33rd USENIX Security Symposium

August 14–16, 2024, Philadelphia, PA, USA

Sponsored by USENIX, the Advanced Computing Systems Association

The USENIX Security Symposium brings together researchers, practitioners, system administrators, system programmers, and others interested in the latest advances in the security and privacy of computer systems and networks. The 33rd USENIX Security Symposium will be held August 14–16, 2024, in Philadelphia, PA.

Important: *In 2023, USENIX Security introduced substantial changes to the review process, aimed to provide a more consistent path towards acceptance and reduce the number of times papers reenter the reviewing process. Detailed information is available at USENIX Security Publication Model Changes. (https://www.usenix.org/conference/usenixsecurity24/publication-model-change).*

All researchers are encouraged to submit papers covering novel and scientifically significant practical works in computer security.

Important Dates

Summer Deadline

- Refereed paper submissions due: **Tuesday, June 6, 2023, 11:59 pm AoE**
- Early reject notification: **Thursday, July 13, 2023**
- Rebuttal Period: **August 21–23, 2023**
- Notification to authors: **Friday, September 1, 2023**
- Final paper files due: **Tuesday, October 10, 2023**

Fall Deadline

- Refereed paper submissions due: **Tuesday, October 17, 2023, 11:59 pm AoE**
- Early reject notification: **Monday, November 27, 2023**
- Rebuttal Period: **January 22–24, 2024**
- Notification to authors: **Thursday, February 1, 2024**
- Final paper files due: **Tuesday, March 5, 2024**

Winter Deadline

- Refereed paper submissions due: **Thursday, February 8, 2024, 11:59 pm AoE**
- Early reject notification: **Monday, March 18, 2024**
- Rebuttal Period: **April 24–26, 2024**
- Notification to authors: **Wednesday, May 8, 2024**
- Final paper files due: **Thursday, June 13, 2024**

- Invited talk and panel proposals due: **Thursday, February 8, 2024**
- Poster proposals due: **Tuesday, July 9, 2024**
  - Notification to poster presenters: **Tuesday, July 16, 2024**

Symposium Organizers

Program Co-Chairs

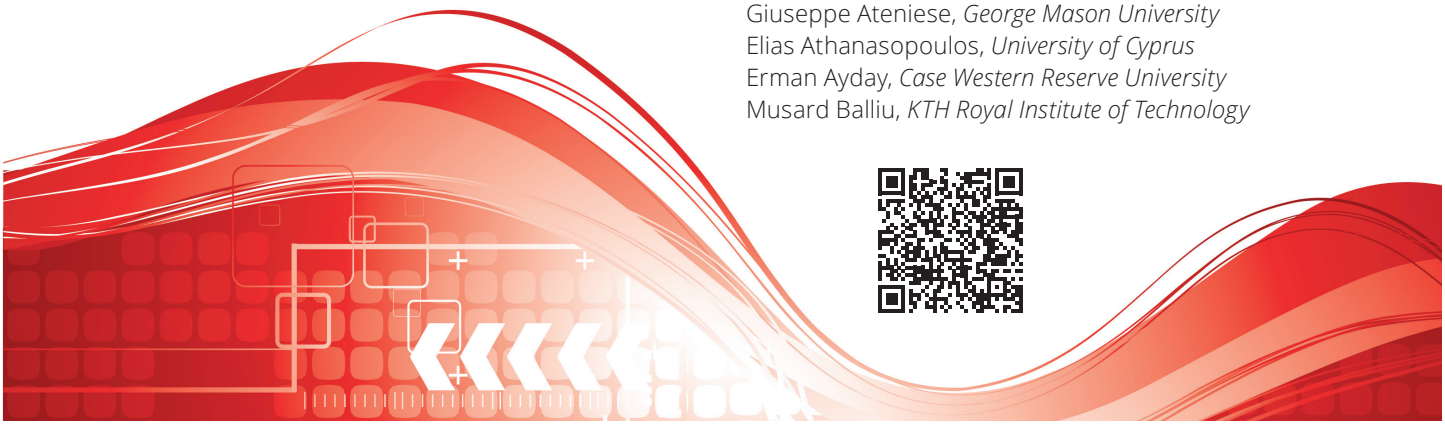
Davide Balzarotti, *Eurecom*
Wenyuan Xu, *Zhejiang University*

Program Vice Co-Chairs

Tiffany Bao, *Arizona State University*
Alexandra Dmitrienko, *University of Wuerzburg*
Qi Li, *Tsinghua University*
Giancarlo Pellegrino, *CISPA Helmholtz Center for Information Security*
Chen Yan, *Zhejiang University*
Yupeng Zhang, *University of Illinois at Urbana–Champaign and Texas A&M University*

