36th USENIX Security Symposium

August 11–13, Denver, CO, USA

Sponsored by USENIX, the Advanced Computing Systems Association

The USENIX Security Symposium brings together researchers, practitioners, and others interested in the latest advances in the security and privacy of computer systems and networks. The 36th USENIX Security Symposium will be held on August 11–13, 2027, in Denver, CO, USA.

Important Information (AoE)

Cycle 1

- Mandatory registration (fixed title, fixed authors, tentative non-blank abstract, and fixed topics) due: Tuesday, August 18, 2026
- Paper submissions due: Tuesday, August 25, 2026
- Submission artifacts due: Friday, August 28, 2026
- Early reject notification: Tuesday, October 6, 2026
- Rebuttal period: Thursday, November 5–12, 2026
- Notification to authors: Thursday, December 3, 2026
- Shepherded approval due: Tuesday, December 15, 2026
- Final papers due: Thursday, January 14, 2027

Cycle 2

- Mandatory registration (tentative title, authors, non-blank abstract, and topics) due: Tuesday, January 19, 2027
- Paper submissions due: Tuesday, January 26, 2027
- Submission artifacts due: Friday, January 29, 2027
- Early reject notification: Tuesday, March 9, 2027
- Rebuttal period: Thursday, April 8–15, 2027
- Notification to authors: Thursday, May 6, 2027
- Shepherded approval due: Tuesday, May 18, 2027
- Final papers due: Thursday, June 3, 2027

Requirements

- Paper submissions can include up to 13 pages of body text
- Papers must include an "Open Science" Appendix on submission
- An Appendix discussing Ethics and Disclosure is recommended
- Overall length:
  - The initial submission can contain unlimited appendices and references
  - Final camera-ready papers can contain a maximum of 20 total pages
- Each author can submit at most seven papers per cycle

All papers accepted in either Cycle will appear in the proceedings of USENIX Security '27. All submissions must be made via the respective submission systems on the call for papers page.

Submitted papers should describe original, scientifically sound work produced by the co-authors. All submissions will be judged on originality, relevance, scientific rigor, correctness, and clarity. Submissions should be finished, complete papers.

Submissions must be in standard PDF format. Please ensure your submission is intelligible when printed/rendered in grayscale.

Summary of main changes from USENIX Security '27, Cycle 1

1. Softened registration-time requirements (fixed vs. tentative).
2. Added guidance on vulnerability disclosure to Ethical Considerations.
3. Logistical changes to OpenScience and Anonymous URLs.
4. Required the use of the LaTeX template.

Summary of main changes from USENIX Security '26 edition

csdsdsdsdsd

1. Ethics appendix is no longer mandatory (but is strongly encouraged).
2. No Replication submissions.
3. Three-day grace period for artifact submissions.
4. USENIX Authorship policy. (https://www.usenix.org/conferences/authorship-policy)

Symposium Topics

Refereed paper submissions are solicited in all areas relating to systems research in security and privacy, and this topic list is not meant to be exhaustive. Papers without a clear application to security or privacy of computing systems will be considered out of scope and may be rejected without full review at the discretion of the chairs.

- System security
  - Operating systems security
  - Distributed systems security
  - Cloud computing security
- Network security
  - Intrusion and anomaly detection and prevention
  - Network infrastructure security
  - Denial-of-service attacks and countermeasures
  - Wireless security
  - Analysis of network and security protocols
- Security and Privacy for Web, Mobile, and Emerging Technologies
  - Web
  - Mobile
  - IoT
  - VR/AR
  - Games
- Software security
  - Malware analysis
  - Forensics and diagnostics for security
  - Automated security analysis of source code and binaries

- Program analysis
- Fuzzing and vulnerability discovery

- Security of ML
  - Read the Submitting ML Work to USENIX Security page (https://www.usenix.org/conference/usenixsecurity27/submitting-ml-work-usenix-security) to prevent desk rejection.
  - USENIX Security is a systems security venue. ML-focused contributions must be relevant to the broader systems security community.
  - This topic is not meant for papers that propose/evaluate/improve ML-based techniques for a security task. Such papers should select the topic most closely related to the task.
- Privacy of ML
  - Read the Submitting ML Work to USENIX Security page (https://www.usenix.org/conference/usenixsecurity27/submitting-ml-work-usenix-security) to prevent desk rejection.
  - USENIX Security is a systems security venue. ML-focused contributions must be relevant to the broader systems security community.
  - This topic is not meant for papers that propose/evaluate/improve ML-based techniques for a privacy task. Such papers should select the topic most closely related to the task.
- Privacy and Anonymity
  - Privacy metrics
  - Anonymity
  - Privacy-preserving computation
  - Privacy attacks
  - Surveillance and censorship
- Human Aspects
  - Usable security and privacy
  - Security and privacy policy and/or ethics
  - Security education and training
  - Understanding and protecting users from online harms (e.g., harassment, abuse, mis/disinformation, etc.)
- Security Measurement Studies
  - Measurements of fraud, malware, spam, or cybercrime
  - Measurements of human behavior and security
- Hardware security
  - Secure computer architectures
  - Embedded systems security
  - Cyber-physical systems security
  - Methods for detection of malicious or counterfeit hardware
  - Side channels
  - Automated security analysis of hardware designs and implementation
- Applications of cryptography
  - Analysis of deployed cryptography and cryptographic protocols
  - Cryptographic implementation analysis
  - New cryptographic protocols with real-world applications
  - Blockchains and distributed ledger security

Systematization of Knowledge

USENIX Security solicits the submission of Systematization of Knowledge (SoK) papers.

SoK papers go beyond simply summarizing previous research (as in a survey). They also include a thorough examination and analysis of existing approaches, identify gaps and limitations, and offer insights or new perspectives on a major research area.

For examples, please see the list of SoK papers at https://oaklandsok.github.io.

These submissions must have their title prefixed with "SoK: ".

Submission Policies and Instructions

Formatting Requirements & Page Limit

Submissions must be in PDF format, typeset using the USENIX Security template and style files (https://www.usenix.org/sites/default/files/usenixsecurity2027_latex_templates.zip): on U.S. letter-sized pages in two-column format in 10-point Times Roman type on 12-point leading (single-spaced), in a text block 7″ x 9″ deep. Note that only the LaTeX template is allowed. The main body of the submission must not exceed 13 pages excluding References and any appendices.

At submission time, there is no limit on the length of the bibliography and optional appendices, but reviewers are not required to read any optional appendices. Papers must be self-contained without the optional appendices.

Authors must meet page limits through the modification of content alone. Any attempts to remove whitespace (e.g., negative vspaces, savetrees, titlesec, removing author blocks, etc.) or change the formatting defaults (e.g., fonts) are forbidden and may result in rejection.

Once accepted, papers must be reformatted to fit in 20 pages, including any "Ethical Considerations" or "Open Science" appendices, the bibliography, and any additional optional appendices.

Ethical Considerations and Disclosure

Papers in-scope for USENIX Security frequently, if not always, have both ethical considerations and implications that should be addressed prior to conducting research. Reviewers will be asked to evaluate the ethics of both the research and the implications of all submissions. At the co-chairs' and PC's discretion, papers may be rejected on ethical grounds. Our expectation however is that the common case, involving established research approaches, will be straightforward and require limited ethical analysis and that substantive efforts (both on the part of submitters and the PC) will be reserved for cases involving new and/or substantive risk of harm.

Authors are strongly encouraged to include a well-labeled section in the Appendix (e.g., "Ethics", "Ethical Considerations", etc.) that discusses the ethical considerations and implications of their work. We may work with authors throughout the review process, and authors who do not include an adequate discussion of ethics may be asked to provide additional information.

A common issue identified by reviewers for papers involving vulnerabilities is a lack of information about disclosure. Authors are expected to complete disclosure, as appropriate for community norms, prior to the paper becoming public. To that end, we strongly recommend papers necessitating disclosure include either a disclosure report, when disclosure has been completed, or a disclosure plan in the ethics section enumerating who has been or will be notified, how, and when.

If the authors do not intend to disclose, articulating that decision is also recommended.

We encourage the authors to consult the Ethics Guidelines (https://www.usenix.org/conference/usenixsecurity26/call-for-papers#ethics) from USENIX Security 2026 for examples of ethics sections, analysis frameworks, and resources to consider when conducting security research.

Open Science Policy

The bedrock of scientific progress is standing on the shoulders of giants, and to do this USENIX Security '27's principle is that research results should be accessible and, if possible, empirical studies should be reproducible.

We encourage all authors to release all artifacts (source code, datasets, models, benchmarks, scripts, etc.) needed to evaluate the paper's core contributions, to the extent possible while maintaining data confidentiality and industry protections. Therefore, all USENIX Security '27 submissions must include an Open Science Appendix describing the artifacts and how to access them or an explicit description of why artifacts cannot be provided.

To preserve double-blind review, artifacts must be shared through anonymous links with no tracking mechanisms. Authors are solely responsible for ensuring no identifying information is exposed (e.g., usernames, organization names, commit history). For source code repositories, we recommend https://anonymous.4open.science, using the conference ID "SEC27" to apply the current cycle's expiration deadline. Check any expiration times carefully: files must remain accessible for the entire evaluation period, until the shepherd approval deadline.

