32nd USENIX Security Symposium

August 9–11, 2023, Anaheim, CA, 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 32nd USENIX Security Symposium will be held August 9–11, 2023, in Anaheim, CA.

Important: *In 2023, we are introducing 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/usenixsecurity23/publication-model-changes).*

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 7, 2022, 11:59 pm AoE
- Early reject notification: July 14, 2022
- Rebuttal Period: August 22–24, 2022
- Notification to authors: September 2, 2022
- Final paper files due: October 4, 2022

Fall Deadline

- Refereed paper submissions due: Tuesday, October 11, 2022, 11:59 pm AoE
- Early reject notification: November 18, 2022
- Rebuttal Period: January 17–19, 2023
- Notification to authors: January 27, 2023
- Final paper files due: February 28, 2023

Winter Deadline

- Refereed paper submissions due: Tuesday, February 7, 2023, 11:59 pm AoE
- Early reject notification: March 17, 2023
- Rebuttal Period: April 24–26, 2023
- Notification to authors: May 8, 2023
- Final paper files due: June 13, 2023

- Invited talk and panel proposals due: Tuesday, January 31, 2023
- Poster proposals due: Thursday, July 6, 2023
  - Notification to poster presenters: Thursday, July 13, 2023

Conference Organizers

Program Co-Chairs

Joe Calandrino, *Federal Trade Commission*
Carmela Troncoso, *EPFL*

Program Co-Chairs

Adam J. Aviv, *The George Washington University*
David Barrera, *Carleton University*
Nataliia Bielova, *CNIL/Inria*
Christina Garman, *Purdue University*
Giancarlo Pellegrino, *CISPA Helmholtz Center for Information Security*

Program Committee

Yousra Aafer, *University of Waterloo*
Karim M. Abdellatif, *Ledger, France*
Aysajan Abidin, *imec-COSIC KU Leuven*
Kendra Albert, *Harvard Law School*
Martin Albrecht, *Royal Holloway, University of London*
Mário S. Alvim, *UFMG*
Abdelrahaman Aly, *CRC, TII and imec-COSIC, KU Leuven*
Ross Anderson, *Cambridge University and Edinburgh University*
Daniele Antonioli, *EURECOM*
Giovanni Apruzzese, *University of Liechtenstein*
Frederico Araujo, *IBM Research*
Giuseppe Ateniese, *George Mason University*
Adam J. Aviv, *The George Washington University*
Erman Ayday, *Case Western Reserve University*
Davide Balzarotti, *Eurecom*
Sébastien Bardin, *CEA LIST, Université Paris Saclay*
David Barrera, *Carleton University*
Adam Bates, *University of Illinois at Urbana–Champaign*

