31st USENIX Security Symposium

August 10–12, 2022, Boston, MA, 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 31st USENIX Security Symposium will be held August 10–12, 2022, in Boston, MA.

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.*

All researchers are encouraged to submit papers covering novel and scientifically significant practical works in computer security. The Symposium will span three days with a technical program including refereed papers, invited talks, posters, panel discussions, and Birds-of-a-Feather sessions. Co-located events will precede the Symposium on August 8 and 9.

Important Dates

Summer Deadline

- Refereed paper submissions due: **Tuesday, June 8, 2021, 11:59 pm AoE**
- Early reject notification: **July 15, 2021**
- Rebuttal Period: **August 23–25, 2021**
- Notification to authors: **September 3, 2021**
- Final paper files due: **October 5, 2021**

Fall Deadline

- Refereed paper submissions due: **Tuesday, October 12, 2021, 11:59 pm AoE**
- Early reject notification: **November 20, 2021**
- Rebuttal Period: **January 10–12, 2022**
- Notification to authors: **January 20, 2022**
- Final paper files due: **February 22, 2022**

Winter Deadline

- Refereed paper submissions due: **Tuesday, February 1, 2022, 11:59 pm AoE**
- Early reject notification: **March 11, 2022**
- Rebuttal Period: **April 18–20, 2022**
- Notification to authors: **May 2, 2022**
- Final paper files due: **June 14, 2022**

- Invited talk and panel proposals due: **Tuesday, February 1, 2022**
- Poster proposals due: **Wednesday, July 6, 2022**
  - Notification to poster presenters: **Wednesday, July 13, 2022**

Conference Organizers

Program Co-Chairs

Kevin Butler, *University of Florida*
Kurt Thomas, *Google*

Program Committee

Yousra Aafer, *University of Waterloo*
Ruba Abu-Salma, *King's College London*
Gunes Acar, *Katholieke Universiteit Leuven*
Sadia Afroz, *International Computer Science Institute (ICSI), Avast*
Devdatta Akhawe, *Dropbox*
Daniel Alexander Zappala, *Brigham Young University*
Ardalan Amiri Sani, *University of California, Irvine*
Olabode Anise, *Google*
Daniele Antonioli, *EPFL, EURECOM*
Maria Apostolaki, *ETH Zurich*
Elias Athanasopoulos, *University of Cyprus*
Davide Balzarotti, *EURECOM*
Tiffany Bao, *Arizona State University*
David Barrera, *Carleton Univeristy*
Adam Bates, *University of Illinois at Urbana–Champaign*
Lejla Batina, *Radboud University*
Lujo Bauer, *Carnegie Mellon University*

