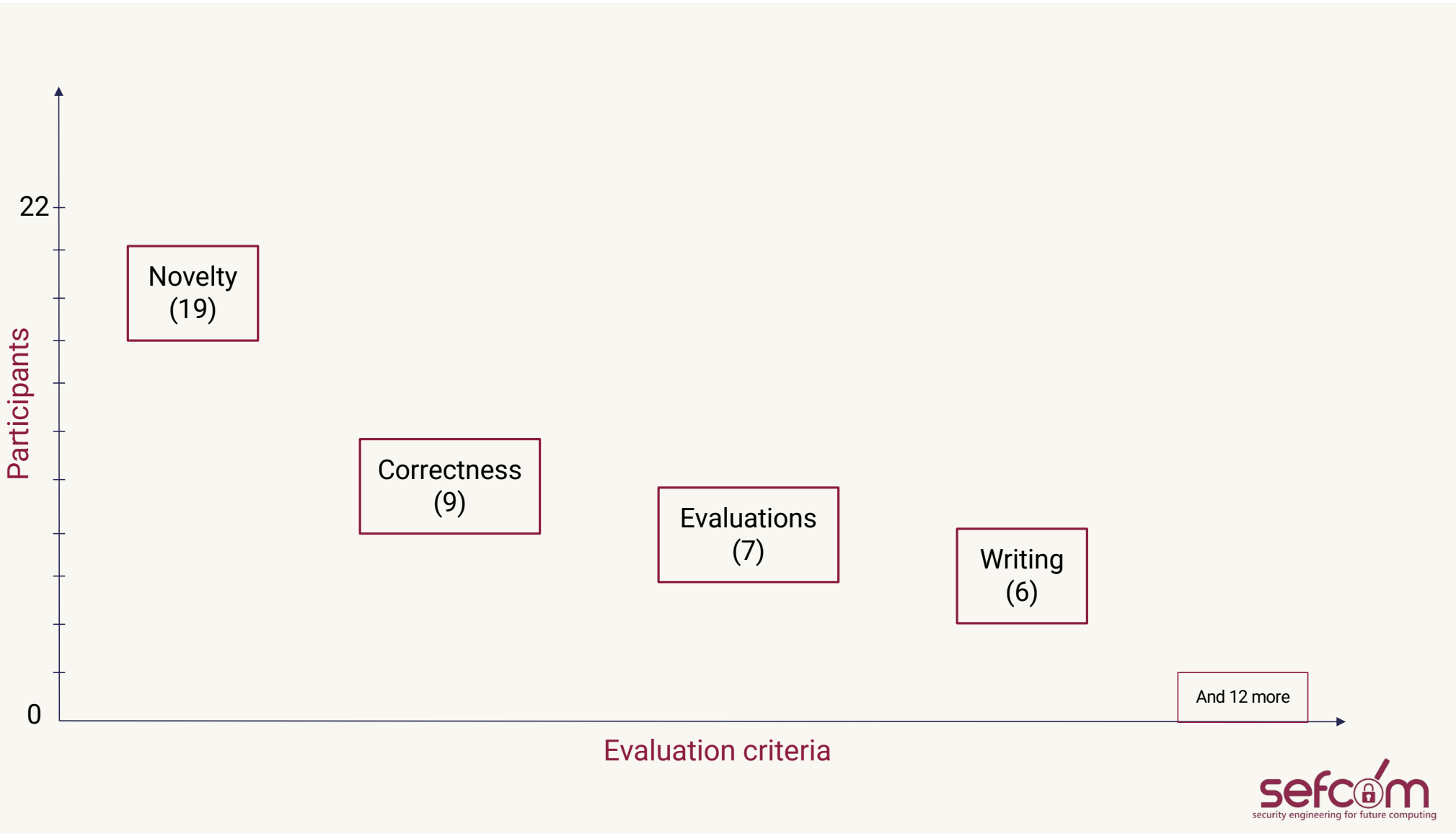
- Increased workload distribution
- Reduced turnaround times
- Less time to write satisfactory reviews
- Exhaustion
- Focus only on how ***ready*** the paper is
- Growing pain to switch (P7)

The Experts' Insights on the Peer Review Process of Evaluating Security Papers

sefcom
security engineering for future computing

Which evaluation metrics do security reviewers use?

> “Security is an area where there are not any kind of hardened established metrics for evaluating security.
>
> - P19, Chair Participant


22
0
Participants
Novelty
(19)
Correctness
(9)
Evaluations
(7)
Writing
(6)
And 12 more
Evaluation criteria

Novelty: a subjective metric

> Novelty is definitely subjective. This is something where different reviewers will see different values out of a paper. Novelty is possibly multi-dimensional in itself in terms of, what are we learning from this, and what information from this is valuable?
>
> - P19, Chair Participant

Red flags

- Total 52
- Content-related
- Argument-related
- Writing-related

> We know that the acceptance rate is so low (at these conferences) that sometimes there can be a tendency from the reviewer side to look for reasons to reject instead of reasons for accepting a paper.

- P9, Non-chair Participant

> But I think it's important to fight that instinct and to always frame reviews constructively and positively.

- P10, Chair Participant

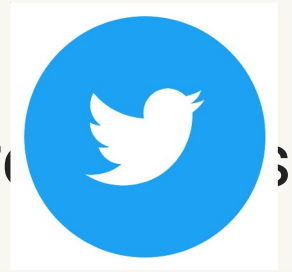
sefcom
security engineering for future computing