Anonymous URLs should be included under the dedicated submission field on HotCRP. To assist reviewers, we also encourage including these URLs in the Open Science Appendix. The Open Science Appendix, describing the artifacts or explaining their absence, must be finalized and included in the paper by the submission deadline. However, a 3-day grace period is provided to anonymize and upload artifacts and update their URLs on HotCRP. During this period, the paper itself cannot be modified. Once the grace period ends, artifacts are considered frozen and must not be updated.

We expect all submitted artifacts to be available publicly on paper acceptance, however we acknowledge that some artifacts cannot be shared publicly e.g., due to licensing restrictions, adversarial risk, or harm to study subjects. Artifacts help the PC to review the paper, therefore, if at all possible, submit the artifacts and note in the Open Science Appendix those which will not be made public. If submission of artifacts is not possible (e.g., due to NDA or legal constraints), the Open Science Appendix must explain such omissions explicitly.

Artifacts will be treated with the same strict confidentiality as the manuscript. Access is restricted to assigned PC members for evaluation purposes only.

For all submitted artifacts that can be made public, paper acceptance is conditional on their public availability. Camera-ready paper versions will include an Open Science Appendix that includes a non-anonymous, stable artifact link. Artifact availability will be re-verified by the Artifact Evaluation Committee.

Authors of accepted papers are additionally encouraged to optionally register their artifacts to be checked for functionality and reproducibility by the Artifact Evaluation Committee.

Anonymous Submission

Papers must be submitted for anonymous review: no author names or affiliations may appear on the title page and authors must not reveal their identity in the text.

When referring to your previous work, do so in the third person, as though it were written by someone else.

Only blind the reference itself in the (unusual) case that a third-person reference is infeasible.

For provided artifacts, neither the link in the paper nor the website itself may suggest the authors' identities nor track reviewers accessing them.

Papers that are not properly anonymized may be rejected without review or during the review process.

While submitted papers must be anonymous, authors may choose to give talks about their work, post a preprint of the paper online, disclose security vulnerabilities to vendors or the public, etc., during the review process. While the PC will not go out of its way to attempt to deanonymize papers, authors should take care to avoid timing of publicity or public announcements of work, and avoid other behaviors that appear to intentionally aim to inform reviewers of their identity.

Use of AI

The use of AI tools to assist in preparing submissions is permitted, and human authors are ultimately responsible for all submitted content and results, ensuring their accuracy, originality, and integrity. Works submitted should constitute self-respecting work that respects the importance of scientific inquiry and integrity and respects the time and energy of reviewers.

However, authors should be cautious about AI assistance in writing, as reviewers have expressed frustration when reading AI-sounding writing. Papers that are human-written stand out positively.

Upon submitting to USENIX Security '27, authors acknowledge that they have reviewed all content that was generated by AI as if they had written it themselves, including text, code, experimental data, and references.

Any violation to this policy which results in fabrications or hallucinations, including non-existing references or incorrect authors, invented claims, and falsified results is considered academic misconduct and might lead to the paper being desk rejected or other sanctions.

Authors are encouraged to evaluate their submissions using the same open-source tools that we will use (https://github.com/gianlucasb/hallucinator).

Submission Limit

Each author can submit at most seven papers per cycle to USENIX Security 2027. Checking will happen right after paper submission (abstracts may be withdrawn). If an author submits more than seven papers, the chairs will retain the seven papers with the lowest submission numbers.

Submission Instructions and Procedures

Registration and additional requirements for submissions

For cycle 2, all papers intended to be submitted must be registered with the tentative title, list of authors, abstract, and topics one week before the submission deadline. No major changes to the title, authors, or topics are allowed after the

registration deadline. Any papers not registered at that time or those missing requirements will not be considered for review.

By submission time, all authors are required to (1) set up or update their HotCRP profile to include their ORCID (https://orcid.org/) and (2) confirm the submission terms within HotCRP. In exceptional cases of unavailability of a co-author, contact the co-chairs with an explanation of why the requirements cannot be fulfilled. In all other cases, papers for which at least one author fails to comply with the requirements will not be considered for review.

Conflicts of Interest

To maintain the integrity of the peer review process, we all need to prevent submissions from being evaluated by reviewers who have a conflict of interest. During the submission process, we ask authors to identify members of the program committee with whom they share a conflict of interest. This includes anyone:

- who shares an institutional affiliation with an author at the time of submission or within the past two years (including secondary affiliations and consulting work)
- who was the advisor or advisee of an author at any time in the past
- with whom the author has collaborated with (includes work in progress) or published in the current year or the two years preceding it
- who is a co-PI or sub-award on grants or funding
- who is affiliated with a party that provides research funding to an author
- with whom you have a close personal relationship

The chairs will contact authors if more information is necessary. Authors should be prepared to explain conflicts.

Note that adversarial or illegitimate conflicts are strictly prohibited. The chairs retain the right to remove conflicts (e.g., because reviewers are potential competitors).

All authors should update their HotCRP profiles to include the names of recent collaborators to help identify missed conflicts.

Program committee members who have conflicts of interest with a paper, including program co-chairs, will be excluded from the evaluation and discussion of the paper.

Final versions of accepted submissions should include all sources of funding in an acknowledgments section. Authors should also disclose any affiliations, interests, or other facts that might be relevant to readers seeking to interpret the work and its implications. Authors may wish to consider the 2023 IEEE S&P Financial Conflicts Policy (https://www.ieee-security.org/TC/SP2023/financial-con.html).

Submission Confidentiality

The program committee and external reviewers are required to treat all submissions as confidential. All papers must only be read for the purposes of evaluation for publication. However, the program co-chairs or designated committee members may share submissions outside the program committee to allow chairs of other conferences to identify dual submissions.

Internet Defense Prize

The Internet Defense Prize recognizes and rewards research that meaningfully makes the internet more secure. Created in 2014, the award is funded by Meta and offered in partnership with USENIX to celebrate contributions to the protection and defense of the internet. Successful recipients of the Internet Defense Prize will provide a working prototype that demonstrates significant contributions to the security of the internet, particularly in the areas of prevention and defense. The intent of the award is to inspire researchers to focus on high-impact areas of research. The USENIX Security Awards Committee—selected by the Program Chairs among the symposium Program Committee members—independently determines the prize, to be distributed by USENIX.

Comparison With Related Work

Authors must relate their submission to all related work they are aware of in their paper, including their own work that is currently under submission (either at USENIX Security or another conference) or have already been accepted (but not yet published). Citations to simultaneously submitted papers should be anonymized; non-anonymous versions of these citations must, however, be emailed to the program co-chairs at sec27chairs@usenix.org. Failure to point out and explain overlap with published, accepted, or simultaneously submitted papers will be grounds for rejection.

Simultaneous Submission and Plagiarism

Simultaneous submission of the same work to multiple venues with archived proceedings, submission of previously published work, and plagiarism constitute dishonesty or fraud. This includes cases in which preliminary reviews from another venue indicate likely rejection but the paper is still considered under submission to the venue. USENIX, similar to other scientific and technical conferences and journals, prohibits these practices and may take action against authors who have committed them. See the USENIX Conference Submissions Policy (https://www.usenix.org/conferences/author-resources/submissions-policy) for details.

All submitted papers are considered to be under review for USENIX Security '27 until authors are notified of a decision by the program committee or the program co-chairs approve a request for withdrawal.

Authorship

USENIX expects authors to adhere to high ethical standards and to ensure transparency and integrity in the publication of their work. Clear and consistent authorship practices support USENIX's core mission and are essential to maintaining confidence in the research record. See the USENIX Authorship Policy (https://www.usenix.org/conferences/authorship-policy) for complete information, including criteria for authorship, details about pseudonymous authorship, and the difference between contributors and authors.

Outcomes and Expectations

Review Process Outcomes

The reviewing process will result in one of the following three outcomes:

- Accepted: In this case, reviewers either see no need for any required edits—the paper could be published as is—or trust the authors to make any required edits.
- Accepted on Shepherd Approval: These papers offer sufficient contributions to be in the USENIX Security program, but the reviewers feel that some changes are needed. Reviewers expect that these changes are highly unlikely to reduce their enthusiasm regarding the paper being published. These can include text changes, clarifications, and explicit discussion of limitations.
- Rejected: This outcome indicates that the paper is not currently appropriate for publication at USENIX Security.

Reviews for such papers will attempt to identify major changes that could move the paper toward a publishable state.

Papers rejected from either cycle of USENIX Security '26 may be submitted. Papers rejected from the first cycle of USENIX Security '27 may not be submitted to the second cycle of USENIX Security '27.

Desk Rejection

The chairs reserve the right to desk-reject papers for any reason they deem necessary, including, but not limited to: severe editorial issues, scope/fit issues, insufficient quality, fabricated references, failure to adhere to the CFP, etc.