Lujo Bauer, *Carnegie Mellon University*
Matthew Bernhard, *VotingWorks*
Nataliia Bielova, *CNIL/Inria*
Battista Biggio, *University of Cagliari, Italy*
Leyla Bilge, *Norton Research Group*
Marina Blanton, *University at Buffalo*
Joseph Bonneau, *New York University*
Marcus Felipe Botacin, *Federal University of Paraná*
Ioana Boureanu, *Surrey Centre for Cybersecurity, University of Surrey*
Cristian Antonio Bravo-Lillo, *Fintual*
Sven Bugiel, *CISPA Helmholtz Center for Information Security*
Nathan Burow, *MIT Lincoln Laboratory*
Juan Caballero, *IMDEA Software Institute*
Stefano Calzavara, *Università Ca' Foscari Venezia*
Yinzhi Cao, *Johns Hopkins University*
Srdjan Čapkun, *ETH Zurich*
Nicholas Carlini, *Google*
Álvaro A. Cárdenas, *University of California, Santa Cruz*
Lorenzo Cavallaro, *University College London*
Berkay Celik, *Purdue University*
Sang Kil Cha, *Korea Advanced Institute of Science and Technology (KAIST)*
Varun Chandrasekaran, *University of Wisconsin—Madison*
Rahul Chatterjee, *University of Wisconsin—Madison*
Sze Yiu Chau, *The Chinese University of Hong Kong*
Yizheng Chen, *University of California, Berkeley*
Qi Alfred Chen, *University of California, Irvine*
Guoxing Chen, *Shanghai Jiao Tong University*
Giovanni Cherubin, *Microsoft Research*
Amrita Roy Chowdhury, *University of California, San Diego*
Nicolas Christin, *Carnegie Mellon University*
Mihai Christodorescu, *Google*
Camille Cobb, *University of Illinois at Urbana–Champaign*
Shaanan Cohney, *University of Melbourne*
Andrea Continella, *University of Twente*
Daniele Cono D'Elia, *Sapienza University of Rome*
Pubali Datta, *University of Illinois Urbana-Champaign*
Nathan Dautenhahn, *Rice University*
Ambra Demontis, *University of Cagliari*
Ghada Dessouky, *Technische Universität Darmstadt*
Alexandra Dmitrienko, *University of Würzburg*
Orr Dunkelman, *University of Haifa, Israel*
Zakir Durumeric, *Stanford University*
Adam Dziedzic, *University of Toronto, Vector Institute*
Laura Edelson, *New York University*
Manuel Egele, *Boston University*
Mohamed Elsabagh, *Kryptowire*
Pardis Emami-Naeini, *University of Washington*
William Enck, *North Carolina State University*
Birhanu Eshete, *University of Michigan, Dearborn*
Habiba Farrukh, *Purdue University*
Giulia Fanti, *Carnegie Mellon University*
Kassem Fawaz, *University of Wisconsin—Madison*
Earlence Fernandes, *University of Wisconsin—Madison*
Domenic Forte, *University of Florida*
Imane Fouad, *Inria/Univ de Lille*
Yanick Fratantonio, *Google*
Alisa Frik, *International Computer Science Institute*
Aymeric Fromherz, *Inria*
Kelsey Fulton, *University of Maryland*
Carlos Gañán, *ICANN*
Simson L. Garfinkel, *NIST/George Washington University*
Christina Garman, *Purdue University*
Carrie Gates, *Bank of America*
Gennie Gebhart, *Electronic Frontier Foundation*
Yossi Gilad, *The Hebrew University of Jerusalem*
Oana Goga, *CNRS*
André Grégio, *Federal University of Paraná, Brazil (UFPR)*
Kathrin Grosse
Marco Guarnieri, *IMDEA Software Institute*
Julie Haney, *National Institute of Standards and Technology*
Shuang Hao, *University of Texas at Dallas*
Hamza Harkous, *Google*
Behnaz Hassanshahi, *Oracle Labs Australia*
Julia Hesse, *IBM Zurich*
Grant Ho, *University of California, San Diego*
Thorsten Holz, *CISPA Helmholtz Center for Information Security*
Sanghyun Hong, *Oregon State University*
Yuan Hong, *Illinois Institute of Technology*
Nicholas Hopper, *University of Minnesota*
Danny Yuxing Huang, *New York University*
Zhen Huang, *DePaul University*
Jun Ho Huh, *Samsung Research*
Alice Hutchings, *University of Cambridge*
Umar Iqbal, *University of Washington*
Cynthia Irvine, *Naval Postgraduate School*
Rikke Bjerg Jensen, *Royal Holloway, University of London*
Dennis Jackson, *Mozilla*
Rob Jansen, *U.S. Naval Research Laboratory*
Bargav Jayaraman, *University of Virginia*
Yuseok Jeon, *Ulsan National Institute of Science and Technology (UNIST)*
Aaron Johnson, *U.S. Naval Research Laboratory*
Dali Kaafar, *Macquarie University*
Gautam Kamath, *University of Waterloo*
Gabriel Kaptchuk, *Boston University*
Marcel Keller, *CSIRO's Data61*
Vasileios Kemerlis, *Brown University*
Florian Kerschbaum, *University of Waterloo*
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)*
Sam King, *University of California, Davis and Stripe*
Lea Kissner, *Twitter*
Katharina Kohls, *Radboud University*
Tadayoshi Kohno, *University of Washington*
Boris *Köpf, Microsoft Research*
Kari Kostiainen, *ETH Zurich*
Platon Kotzias, *Norton Research Group*
Steve Kremer, *Inria Nancy*
Srikanth Krishnamurthy, *University of California, Riverside*
Joshua A. Kroll, *Naval Postgraduate School*
Katharina Krombholz, *CISPA Helmholtz Center for Information Security*
Pierre Laperdrix, *CNRS*
Kevin Leach, *Vanderbilt University*
Tancrède Lepoint, *Amazon Web Services*
Bo Li, *University of Illinois Urbana-Champaign*
Qi Li, *Tsinghua University*

