Message from the
USENIX Security '20 Program Co-Chairs

Welcome to our fully virtual USENIX Security Symposium! While we are very sad not to welcome you to an in-person conference in Boston this year, the COVID-19 situation would not have allowed us to do so safely. We are nevertheless excited to welcome you to the virtual event, featuring a record 157 technical papers, two extremely timely panels on contact tracing and voting, and numerous opportunities for online engagement with authors and other participants around the world. We chose to simplify the program compared to recent years (e.g., omitting a poster session and full invited talks track) in order to focus on these core parts of the experience while navigating global time zones and the new online format.

In putting together this year's technical program, we followed in the footsteps of the 28th USENIX Security Symposium, which introduced a multiple submission model with journal-style revisions. Whereas 2019 was a transition year with only two deadlines, USENIX Security 2020 had the full planned set of quarterly deadlines on May 15, 2019 (Spring), August 23, 2019 (Summer), November 15, 2019 (Fall), and February 15, 2020 (Winter). (Next year's USENIX Security Symposium has reduced this to only three deadlines throughout the year, an adjustment that we support based on our experience.) As in previous years, for each submission deadline, we used a double-blind review process with two rounds of reviews, and with an opportunity for authors of papers not rejected before the second round to respond to the first-round reviews.

Like in 2019, submitted papers could receive one of the following five outcomes:

- Accept: These papers were accepted without conditions.
- Minor Revision: These papers were accepted under the condition that textual changes would be made, under the guidance of a shepherd.
- Major Revision: These papers were returned to the authors with a specific list of revision requirements from the reviewers. These papers could resubmit a revised version, along with a letter to the reviewers about how the requested changes had been made, to a subsequent deadline (not the immediately next deadline, but either of the following two). Papers were still considered under revision during this time (unless explicitly withdrawn by the authors), and to the extent possible, we re-assigned resubmissions to the original set of reviewers. Decisions on Major Revision resubmission were typically made in the first round of our reviewing process.
- Reject & Resubmit: These papers were rejected, but reviewers did not rule out that a substantial revision might lead to a strong paper in the future (though could not sufficiently specify the path for such a revision). These papers could not be resubmitted for the next two deadlines.
- Reject: These papers were rejected and not permitted to submit again for a full year.

Anticipating a large number of submissions, we assembled a strong and diverse program committee consisting of over 100 members, and we added additional new members as submission volumes rose throughout the year. Over the course of the year, 120 people served on our PC, of which 22% were women, 13% came from industry, government, or non-profits, and included researchers from around the globe, although predominantly from the US (65%) and Europe (25%). We are also grateful for the contributions of many external reviewers.

We received the highest number of submissions ever to USENIX Security: 977 (an increase of 32% over the previous record-breaking year). The most popular deadline was the last (Winter) cycle, when we received 49% of submissions. We ultimately accepted a record-high number of papers, 157, with an overall acceptance rate of 16.1%. Of the accepted papers, 38% were resubmissions of Major Revisions. We found that the acceptance rate of resubmissions was very high: 85.7%. We view this as a validation of the Major Revision model, suggesting that some of these formerly borderline papers find their way to acceptance through the mentored revision process in the large majority of cases. We congratulate all of these authors on their excellent work and thank all the involved reviewers for their constructive feedback and guidance!

For those of you interested in the full breakdown of submission and outcome statistics per cycle:

- Spring 2019: We received 58 submissions, 13 of which were Major Revision resubmissions. Of new submissions, 4 were Desk Rejected (for CFP violations), 0 received an Accept outcome, 3 a Minor Revision, 7 a Major Revision, 25 a Reject & Resubmit (11 of these in round 1), 4 a Reject (3 of these in round 1), and 2 were Withdrawn. Of Major Revision resubmissions, 5 received an Accept outcome, 5 a Minor Revision, 3 a Reject & Resubmit, and 0 a Reject. We did not give resubmissions a second Major Revision outcome.