Attendance and Publishing Accepted Papers

Papers that have been formally reviewed and accepted will be presented during the Symposium and published in the Symposium Proceedings. By submitting a paper, you agree that, if the paper is accepted, at least one of the authors will register to attend the Symposium at full price (i.e., not the student rate) and to present the paper; USENIX members at the Sustainer level and higher may apply their membership discounts to their registrations. If an author plans to present more than one paper, one full-price registration will still be required for each paper. If the registration fee will pose a hardship for the presenter of the accepted paper, please contact conference@usenix.org.

A major mission of the USENIX Association is to provide for the creation and dissemination of new knowledge. USENIX allows authors to retain ownership of the copyright in their work, requesting only that USENIX be granted the right to be the first publisher of that work. See our sample consent form for the complete terms of publication.

Papers accepted during the first reviewing cycle will be published on the USENIX Security website after the final paper deadline for the first reviewing cycle. Papers accepted during the second reviewing cycle will be published on the first day of the symposium.

Embargo Requests

Authors may request an embargo for their papers by the deadlines listed below. All embargoed papers will be released on the first day of the symposium, Wednesday, August 11, 2027.

- Cycle 1 deadline for embargo requests: **Thursday, February 11, 2027**
- Cycle 2 deadline for embargo requests: **Thursday, July 1, 2027**

If your accepted paper should not be published prior to the event, please notify production@usenix.org after you submit your final paper.

Presentation of Papers

At this time, the exact format for the presentations at USENIX Security '27 has not been decided and will follow based on the experience of presenters and attendees of USENIX Security '26.

Contact Information

Specific questions about submissions may be sent to the program co-chairs at sec27chairs@usenix.org. The chairs will respond to individual questions about the registration process if contacted at least a week before the registration deadline and will respond to individual questions about the submission process if contacted at least a week before the submission deadline.

Further questions? Contact your program co-chairs, sec27chairs@usenix.org, or the USENIX office, submissionspolicy@usenix.org.

Symposium Organizers

Program Co-Chairs

Adam Doupé, Arizona State University
Andrei Sabelfeld, Chalmers University of Technology

Program Vice Co-Chairs

Yousra Aafer, University of Waterloo
Patricia Arias-Cabarcos, EU Joint Research Centre (JRC)
Musard Balliu, KTH Royal Institute of Technology
Marcus Botacin, Texas A&M University
Juan Caballero, IMDEA Software Institute
Stefano Calzavara, Università Ca' Foscari Venezia
James Davis, Purdue University
Manuel Egele, Boston University
Roya Ensafi, University of Michigan
Aurore Fass, Inria
Christina Garman, Purdue University
Martin Henze, RWTH Aachen University and Fraunhofer FKIE
Nick Hopper, University of Minnesota
Charlie Jacomme, Inria
Rikke Bjerg Jensen, Royal Holloway, University of London
Vasileios Kemerlis, Brown University
Florian Kerschbaum, University of Waterloo
Christopher Kruegel, University of California, Santa Barbara
Piotr Mardziel, RealmLabsAI
Karola Marky, Ruhr-Universität Bochum
Joachim Neu, a16z Crypto Research
Tobias Pulls, Karlstad University
Sebastian Roth, University of Bayreuth
Lea Schönherr, CISPA Helmholtz Center for Information Security
Filipo Sharevski, DePaul University
Micah Sherr, Georgetown University
Yan Shoshitaishvili, Arizona State University
Florian Tramèr, ETH Zurich
Mathy Vanhoef, KU Leuven
Xinyu Xing, Northwestern University
Ziming Zhao, Northeastern University

Program Committee

Syed Ghazanfar Abbas, Purdue University
Bhupendra Acharya, University of Louisiana at Lafayette
David Adei, North Carolina State University
David Adrian, Unaffiliated
Amit Agarwal, Category Labs
Shubham Agarwal, Max Planck Institute for Security and Privacy
Md Mojibur Rahman Redoy Akanda, Texas A&M University
Olawale Akanji, Boston University
Mete Akgün, University of Tübingen
Mahdi Akil, University of Salzburg
Mitsuaki Akiyama, NTT, Inc.
Kemal Akkaya, Virginia Commonwealth University
Can Aknesil, KTH Royal Institute of Technology
Eyhab Al-Masri, University of Washington
Munshi Rejwan Ala Muid, Virginia Tech
Mohammed Aldeen, Clemson University
Masood Ali, Palo Alto Networks
Shiza Ali, George Washington University
Aisha Ali-Gombe, Louisiana State University
Majed Almansoori, University of Wisconsin–Madison and United Arab Emirates University (UAEU)
Magnus Almgren, Chalmers University of Technology
Amit Seal Ami, University of South Florida
Babak AminAzad, Cloudflare
Mahmoud Ammar, Huawei Research
Paschal Amusuo, Purdue University
Shengwei An, Virginia Tech
Panagiotis Andriotis, University of Birmingham
Simone Aonzo, EURECOM
Budi Arief, University of Kent
MD Armanuzzaman, The University of Texas at El Paso
Daniel Arp, TU Wien
Arjun Arunasalam, Florida International University
Elias Athanasopoulos, University of Cyprus
Man Ho Au, The Hong Kong Polytechnic University
Lukas Aumayr, University of Edinburgh and Common Prefix
Zeta Avarikioti, TU Wien and Common Prefix
Athanasios Avgetidis, Voreas Laboratories
Louise Axon, University of Oxford
Jessy Ayala, University of California, Irvine
Erman Ayday, Case Western Reserve University
Ruben Baecker, Friedrich-Alexander-Universität Erlangen-Nürnberg
Pouneh Bahrami, Apple
Guangdong Bai, City University of Hong Kong
Weiheng Bai, University of Minnesota
Alexandros Bakas, Nokia Bell Labs
Teodora Baluta, Georgia Institute of Technology
Alex Bardas, University of Kansas
Sébastien Bardin, CEA List and Université Paris-Saclay
Alexandre Bartel, Umeå University
Zion Leonahenahe Basque, University of Georgia
Steffen Becker, Ruhr-Universität Bochum
Rosanna Bellini, New York University
Emad Heydari Beni, KU Leuven and Nokia Bell Labs
Nathaniel Bennett, Brigham Young University
Pascal Berrang, University of Birmingham
Clara Bertolissi, INSA CVL - LIFO
Abhishek Vasisht Bhaskar, Georgia Institute of Technology
Nishant Bhaskar, MQ Prime LLC
Adithya Bhat, Visa Research
Manish Bhatt, Amazon Leo Security
Kaustav Bhattacharjee, Pacific Northwest National Laboratory
Atri Bhattacharyya, Oracle
Rishiraj Bhattacharyya, University of Birmingham
Song Bian, Beihang University
Giuseppe Bianchi, University of Roma Tor Vergata
Abhishek Bichhawat, Indian Institute of Technology Gandhinagar
Igor Bilogrevic, Google
Eleanor Birrell, Pomona College
William Blair, SpaceX
Roberto Blanco, Eindhoven University of Technology
Erik-Oliver Blass, Airbus
Olivier Blazy, Ecole Polytechnique
Marton Bognar, DistriNet, KU Leuven
Joseph Bonneau, New York University
Jay Bosamiya, Microsoft Research
Mouhamed Amine Bouchiha, Telecom SudParis, Institut Polytechnique de Paris
Guillaume Bouffard, National Cybersecurity Agency of France (ANSSI)
Elijah Bouma-Sims, DePaul University