Program Committee

Yousra Aafer, *University of Waterloo*
Aysajan Abidin, *imec-COSIC KU Leuven*
Ruba Abu-Salma, *King's College London*
Magnus Almgren, *Chalmers University of Technology*
Mário S. Alvim, *Universidade Federal de Minas Gerais*
Abdelrahaman Aly, *Technology Innovation Institute (TII)*
Manos Antonakakis, *Georgia Tech*
Daniele Antonioli, *EURECOM*
Simone Aonzo, *EURECOM*
Frederico Araujo, *IBM Research*
Giuseppe Ateniese, *George Mason University*
Elias Athanasopoulos, *University of Cyprus*
Erman Ayday, *Case Western Reserve University*
Musard Balliu, *KTH Royal Institute of Technology*



Sébastien Bardin, *CEA LIST, Université Paris-Saclay*
Lejla Batina, *Radboud University*
Lujo Bauer, *Carnegie Mellon University*
Matthew Bernhard, *VotingWorks*
Konstantin (Kosta) Beznosov, *University of British Columbia*
Battista Biggio, *University of Cagliari*
Joseph Bonneau, *New York University*
Marcus Botacin, *Texas A&M University*
Sven Bugiel, *CISPA Helmholtz Center for Information Security*
Nathan Burow, *MIT Lincoln Laboratory*
Juan Caballero, *IMDEA Software Institute*
Patricia Arias Cabarcos, *Paderborn University*
Stefano Calzavara, *Università Ca' Foscari Venezia*
Yinzhi Cao, *Johns Hopkins University*
Srdjan Capkun, *ETH Zurich*
Alvaro A. Cardenas, *University of California, Santa Cruz*
Nicholas Carlini, *Google*
Lorenzo Cavallaro, *University College London*
Z. Berkay Celik, *Purdue University*
Sang Kil Cha, *Korea Advanced Institute of Science and Technology (KAIST)*
Varun Chandrasekaran, *University of Illinois at Urbana–Champaign and Microsoft Research*
Rahul Chatterjee, *University of Wisconsin—Madison*
Sze Yiu Chau, *The Chinese University of Hong Kong*
Alfred Chen, *University of California, Irvine*
Guoxing Chen, *Shanghai Jiao Tong University*
Hao Chen, *University of California, Davis*
Kai Chen, *Institute of Information Engineering, Chinese Academy of Sciences*
Yanjiao Chen, *Zhejiang University*
Yizheng Chen, *University of Maryland*
Yushi Cheng, *Tsinghua University*
Giovanni Cherubin, *Microsoft*
Euijin Choo, *University of Alberta*
Sherman S. M. Chow, *The Chinese University of Hong Kong*
Nicolas Christin, *Carnegie Mellon University*
Mihai Christodorescu, *Google*
Shaanan Cohney, *University of Melbourne*
Mauro Conti, *University of Padova*
Andrea Continella, *University of Twente*
Manuel Costa, *Azure Research, Microsoft*
Daniele Cono D'Elia, *Sapienza University of Rome*
Savino Dambra, *Norton Research Group*
Lucas Davi, *University of Duisburg-Essen*
Ambra Demontis, *University of Cagliari*
Changyu Dong, *Guangzhou University*
Adam Doupé, *Arizona State University*
Tudor Dumitras, *University of Maryland, College Park*
Zakir Durumeric, *Stanford University*
Laura Edelson, *New York University*