- Summer 2019: We received 187 submissions, 26 of which were Major Revision resubmissions. Of new submissions, 5 were Desk Rejected, 1 received an Accept outcome, 15 a Minor Revision, 30 a Major Revision, 82 a Reject & Resubmit (49 of these in round 1), and 28 a Reject (25 of these in round 1). Of Major Revision resubmissions, 8 received an Accept outcome, 15 a Minor Revision, 3 a Reject & Resubmit, and 0 a Reject.
- Fall 2019: We received 255 submissions, 6 of which were Major Revision resubmissions. Of new submissions, 5 were Desk Rejected, 5 received an Accept outcome, 33 a Minor Revision, 38 a Major Revision, 141 a Reject & Resubmit (78 of these in round 1), 26 a Reject (23 of these in round 1), and 1 was Withdrawn. Of Major Revision resubmissions, 4 received an Accept outcome, 1 a Minor Revision, 1 a Reject & Resubmit, and 0 a Reject.
- Winter 2020: We received 477 submissions, 25 of which were Major Revision resubmissions. Of new submissions, 14 were Desk Rejected, 3 received an Accept outcome, 37 a Minor Revision (originally 38, but one was transitioned to a Major Revision during the shepherding process), 72 a Major Revision, 285 a Reject & Resubmit (142 of these in round 1), 36 a Reject (31 of these in round 1), and 5 were Withdrawn. Of Major Revision resubmissions, 7 received an Accept outcome, 15 a Minor Revision, 3 a Reject & Resubmit, and 0 a Reject.

We are excited that this year's USENIX Security is the first to include an Artifact Evaluation, thanks to the initiative and leadership by Thorsten Holz and Brendan Dolan-Gavitt. A 35-person Artifact Evaluation Committee evaluated a total of 40 artifacts, of which 38 passed the evaluation. These papers are identified by the "Evaluated Artifact" badge included in the final versions of their papers.

We had planned to hold two in-person PC meetings, one in August co-located with USENIX Security 2019, and one in April in Zurich. The August meeting took place, focusing mostly on a town hall discussion about reviewing norms, policies, and plans for the year (enabled in part by a low volume of Spring submissions). We chose to cancel the April meeting in early March, when it became clear that worsening pandemic conditions would make travel uncertain if not dangerous. While we considered holding a synchronous online PC meeting, we chose not to do so due to the challenges of coordinating logistics on short notice and given the challenges everyone was facing in April, and because we had already seen and practiced successful discussion and thoughtful deliberation in our earlier online-only review cycles. While we sorely missed the opportunity to meet and discuss with our wonderful PC in person (and believe the meetings serve a valuable purpose when possible), we greatly appreciated the continued deep engagement of reviewers in our online discussion process even under these challenging conditions.

We are extremely grateful to the authors, our program committee, our artifact evaluation committee, many external reviewers, our Review Task Force (who helped ensure high review and discussion quality: Michael Bailey, Rachel Greenstadt, Tadayoshi Kohno, Mathias Payer, Patrick Traynor), the USENIX staff (especially Casey Henderson and Jasmine Murcia), the USENIX Security steering committee, and others for the extensive and incredible work that they have done throughout a year that was challenging in many ways. We are excited to bring you the largest-ever USENIX Security program, and we look forward to the opportunity to engage with many of you online in new ways—and with more participants—that might not even have been possible in person.

We are also excited to pass the baton to Michael Bailey and Rachel Greenstadt as next year's co-chairs (though we will continue to handle the resubmissions of papers that received Major Revisions during the 2020 review period). Finally, we look forward to seeing you online at the USENIX Security 2020 and hopefully again in person in 2021. In the meantime, most importantly, stay well.

Srdjan Čapkun, *ETH Zurich*
Franziska Roesner, *University of Washington*
USENIX Security '20 Program Co-Chairs