Samuel Breckenridge, Cornell Tech
Marcus Brinkmann, Ruhr-Universität Bochum
Mikaela Brough, Royal Holloway, University of London
Erik Buchholz, CSIRO
Sven Bugiel, CISPA Helmholtz Center for Information Security
Luis Burbano, University of California, Santa Cruz
Quinn Burke, University of Arizona
Nathan Burow, MIT Lincoln Laboratory
Kevin Butler, University of Florida
Haipeng Cai, University at Buffalo
Yifeng Cai, Peking University
Seyit Camtepe, CSIRO
Alessandro Cantelli-Forti, CNIT-RaSS
Jiahao Cao, Tsinghua University
Sicong Cao, Nanjing University of Posts and Telecommunications
Zhenfu Cao, East China Normal University
Srdjan Capkun, ETH Zurich
Michele Carminati, Politecnico di Milano
Xavier Carpent, University of Nottingham
Sebastian Castro, Google
Katharina Ceesay-Seitz, ETH Zurich
Sofia Celi, Brave and University of Bristol
Carmine Cesarano, KTH Royal Institute of Technology
Sang Kil Cha, Korea Advanced Institute of Science and Technology (KAIST)
Rohit Chadha, University of Missouri
Zimo Chai, Stanford University and University of California, Berkeley
Anrin Chakraborti, University of Illinois Chicago
Anirban Chakraborty, Max Planck Institute for Security and Privacy
Prabuddha Chakraborty, University of Maine
Stefanos Chaliasos, University of Athens
Ee-Chien Chang, National University of Singapore
Jiamin Chang, University of New South Wales
Yijia Chang, The Hong Kong Polytechnic University
Sylvain Chatel, CISPA Helmholtz Center for Information Security
Rahul Chatterjee, University of Wisconsin–Madison
Sudipta Chattopadhyay, University of Missouri-Kansas City
Bihuan Chen, Fudan University
Chen Chen, Texas A&M University
Donglong Chen, Beijing Normal-Hong Kong Baptist University
Guangke Chen, Wuhan University
Jiachi Chen, Zhejiang University
Jing Chen, Wuhan University
Jinjun Chen, Swinburne University of Technology
Jinpeng Chen, Beijing University of Posts and Telecommunications
Joann Chen, San Diego State University
Kai Chen, Institute of Information Engineering, Chinese Academy of Sciences
Kangjie Chen, Tianjin University
Kejiang Chen, University of Science and Technology of China
Lanxiang Chen, Fujian Normal University
Liquan Chen, Southeast University
Pei Chen, Fudan University
Rongmao Chen, National University of Defense Technology
Sen Chen, Nankai University
Ting Chen, University of Electronic Science and Technology of China
Yanjiao Chen, Zhejiang University
Yanju Chen, University of California, San Diego
Yi Chen, The University of Hong Kong
Yi-Chao Chen, Shanghai Jiao Tong University
Yingying Chen, Rutgers University
Yizheng Chen, University of Maryland
Zhihao Chen, Griffith University
Zitao Chen, University of Kansas
Binlin Cheng, Shandong University
Ke Cheng, Xidian University
Peng Cheng, Zhejiang University
Xiuzhen Cheng, Shandong University
Eduardo Chielle, New York University Abu Dhabi
Euijin Choo, University of Alberta
Sherman S. M. Chow, The Chinese University of Hong Kong
Mihai Christodorescu, Google
Tijay Chung, Virginia Tech
Daniel Collins, New York University and The Hebrew University of Jerusalem
Tianshuo Cong, Shandong University
Scott Constable, Intel Corporation
Mauro Conti, University of Padua and Örebro University
Andrea Continella, University of Twente
Marco M. Cook, University of Glasgow
Addison Crump, CISPA Helmholtz Center for Information Security
Jian Cui, University of Illinois Urbana–Champaign
Minhao Cui, Seoul National University
Daniele Cono D'Elia, Sapienza University of Rome
Alaa Daffalla, Cornell University
Hong-Ning Dai, Hong Kong Baptist University
Jiarun Dai, Fudan University
Tianxiang Dai, Lancaster University Leipzig
Yanbo Dai, The Hong Kong University of Science and Technology
Savino Dambra, Gen Digital
Vishnu Dasu, The Pennsylvania State University
Pubali Datta, University of Massachusetts Amherst
Lucas Davi, University of Duisburg-Essen
Xavier de Carné de Carnavalet, Radboud University
Jose Maria de Fuentes, Universidad Carlos III de Madrid
Stéphanie Delaune, Université de Rennes, CNRS, IRISA
José Luis Delgado, Universitat Oberta de Catalunya
Ioannis Demertzis, University of California, Santa Cruz
Luca Demetrio, University of Genoa
Xinhao Deng, Ant Group and Tsinghua University
Zehang Deng, Swinburne University of Technology
Zizhuang Deng, Shandong University
Aritra Dhar, Huawei Research
Michalis Diamantaris, Technical University of Crete
Wenrui Diao, Shandong University
Sayanton Dibbo, University of Alabama
Zainul Abi Din, Adobe Inc.
Anh Dinh, Deakin University
Kha Dinh, University of British Columbia
Alexandra Dmitrienko, University of Duisburg-Essen
Kyle Domico, University of Wisconsin–Madison
Changyu Dong, Guangzhou University
Feng Dong, Huazhong University of Science and Technology
Kai Dong, Southeast University

Tian Dong, The University of Hong Kong
Wei Dong, Nanyang Technological University
Xiaolei Dong, East China Normal University
Ye Dong, National University of Singapore
Yilu Dong, The Pennsylvania State University
Linkang Du, Xi'an Jiaotong University
Minxin Du, The Hong Kong Polytechnic University
Xiaojiang Du, Stevens Institute of Technology
Yuntao Du, Purdue University
Huayi Duan, The Hong Kong University of Science and Technology (Guangzhou)
Rui Duan, University of Missouri-Kansas City
Ruian Duan, Palo Alto Networks
Sisi Duan, Tsinghua University
Yue Duan, Singapore Management University
Vasisht Duddu, Vector Institute
Markus Duermuth, Leibniz University Hannover
Orr Dunkelman, University of Haifa and Technische Universität Berlin
Betül Durak, Microsoft Research
Sayon Duttagupta, COSIC, KU Leuven
Kasra Edalatnejad, Technische Universität Darmstadt
Laura Edelson, Northeastern University
Jide Edu, University of Strathclyde
Thomas Eisenbarth, University of Luebeck & DFKI
Nour El Madhoun, LISITE Laboratory, Isep: École d'ingénieurs du numérique
Hossam ElAtali, Arm
Mohamed Elsabagh, Quokka.io
Pardis Emami-Naeini, Duke University
William Enck, North Carolina State University
Håkan Englund, Ericsson AB
Alessandro Erba, Karlsruhe Institute of Technology
Benjamin Eriksson, Chalmers University of Technology and University of Gothenburg
Muhammed F. Esgin, Monash University
Zachary Espiritu, MongoDB Research and New York University
Francesca Falzon, Lucerne University of Applied Sciences and Arts
Shengyu Fan, Shandong University
Chunrong Fang, Nanjing University
Huiyu Fang, Nanjing University of Science and Technology
Zheng Fang, Wuhan University
Habiba Farrukh, University of California, Irvine
Matthias Fassl, EPFL
Kai Feng, University of Glasgow
Yu Feng, University of California, Santa Barbara
Christof Ferreira Torres, INESC-ID and Instituto Superior Técnico, University of Lisbon
Tobias Fiebig, TU Wien
Marius Fleischer, NVIDIA
Danilo Francati, Sapienza University of Rome
Gertjan Franken, DistriNet, KU Leuven
Daniele Friolo, Independent Researcher
Anmin Fu, Nanjing University of Science and Technology
Chenglong Fu, University of North Carolina at Charlotte
Chuanpu Fu, Nanyang Technological University
Jie Fu, Stevens Institute of Technology
Ximing Fu, Harbin Institute of Technology, Shenzhen, and Pengcheng Laboratory
Xinwen Fu, University of Massachusetts Lowell
Benjamin Fuller, University of Connecticut
Jonathan Fuller, United States Military Academy
Kelsey Fulton, Colorado School of Mines
Alexander Gaidis, Brown University
Kevin Gallagher, NOVA LINCS and NOVA School of Science and Technology
Hao Gao, Beihang University
Ming Gao, Nanjing University of Posts and Telecommunications
Peng Gao, Virginia Tech
Shang Gao, The Hong Kong Polytechnic University
Xing Gao, University of Delaware
Yansong Gao, The University of Western Australia
Joshua Garcia, University of California, Irvine
Marilyn George, MongoDB Research
Dañiel Gerhardt, CISPA Helmholtz Center for Information Security
Paul Gerhart, TU Wien
Lukas Gerlach, CISPA Helmholtz Center for Information Security
Sepideh Ghanavati, University of Maine
Giorgio Giacinto, University of Cagliari, Italy
Alexander Giehl, Fraunhofer AISEC
Shlok Gilda, Meta
Rosario Giustolisi, IT University of Copenhagen
Maximilian Golla, CISPA Helmholtz Center for Information Security
Xueluan Gong, Nanyang Technological University
Xun Gong, Google
Zirui Gong, Griffith University
Devashish Gosain, Indian Institute of Technology Bombay
Harm Griffioen, Delft University of Technology
Daniel Gruss, Graz University of Technology
Guofei Gu, Texas A&M University
Yacong Gu, Tsinghua University
Jorge Guajardo Merchan, Bosch Research
Ji Guan, Institute of Software Chinese Academy of Sciences
Jiaping Gui, Shanghai Jiao Tong University
Zichen Gui, University of Georgia
Merve Gülmez, Ericsson Research
Berk Gulmezoglu, Iowa State University
Hao Guo, The Chinese University of Hong Kong, Shenzhen
Keyan Guo, University at Buffalo
Wenbo Guo, University of California, Santa Barbara
Yanan Guo, University of Rochester
Gaurav Gupta, Ministry of Electronics and Information Technology, Govt. of India
Badis HAMMI, SAMOVAR, Télécom SudParis, Institut Polytechnique de Paris, France
Dianqi Han, The University of Texas at Arlington
Dongqi Han, Beijing University of Posts and Telecommunications
Jinsong Han, Zhejiang University
Jun Han, Korea Advanced Institute of Science and Technology (KAIST)
Shuai Han, Shanghai Jiao Tong University
Xingshuo Han, Nanjing University of Aeronautics and Astronautics
Florian Hantke, Northeastern University
Meng Hao, Singapore Management University
Qingying Hao, ShanghaiTech University
Shuai Hao, Old Dominion University