Manuel Egele, *Boston University*
Thomas Eisenbarth, *University of Lübeck*
Mohamed Elsabagh, *Quokka*
Pardis Emami-Naeini, *Duke University*
William Enck, *North Carolina State University*
Sascha Fahl, *CISPA Helmholtz Center for Information Security*
Tobias Fiebig, *Max Planck Institute for Software Systems (MPI-SWS)*
Bryan Ford, *EPFL*
Alisa Frik, *International Computer Science Institute (ICSI)*
Aymeric Fromherz, *Inria*
Kevin Fu, *Northeastern University*
Xinwen Fu, *University of Massachusetts Lowell*
Kelsey Fulton, *Colorado School of Mines*
Carlos Gañán, *ICANN*
Tal Garfinkel, *University of California, San Deigo*
Carrie Gates, *Bank of America*
Esha Ghosh, *Microsoft Research*
Yossi Gilad, *The Hebrew University of Jerusalem*
Andre Ricardo Abed Gregio, *Federal University of Parana (UFPR)*
Daniel Gruss, *Graz University of Technology*
Guofei Gu, *Texas A&M University*
Marco Guarnieri, *IMDEA Software Institute*
Wenbo Guo, *Purdue University*
Ariel Hamlin, *Northeastern University*
Jun Han, *Yonsei University*
Weili Han, *Fudan University*
Shuang Hao, *The University of Texas at Dallas*
Hamza Harkous, *Google*
Behnaz Hassanshahi, *Oracle Labs*
Nguyen Phong Hoang, *University of Chicago*
Thorsten Holz, *CISPA Helmholtz Center for Information Security*
Houman Homayoun, *University of California, Davis*
Nicholas Hopper, *University of Minnesota*
Danny Yuxing Huang, *New York University*
Jun Ho Huh, *Samsung Research*
Alice Hutchings, *University of Cambridge*
Luca Invernizzi, *Google*
Cynthia Irvine, *Naval Postgraduate School*
Dennis Jackson, *Mozilla*
Charlie Jacomme, *Inria Paris*
Rob Jansen, *U.S. Naval Research Laboratory*
Rikke Bjerg Jensen, *Royal Holloway, University of London*
Yuseok Jeon, *UNIST (Ulsan National Institute of Science and Technology)*
Xiaoyu Ji, *Zhejiang University*
Aaron Johnson, *U.S. Naval Research Laboratory*
Gabriel Kaptchuk, *Boston University*
Umit Karabiyik, *Purdue University*
Marcel Keller, *CSIRO's Data61*
Vasileios Kemerlis, *Brown University*
Dmitry Khovratovich, *Ethereum Foundation*
Taegyu Kim, *The Pennsylvania State University*
Taesoo Kim, *Georgia Institute of Technology and Samsung Research*
Yongdae Kim, *Korea Advanced Institute of Science and Technology (KAIST)*
Tadayoshi Kohno, *University of Washington*
Kari Kostiainen, *ETH Zurich*
Platon Kotzias, *Norton Research Group*
Steve Kremer, *Inria*
Katharina Krombholz, *CISPA Helmholtz Center for Information Security*
Christopher Kruegel, *University of California, Santa Barbara*
Giovanni Lagorio, *University of Genoa*
Andrea Lanzi, *University of Milan*
Pierre Laperdrix, *CNRS*
Tancrède Lepoint, *Amazon Web Services*
Frank Li, *Georgia Institute of Technology*
Ming Li, *University of Arizona*
Song Li, *Zhejiang University*

