Message from the USENIX Security ’23 Program Co-Chairs

On behalf of USENIX, we want to welcome you to the proceedings of the 32nd USENIX Security Symposium. Over more than a year and a half, we have been honored to work with everyone who helped make the symposium a reality. We are proud of what our community has accomplished together.

We drew upon the rich history of the USENIX Security Symposium for guidance in building this year’s technical program. We retained a multi-cycle submission model, with Summer (June 7, 2022), Fall (October 11, 2022), and Winter (February 7, 2023) submission deadlines. We continued to use a double-blind review process. To address the record volume of submissions while ensuring that accepted papers received crucial feedback, we preserved a two-round review process. Papers that received support in the first round proceeded to the second round, where authors received additional reviews and an opportunity to respond to the reviewers’ thoughts. We also continued to require reviews from prior submissions, allowing authors to explain how they addressed these reviews. We revealed the existence and content of prior reviews after reviewers submitted an initial version of their review but before final decisions.

One significant change this year was the addition of program vice co-chairs. These vice chairs managed significant logistical aspects of the reviewing process. Among their many contributions, vice chairs helped ensure that paper decisions were a product of engaged discussion by reviewers, verify that submissions complied with requirements, identify reviewers that seemed to be encountering challenges, and generally keep a chaotic process running smoothly. We cannot adequately express our gratitude to this year’s inaugural vice chairs: Adam J. Aviv, David Barrera, Nataliia Bielova, Christina Garman, and Giancarlo Pellegrino.

We retained a Research Ethics Committee (REC) from last year to ensure thoughtful consideration and feedback regarding possible unmitigated ethics concerns. If reviewers raised concerns for a submission, two members of the REC examined the submission, its reviews, and the reviewers’ discussion. If the REC assignees and reviewers failed to reach consensus regarding the concerns or required steps, we invited all non-conflicted REC members to the discussion. To help manage the process this year, we added a REC chair. Our REC consisted of 12 PC members with expertise on a broad range of ethical best practices: Lujo Bauer, Joseph Bonneau, Srdjan Capkun, Zakir Durumeric. Manuel Egele, William Enck, Thorsten Holz, Sarah Meiklejohn, Franziska Roesner, Wendy Seltzer, Gianluca Stringhini, and Juan Tapiador (chair). We are grateful to them for their valuable guidance to authors, the PC, and us.

We introduced substantial changes to the USENIX Security revision model, with the goal of reducing uncertainty, time to publication, and review load. In recent years, USENIX Security has divided revisions between those that required only minor changes, typically of editorial nature—which underwent a short shepherding process—and revisions that required more substantial changes—which underwent full review in a future review cycle. This year, we emphasized that required experiments can have a place under the umbrella of minor changes if the experiments’ outcomes are unlikely to impact reviewers’ assessment of the paper meaningfully. For major revisions, we switched to an interactive shepherding process in which shepherds could discuss requirements with authors and approve an acceptable revised draft immediately. This change allows papers to be accepted well before a future review cycle’s notification deadline. The impact for our final submission cycle was particularly significant: authors of 56 papers were able to address reviewer requirements sufficiently early to present their work at USENIX Security ’23 rather than wait until USENIX Security ’24.

Alongside changes to the revision model, we switched to an anonymous shepherding process via HotCRP. Our intent was to help counter factors like biases and power imbalances that could influence the process, particularly given the use of shepherding for major revisions. This change also facilitated participation by all reviewers in the shepherding process, reducing friction and the likelihood of misunderstandings. We are grateful to PC members who shepherded papers for USENIX Security ’23, particularly those who anonymously devoted considerable time to a new process for shepherding major revisions.

We merged all rejection decisions into a single category this year. We provided authors of papers receiving this decision with an option for requesting the same reviewers (as available) in a future review cycle. Ideally, this will yield a more reliable process for authors who believe their changes rigorously address reviewer concerns.

A considerable number of papers in this year’s program are the result of Major Revision decisions from the USENIX Security ’22 review cycles and revision model (62 for our Summer cycle and 42 for our Fall cycle). We continued the practice of having the previous year’s chairs coordinate Major Revisions originating during their cycles. We were very fortunate to have last year’s chairs, Kevin Butler and Kurt Thomas, assigning reviewers, leading discussion, and making decisions for the Major Revision papers from USENIX Security ’22. Their excellence and dedication is something we aspire to as we manage the remaining revisions from USENIX Security ’23. We are also grateful to Kevin and Kurt for always being available to help and for their generosity with advice and guidance.

To implement the review process, we invited members of the community—previous authors, previous PC members, community recommendations and referrals, and self-nominations—to participate. Conscious of the very large set of submissions received last year, we assembled a large PC this year, comprising 285 members. We sought to assure the diversity of PC members in terms of representation, geographical diversity, inclusion of members from industry and government, and seniority within our community. Across the three submission cycles, this committee oversaw the largest number of papers ever submitted to USENIX Security—388 for the Summer cycle, 531 in Fall '23, and 525 in Winter '23—for a total of 1,444 reviewed submissions. This total excludes submitted papers that authors withdrew after we assigned reviewers (6) and papers that we administratively rejected at any point for failing to conform to the submission policies (83).