Shuang Hao, The University of Texas at Dallas
Sebastian Hasler, Aarhus University
Wajih Ul Hassan, University of Virginia
Chaoxiang He, Shanghai Jiao Tong University
Jingxuan He, University of California, Berkeley
Lipeng He, University of Waterloo
Ningyu He, The Hong Kong Polytechnic University
Yi He, Wuhan University
Yiling He, University College London
Zheyuan He, The Hong Kong Polytechnic University
Xiali Hei, University of Louisiana at Lafayette
Michael Heinzl, Unaffiliated
Chris Hicks, Alan Turing Institute
Lucca Hirschi, Inria
Blaine Hoak, The University of Texas at Dallas
Nguyen Phong Hoang, University of British Columbia
Hans-Joachim Hof, Technische Hochschule Ingolstadt
Florian Hofhammer, EPFL
Jana Hofmann, Max Planck Institute for Security and Privacy
Soamar Homsi, Air Force Research Laboratory
Byeongdo Hong, The Affiliated Institute of ETRI
Cheng Hong, Ant Group
Geng Hong, Fudan University
Hong Hu, The Pennsylvania State University
Hongsheng Hu, Shanghai Jiao Tong University
Hongxin Hu, University at Buffalo
Jie Hu, Arizona State University
Pengfei Hu, Shandong University
Yuncong Hu, Shanghai Jiao Tong University
Zhaojie Hu, University of Central Florida
Cheng Huang, Sichuan University
Heqing Huang, City University of Hong Kong
Kaifeng Huang, Tongji University
Xuanbo Huang, Xi'an Jiaotong University
Yujin Huang, The University of Melbourne
Zhicong Huang, Ant Group
Zonghao Huang, Duke University
Kévin Huguenin, University of Lausanne
Jun Ho Huh, Sungkyunkwan University
Bo Hui, Johns Hopkins University
Wei Huo, Institute of Information Engineering, Chinese Academy of Sciences
Syed Rafiul Hussain, The Pennsylvania State University
Michele Ianni, University of Calabria, Italy
Muhammad Ibrahim, Georgia Institute of Technology
Panagiotis Ilia, Cyprus University of Technology
Luca Invernizzi, Google
Saba Iqbal, Brigham Young University
Umar Iqbal, Washington University in St. Louis
Fabian Ising, Fraunhofer SIT and ATHENE National Research Center for Applied Cybersecurity
Mazharul Islam, Uber Technologies
Katherine Izhikevich, University of California, San Diego
Liz Izhikevich, University of California, Los Angeles
Dennis Jackson, Mozilla
Murtuza Jadliwala, The University of Texas at San Antonio
Rhongho Jang, Wayne State University
Patrick Jattke, ETH Zurich
Dae R. Jeong, Seoul National University
Fujiao Ji, University of Tennessee
Tianxi Ji, Texas Tech University
Xiaoyu Ji, Zhejiang University
Yuede Ji, The University of Texas at Arlington
Zhenlan Ji, Nara Institute of Science and Technology
Jinyuan Jia, The Pennsylvania State University
Xiangkun Jia, Institute of Software Chinese Academy of Sciences
Yan Jia, Nankai University
Yanxue Jia, Illinois Institute of Technology
Qinhong Jiang, The Hong Kong Polytechnic University
Wenbo Jiang, University of Electronic Science and Technology of China
Yu Jiang, Tsinghua University
Yu Jin, Tsinghua University
Lei Ju, Shandong University
Nesrine Kaaniche, Télécom SudParis, Institut Polytechnique de Paris
Wei Kaimin, Jinan University
Ingab Kang, University of Michigan
Min Suk Kang, Korea Advanced Institute of Science and Technology (KAIST)
Zifeng Kang, Beijing University of Posts and Telecommunications
Chris Kanich, University of Illinois Chicago
Murat Kantarcioglu, Virginia Tech
Alexandros Kapravelos, North Carolina State University and Socket Inc
Gabriel Kaptchuk, University of Maryland
Umit Karabiyik, George Mason University
Ghassan Karame, Ruhr-Universität Bochum
Frank Kargl, University of Ulm
Imtiaz Karim, The University of Texas at Dallas
Jonas Kaspereit, FH Münster
Basel Katt, The Norwegian University of Science and Technology
Jonathan Katz, Google
Smirity Kaushik, The George Washington University
Alireza Kavousi, University College London
Yigitcan Kaya, University of California, Santa Barbara and Indiana University
Arslan Khan, The Pennsylvania State University
Nora Khayata, Technische Universität Darmstadt
Abdallah Khreishah, New Jersey Institute of Technology
Mudita Khurana, Airbnb
Beom Heyn Kim, Hanyang University
Chung Hwan Kim, The University of Texas at Dallas
Doowon Kim, University of Tennessee
Hyoungshick Kim, Sungkyunkwan University
Hyungsub Kim, Indiana University
Jiwon Kim, Purdue University
Seulbae Kim, Pohang University of Science and Technology
Yongdae Kim, Korea Advanced Institute of Science and Technology (KAIST)
Young-Sik Kim, Daegu Gyeongbuk Institute of Science and Technology
Engin Kirda, Northeastern University
Lea Kissner, LinkedIn
Amit Klein, The Hebrew University of Jerusalem
Jan H. Klemmer, CISPA Helmholtz Center for Information Security
Philip Klostermeyer, CISPA Helmholtz Center for Information Security
Andreas Kogler, Apple

Dimitris Kolonelos, University of California, Berkeley
Fanyu Kong, Shandong University
Boris Köpf, Azure Research, Microsoft
Evgenios Kornaropoulos, George Mason University
Platon Kotzias, BforeAI
Anne Josiane Kouam, Inria and Technische Universität Berlin
Srikanth Krishnamurthy, University of California, Riverside
Joshua Kroll, Naval Postgraduate School
Karel Kubicek, Vault JS
Akshay "AK" Kulkarni, Prairie View A&M University
Abhinav Kumar, University of Massachusetts Amherst
Piyush Kumar, Indian Institute of Technology Delhi
Sam Kumar, University of California, Los Angeles
Anil Kurmus, IBM Research
Donghyun Kwon, Pusan National University
Massimo La Morgia, Sapienza University of Rome
Shangqi Lai, The University of Melbourne
Daniele Lain, ETH Zurich
Lukas Lamster, Graz University of Technology
Leona Lassak, Max Planck Institute for Security and Privacy
Dang Le, Northwestern University
Tu Le, The University of Alabama
Kevin Leach, Vanderbilt University
Diane Leblanc-Albarel, KU Leuven
Dongyoon Lee, Stony Brook University
Hao-Ping (Hank) Lee, Carnegie Mellon University
Heejo Lee, Korea University
Keewoo Lee, Ethereum Foundation
Kyu Hyung Lee, University of Georgia
Sangho Lee, Microsoft Research
Suyoung Lee, Korea Advanced Institute of Science and Technology (KAIST)
Wenke Lee, Georgia Institute of Technology
Yoochan Lee, Max Planck Institute for Security and Privacy
Yu Lei, University of Texas at Arlington
Bingyu Li, Beihang University
Changjiang Li, Palo Alto Networks
Dawei Li, Beihang University
Ding Li, Peking University
Fengjun Li, University of Kansas
Hui Li, Xidian University
Jingjie Li, University of Edinburgh
Kai Li, Stevens Institute of Technology
Kaixuan Li, Nanyang Technological University
Kecen Li, National University of Singapore
Meng Li, Hefei University of Technology
Ming F. Li, University of Arizona
Minghang Li, Beihang University
Ninghui Li, Perplexity AI and Purdue University
Penghui Li, Nanyang Technological University
Rui Li, Dawn Computing
Ruixuan Li, Tsinghua University
Rujia Li, Tsinghua University
Shanshan Li, National University of Defense Technology
Shaofeng Li, Southeast University
Shujun Li, University of Kent
Siyuan Li, Shandong University
Song Li, Zhejiang University
Weitong Li, Virginia Tech
Xiang Li, Nankai University
Xiangxue Li, East China Normal University
Xinfeng Li, The Hong Kong Polytechnic University
Ya-Nan Li, The University of Sydney
Yiming Li, Nanyang Technological University
Yuan Li, Zhongguancun Laboratory
Zheng Li, Shandong University
Zhenyuan Li, Zhejiang University
Zihao Li, University of Electronic Science and Technology of China
Ziqiang Li, Nanjing University of Information Science and Technology
Zongjie Li, The Hong Kong University of Science and Technology
Bei Liang, Beijing Institute of Mathematical Sciences and Applications
Junkai Liang, Peking University
Kaitai Liang, University of Turku and TU Delft
Song Liao, Texas Tech University
Wei Yang Bryan Lim, Nanyang Technological University
Chao Lin, Nanjing University of Aeronautics and Astronautics
Miaoqian Lin, The University of Hong Kong
Peihong Lin, National University of Defense Technology
Qixiao Lin, Beihang University
Yan Lin, Jinan University
Yun Lin, Shanghai Jiao Tong University
Zilong Lin, University of Missouri-Kansas City
Andreas Lindner, Uppsala University
Qi Ling, Purdue University
Xiang Ling, Institute of Software Chinese Academy of Sciences
Zhen Ling, Southeast University
Bo Liu, University of Technology Sydney
Chang Liu, National University of Singapore
Dinghao Liu, Shandong University
Gaoyang Liu, Huazhong University of Science and Technology
Guannan Liu, Colorado School of Mines
Hanlin Liu, Northwestern University
Jian Liu, University of Georgia
Jiawei Liu, Wuhan University
Jinfei Liu, Zhejiang University
Mingxuan Liu, Zhongguancun Laboratory
Peiyu Liu, Zhejiang University
Puzhuo Liu, Tsinghua University and Ant Group
Renyang Liu, National University of Singapore
Shinan Liu, The University of Hong Kong
Si Liu, Texas A&M University
Side Liu, Tulane University
Xiaoning Liu, RMIT University
Yang Liu, Swansea University
Yi Liu, Griffith University
Yi Liu, City University of Hong Kong
Yinxi Liu, Rochester Institute of Technology
Yizhong Liu, Beihang University
Yuxin "Myles" Liu, University of California, Los Angeles
Zhaoqian Liu, The Chinese University of Hong Kong, Shenzhen
Zhenguang Liu, Zhejiang University
Zhibo Liu, Nanjing University
Zhuoran Liu, University of Amsterdam
Zhuotao Liu, Tsinghua University
Chen-Da Liu-Zhang, Lucerne University of Applied Sciences and Arts
Yan Long, The Hong Kong University of Science and Technology (Guangzhou)