Christopher Liebchen, *Google*
Zhiqiang Lin, *The Ohio State University*
Ting Liu, *Xi'an Jiaotong University*
Yao Liu, *University of South Florida*
Wouter Lueks, *CISPA Helmholtz Center for Information Security*
Lannan Lisa Luo, *George Mason University*
Mulong Luo, *Cornell University*
Xiapu Luo, *The Hong Kong Polytechnic University*
Matteo Maffei, *Technische Universität Wien*
Nathan Malkin, *University of Maryland*
Michail Maniatakos, *New York University Abu Dhabi*
Ivan Martinovic, *University of Oxford*
Sahar Mazloom, *JPMorgan Chase*
Jon McCune, *Google*
Allison McDonald, *Boston University*
Catherine Meadows, *U.S. Naval Research Laboratory*
Sarah Meiklejohn, *Google and University College London*
Yan Meng, *Shanghai Jiao Tong University*
Markus Miettinen, *Technische Universität Darmstadt*
Mainack Mondal, *Indian Institute of Technology, Kharagpur*
Veelasha Moonsamy, *Ruhr University Bochum*
Marius Muench, *University of Birmingham*
Takao Murakami, *AIST*
Moses Namara, *Meta*
Shravan Ravi Narayan, *The University of Texas at Austin*
Ivan De Oliveira Nunes, *Rochester Institute of Technology*
Adam Oest, *Paypal*
Hamed Okhravi, *MIT Lincoln Laboratory*
Cristina Onete, *Université de Limoges, XLIM, and CNRS 7252*
Simon Oya, *University of Waterloo*
Fabio Pagani, *Binarly*
Panos Papadimitratos, *KTH Royal Institute of Technology*
Dimitrios Papadopoulos, *The Hong Kong University of Science and Technology*
Andrew Paverd, *Microsoft*
Paul Pearce, *Georgia Institute of Technology*
Sai Teja Peddinti, *Google*
Amreesh Phokeer, *Internet Society*
Stjepan Picek, *Radboud University*
Fabio Pierazzi, *King's College London*
Georgios Portokalidis, *Stevens Institute of Technology*
Niels Provos, *Lacework*
Chenxiong Qian, *The University of Hong Kong*
Sara Rampazzi, *University of Florida*
Aanjhan Ranganathan, *Northeastern University*
Kasper Rasmussen, *University of Oxford*
Mariana Raykova, *Google*
Elissa Redmiles, *Max Planck Institute for Software Systems (MPI-SWS)*
Oscar Reparaz, *Block, Inc.*
Tamara Rezk, *Inria*
Konrad Rieck, *Technische Universität Berlin*
Florentin Rochet, *UNamur*
Franziska Roesner, *University of Washington*
Eyal Ronen, *Tel Aviv University*
Stefanie Roos, *RPTU Kaiserslautern-Landau*
Christian Rossow, *CISPA Helmholtz Center for Information Security*
Kevin Alejandro Roundy, *Gen Digital*
Scott Ruoti, *University of Tennessee, Knoxville*
Andrei Sabelfeld, *Chalmers University of Technology*
Ahmad-Reza Sadeghi, *Technische Universität Darmstadt*
Merve Sahin, *SAP Security Research*
Kazue Sako, *Waseda University*
Iskander Sanchez-Rola, *Norton Research Group*
Nuno Santos, *INESC-ID and Instituto Superior Técnico, University of Lisbon*
Sebastian Schinzel, *Münster University of Applied Sciences, Fraunhofer SIT, and ATHENE*
Michael Schwarz, *CISPA Helmholtz Center for Information Security*
Wendy Seltzer, *Tucows*
Bingyu Shen, *Meta Platforms, Inc.*
Johanna Sepúlveda, *Airbus Defence and Space*
Chao Shen, *Xi'an Jiaotong University*
Shweta Shinde, *ETH Zurich*
Haya Shulman, *Goethe-Universität Frankfurt, Fraunhofer SIT, and ATHENE*
Manya Sleeper, *Google*
Peter Snyder, *Brave Software*
Sooel Son, *Korea Advanced Institute of Science and Technology (KAIST)*
Dokyung Song, *Yonsei University*
Alessandro Sorniotti, *IBM Research Europe*
Ben Stock, *CISPA Helmholtz Center for Information Security*
Gianluca Stringhini, *Boston University*
Martin Strohmeier, *armasuisse Science and Technology, Cyber-Defence Campus*
Guillermo Suarez-Tangil, *IMDEA Networks Institute*
Wei Sun, *University of California, San Diego*
Qiang Tang, *The University of Sydney*
Juan Tapiador, *UC3M*
Yuan Tian, *University of California, Los Angeles*
Nils Ole Tippenhauer, *CISPA Helmholtz Center for Information Security*
Rahmadi Trimananda, *University of California, Irvine*
Selcuk Uluagac, *Florida International University*
Blase Ur, *University of Chicago*
Anjo Vahldiek-Oberwagner, *Intel Labs*
Michel van Eeten, *Delft University of Technology*
Mayank Varia, *Boston University*
Venkat Venkatakrishnan, *University of Illinois Chicago*
Luca Viganò, *King's College London*
Giovanni Vigna, *University of California, Santa Barbara*
Daniel Votipka, *Tufts University*
David Wagner, *University of California, Berkeley*
Cong Wang, *City University of Hong Kong*
Fish Wang, *Arizona State University*
Gang Wang, *University of Illinois at Urbana–Champaign*
Qian Wang, *Wuhan University*
Shuai Wang, *The Hong Kong University of Science and Technology*
Ting Wang, *The Pennsylvania State University*
Xiao Wang, *Northwestern University*
Zhibo Wang, *Zhejiang University*
Josephine Wolff, *Tufts University*
Christian Wressnegger, *Karlsruhe Institute of Technology (KIT)*
Yang Xiang, *Swinburne University of Technology*
Liang Xiao, *Xiamen University*
Chenren Xu, *Peking University*
Jason (Minhui) Xue, *CSIRO's Data61*
Chen Yan, *Zhejiang University*
Yuval Yarom, *Ruhr University Bochum*
Yu Yu, *Shanghai Jiao Tong University*
Xu Yuan, *University of Louisiana at Lafayette*

