Chairs' Introduction and Welcome to AISec 2026

It is our pleasure to welcome you to the 19th ACM Workshop on Artificial Intelligence and Security (AISec '26). The workshop brings together researchers working at the intersection of security, privacy, artificial intelligence, and machine learning. It provides an opportunity to exchange ideas on how AI can address practical security problems, as well as on how intelligent systems themselves can be made more secure and trustworthy. The field encompasses a wide range of questions: learning in adversarial environments, privacy-aware methods, robustness of machine learning, and applications to malware, spam, and intrusion detection, among others. We hope the workshop will encourage new collaborations across these research communities.

AISec 2026 received 263 submissions from academic and industrial institutions around the world. Of these 263, 221 were deemed eligible for being included in the program. Following the review process, 39 submissions (17.6%, 39/221) were selected for publication and presentation. To handle the unforeseeable rise in submissions[1] without overwhelming the PC members with a high number of papers to review, we revised our initial plan of having each paper be reviewed by three or four reviewers, as is customary in the field. Instead, every paper would receive two reviews, and we specifically asked PC members to engage in a discussion to determine if the paper should be accepted or not. The ensuing discussions were constructive and insightful, and some exceeded 2,500 words in length for a single paper. In cases where a decision could not be taken with just two reviews and subsequent discussion, a third "tiebreaker" review would be requested from another volunteer PC member. Overall, 13 papers received a third review, and four of these papers were ultimately accepted. The discussions were overseen by the PC chairs, who also acted as moderators and engaged with PC members whenever needed.

AISec 2026 solicited four types of submissions: Original Research, Position and Open Problem, Systematization of Knowledge, as well as Benchmark papers—the latter being introduced for this edition. Below we report the counts and acceptance rates for each submission type:

Submission Type	***Reviewed***	***Accepted***	***Rate***
Original Research Papers	161	31	19%
Position and Open Problem Papers	30	3	10%
Systematization of Knowledge Papers	5	0	0%
Benchmark Papers	25	5	20%

The accepted papers were organized into two thematic tracks: **AI for Security & Privacy** (counting 15 papers) and **Security & Privacy of AI** (counting 24 papers). All papers will be presented as posters in respective poster sessions during the workshop. In addition, following a supplementary examination by the Program Committee, four papers for each track (8 in total, $\approx$20% of accepted papers) were deemed particularly noteworthy and will be given the opportunity of being presented via "spotlight" talks right before the corresponding poster sessions.

Alongside the spotlight presentations and poster sessions, the workshop features two keynote talks intended to connect current research results with important open questions and promising directions. The invited speakers are:

- Alexandra Dmitrienko, Professor at the University of Duisburg-Essen, Germany;
- Boris Köpf, Scientist at Microsoft's Azure Research.

[1] The 2024 and 2025 editions of AISec both received 72 submissions each—meaning that AISec '26 received 3.65$\times$ as many submissions as AISec '24 or '25, which had to be handled by 142 program-committee (PC) members in $\sim$1 month.

We are grateful to everyone who helped make AISec 2026 possible. We especially thank all authors for sharing their work with the community, and the PC members for generously contributing their time, expertise, and thoughtful feedback: altogether, for AISec 2026, 475 reviews have been submitted (20 reviews were for papers that, unfortunately, have been administratively rejected) encompassing 257,002 words overall; and 1,350 comments have been posted on HotCRP, spanning 88,574 words overall. We also thank the invited speakers, the steering committee, our colleagues involved in the proceedings, and those handling the many organizational details behind the scenes.

In addition to the above, we want to particularly recognize select PC members for their outstanding efforts. To this purpose, and for the first time at AISec, we have derived a number of *recognition categories* used to highlight specific (and objectively measurable) accomplishments, which denote remarkable dedication and/or helpfulness. Specifically:

- **Speedy**: Awarded to the top 5% (7) PC members who were the first to submit two reviews (with no late reviews).
- **Commenter:** Awarded to the top 5% (9 in total) PC members with the highest word count across all comments *or* with the highest number of submitted comments.
- **Elaborate:** Awarded to the top 5% (7) PC members with the highest cumulative word count across all reviews (with no late reviews).
- **Committed:** Awarded to those PC members (16 in total) who placed $\geq$10 bids, set topic preferences for *all* topics, were not late, and submitted $\geq$2 reviews.
- **Alacritous:** Awarded to those PC members (10 in total) who initiated the discussion for at least two distinct papers without being prompted to do so by the PC chairs.
- **Firefighter:** Awarded to those PC members (22 in total) who submitted $\geq$2 reviews as well as an extra (emergency or tiebreaker) review.
- **Appreciated:** Awarded to the top 5% PC members (8, accounting for ties) with the highest upvotes received on HotCRP.

Importantly, for the purposes of these recognitions, PC members who proactively informed us of anticipated delays and subsequently met their self-imposed deadlines were not considered late.

Finally, to acknowledge those members that demonstrated excellence across a diverse set of particularly positive (and quantifiable) behaviors, we devised the **Distinguished PC Member** award, which we awarded to those PC members that met at least eight of the following twelve criteria: submitting $\geq$ 10 bids; setting topic preferences for paper-assignment across all topics; submitting all reviews on time; being ranked in the top 30% of PC members by total number of comments posted; being ranked in the top 30% of PC members by aggregated length of comments; having submitted $\geq$3 reviews; being in the top 30% of PC members by average review length; being in the top 30% by total upvotes received; having initiated $\geq$1 discussion on an assigned paper; having submitted one emergency or tiebreaker review; having submitted all reviews at least 48 hours before the planned deadline (excluding extra reviews); having voted in the spotlight paper selection. A total of 24 PC members (17% of the PC size) received such an award—to which goes our most heartfelt thanks: Advije Rizvani, Andrew Paverd, Bhavna Soman, Daryna Oliynyk, David Pape, Dimitri Galli, Giorgia Di Pietro, Giuseppe Parrella, Hannan Mahadik, Jean-Charles Noirot Ferrand, Jonathan Evertz, Jose Sanchez Vicarte, Kerri Prinos, Kristina Nikolić, Lea Schönherr, Lorenzo Cavallaro, Luca Pajola, Marco Di Gennaro, Matteo Gioele Collu, Maura Pintor, Stefanos Koffas, William Corrias, Zeya Umayya, Zied Ben Houidi.

We hope the program will stimulate lively discussion and useful exchange of ideas.

Sahar Abdelnabi
ELLIS Institute Tübingen & MPI-IS,
Tübingen, Germany
sahar.abdelnabi@tue.ellis.eu

Giovanni Apruzzese
Reykjavik University
Reykjavik, Iceland
giovannia@ru.is

Matthew Jagielski
Anthropic
Boston, USA
jagielski@anthropic.com