Jethro Beekman, *Fortanix*
Antonio Bianchi, *Purdue University*
Battista Biggio, *University of Cagliari*
Leyla Bilge, *NortonLifeLock Research Group*
Vincent Bindschaedler, *University of Florida*
Priyam Biswas, *Intel*
Marina Blanton, *University at Buffalo*
Erik-Oliver Blass, *Airbus*
Tamara Bonaci, *Northeastern University*
Joseph Bonneau, *New York University*
Glencora Borradaile, *Oregon State University*
Marcus Botacin, *Federal University of Paraná*
Ioana Boureanu, *University of Surrey*
Nathan Burow, *MIT Lincoln Laboratory*
Joseph Calandrino, *Federal Trade Commission*
Stefano Calzavara, *Università Ca' Foscari Venezia*
Yinzhi Cao, *Johns Hopkins University*
Srdjan Capkun, *ETH Zurich*
Alvaro 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)*
Neha Chachra, *Facebook*
Rahul Chatterjee, *University of Wisconsin—Madison*
Sze Yiu Chau, *The Chinese University of Hong Kong*
Kai Chen, *Institute of Information Engineering, Chinese Academy of Sciences*
Qi Alfred Chen, *University of California, Irvine*
Yizheng Chen, *Columbia University*
Sherman S. M. Chow, *The Chinese University of Hong Kong*
Amrita Roy Chowdhury, *University of Wisconsin—Madison*
Nicolas Christin, *Carnegie Mellon University*
Chitchanok Chuengsatiansup, *The University of Adelaide*
Camille Cobb, *Carnegie Mellon University*
Shaanan Cohney, *Princeton University and University of Melbourne*
Andrea Continella, *University of Twente*
Cas Cremers, *CISPA Helmholtz Center for Information Security*
Bruno Crispo, *University of Trento*
Weidong Cui, *Microsoft Research*
Anupam Das, *North Carolina State University*
Pubali Datta, *University of Illinois at Urbana–Champaign*
Nathan Dautenhahn, *Rice University*
Alexandra Dmitrienko, *University of Wuerzburg*
Adam Doupe, *Arizona State University*
Tudor Dumitras, *University of Maryland*
Zakir Durumeric, *Stanford University*
Manuel Egele, *Boston University*
Thomas Eisenbarth, *University of Lübeck*
Mary Ellen Zurko, *MIT Lincoln Laboratory*
Mohamed Elsabagh, *Kryptowire*
Pardis Emami-Naeini, *University of Washington*
William Enck, *North Carolina State University*
Roya Ensafi, *University of Michigan*
Birhanu Eshete, *University of Michigan*
Saba Eskandarian, *The University of North Carolina at Chapel Hill*
Sascha Fahl, *CISPA Helmholtz Center for Information Security*
Kassem Fawaz, *University of Wisconsin—Madison*
Yunsi Fei, *Northeastern University*
Earlence Fernandes, *University of Wisconsin—Madison*
Domenic Forte, *University of Florida*
Aurélien Francillon, *EURECOM*
Michael Franz, *University of California, Irvine*
Yanick Fratantonio, *Cisco Talos*
David Freeman, *Facebook*
Aymeric Fromherz, *Inria*
Patrick Gage Kelley, *Google*
Eva Galperin, *Electronic Frontier Foundation*
Vinod Ganapathy, *Indian Institute of Science (IISc)*
Christina Garman, *Purdue University*
Carrie Gates, *Bank of America*
Genevieve Gebhart, *University of Washington Information School*
Daniel Genkin, *University of Michigan*
Ryan Gerdes, *Virginia Tech*
Arthur Gervais, *Imperial College London*
Irene Giacomelli, *Protocol Labs*
Yossi Gilad, *The Hebrew University of Jerusalem*
Neil Gong, *Duke University*
Tyrone Grandison, *The Data-Driven Institute*
Daniel Gruss, *Graz University of Technology*
Guofei Gu, *Texas A&M University*
Le Guan, *University of Georgia*
Shuang Hao, *The University of Texas at Dallas*
Wajih Ul Hassan, *University of Illinois at Urbana–Champaign*
Christophe Hauser, *USC/Information Sciences Institute*
Xiali Hei, *University of Louisiana at Lafayette*
Grant Hernandez, *Qualcomm*
Matthew Hicks, *Virginia Tech*
Ralph Holz, *University of Twente*
Thorsten Holz, *Ruhr University Bochum*
Nick Hopper, *University of Minnesota*
Diane Hosfelt, *Apple*
Syed Rafiul Hussain, *The Pennsylvania State University*
Luca Invernizzi, *Google*
Sotiris Ioannidis, *Technical University of Crete*
Cynthia Irvine, *Naval Postgraduate School*
Suman Jana, *Columbia University*
Ramya Jayaram Masti, *Intel*
Yuseok Jeon, *UNIST (Ulsan National Institute of Science and Technology)*
Yier Jin, *University of Florida*
Brent Byunghoon Kang, *Korea Advanced Institute of Science and Technology (KAIST)*
Chris Kanich, *University of Illinois at Chicago*
Apu Kapadia, *Indiana University Bloomington*
Alexandros Kapravelos, *North Carolina State University*
Vasileios Kemerlis, *Brown University*
Florian Kerschbaum, *University of Waterloo*
Taesoo Kim, *Georgia Institute of Technology*
Yongdae Kim, *Korea Advanced Institute of Science and Technology (KAIST)*
Sam King, *University of California, Davis and Bouncer Technologies*
Michel Kinsy, *TAMU*
Engin Kirda, *Northeastern University*
Katharina Kohls, *Radboud University*
Tadayoshi Kohno, *University of Washington*
Kari Kostiainen, *ETH Zurich*
Srikanth Krishnamurthy, *University of California, Riverside*
Joshua A Kroll, *Naval Postgraduate School*