Savvas Zannettou, *Delft University of Technology*
Daniel Zappala, *Brigham Young University*
Sarah Zennou, *Airbus*
Fan Zhang, *Yale University*
Fengwei Zhang, *Southern University of Science and Technology (SUSTech)*
Kehuan Zhang, *The Chinese University of Hong Kong*
Mu Zhang, *University Of Utah*
Ning Zhang, *Washington University*
Xiaokuan Zhang, *George Mason University*
Yuan Zhang, *Fudan University*
Yue Zhang, *The Ohio State University*
Haojin Zhu, *Shanghai Jiao Tong University*
Saman Zonouz, *Georgia Tech*
Yixin Zou, *Max Planck Institute for Security and Privacy*
Mary Ellen Zurko, *MIT Lincoln Laboratory*

Steering Committee

Michael Bailey, *Georgia Institute of Technology*
Matt Blaze, *Georgetown University*
Dan Boneh, *Stanford University*
Kevin Butler, *University of Florida*
Srdjan Capkun, *ETH Zurich*
William Enck, *North Carolina State University*
Kevin Fu, *University of Michigan*
Rachel Greenstadt, *New York University*
Casey Henderson, *USENIX Association*
Nadia Heninger, *University of California, San Diego*
Thorsten Holz, *Ruhr-Universität Bochum*
Engin Kirda, *Northeastern University*
Tadayoshi Kohno, *University of Washington*
Thomas Ristenpart, *Cornell Tech*
Franziska Roesner, *University of Washington*
Kurt Thomas, *Google*
Patrick Traynor, *University of Florida*
David Wagner, *University of California, Berkeley*

Symposium Topics

Refereed paper submissions are solicited in all areas relating to systems research in security and privacy. This topic list is not meant to be exhaustive; USENIX Security is interested in all aspects of computing systems security and privacy. Papers without a clear application to security or privacy of computing systems, however, will be considered out of scope and may be rejected without full review.

- System security
  - Operating systems security
  - Web security
  - Mobile 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
- Security analysis
  - Malware analysis
  - Analysis of network and security protocols
  - Attacks with novel insights, techniques, or results
  - Forensics and diagnostics for security
  - Automated security analysis of hardware designs and implementation
  - Automated security analysis of source code and binaries
  - Program analysis
  - Fuzzing and Vulnerability Discovery
  - Formal methods for Security
- Machine learning security and privacy
  - Machine learning applications to security and privacy
  - Machine learning privacy issues and methods
  - Adversarial machine learning
- Data-driven security and measurement studies
  - Measurements of fraud, malware, spam
  - Measurements of human behavior and security
- Privacy
  - Privacy metrics
  - Anonymity
  - Web and mobile privacy
  - Privacy-preserving computation
  - Privacy attacks
- Usable security and privacy
- Language-based security
- Hardware security
  - Secure computer architectures
  - Embedded systems security
  - Cyber-physical systems security
  - Methods for detection of malicious or counterfeit hardware
  - Side channels
- Research on surveillance and censorship
- Social issues and security
  - Research on computer security law and policy
  - Ethics of computer security research
  - Research on security education and training
  - Information manipulation, misinformation, and disinformation
  - Protecting and understanding at-risk users
  - Emerging threats, harassment, extremism, and online abuse
- 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

Starting this year, USENIX Security solicits the submission of Systematization of Knowledge (SoK) papers, which have been very valuable to help our community to clarify and put into context complex research problems.

It is important to stress that SoK papers go beyond simply summarizing previous research (like in a survey) but also include a thorough examination and analysis of existing approaches, identify gaps and limitations, and offer insights or new perspectives on a given, major research area.

While both SoK and survey papers may involve summarizing ex-

isting research, the key difference is that a SoK paper provides a more structured and insightful overview, which might also involve new experiments to replicate and compare previous solutions. Please refer to the IEEE Symposium on Security and Privacy for recent SoK papers at https://oaklandsok.github.io/.

We encourage the authors to distinguish SoK submissions by adding the "SoK:" prefix to the title.

Refereed 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 at least one of the authors will attend the conference to present it. Alternative arrangements will be made if global health concerns persist. If the conference 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. In keeping with this and as part of USENIX's open access policy, the Proceedings will be available online for registered attendees before the Symposium and for everyone starting on the opening day of the technical sessions. USENIX also allows authors to retain ownership of the copyright in their works, requesting only that USENIX be granted the right to be the first publisher of that work. See our sample consent form at www.usenix.org/sample_consent_form.pdf for the complete terms of publication.

Go to Paper Submission Policies and Instructions page at www.usenix.org/conference/usenixsecurity24/submission-policies-and-instructions for more information.

Artifact Evaluation

The Call for Artifacts will be available soon.