Stefano Longari, Politecnico di Milano
Jian Lou, Sun Yat-sen University
Li Lu, Zhejiang University
Yuan Lu, Agency for Science, Technology and Research (A*STAR)
Zhenliang Lu, City University of Hong Kong
Zhi Lu, National University of Singapore
Zhigang Lu, Western Sydney University
Zhuo Lu, University of South Florida
Bo Luo, The University of Kansas
Changhua Luo, Wuhan University
Feng Luo, The Hong Kong Polytechnic University
Meng Luo, Zhejiang University
Shaocheng Luo, Duke University
Xinjian Luo, Shanghai Jiao Tong University
Yu Luo, Mississippi State University
Zhengxiong Luo, National University of Singapore
Peizhuo Lv, Nanyang Technological University
Yunlong Lyu, The University of Hong Kong
Pingchuan Ma, Zhejiang University of Technology
Siqi Ma, The University of Wollongong
Yihan Ma, CISPA Helmholtz Center for Information Security
Zane Ma, Oregon State University
Marcel Maehren, Ruhr-Universität Bochum
Andrea Mambretti, IBM Research - Zurich
Prianka Mandal, College of William & Mary
Stefan Mangard, Graz University of Technology
Michail Maniatakos, New York University Abu Dhabi
Yunlong Mao, Nanjing University
Michele Marazzi, Google
Evangelia Anna Markatou, TU Delft
Athina Markopoulou, University of California, Irvine
Srdjan Matic, Universidad Carlos III de Madrid
Carlo Mazzocca, University of Salerno
Federico Mazzone, Carl von Ossietzky Universität Oldenburg
McKenna McCall, Colorado State University
Susan McGregor, Columbia University
Dongyu Meng, Palo Alto Networks
Guozhu Meng, Institute of Information Engineering, Chinese Academy of Sciences
Ruijie Meng, CISPA Helmholtz Center for Information Security
Xiangtao Meng, Shandong University
Robert Merget, Technology Innovation Institute
Alessio Merlo, Centro Alti Studi Difesa (CASD)
Mohamed-Lamine Messai, University of Lyon 2
Ulrike Meyer, RWTH Aachen University
Jiang Ming, Tulane University
Jaron Mink, Arizona State University
Donika Mirdita, Goethe University Frankfurt and ATHENE National Research Center for Applied Cybersecurity
Ilya Mironov, Meta
Shujaat Mirza, Microsoft
Pratyush Mishra, University of Pennsylvania
Vladislav Mladenov, Ruhr-Universität Bochum
Sebastian Mödersheim, Danmarks Tekniske Universitet (DTU)
David Mohaisen, University of Central Florida
Reham Mohamed Aburas, American University of Sharjah
Ameer Mohammed, Kuwait University
Jonas Möller, BIFOLD and Technische Universität Berlin
Jean-Philippe Monteuuis, Qualcomm
Hyungon Moon, UNIST (Ulsan National Institute of Science and Technology)
Pedro Moreno-Sanchez, IMDEA Software Institute and Max Planck Institute for Security and Privacy
Tatsuya Mori, Waseda University
Kazi Samin Mubasshir, Purdue University
Kunal Mukherjee, Virginia Tech
Pratyay Mukherjee, Hashgraph
Antonio Muñoz, University of Malaga
Collins Munyendo, University of California, Berkeley
Aleksandr Nahapetyan, North Carolina State University
Hocheol Nam, Korea Advanced Institute of Science and Technology (KAIST)
Kevin Nam, Kyung Hee University
Yuhong Nan, Sun Yat-sen University
Ben Nassi, Tel Aviv University
Hamed Nemati, KTH Royal Institute of Technology
Jianbing Ni, Queen's University
Tao Ni, King Abdullah University of Science and Technology
Jianting Ning, Zhejiang Sci-Tech University
Alexandra Nisenoff, Carnegie Mellon University
Jianyu Niu, City University of Hong Kong
Maximilian Noppel, Karlsruhe Institute of Technology
Boubakr Nour, Ericsson Research
DaeHun Nyang, Ewha Womans University
Se Eun Oh, Ewha Womans University
Hamed Okhravi, MIT Lincoln Laboratory
Gabriele Oligeri, Hamad Bin Khalifa University
Cristina Onete, University of Limoges/XLIM/CNRS 7252
Samson Oruma, Norwegian University of Science and Technology (NTNU)
David Oswald, Durham University
Harun Oz, Meta
Alex Ozdemir, Georgia Institute of Technology
Muslum Ozgur Ozmen, Arizona State University
Miroslav Pajic, Duke University
Balaji Palanisamy, University of Pittsburgh
Frank Pallas, University of Salzburg
Shidong Pan, Unaffiliated
Xudong Pan, Fudan University and Shanghai Innovation Institute
Yepeng Pan, CISPA Helmholtz Center for Information Security
Qi Pang, Carnegie Mellon University
Xiaoyi Pang, The Hong Kong University of Science and Technology
Gaurav Panwar, New Mexico State University
Dimitrios Papadopoulos, The Hong Kong University of Science and Technology
CheolJun Park, Kyung Hee University
Thomas Pasquier, University of British Columbia
Kenneth Paterson, ETH Zurich
Sikhar Patranabis, IBM Research
Protik Kumar Paul, TU Darmstadt
Mathias Payer, EPFL
Sai Teja Peddinti, Google
Giancarlo Pellegrino, CISPA Helmholtz Center for Information Security
Feargus Pendlebury, Meta
Zhiniang Peng, Huazhong University of Science and Technology
Jan Pennekamp, RWTH Aachen University
Octavio Perez-Kempner, NTT Social Informatics Laboratories