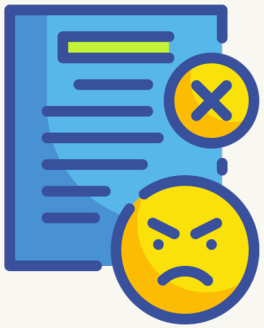
Recommendations

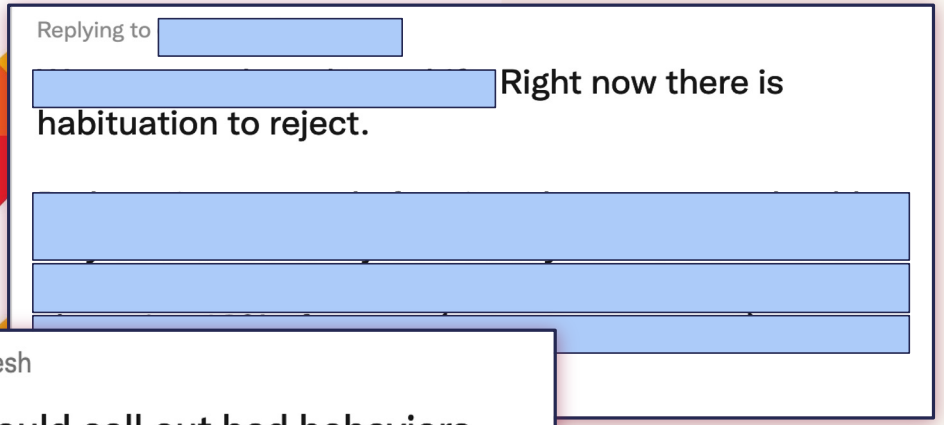
> Of course, I want to review early but quite often I did not.
>
> - P17, Chair Participant