Ming Li, *University of Arizona*
David Lie, *University of Toronto*
Janne Lindqvist, *Aalto University*
Wouter Lueks, *EPFL*
Lannan Lisa Luo, *University of South Carolina*
Xiapu Luo, *The Hong Kong Polytechnic University*
Matteo Maffei, *TU Wien*
Nathan Malkin, *University of Maryland*
Stefan Mangard, *Graz University of Technology*
Michail Maniatakos, *New York University Abu Dhabi*
Athina Markopoulou, *University of California, Irvine*
Abigail Marsh, *Macalester College*
Ramya Jayaram Masti, *Qualcomm*
Arunesh Mathur, *Competition and Markets Authority*
Jonathan Mayer, *Princeton University*
René Mayrhofer, *Johannes Kepler University Linz*
Jon McCune, *Google*
Patrick McDaniel, *The Pennsylvania State University*
Allison McDonald, *Boston University*
Susan McGregor, *Columbia University, Data Science Institute*
Catherine Meadows, *Naval Research Laboratory*
Shagufta Mehnaz, *Dartmouth College*
Aastha Mehta, *University of British Columbia, Vancouver*
Sarah Meiklejohn, *Google and University College London*
Nele Mentens, *Leiden University and KU Leuven*
Ariana Mirian, *University of California, San Diego*
Jelena Mirkovic, *USC Information Sciences Institute*
Omid Mirzaei, *Elastic*
Esfandiar Mohammadi, *University of Luebeck*
Mainack Mondal, *Indian Institute of Technology, Kharagpur*
Veelasha Moonsamy, *Ruhr University Bochum*
Pedro Moreno-Sanchez, *IMDEA Software Institute*
Marius Muench, *Vrije Universiteit Amsterdam*
Imani Munyaka, *University of California, San Diego*
Toby Murray, *University of Melbourne*
Adwait Nadkarni, *William & Mary*
Moses Namara, *Clemson University*
Shravan Ravi Narayan, *University of California, San Diego*
Shirin Nilizadeh, *University of Texas at Arlington*
Adam Oest, *PayPal, Inc.*
Jeremiah Onaolapo, *University of Vermont*
Cristina Onete, *University of Limoges/XLIM/CNRS 7252*
Yossi Oren, *Ben-Gurion University of the Negev*
Rebekah Overdorf, *EPFL*
Simon Oya, *University of Waterloo*
Miroslav Pajic, *Duke University*
Dimitrios Papadopoulos, *The Hong Kong University of Science and Technology*
Dario Pasquini, *EPFL*
Andrew Paverd, *Microsoft*
Giancarlo Pellegrino, *CISPA Helmholtz Center for Information Security*
Roberto Perdisci, *University of Georgia and Georgia Institute of Technology*
Amreesh Phokeer, *Internet Society*
Fabio Pierazzi, *King's College London*
Niels, Provos, *Stripe*
Apostolos Pyrgelis, *EPFL*
Sazzadur Rahaman, *University of Arizona*
Amir Rahmati, *Stony Brook University*
Sara Rampazzi, *University of Florida*
Aanjhan Ranganathan, *Northeastern University*
Mariana Raykova, *Google*
Joel Reardon, *University of Calgary*
Bradley Reaves, *North Carolina State University*
Raphael Reischuk, *Zuehlke and digitalswitzerland*
Oscar Reparaz, *CashApp (at Square)*
Irwin Reyes, *Two Six Technologies*
Konrad Rieck, *TU Braunschweig*
Luc Rocher, *University of Oxford*
Florentin Rochet, *University of Namur*
Franziska Roesner, *University of Washington*
Eyal Ronen, *Tel Aviv University*
Stefanie Roos, *TU Delft*
Christian Rossow, *CISPA Helmholtz Center for Information Security*
Kevin Alejandro Roundy, *Norton Research Group*
Scott Ruoti, *The University of Tennessee*
Sherman S. M. Chow, *The Chinese University of Hong Kong*
Andrei Sabelfeld, *Chalmers University of Technology*
Ahmad-Reza Sadeghi, *Technical University of Darmstadt*
Merve Sahin, *SAP Security Research*
Kazue Sako, *Waseda University*
Iskander Sanchez-Rola, *Norton Research Group*
Nuno Santos, *INESC-ID / Instituto Superior Técnico, University of Lisbon*
Igor Santos-Grueiro, *Mondragon Unibertsitatea*
Sarah Scheffler, *Princeton University*
Sebastian Schinzel, *Münster University of Applied Sciences*
Thomas Schneider, *TU Darmstadt*
Lea Schönherr, *CISPA Helmholtz Center for Information Security*
Michael Schwarz, *CISPA Helmholtz Center for Information Security*
Wendy Seltzer, *W3C/MIT*
Johanna Sepúlveda, *Airbus Defence and Space*
Hovav Shacham, *The University of Texas at Austin*
Mahmood Sharif, *Tel Aviv University*
Shweta Shinde, *ETH Zurich*
Anastasia Shuba, *DuckDuckGo*
Haya Shulman, *ATHENE & Goethe-Universität Frankfurt and Fraunhofer SIT*
Ilia Shumailov, *University of Cambridge & Vector Institute*
Manya Sleeper, *Google*
Peter Snyder, *Brave Software*
Sooel Son, *Korea Advanced Institute of Science and Technology (KAIST)*
Alessandro Sorniotti, *IBM Research Europe*
Michael Specter, *Google*
Emily Stark, *Google*
Deian Stefan, *University of California, San Diego*
Elizabeth Stobert, *Carleton University*
Ben Stock, *CISPA Helmholtz Center for Information Security*
Gianluca, Stringhini, Boston University
Martin Strohmeier, *Cyber-Defence Campus, armasuisse Science + Technology*
Guillermo Suarez-Tangil, *IMDEA Networks Institute*
Juan Tapiador, *UC3M*
Vanessa Teague, *Australian National University and Thinking Cybersecurity Pty Ltd*
Stefano Tessaro, *University of Washington*
Yuan Tian, *University of Virginia*
Nils Ole Tippenhauer, *CISPA Helmholtz Center for Information Security*
Santiago Torres-Arias, *Purdue University*