Symposium Activities

Invited Talks, Panels, and Poster Session

In addition to the refereed papers and the keynote presentation, the technical program will include invited talks, panel discussions, and a poster session. You are invited to make suggestions regarding topics or speakers in any of these sessions via email to the contacts listed below or to the program co-chairs at sec24chairs@usenix.org.

Invited Talks and Panel Discussions

Invited talks and panel discussions will be held in parallel with the refereed paper sessions. Please submit topic suggestions and talk and panel proposals via email to sec24it@usenix.org by Thursday, February 8, 2024.

Poster Session

Would you like to share a provocative opinion, an interesting preliminary work, or a cool idea that will spark discussion at this year's USENIX Security Symposium? The poster session is the perfect venue to introduce such new or ongoing work. Poster presenters will have the entirety of the evening reception to discuss their work, get exposure, and receive feedback from attendees.

To submit a poster, please submit a draft of your poster, in PDF (maximum size 36" by 48"), or a one-page abstract via the poster session submission form, which will be available here soon, by Tuesday, July 9, 2024. Decisions will be made by Tuesday, July 16, 2024. Posters will not be included in the proceedings but may be made available online if circumstances permit. Poster submissions must include the authors' names, affiliations, and contact information. At least one author of each accepted poster must register for and attend the Symposium to present the poster.

Submission Policies

USENIX Security '24 submissions deadlines are as follows:

- **Summer Deadline:** Tuesday, June 6, 2023, 11:59 pm AoE
- **Fall Deadline:** Tuesday, October 17, 2023, 11:59 pm AoE
- **Winter Deadline:** Thursday, February 8, 2024, 11:59 pm AoE

All papers that are accepted by the end of the winter submission reviewing cycle (February–June 2024) will appear in the proceedings for USENIX Security '24. All submissions will be made online via their respective web forms on the Call for Papers webpage. We do not accept email submissions.

Submissions should be finished, complete papers. We may decide to desk-reject papers that have severe editorial problems (broken references, egregious spelling or grammar errors, missing figures, etc.), are submitted in violation of the Submission Instructions outlined below, are outside of the scope of the symposium, or are deemed clearly of insufficient quality to appear in the program.

All initial paper submissions should be at most 13 typeset pages, excluding bibliography and well-marked appendices. To accommodate changes, the revisions for "Accept Conditional on Major Revision" decisions can have up to 14 typeset pages, excluding bibliography and well-marked appendices. These appendices may be included to assist reviewers who may have questions that fall outside the stated contribution of the paper on which your work is to be evaluated, or to provide details that would only be of interest to a small minority of readers. There is no limit on the length of the bibliography and appendices but reviewers are not required to read any appendices. The paper should be self-contained without appendices.

Once accepted, the camera-ready version should be no longer than 18 pages, including the bibliography and any appendices.

Reasons for Desk Rejection

Papers should be typeset 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. Authors must use the USENIX's LaTeX template and style files when preparing the paper for submission. Failure to adhere to the page limit and formatting requirements can be grounds for rejection.

Papers should not attempt to "squeeze space" by exploiting underspecified formatting criteria (e.g., columns) or through manipulating other document properties (e.g., page layout, spacing, fonts, figures and tables, headings). Papers that, in the chair's assessment, make use of these techniques to receive an unfair advantage, will be rejected, even if they comply with the above specifications. We offer several examples (https://www.usenix.org/sites/default/files/disallowed-squeezing-examples.pdf) of observed techniques that have or could lead to rejection. Authors should seek to meet page limits through the modification of content alone. Any other techniques (whether appearing in these examples or not) may result in rejection.

Please make sure your paper successfully returns from the PDF checker (visible upon PDF submission) and that document properties, such as font size and margins, can be verified via PDF editing tools such as Adobe Acrobat. Papers where the chairs can not verify compliance with the CFP will be rejected.

During the paper submission, the authors need to select among the available topics the ones that are more appropriate for their work. A failure to select topics or a clear attempt at selecting inappropriate or misleading entries may be grounds

for administrative rejection.

If the paper contains experiments conducted against live systems, the authors need to include a clearly identified subsection (or appendix) to explain the IRB process (or equivalent if the institution does not have one) and all alternatives that the authors considered and the reason they were discarded.

Simply citing previous work that relied on live systems attacks is not a sufficient reason to decide that such attacks are justified and ethical. Thus, every paper that relies on techniques that can be considered unethical needs to discuss the need to resort to those techniques independently of previous work. Failing to comply is grounds for rejection. If authors are unsure whether their work falls in this category, they should contact the chairs before the submission.