Rec. #1: Help reviewers with timely review submissions

Rec. #2: Recognize and reward good r[redacted]s



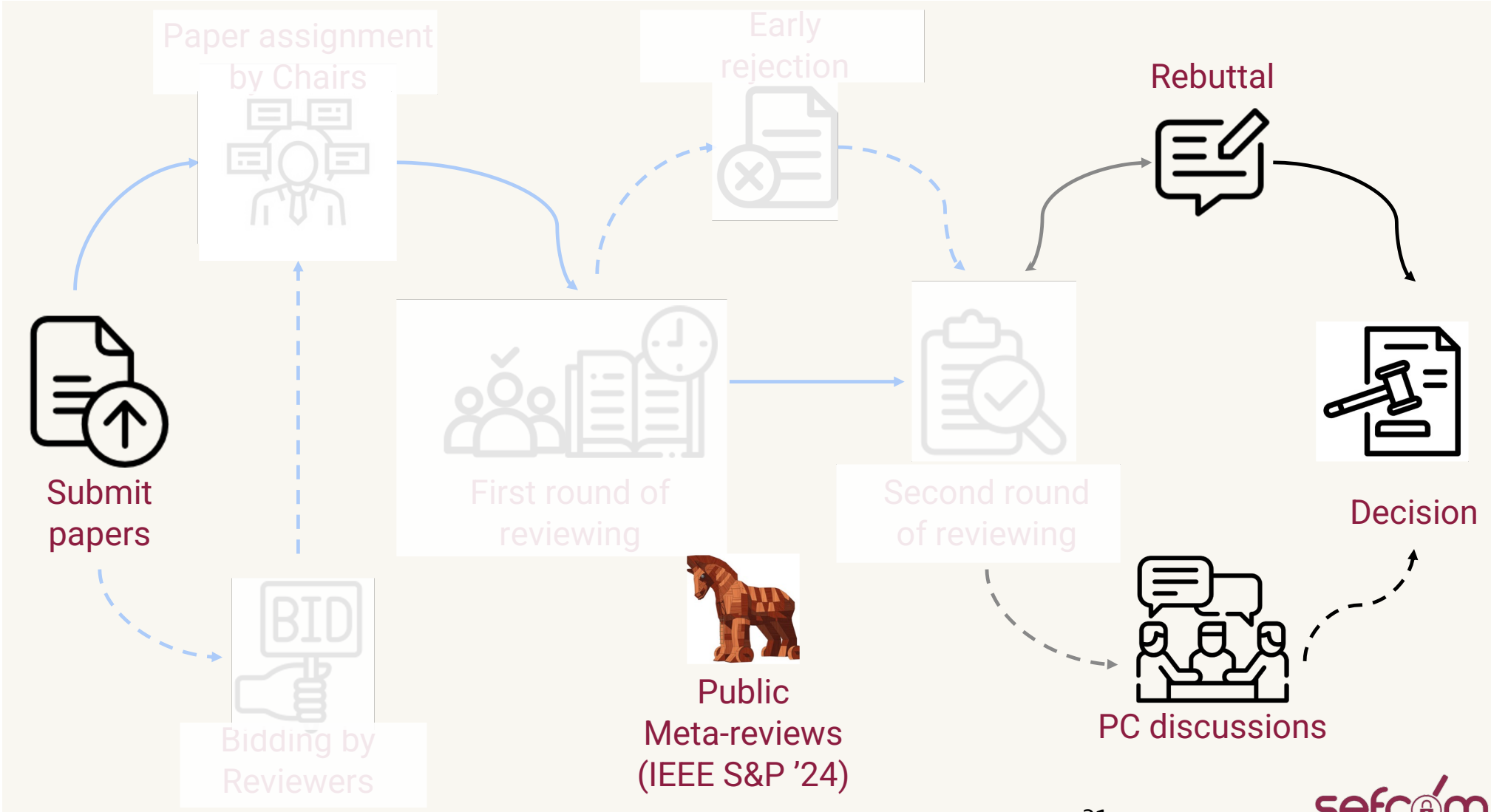




sefcom
security engineering for future computing

Submit papers

Decision

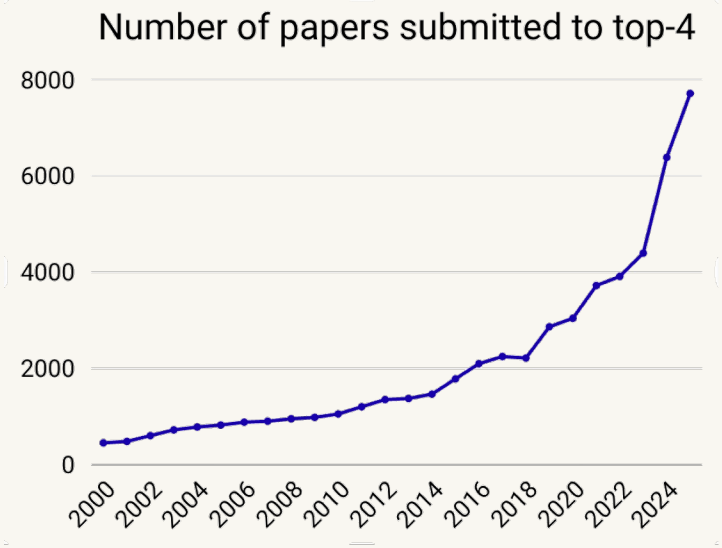


sefcom
security engineering for future computing

Rec. #3: Improve transparency

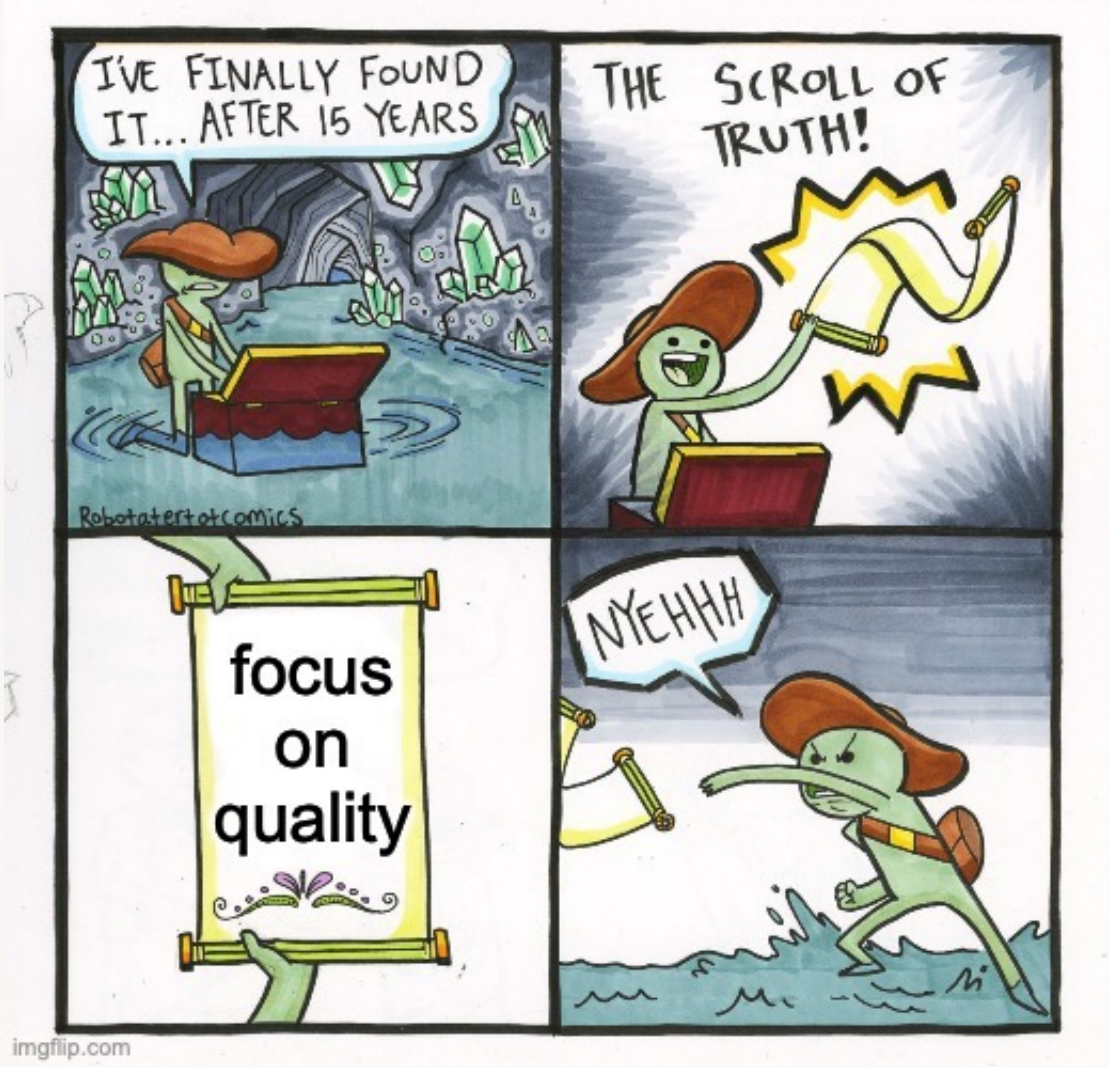

YEAH, WELL THAT'S JUST LIKE,
YOUR OPINION, MAN.
quickmeme.com

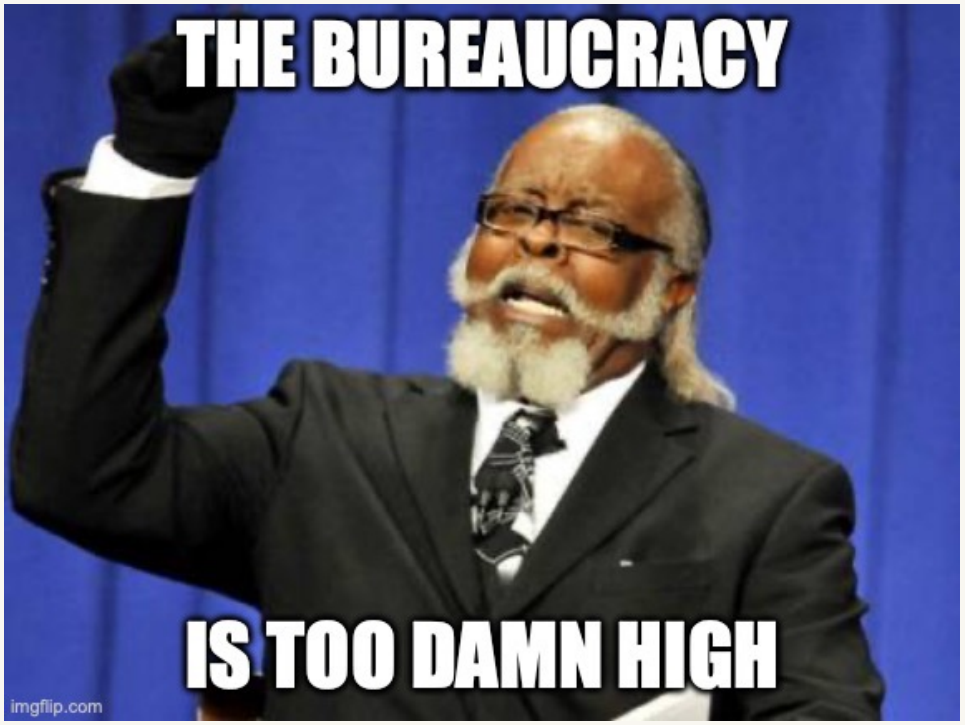