We are tremendously grateful to the PC. PC members made a substantial commitment to reviewing across three submission cycles and put forth a massive effort, writing 5,241 reviews and engaging in robust discussions generating more than 27,656 comments. This reflects tens of thousands of hours of work, without which the excellent program in these proceedings would have been impossible. Due to the size of the PC, the length of the commitment, and life's general unpredictability, issues invariably arise whereby reviewers are unable to serve during certain cycles or are unable to complete their reviews. PC members generously devoted countless hours—sometimes with little notice—to assisting other reviewers facing difficult circumstances. As a result, authors were able to respond to 100% of reviews in all three review cycles!

Each reviewing cycle concluded with a virtual PC meeting. In PC meetings, we discussed a limited number of papers (typically under 5% of submitted papers) for which reviewers did not reach consensus in online discussion. In these meetings, reviewers discussed the papers with each other and with the wider program committee. Discussions also sometimes broached broader issues, such as common ethics concerns. We are thankful to all PC members who participated in these meetings, especially those whose time zones made attendance particularly challenging.

The incredible effort we describe resulted in the 2023 proceedings, which include 422 accepted papers. We congratulate the authors of these papers for producing innovative and exciting work. We look forward to the impact that these papers will have in the years to come. This year's program size is a 65% increase over the previous year's record. The acceptance rate for the proceedings was 29%. While we are pleased by this higher-than-typical acceptance rate, we note that it is partially a product of two quirks. First, this year's program contains not only papers accepted via the USENIX Security '22 major revision process but also major revisions accepted via the faster revision process we introduced this year. Second, the new revision process reduces the number of submissions by eliminating resubmission of major revisions.

During the review process, 51% of new submissions advanced to the second round of review. Fifteen percent of all submissions and 8% of new submissions were accepted directly or accepted with minor changes. For major revisions from USENIX Security '22 cycles, the acceptance rate was 86%. While the Winter '23 cycle shepherding process is ongoing, shepherds approved 96% of papers receiving major revision decisions for the Summer '23 and Fall '23 cycles. Papers accepted directly or with minor changes constitute 25% of the final program, and the remaining 75% underwent a major revision.

Four important processes begin after paper selection: artifact evaluation, awards, lightning talks, and posters. We extend a special thanks to Cristiano Giuffrida and Anjo Vahldiek-Overwagner for spearheading the artifact evaluation process. Cristiano and Anjo assembled a 128-member Artifact Evaluation Committee. Over three cycles, that committee evaluated 143 artifact submissions for "Artifact Available," "Artifact Functional," and "Results Reproduced" badges.

Our Distinguished Paper Award and Internet Defense Prize selection process started with selection of PC members to form an Awards Committee. We solicited paper nominees from the full PC. The awards committee extensively discussed nominees and, eventually, voted on them. This year's Awards Committee consisted of Christina Garman, Nicholas Hopper, Kari Kostiainen, Franziska Roesner, Andrei Sabelfeld, Martin Strohmeier, Matthew Wright, and Mary Ellen Zurko. We are grateful for the care and thought they put into selecting the winners. USENIX Security also continued to offer a Test of Time Award this year. A committee consisting of Dan Boneh, Srdjan Capkun, Lorrie Cranor, Nick Feamster, Kevin Fu, Fabian Monrose, David Wagner, Dan Wallach, and Wenyuan Xu examined the history of USENIX Security proceedings to select the winners.

This year's symposium will have lightning talks for the first time since 2019. We are thankful to Imani Munyaka for serving as this year's lightning talks chair. We are also grateful to Earlence Fernandes and Rikke Bjerg Jensen for taking on the role of poster session co-chairs for this year's symposium.

Chairing a symposium the size of USENIX Security is a daunting task. From day one, the continuous support of the USENIX team made our job feasible and less intimidating. We are indebted to the entire team—Cathy Bergman, Arnold Gatilao, Casey Henderson, Jessica Kim, Liz Markel, Mo Moreno, Camille Mulligan, Jasmine Murcia, Heidi Sherwood, Ginny Staubach, Sarah TerHune, and Olivia Vernetti—for always making themselves promptly available with a helping hand, for their infinite patience assisting us with the year's expected and unexpected challenges (including those stemming from a new revision model), and for the visible and less visible work they do to support the symposium and community. We feel truly fortunate for the opportunity to work with them. A special shout out goes to the Production team, both for turning 422 accepted papers into these proceedings and for working with us to overcome countless challenges in assembling a program of unprecedented size. We also want to thank William Enck for serving as our USENIX Board liaison and for his reliably thoughtful perspective and guidance. Finally, we would like to extend a very special thank you to Casey Henderson, USENIX Executive Director, for her steadfast guidance and support throughout the process, particularly her support in reconciling our roles as program co-chairs and new parents.

Both of us became parents (of three children in total!) in the months before the first USENIX Security '23 submission cycle. Balancing our commitments was difficult. Doing so would have been impossible without the incredible support of USENIX, the vice chairs, and many others we mention above. We also would add a special note of appreciation to our families for their support and sacrifices. Thank you, Alexandre, Amy, Anthony, Oliver, and Rebekah!

In closing, we want to express our immeasurable gratitude to the community without whom these proceedings would not be possible. We also wish the best to next year's chairs, Davide Balzarotti and Wenyuan Xu. We are looking forward to the proceedings they will assemble. We hope their experience is as gratifying as ours serving the USENIX Security community as program co-chairs.

Joseph Calandrino, *Federal Trade Commission*
Carmela Troncoso, *EPFL*
USENIX Security '23 Program Co-Chairs