Prepublication of Papers

Prepublication versions of papers accepted for USENIX Security '24 will be published and open and accessible to everyone without restrictions on the following dates:

- Summer Deadline: Tuesday, November 14, 2023
- Fall Deadline: Tuesday, April 9, 2024
- Winter Deadline: TBD (final papers will be published with the full conference proceedings)

Embargo Requests

Authors may request an embargo for their papers by the deadline dates listed below. All embargoed papers will be released on the first day of the conference, Wednesday, August 9, 2023.

- Summer Deadline: Tuesday, November 1, 2022
- Fall Deadline: Tuesday, March 28, 2023
- Winter Deadline: Tuesday, July 11, 2023

Embargo Requests

Authors may request an embargo for their papers by the deadline dates listed below. All embargoed papers will be released on the first day of the conference, Wednesday, August 9, 2023.

- Summer Deadline: Tuesday, November 7, 2023
- Fall Deadline: Tuesday, April 2, 2024
- Winter Deadline: Thursday, July 11, 2024

Conflicts of Interest

The program co-chairs require cooperation from both authors and program committee members to prevent submissions from being evaluated by reviewers who have a conflict of interest. During the submission process, we will ask authors to identify members of the program committee with whom they share a conflict of interest. This includes: (1) anyone who shares an institutional affiliation with an author at the time of submission (including secondary affiliations and consulting work), (2) anyone who was the advisor or advisee of an author at any time in the past, (3) anyone the author has collaborated or published with in the prior two years, (4) anyone who is affiliated with a party that funds your research, or (5) close personal relationships. For other forms of conflict, authors must contact the chairs and explain the perceived conflict. In addition to selecting program committee conflicts when submitting, we recommend that all authors ensure they have up-to-date HotCRP profiles listing all known conflicts.

Program committee members who are conflicts of interest with a paper, including program co-chairs, will be excluded from both online and in-person evaluation and discussion of the paper by default.

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) for examples.

Early Rejection Notification

The review process will consist of several reviewing rounds. In order to allow authors time to improve their work and submit to other venues, authors of submissions for which there is a consensus on rejection will be notified earlier.

Author Responses

Authors of papers that have not been rejected early will have an opportunity to respond to an initial round of reviews. We encourage authors to focus on questions posed by reviewers and significant factual corrections. Once reviews are released to authors for rebuttal, we will not process requests to withdraw the paper and the paper will be viewed as under submission until the end of the cycle.

Anonymous Submission

The review process will be anonymous. Papers must be submitted in a form suitable for anonymous review:

- The title page should not contain any author names or affiliations.
- Authors should carefully review figures and appendices (especially survey instruments) to ensure affiliations are not accidentally included.
- When referring to your previous work, do so in the third person, as though it were written by someone else. Anonymous references are only allowed in the (unusual) case that a third-person reference is infeasible, and after approval of the chairs.
- Authors may include links to websites that contain source code, tools, or other supplemental material. Neither the link in the paper nor the website itself should suggest the authors' identities (e.g., the website should not contain the authors' names or affiliations).
- Authors should carefully check any submitted prior reviews for identifying details.

Papers that are not properly anonymized may be rejected without review.

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.

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. This award is meant to recognize the direction of the research and not necessarily its progress to date. 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.

You may submit your USENIX Security '24 paper submission for consideration for the Prize as part of the regular submission process.

Ethical Considerations and Proactive Harm Prevention

We expect authors to carefully consider and address the potential harms associated with carrying out their research, as well as the potential negative consequences that could stem from publishing their work. Failure to do so may result in rejection of a submission regardless of its quality and scientific value.

Although causing harm is sometimes a necessary and legitimate aspect of scientific research in computer security and privacy, authors are expected to document how they have addressed and mitigated the risks. This includes, but is not limited to, considering the impact of your research on deployed systems, understanding the costs your research imposes on others, safely and appropriately collecting data, and following responsible disclosure. In particular, if the submission deals with vulnerabilities (e.g., software vulnerabilities in a given program or design weaknesses in a hardware system), the authors need to discuss in detail the steps they have already taken or plan to take to address these vulnerabilities (e.g., by disclosing vulnerabilities to the vendors).

Papers should include a clear statement about why the benefit of the research outweighs the harms, and how the authors have taken measures and followed best practices to ensure safety and minimize the potential harms caused by their research.