OPTIMISTIC PRIME


Number of papers submitted to top-4
8000
6000
4000
2000
0
2000
2002
2004
2006
2008
2010
2012
2014
2016
2018
2020
2022
2024


Congratulations
Presented to the security community
for doing your best peer review
You did it!
Date
Signed
imgflip.com

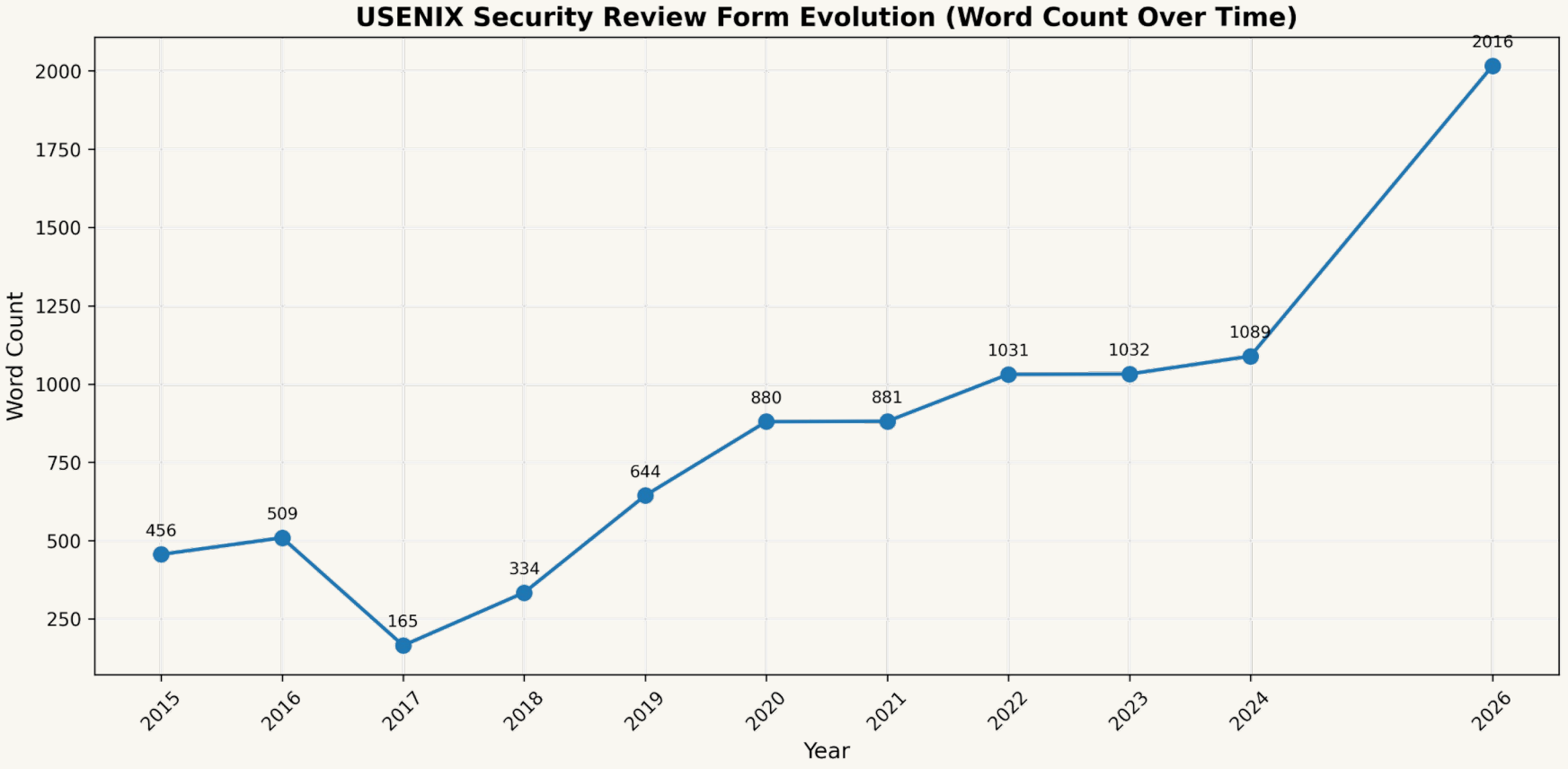

WE HAVE SO MANY PAPERS
OUR COMMUNITY IS GROWING
imgflip.com
GENIUS


I'VE FINALLY FOUND IT... AFTER 15 YEARS
Robotatertotcomics
THE SCROLL OF TRUTH!
focus on quality
NYEHHH
imgflip.com