Katharina Krombholz, *CISPA Helmholtz Center for Information Security*
Christopher Kruegel, *University of California, Santa Barbara*
Deepak Kumar, *Stanford University*
Anil Kurmus, *IBM Research Europe*
Andrea Lanzi, *University of Milan*
Pavel Laskov, *University of Liechtenstein*
Byoungyoung Lee, *Seoul National University*
Kyu Hyung Lee, *University of Georgia*
Sangho Lee, *Microsoft Research*
Wenke Lee, *Georgia Institute of Technology*
Tancrède Lepoint, *Google*
Ada Lerner, *Wellesley College*
Frank Li, *Georgia Institute of Technology*
Qi Li, *Tsinghua University*
Tianshi Li, *Carnegie Mellon University*
David Lie, *University of Toronto*
Zhiqiang Lin, *Ohio State University*
Martina Lindorfer, *TU Wien*
Guyue Liu, *Carnegie Mellon University*
Kangjie Lu, *University of Minnesota*
Wouter Lueks, *EPFL*
Xiapu Luo, *The Hong Kong Polytechnic University*
Matteo Maffei, *TU Wien*
Stefan Mangard, *Graz University of Technology*
Mohammad Mannan, *Concordia University*
Ivan Martinovic, *Oxford University*
Michelle Mazurek, *University of Maryland*
Patrick McDaniel, *The Pennsylvania State University*
Shagufta Mehnaz, *Dartmouth College*
Aastha Mehta, *University of British Columbia, Vancouver*
Sarah Meiklejohn, *University College London and Google*
Marcela Melara, *Intel Labs*
Nele Mentens, *Leiden University and Katholieke Universiteit Leuven*
Jiang Ming, *The University of Texas at Arlington*
Ariana Mirian, *University of California, San Diego*
Jelena Mirkovic, *University of Southern California*
Daniel Moghimi, *University of California, San Diego*
Esfandiar Mohammadi, *University of Lübeck*
Mainack Mondal, *Indian Institute of Technology, Kharagpur*
Soo-Jin Moon, *Google*
Veelasha Moonsamy, *Ruhr University Bochum*
Thomas Moyer, *University of North Carolina*
Marius Muench, *Vrije Universiteit Amsterdam*
Takao Murakami, *AIST*
Toby Murray, *University of Melbourne*
Nick Nikiforakis, *Stony Brook University*
Anita Nikolich, *University of Illinois at Urbana–Champaign*
Shirin Nilizadeh, *The University of Texas at Arlington*
Adam Oest, *PayPal*
Hamed Okhravi, *MIT Lincoln Laboratory*
Melek Önen, *EURECOM*
Cristina Onete, *University of Limoges/XLIM/CNRS 7252*
Yossi Oren, *Ben-Gurion University of the Negev*
Rebekah Overdorf, *EPFL*
Miroslav Pajic, *Duke University*
Dimitrios Papadopoulos, *The Hong Kong University of Science and Technology*
Bryan Parno, *Carnegie Mellon University*
Mathias Payer, *EPFL*
Paul Pearce, *Georgia Institute of Technology, International Computer Science Institute (ICSI)*
Giancarlo Pellegrino, *CISPA Helmholtz Center for Information Security*
Roberto Perdisci, *University of Georgia and Georgia Institute of Technology*
Radia Perlman, *Dell EMC*
Peter Peterson, *University of Minnesota*
Fabio Pierazzi, *King's College London*
Christina Poepper, *New York University Abu Dhabi*
Niels Provos, *Stripe*
Amir Rahmati, *Stony Brook University*
Jeyavijayan Rajendran, *Texas A&M University*
Sara Rampazzi, *University of Florida*
Mariana Raykova, *Google*
Joel Reardon, *University of Calgary*
Bradley Reaves, *North Carolina State University*
Elissa Redmiles, *Max Planck Institute for Software Systems (MPI-SWS)*
Michael K. Reiter, *Duke University*
Konrad Rieck, *Technische Universität Braunschweig*
William Robertson, *Northeastern University*
Franziska Roesner, *University of Washington*
Eyal Ronen, *Tel Aviv University*
Stefanie Roos, *TU Delft*
Ahmad-Reza Sadeghi, *Technische Universität Darmstadt*
Brendan Saltaformaggio, *Georgia Institute of Technology*
Nitesh Saxena, *University of Alabama at Birmingham*
Sebastian Schinzel, *Münster University of Applied Sciences*
Michael Schwarz, *CISPA Helmholtz Center for Information Security*
Jörg Schwenk, *Ruhr University Bochum*
Wendy Seltzer, *W3C and Massachusetts Institute of Technology*
Johanna Sepulveda, *Airbus*
Mahmood Sharif, *Tel Aviv University and VMware*
Imani N. Sherman, *University of Florida*
Shweta Shinde, *ETH Zurich*
Fatemeh Shirazi, *Web3 Foundation*
Maliheh Shirvanian, *Visa Research*
Yan Shoshitaishvili, *Arizona State University*
Haya Shulman, *Fraunhofer SIT*
Peter Snyder, *Brave Browser*
Sooel Son, *Korea Advanced Institute of Science and Technology (KAIST)*
Chengyu Song, *University of California, Riverside*
Alessandro Sorniotti, *IBM Research Europe*
Kyle Soska, *University of Illinois at Urbana–Champaign*
Michael Specter, *Massachusetts Institute of Technology*
Drew Springall, *Auburn University*
Jessica Staddon, *JPMorgan Chase*
Emily Stark, *Google*
Angelos Stavrou, *Virginia Tech*
Deian Stefan, *University of California, San Diego*
Ben Stock, *CISPA Helmholtz Center for Information Security*
Gianluca Stringhini, *Boston University*
Yixin Sun, *University of Virginia*
Yuqiong Sun, *Facebook*
Qiang Tang, *The University of Sydney*
Dave (Jing) Tian, *Purdue University*
Yuan Tian, *University of Virginia*
Nils Ole Tippenhauer, *CISPA Helmholtz Center for Information Security*