Due to the complexity of today's computing systems, humans can be harmed directly or indirectly in unexpected ways (see The Menlo Report at https://www.dhs.gov/sites/default/files/publications/CSD-MenloPrinciplesCORE-20120803_1.pdf). If the submitted research has potential to cause harm, and authors have access to an Institutional Review Board (IRB), we encourage authors to consult this IRB and document its response and recommendations in the paper. We note, however, that IRBs are not expected to understand computer security research well or to know about best practices and community norms in our field, so IRB approval does not absolve researchers from considering ethical aspects of their work. In particular, IRB approval is not sufficient to guarantee that the PC will not have additional concerns with respect to harms associated with the research.

Contact the program co-chairs at sec24chairs@usenix.org if you have any questions.

Reviews from Prior Submissions

For papers that were previously submitted to, and rejected from, a conference (including USENIX Security), authors are required to submit a separate document containing the prior reviews along with a description of how those reviews were addressed in the current version of the paper. Authors are only required to include reviews from the last time the paper was submitted, but may add more if they consider it relevant for the reviewers. This includes withdrawn papers if reviews were received. Reviewers will submit their initial reviews prior to becoming aware of previous reviews and summaries of changes to avoid being biased in formulating their own opinions; once their initial reviews are submitted, however, reviewers will be given the opportunity to update their thoughts based on the submission history of the paper. Authors who try to circumvent this rule (e.g., by changing the title of the paper without significantly changing the content) may have their papers rejected without further consideration, at the discretion of the PC chairs.

Submission Instructions

All submissions will be made online via their respective web forms. Do not email submissions. Submissions must be in PDF format. LaTeX users can use the "pdflatex" command to convert a LaTeX document into PDF format. Please make sure your submission can be opened using Adobe Reader. Please also make sure your submission, and all embedded figures, are intelligible when printed in grayscale.

For revisions of submissions receiving "Accept Conditional on Major Revision" decisions during one of the USENIX Security '24 submission periods, authors who revise their papers must submit a separate PDF that includes the verbatim revision criteria, a list of changes to the paper, and a statement of how the changes address the criteria. The authors must also submit as part of the PDF a "PDF 'diff'" to assist the shepherd in identifying your modifications. Ideally this would be a latexdiff-like document. However, if papers have gone through major changes that would make the diff unreadable, authors are free to provide another format that helps the shepherd to identify changes efficiently.

For resubmissions of "Major Revisions" from USENIX Security '23, please look at USENIX Security '23 Submission Policies (https://www.usenix.org/conference/usenixsecurity23/submission-policies-and-instructions) and Instructions for requirements.

For papers that were previously submitted to, and rejected from, another conference, the required document (see Reviews from Prior Submissions above) should be submitted as a PDF file using the "Prior Reviews" field in the submission forms, not via an appendix.

All submissions will be judged on originality, relevance, correctness, and clarity. In addition to citing relevant published work, authors should relate their submission to any other relevant submissions of theirs in other venues that are under review at the same time as their submission to the Symposium. These citations to simultaneously submitted papers should be anonymized; non-anonymous versions of these citations must, however, be emailed to the program co-chairs at sec24chairs@usenix.org.

Simultaneous submission of the same work to multiple venues, submission of previously published work, or plagiarism constitutes dishonesty or fraud. Failure to point out and explain overlap will be grounds for rejection. USENIX, like 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 for details.

Note that under the changes to the USENIX Security publication model, papers that have received a decision of "Accept Conditional on Major Revision" from USENIX Security are still considered to be under review until accepted or rejected by the reviewers; authors must formally withdraw their paper if they wish to submit to another venue. See USENIX Security Publication Model Changes (https://www.usenix.org/conference/usenixsecurity24/publication-model-changes) for details. For submissions that received Reject decisions from USENIX Security '23, resubmissions must follow the rules laid out for when they can be resubmitted.

Questions? Contact your program co-chairs, sec24chairs@usenix.org, or the USENIX office, submissionspolicy@usenix.org.

The program committee and external reviewers are required to treat all submissions as confidential. 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.

Papers that do not comply with the submission requirements, including length and anonymity, that do not comply with resubmission policies, or that do not have a clear application to security or privacy may be rejected without review. Papers accompanied by nondisclosure agreement forms will not be considered.

All papers will be available online before the symposium. If your accepted paper should not be published prior to the event, please notify production@usenix.org after you submit your final paper. See the Embargo Requests section above for deadlines.

Specific questions about submissions may be sent to the program co-chairs at sec24chairs@usenix.org. The chairs will respond to individual questions about the submission process if contacted at least a week before the submission deadline.