THE BUREAUCRACY
IS TOO DAMN HIGH
imgflip.com

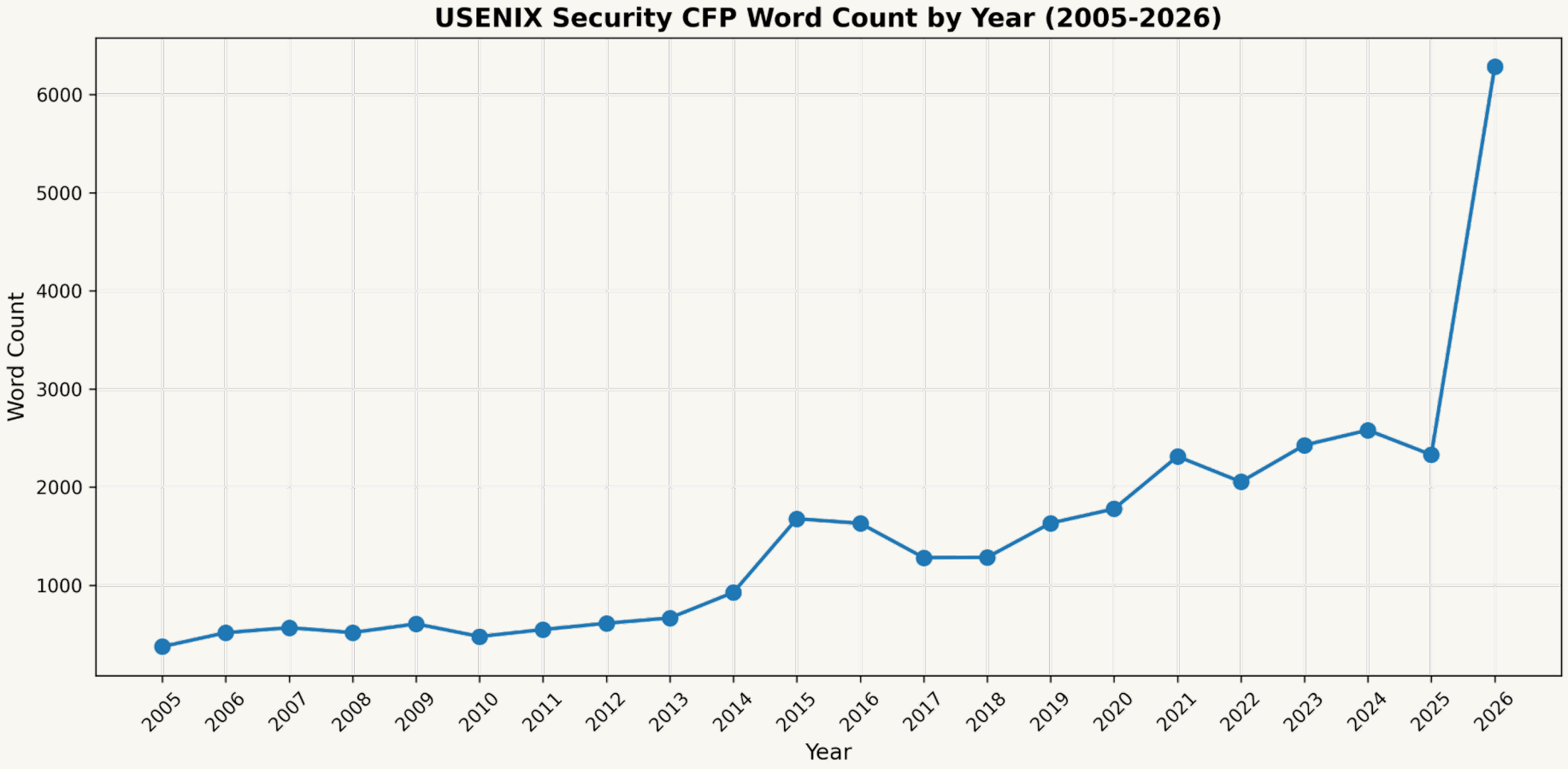
> Of the 2,385 submissions, 350 (14.7%) were administratively rejected (245 in Cycle 1 and 105 in Cycle 2) for not being compliant with the submission policies.

- Message from the USENIX Security ’25 Program Co-Chairs



Best effort data collection by
Adam Doupé

sefcom
security engineering for future computing



Best effort data collection by
Adam Doupé

sefcom
security engineering for future computing

sefcom
security engineering for future computing

> COI developed during the reviewing process: Authors starting new collaborations during the review period should make all their new collaborators aware that they have submitted papers to S&P and refrain from starting such collaborations as they can create COI.
>
> - 2026 IEEE Security and Privacy CFP

Fairness Should Not Come at the Expense of Quality

Limits on Science

> … six individuals appear as co-authors on 20 or more submissions, with two authors appearing on 36 and 39 submissions respectively. At such volume, it becomes difficult not to question the nature and depth of the contributions attributed to these individuals.
>
> - Message from the USENIX Security ’25 Program Co-Chairs


Ah [redacted] here we go again.

> Bulk Submissions: Special rules apply to all submissions by authors who submit more than 3 non-SoK papers. If the paper has been previously considered at other conferences, journals, or workshops, the submitted version must include an appendix that lists: (a) the year and full name of those venues, (b) the complete set of reviews, and (c) detailed description of the changes made since.
>
> - 2016 IEEE Security and Privacy CFP

https://www.ieee-security.org/TC/SP2016/cfpapers.html

sefcom
security engineering for future computing

> Bulk Submissions: Special rules apply to all submissions by authors who submit more than 3 non-SoK papers. **The title of every submission from such an author must start with "BULK SUBMISSION:"**. If the paper has been previously considered at other conferences, journals, or workshops, the submitted version must include an appendix that lists:

- 2017 IEEE Security and Privacy CFP

https://www.ieee-security.org/TC/SP2017/cfpapers.html

Bulk submissions

Some submissions specially-marked with pre
- only when authors had >3 non-SoK submis
- **controversial**

Non-bulk acceptance rate: 53/378 = 14%

41 bulk out of 419 submitted, with 7/60 accepted; rate of 7/41 or 17%

Not successful: policy has only a limited effect, is controversial & annoying

- Will **NOT** be continued

https://www.ieee-security.org/TC/Reports/2017/SP2017-PCChairReport.pdf

> … six individuals appear as co-authors on 20 or more submissions, with two authors appearing on 36 and 39 submissions respectively. At such volume, it becomes difficult not to question the nature and depth of the contributions attributed to these individuals.
>
> - Message from the USENIX Security ’25 Program Co-Chairs

Bulk Submission Limitation

Each author can submit a maximum of six (6) submissions per cycle, 12 total. That is, an author cannot be listed on more than six submissions per cycle. We encourage the authors to select their highest-quality papers for submission to NDSS Symposium 2026.