Vincent Toubiana, *CNIL*
Benjamin E. Ujcich, *Georgetown University*
Blase Ur, *University of Chicago*
Anjo Vahldiek-Oberwagner, *Intel Labs*
Narseo Vallina-Rodriguez, *IMDEA Networks/AppCensus*
Thyla van der Merwe, *Google*
Michel van Eeten, *Delft University of Technology*
Mayank Varia, *Boston University*
Nikos Vasilakis, *Brown University and Massachusetts Institute of Technology*
Ingrid Verbauwhede, *KU Leuven COSIC*
Luca Viganò, *King's College London, UK*
Hayawardh Vijayakumar, *Samsung Research America*
Daniel Votipka, *Tufts University*
Satyanarayana Vusirikala, *Dfinity Foundation*
David Wagner, *University of California, Berkeley*
Gang Wang, *University of Illinois at Urbana–Champaign*
Liang Wang, *Princeton University*
Shuai Wang, *Hong Kong University of Science and Technology*
Xiao Wang, *Northwestern University*
Rick Wash, *Michigan State University*
Christian Weinert, *Royal Holloway, University of London*
Tara Whalen, *Cloudflare*
Philipp Winter, *Brave Software*
Josephine Wolff, *Tufts University*
Christian Wressnegger, *Karlsruhe Institute of Technology (KIT), KASTEL Security Research Labs*
Matthew Wright, *Rochester Institute of Technology*
Jason (Minhui) Xue, *CSIRO's Data61*
Jie Yang, *Florida State University*
Yuval Yarom, *The University of Adelaide*
Savvas Zannettou, *TU Delft*
Daniel Zappala, *Brigham Young University*
Fengwei Zhang, *Southern University of Science and Technology (SUSTech)*
Yuan Zhang, *Fudan University*
Yupeng Zhang, *Texas A&M University*
Haojin Zhu, *Shanghai Jiao Tong University*
Yixin Zou, *University of Michigan*
Mary Ellen Zurko, *MIT Lincoln Laboratory*