Mert Pesé, Clemson University
Sandro Pinto, Universidade do Minho
Pansilu Pitigalaarachchi, CISPA Helmholtz Center for Information Security
Alexander Ponticello, CISPA Helmholtz Center for Information Security
Christina Pöpper, New York University Abu Dhabi
Bart Preneel, KU Leuven
Niels Provos, Unaffiliated
Lina Pu, University of Alabama
Sihang Pu, East China Normal University
Maxime Puys, Université Clermont Auvergne
Kaihua Qin, University of Warwick
Lancheng Qin, Zhongguancun Laboratory
Wenjun Qiu, University of Toronto
Wenjie Qu, National University of Singapore
Yiting Qu, CISPA Helmholtz Center for Information Security
Srinivasan Raghuraman, Visa Research and Massachusetts Institute of Technology
Sazzadur Rahaman, University of Arizona
Mahdi Rahimi, COSIC, KU Leuven
Amir Rahmati, Stony Brook University
JV Rajendran, Texas A&M University
Kopo Marvin Ramokapane, University of Bristol
Ali Ranjbar, The Pennsylvania State University
Md Mamunur Rashid, Deakin University
Zachary Ratliff, ETH Zürich
Anna Raymaker, Georgia Institute of Technology
Taqi Raza, University of Massachusetts Amherst
Kaveh Razavi, ETH Zurich
Brad Reaves, North Carolina State University
Pascal Reisert, University of Stuttgart
Nathan Reitinger, Northwestern Pritzker School of Law
Veronica Rivera, Georgia Institute of Technology
Ricardo J. Rodríguez, Universidad de Zaragoza
Thomas Rokicki, CentraleSupélec, Inria, CNRS, IRISA
Simon Pietro Romano, University of Napoli Federico II
Eyal Ronen, Tel Aviv University
Christian Rossow, CISPA Helmholtz Center for Information Security
Na Ruan, Shanghai Jiao Tong University
Nicola Ruaro, Meta
Scott Ruoti, University of Tennessee
Abhinaya S.B., North Carolina State University
Aafaq Sabir, North Carolina State University
Sayak Saha Roy, Louisiana State University
Gururaj Saileshwar, University of Toronto
A H M Nazmus Sakib, The University of Texas at San Antonio
Amin Sakzad, Monash University
Jordan Samhi, University of Luxembourg
Somitra Sanadhya, Indian Institute of Technology Kanpur
Jose Sanchez Vicarte, Microsoft
Iskander Sanchez-Rola, Norton
Igor Santos-Grueiro, International University of La Rioja
Roozbeh Sarenche, COSIC, KU Leuven
Pratik Sarkar, Obsidus Labs
Francesco Sassi, Sapienza University of Rome
Takami Sato, Keio University
Neetesh Saxena, Cardiff University
Sarah Scheffler, Carnegie Mellon University
Moritz Schloegel, CISPA Helmholtz Center for Information Security
Thomas Schneider, Technische Universität Darmstadt
Michael Schwarz, CISPA Helmholtz Center for Information Security
Jörg Schwenk, Ruhr-Universität Bochum
Kent Seamons, Brigham Young University
Wendy Seltzer, Unaffiliated
Jae Hong Seo, Hanyang University
Avital Shafran, ETH Zurich
Arash Shaghaghi, The University of New South Wales
Ahmad Salehi Shahraki, La Trobe University
Liqun Shan, Georgia Southern University
Shawn Shan, Dartmouth College
Shuai Shang, University of Electronic Science and Technology of China
Pradip Sharma, University of Aberdeen
Shantanu Sharma, New Jersey Institute of Technology
Shashank Sharma, Purdue University
Jiachen Shen, East China Normal University
Jian Shen, Zhejiang Sci-Tech University
Wenbo Shen, Zhejiang University
Xinyue Shen, CISPA Helmholtz Center for Information Security
Faysal Hossain Shezan, The University of Texas at Arlington
Chenghang Shi, Institute of Computing Technology, Chinese Academy of Sciences
Weidong Shi, University of Houston
Yizhe Shi, Fudan University
He (Shawn) Shuang, Palo Alto Networks
Shubhi Shukla, Indian Institute of Technology Kharagpur
Yan Shvartzshnaider, York University
Jeremy Singer, University of Glasgow
Nikhilesh Singh, Technische Universität Darmstadt
Mohit Singhal, Northeastern University
Rohit Sinha, Hashgraph
Jackson Sippe, University of Colorado Boulder
Kostas Solomos, Brandeis University
Flavien Solt, National University of Singapore
Juraj Somorovsky, Paderborn University
Ananta Soneji, University of Nebraska Omaha
Dokyung Song, Yonsei University
Suhwan Song, Samsung Electronics
Xiangfu Song, Nanyang Technological University
Alberto Sonnino, Mysten Labs and University College London
Alessandro Sorniotti, IBM Research
Katerina Sotiraki, Yale University
Noah Spahn, The Open University
Michael Specter, Georgia Institute of Technology
Riccardo Spolaor, Shandong University
Marco Squarcina, TU Wien
Harshini Sri Ramulu, Paderborn University
Supraja Sridhara, Google
Paul Staat, Ruhr-Universität Bochum
Dario Stabili, University of Modena and Reggio Emilia
Ron Steinfeld, Monash University
Sophie Stephenson, The University of Texas at Arlington
Ben Stock, CISPA Helmholtz Center for Information Security
Guillermo Suarez-Tangil, IMDEA Networks Institute
Jose Such, INGENIO (CSIC-UPV)
Takeshi Sugawara, The University of Electro-Communications
Nazatul Sultan, CSIRO

Cong Sun, Xidian University
Ruimin Sun, Florida International University
Ruoxi Sun, CSIRO
Shi-Feng Sun, Shanghai Jiao Tong University
Tong Sun, Zhejiang University
Wei Sun, Wright State University
Wenhai Sun, Purdue University
Zhibo "Eric" Sun, Drexel University
Willy Susilo, University of Wollongong
Fnu Suya, University of Tennessee
Nina Taft, Google
Erkan Tairi, University of California, Berkeley
Kunal Talwar, Apple
Chee Wei Tan, Nanyang Technological University
Gefei Tan, Northwestern University
Leonie Tanczer, University College London
Guofeng Tang, Singapore Management University
Kunsheng Tang, University of Science and Technology of China
Tianxin Tang, University of Glasgow
Yuzhe Tang, Syracuse University
Zhaozhou Tang, Georgia Institute of Technology
Guanhong Tao, University of Utah
Kazem Taram, Purdue University
Teryl Taylor, IBM Research
Kurt Thomas, Google
Poojitha Thota, The University of Texas at Arlington
Dave (Jing) Tian, Purdue University
Yunpeng Tian, The Hong Kong Polytechnic University
Zhihong Tian, Guangzhou University
Afonso Tinoco de Faria Cecilio dos Santos, Carnegie Mellon University and Universidade de Lisboa
Nils Ole Tippenhauer, CISPA Helmholtz Center for Information Security
Flavio Toffalini, Ruhr-Universität Bochum
Wei Tong, Nanjing University
Jacob Torrey, Thinkst Applied Research
Reza Tourani, Saint Louis University
Rahmadi Trimananda, Comcast Cybersecurity and Privacy Research
Kien Tuong Truong, ETH Zurich
Florian Tschorsch, Technische Universität Dresden
Nektarios Georgios Tsoutsos, University of Delaware
Taro Tsuchiya, Carnegie Mellon University
Guliz Tuncay, Google
Nirvan Tyagi, University of Washington
Md Palash Uddin, Deakin University
Blase Ur, University of Chicago
Warda Usman, Walmart Information Security
Thijs van Ede, University of Twente
Michel van Eeten, Delft University of Technology
Jennifer Vander Loop, DePaul University
Mayank Varia, Boston University
Dimitrios Vasilopoulos, Unaffiliated
Marco Vassena, Utrecht University
Yash Vekaria, University of California, Davis
Maryna Veksler, Virginia Commonwealth University
Alexander Viand, Belfort Labs and University of Cambridge
Corrado Aaron Visaggio, University of Foggia
Ivan Visconti, Sapienza University of Rome
Viet Vo, Swinburne University of Technology
Niklas Vogel, Goethe University Frankfurt and ATHENE National Research Center for Applied Cybersecurity
Daniel Votipka, Tufts University
Alexios Voulimeneas, TU Delft
Naga Sujitha Vummaneni, Cornell University
Sarisht Wadhwa, Duke University and University of Michigan
David Wagner, University of California, Berkeley
Eric Wagner, University of Luxembourg
Isabel Wagner, University of Basel
Ryan Wails, Georgetown University
Anyu Wang, Tsinghua University
Binghui Wang, Illinois Institute of Technology
Cheng-Long Wang, Unaffiliated
Chenxu Wang, Southern University of Science and Technology (SUSTech) and The Hong Kong Polytechnic University
Chenyi Wang, University of Arizona
Dawei Wang, Zhongguancun Laboratory
Derui Wang, CSIRO
Ding Wang, Nankai University
Han Wang, The University of Kansas
Haoyu Wang, Huazhong University of Science and Technology
Haozhao Wang, Huazhong University of Science and Technology
Jialai Wang, National University of Singapore
Jianfeng Wang, Xidian University
Jingyi Wang, Zhejiang University
Meng Wang, CISPA Helmholtz Center for Information Security
Mingyuan Wang, University of Delaware
Qi Wang, Tsinghua University
Qin Wang, CSIRO
Qinying Wang, EPFL
Run Wang, Wuhan University
Ruoyu "Fish" Wang, Arizona State University
Shan Wang, Shandong University
Shang Wang, University of Technology Sydney
Shaowei Wang, Guangzhou University
Shuo Wang, Shanghai Jiao Tong University
Songlei Wang, Shenzhen University
Tao Wang, University of North Texas
Weijia Wang, Shandong University
Weizheng Wang, Guangzhou University
Wenhao Wang, Institute of Information Engineering, Chinese Academy of Sciences
Xinda Wang, The University of Texas at Dallas
Xinqian Wang, RMIT University
Xuechao Wang, The Hong Kong University of Science and Technology (Guangzhou)
Xueqiang Wang, University of Central Florida
Yan Wang, Temple University
Yunhao Wang, Yale University
Zhen Wang, Hangzhou Dianzi University
Zhipeng Wang, The University of Manchester
Zihan Wang, The University of Queensland
Zixuan Wang, University of California, San Diego
Noel Warford, The George Washington University
Mingkui Wei, George Mason University
Shiyi Wei, The University of Texas at Dallas
Xu Wei, Xidian University
Yu Wei, Georgia Institute of Technology
Christian Weinert, Royal Holloway, University of London
Ben Weintraub, University of Notre Dame