Cap on number of submissions

Any author may not submit more than 6 papers per cycle. In the event an author submitted more than 6 papers in a cycle, all the papers they submitted in that cycle will be desk-rejected.

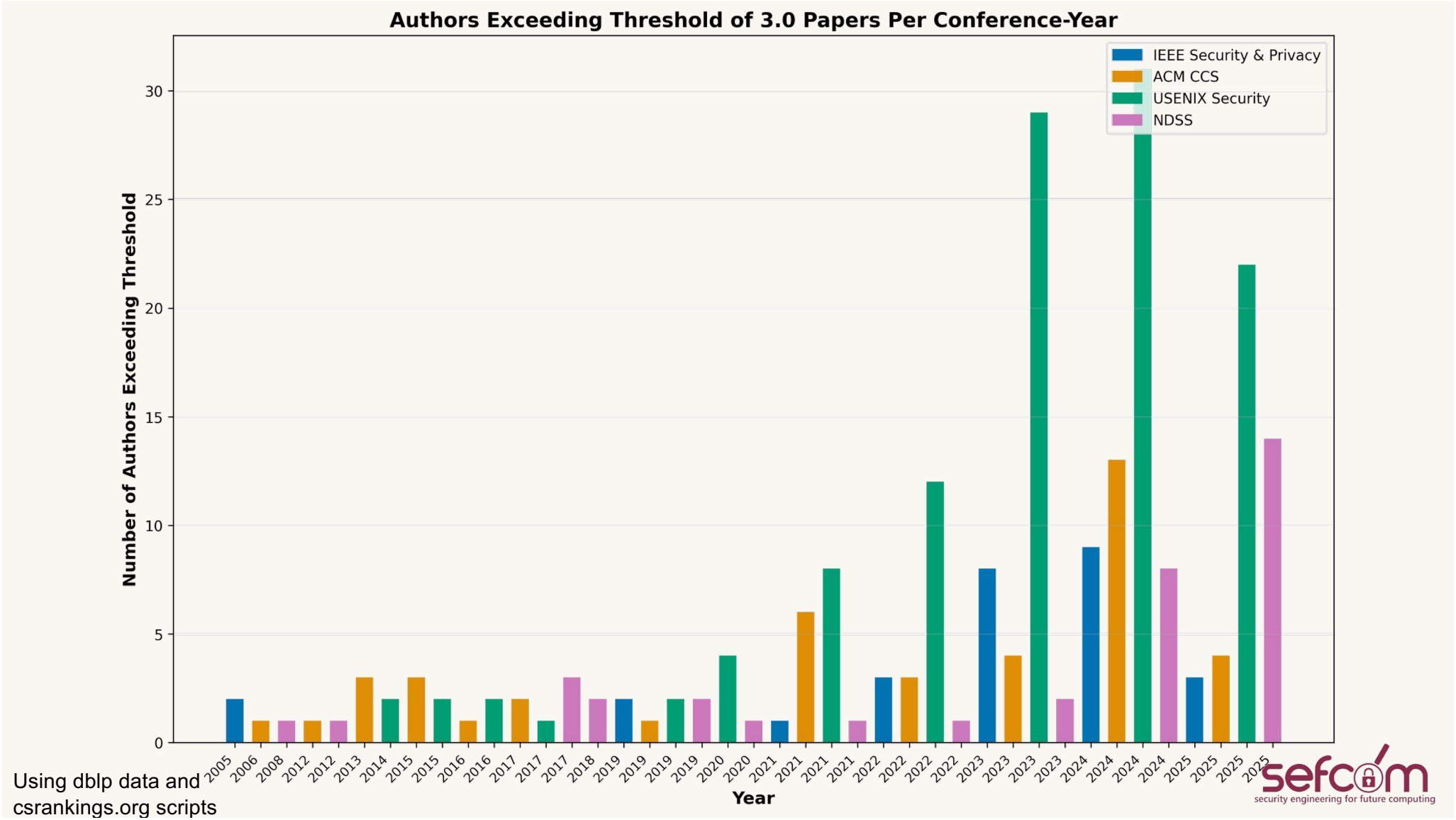
Bulk Submissions

Each author can submit at most seven papers per cycle to USENIX Security 2026. For authors submitting more than seven papers, the chairs will only retain the seven papers with the lowest submission numbers. This rule is enforced per author, i.e., authors may have papers rejected even if they stay under the limit in cases where a co-author violates the requirement. Once the registration deadline has passed, the submission's author list may not be changed. Even if one of the first seven papers is later withdrawn, this does not change the reject status of the paper(s) submitted 8th+ as of the submission deadline. Any attempts to bypass this rule (e.g., by having multiple HotCRP accounts) will be escalated to the Steering Committee.