Steering Committee

Michael Bailey, *University of Illinois at Urbana–Champaign*
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
- 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
  - 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

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/usenixsecurity23/submission-policies-and-instructions for more information.

Artifact Evaluation

View the Call for Artifacts at www.usenix.org/conference/usenixsecurity23/call-for-artifacts.

Symposium Activities

Invited Talks, Panels, Poster Session, Lightning Talks, and BoFs

In addition to the refereed papers and the keynote presentation, the technical program will include invited talks, panel discussions, a poster session, lightning talks, and Birds-of-a-Feather sessions (BoFs). 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 sec23chairs@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 sec23it@usenix.org by January 31, 2023.

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 July 6, 2023. Decisions will be made by July 13, 2023. 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.

Lightning Talks

Information about lightning talks will be available soon.

Birds-of-a-Feather Sessions (BoFs)

Birds-of-a-Feather sessions (BoFs) will be held Tuesday, Wednesday, and Thursday evenings. Birds-of-a-Feather sessions are informal gatherings of persons interested in a particular topic. BoFs often feature a presentation or a demonstration followed by discussion, announcements, and the sharing of strategies. BoFs can be scheduled on-site or in advance. To schedule a BoF, please send an email to the USENIX Conference Department at bofs@usenix.org with the title and a brief description of the BoF; the name, title, affiliation, and email address of the facilitator; and your preference of date and time.

Submission Policies

Important: *The USENIX Security Symposium moved to multiple submission deadlines in 2019 and included changes to the review process and submission policies. Detailed information is available at USENIX Security Publication Model Changes at www.usenix.org/conference/usenixsecurity23/publication-model-change.*

USENIX Security '23 submissions deadlines are as follows:

- **Summer Deadline:** Tuesday, June 7, 2022, 11:59 pm AoE
- **Fall Deadline:** Tuesday, October 11, 2022, 11:59 pm AoE
- **Winter Deadline:** Tuesday, February 7, 2023, 11:59 pm AoE

All papers that are accepted by the end of the winter submission reviewing cycle (February–June 2023) will appear in the proceedings for USENIX Security '23. All submissions will be made online via their respective web forms: Summer Deadline, Fall Deadline, Winter Deadline. We do not accept email submissions.

Submissions should be finished, complete papers. We may reject papers without review 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 paper submissions, including revisions for "Accept Conditional on Major Revision" decisions, should be at most 13 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, papers must be reformatted to fit in 18 pages, including the bibliography and any appendices.

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 are encouraged to make use of USENIX's LaTeX template and style files available at www.usenix.org/paper-templates when preparing your 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.

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.

Prepublication of Papers

Prepublication versions of papers accepted for USENIX Security '23 will be published and open and accessible to everyone without restrictions on the following dates:

- **Summer Deadline:** Tuesday, November 8, 2022
- **Fall Deadline:** Tuesday, April 4, 2023
- **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

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 '23 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 sec23chairs@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 complete their reviews prior to becoming aware of previous reviews and summaries of changes to avoid being biased in formulating their own opinions; once their reviews are complete, however, reviewers will be given the opportunity to provide additional comments 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 '23 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 '22, please look at USENIX Security '22 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 sec23chairs@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/usenixsecurity23/publication-model-changes) for details. For submissions that received Reject decisions from USENIX Security '22, resubmissions must follow the rules laid out for when they can be resubmitted.

Questions? Contact your program co-chairs, sec23chairs@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 sec23chairs@usenix.org. The chairs will respond to individual questions about the submission process if contacted at least a week before the submission deadline.