Rui Wen, Institute of Science Tokyo
Sheng Wen, Swinburne University of Technology
Chenkai Weng, Arizona State University
Dominik Wermke, North Carolina State University
Seongil Wi, UNIST (Ulsan National Institute of Science and Technology)
Thom Wiggers, PQShield
Hans Winderix, DistriNet, KU Leuven
Seunghoon Woo, Korea University
Bang Wu, RMIT University
Daoyuan Wu, Lingnan University
Hao Wu, Nanjing University
Jianliang Wu, Simon Fraser University
Lei Wu, Zhejiang University
Lichao Wu, University of Bristol
Mingli Wu, The Hong Kong Polytechnic University
Nan Wu, University of Technology Sydney
Pengfei Wu, Singapore Management University
Shujiang Wu, Beihang University
Stanley Wu, University of Chicago
Yanzhao Wu, Florida International University
Yuncheng Wu, Renmin University of China
Karl Wüst, Mysten Labs
Xiaoyu Xia, RMIT University
Liyao Xiang, Shanghai Jiao Tong University
Tao Xiang, Chongqing University
Yang Xiang, Monash University
Zihang Xiang, University of California, Los Angeles
Bin Xiao, The Hong Kong Polytechnic University
Fu Xiao, Nanjing University of Posts and Telecommunications
Hanshen Xiao, Purdue University
Madelyne Xiao, Princeton University
Rui Xiao, Shanghai University of Finance and Economics
Yang Xiao, University of Kentucky
Yang Xiao, Institute of Information Engineering, Chinese Academy of Sciences
Luyi Xing, University of Illinois Urbana–Champaign
Junjie Xiong, Missouri University of Science and Technology
Dongyan Xu, Purdue University
Fengyuan Xu, Nanjing University
Jiacen Xu, Microsoft
Jun Xu, The University of Utah
Lei Xu, Nanjing University of Science and Technology
Ming Xu, National University of Singapore
Shengmin Xu, Fujian Normal University
Xiangyu Xu, Southeast University
Xiaoyun Xu, Zhongguancun Academy
Yuanchao Xu, University of California, Santa Cruz
Haiyang Xue, Singapore Management University
Kaiping Xue, University of Science and Technology of China
Lei Xue, Sun Yat-sen University
Chen Yan, Zhejiang University
Shenao Yan, University of Connecticut
Zheng Yan, Xidian University
Kang Yang, State Key Laboratory of Cryptology
Nanzi Yang, Old Dominion University
Songtao Yang, Zhongguancun Laboratory
Tianchang Yang, The Pennsylvania State University
Yaxi Yang, Nanyang Technological University
Yibin Yang, University of Toronto
Yinghao Yang, Institute of Computing Technology, Chinese Academy of Sciences
Yuqing Yang, CISPA Helmholtz Center for Information Security
Zhemin Yang, Fudan University
Zheng Yang, Microsoft
Zhice Yang, ShanghaiTech University
Zhuolin Yang, University of Arizona
Ziqi Yang, Zhejiang University
Mingxuan Yao, Georgia Institute of Technology
Yaxing Yao, Johns Hopkins University
Zephyr Yao, New Jersey Institute of Technology
Tuba Yavuz, University of Florida
Dayong Ye, City University of Macau
Yutong Ye, Institute of Software Chinese Academy of Sciences
Doguhan Yeke, Purdue University
Biao Yi, East China University of Science and Technology
Wei You, Renmin University of China
Bo Yu, National University of Defense Technology
Chia-Mu Yu, National Yang Ming Chiao Tung University
Dongxiao Yu, Shandong University
Jason Zhijingcheng Yu, Jane Street
Jiadi Yu, Shanghai Jiao Tong University
Jiahao Yu, Northwestern University
Jiongchi Yu, Nanyang Technological University
Zhiyuan Yu, Texas A&M University
Xiaoyong (Brian) Yuan, Clemson University
Xingliang Yuan, The University of Melbourne
Xuejing Yuan, Beijing University of Posts and Telecommunications
Ying Yuan, Örebro University
Yuanyuan Yuan, Tsinghua University
Peterson Yuhala, University of British Columbia
Gabriel Zaid, CryptoExperts
Stefano Zanero, Politecnico di Milano
Dongrui Zeng, Palo Alto Networks
Kyle Zeng, OpenAI
Rui Zeng, Zhejiang University
Mingming Zha, Indiana University
Chuan Zhang, Beijing Institute of Technology
Chuqi Zhang, National University of Singapore
Danfeng Zhang, Duke University
Fan Zhang, Yale University
Guangsheng Zhang, University of Technology Sydney
Han Zhang, Tsinghua University
Hang Zhang, Indiana University
Haotian Zhang, New Jersey Institute of Technology
He Zhang, Griffith University
Jialong Zhang, Xi'an Jiaotong University
Jianting Zhang, Purdue University
Jipeng Zhang, National University of Singapore
Kaiyuan Zhang, Rutgers University and Perplexity AI
Lan Zhang, Northern Arizona University
Lei Zhang, East China Normal University
Liang Feng Zhang, ShanghaiTech University
Mingming Zhang, Zhongguancun Laboratory
Mingxue Zhang, Zhejiang University
Minxing Zhang, CISPA Helmholtz Center for Information Security
Mu Zhang, University of Utah
Ning Zhang, Washington University in St. Louis

Qifan Zhang, Palo Alto Networks
Qiguang Zhang, Southeast University
Quan Zhang, East China Normal University
Ruiyi Zhang, CISPA Helmholtz Center for Information Security
Runze Zhang, Meta Platforms
Shengzhi Zhang, Boston University
Shenyi Zhang, Wuhan University
Xiang Zhang, Tianjin University
Xiaohan Zhang, Fudan University
Xiaokuan Zhang, George Mason University
Xinwei Zhang, The Hong Kong Polytechnic University
Yifan Zhang, San Diego State University
Yiming Zhang, Tsinghua University
Youqian Zhang, The Hong Kong Polytechnic University
Yuan Zhang, Fudan University
Yuan Zhang, University of Electronic Science and Technology of China
Yuhui Zhang, Institute of Information Engineering, Chinese Academy of Sciences
Zhi Zhang, The University of Western Australia
Zhikun Zhang, Zhejiang University
Zhiyuan Zhang, Max Planck Institute for Security and Privacy
Zijian Zhang, Beijing Institute of Technology
Ziqi Zhang, University of Illinois Urbana–Champaign
Chuan Zhao, University of Jinan and Quan Cheng Laboratory
Kunsong Zhao, The Hong Kong Polytechnic University
Lianying Zhao, Carleton University
Mang Zhao, Wuhan University
Shangqing Zhao, University of Oklahoma
Shixuan Zhao, The Ohio State University
Yanjie Zhao, Huazhong University of Science and Technology
Zhengyu Zhao, Xi'an Jiaotong University
Yury Zhauniarovich, TU Delft
Fangyu Zheng, University of Chinese Academy of Sciences
Haitao Zheng, University of Chicago
Mengce Zheng, Zhejiang Wanli University
Yifeng Zheng, The Hong Kong Polytechnic University
Ce Zhou, Missouri University of Science and Technology
Chijin Zhou, East China Normal University
Hao Zhou, The Hong Kong Polytechnic University
Huancheng Zhou, Texas A&M University
Kai Zhou, The Hong Kong Polytechnic University
Lei Zhou, National University of Defense Technology
Liyi Zhou, The University of Sydney
Yufei Zhou, Sun Yat-sen University
Tianqing Zhu, City University of Macau
Weidong Zhu, Florida International University
Jianwei Zhuge, Tsinghua University
Yunkai Zou, Nankai University
Chaoshun Zuo, University of Electronic Science and Technology of China

AI Integrity Chair
Gianluca Stringhini, Boston University

Ethics Committee Chair
Paul Pearce, University of California, Irvine

Ethics Committee
David Adrian, Unaffiliated
Joseph Bonneau, New York University
Kevin Butler, University of Florida
Zimo Chai, Stanford University and University of California, Berkeley
Liz Izhikevich, University of California, Los Angeles
Chris Kanich, University of Illinois Chicago
Gabriel Kaptchuk, University of Maryland
Mathias Payer, EPFL
Nguyen Phong Hoang, University of British Columbia
Sarah Scheffler, Carnegie Mellon University

Open Science and Compliance Chair
Jo Van Bulck, DistriNet, KU Leuven

Awards Committee Chair
Joseph Calandrino, Carnegie Mellon University

Artifact Evaluation Committee Co-Chairs
Clement Fung, University of Maryland, Baltimore County
Tiago Heinrich, Max Planck Institute for Informatics
Christian Wressnegger, Karlsruhe Institute of Technology

Artifact Evaluation Committee
TBA

Steering Committee
Michael Bailey, Georgia Institute of Technology
Lujo Bauer, Carnegie Mellon University
Kevin Butler, University of Florida
Joe Calandrino, Carnegie Mellon University
William Enck, North Carolina State University
Rachel Greenstadt, New York University
Casey Henderson-Ross, USENIX Association
Thorsten Holz, Max Planck Institute for Security and Privacy
Tadayoshi Kohno, Georgetown University
Franziska Roesner, University of Washington
Ben Stock, CISPA Helmholtz Center for Information Security
Kurt Thomas, Google
Carmela Troncoso, Max Planck Institute for Security and Privacy and EPFL