Issue 1: Assuming Uniform Distribution

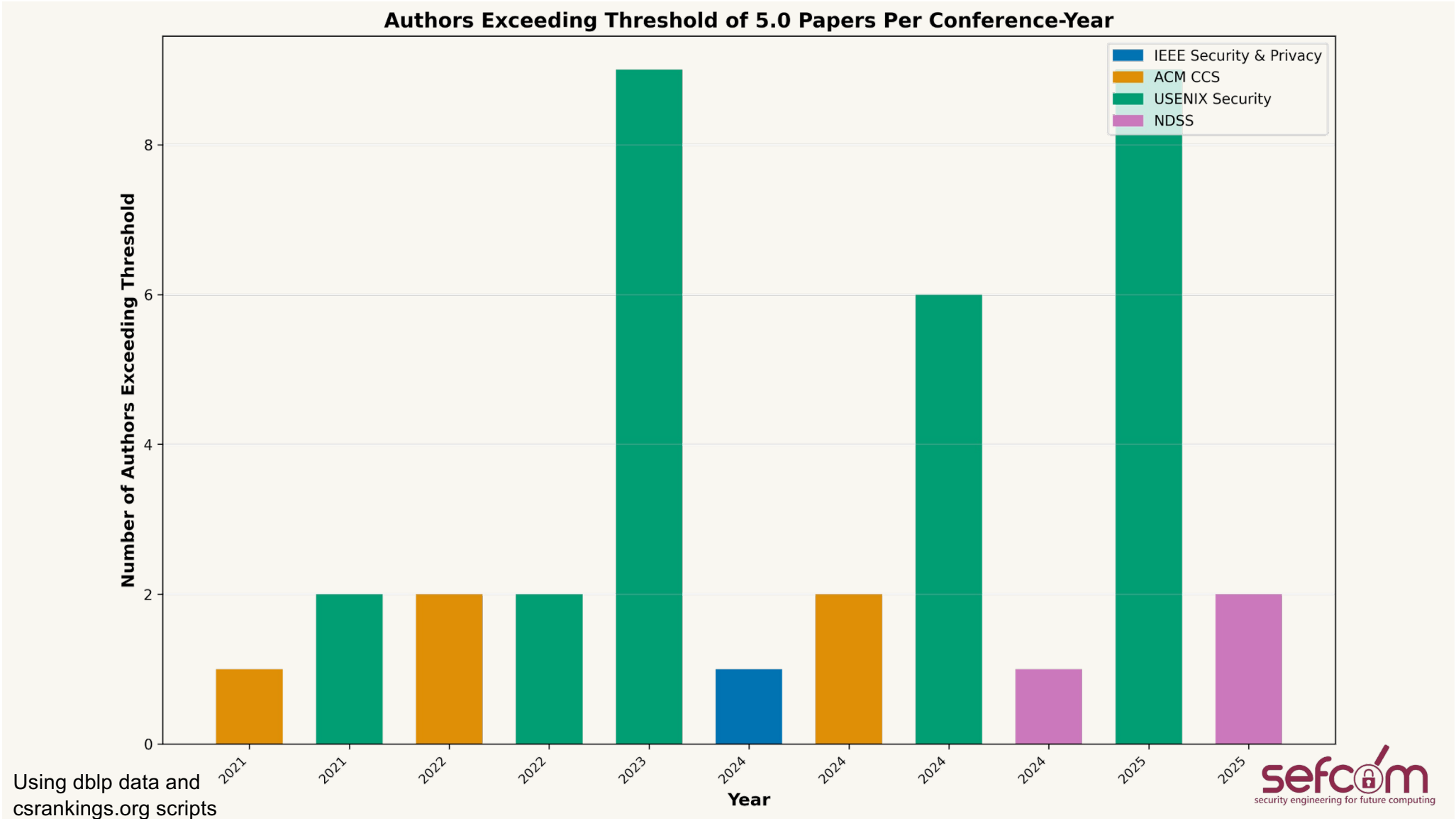
USENIX Security Example

- Limit is 12 total
- At 17% acceptance rate, that's 2 papers published (the data that we can see)
- Let's say >=4 to be conservative (33% acceptance rate)



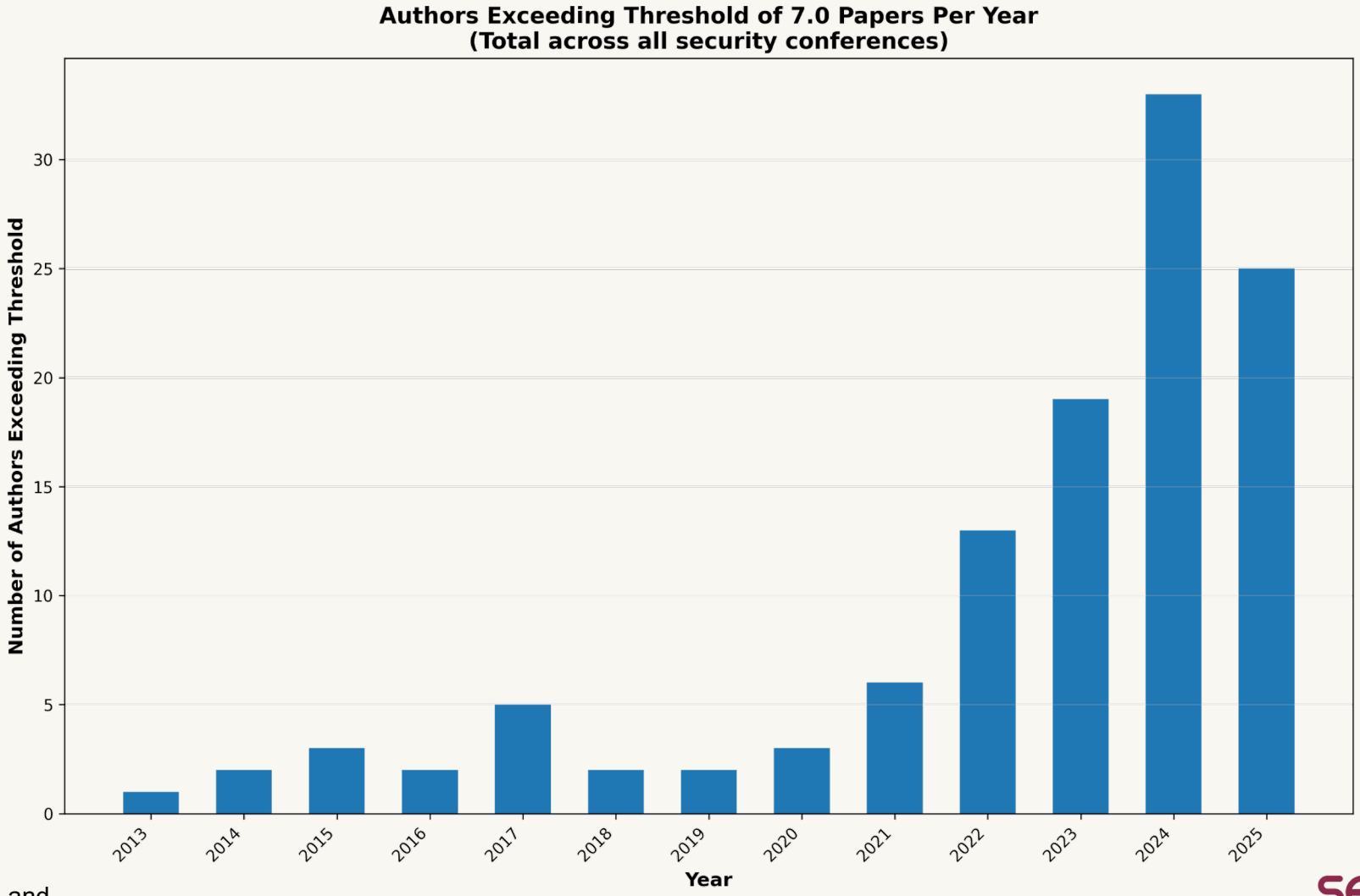
Using dblp data and csrankings.org scripts

sefcom
security engineering for future computing



Using dblp data and csrankings.org scripts

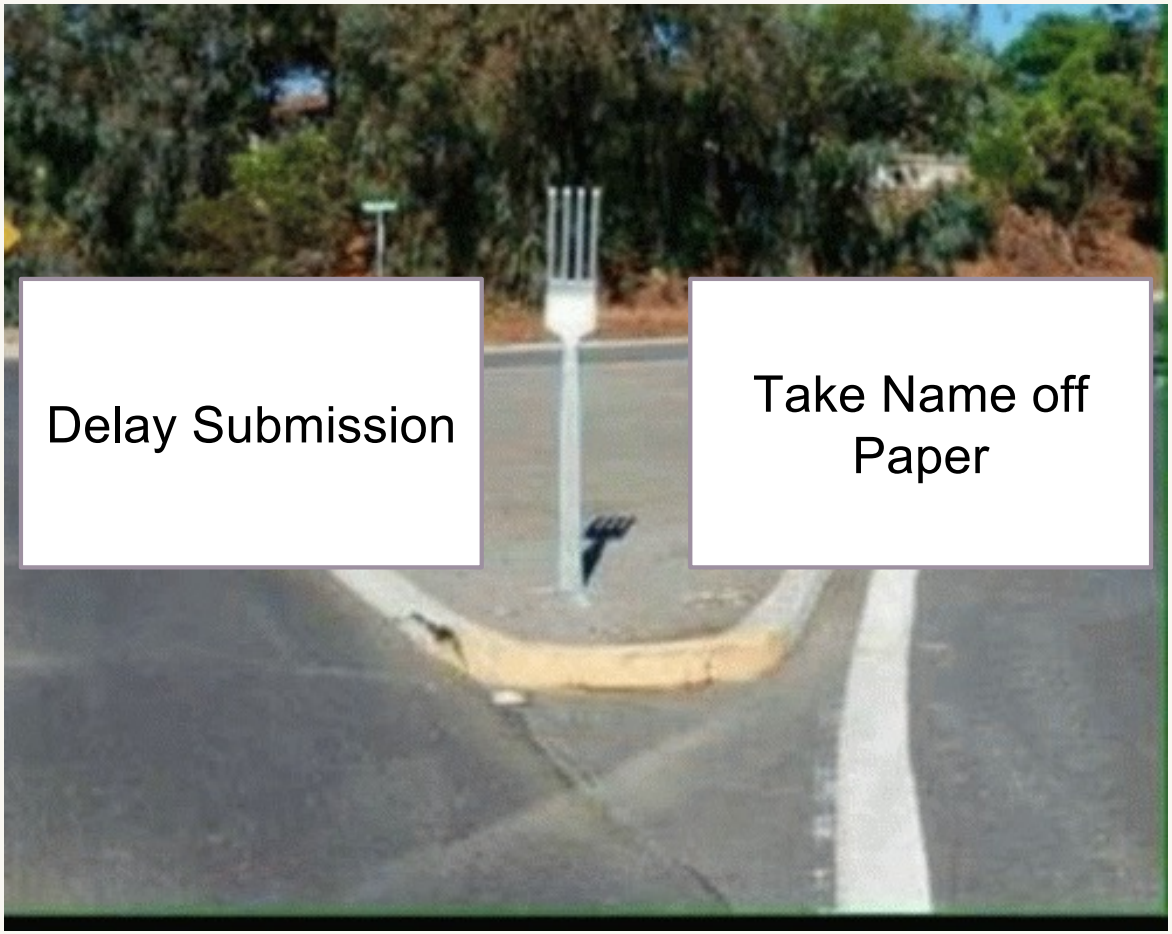
sefcom
security engineering for future computing



Using dblp data and
csrankings.org scripts

sefcom
security engineering for future computing

Issue 2: What to do?



Delay Submission

Take Name off Paper

Take Name off Paper

- Conflict of Interest
  - Advisor's conflicts not specified on submission
  - Publication does not generate future conflicts
- Misleading CV for student: paper in CV seen as no advisor input

- **Ghost Authorship*** – when co-authorship by someone who did contribute significantly to a Work is concealed to hide a potential conflict of interest with reviewers, hide an author who drafts a Work on behalf of an industry backer, or in some other way deceive the reader about the authors involved. ACM views ghost authorship as problematic, since the ghost author is not in a position to verify the validity of the content of the article…only to ensure that the article is readable and clearly presented, which is why ghost authors do not meet ACM's criteria for authorship.

https://www.acm.org/publications/policies/frequently-asked-questions

Address Authorship Concerns Without Adding Harm

Require Contribution Statement!
Post publication investigation about authorship contributions?

sefcom
security engineering for future computing

Continue Experimenting!

sefcom
security engineering for future computing

An Analysis of the Peer Review Process in Security

CSET 2025

Adam Doupé
https://adamdoupe.com
Arizona State University