Alin Tomescu, *VMware Research*
Shruti Tople, *Microsoft Research*
Santiago Torres-Arias, *Purdue University*
Florian Tramèr, *Stanford University*
Patrick Traynor, *University of Florida*
Carmela Troncoso, *EPFL*
Güliz Seray Tuncay, *Google*
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*
Ingrid Verbauwhede, *Katholieke Universiteit Leuven*
Luca Viganò, *King's College London*
Hayawardh Vijayakumar, *Samsung Research America*
Bimal Viswanath, *Virginia Tech*
Daniel Votipka, *Tufts University*
David Wagner, *University of California, Berkeley*
Michael Waidner, *Technische Universität Darmstadt*
Gang Wang, *University of Illinois at Urbana–Champaign*
Ting Wang, *The Pennsylvania State University*
XiaoFeng Wang, *Indiana University Bloomington*
Michael Weissbacher, *Block, Inc.*
Tara Whalen, *Carleton University*
Christian Wressnegger, *Karlsruhe Institute of Technology (KIT)*
Matthew Wright, *Rochester Institute of Technology*
Eric Wustrow, *University of Colorado Boulder*
Jason (Minhui) Xue, *The University of Adelaide*
Daphne Yao, *Virginia Tech*
Yuval Yarom, *The University of Adelaide and Data61*
Tuba Yavuz, *University of Florida*
Yanfang (Fanny) Ye, *Case Western Reserve University*
Heng Yin, *University of California, Riverside*
Qiang Zeng, *University of South Carolina*
Sarah Zennou, *Airbus*
Fengwei Zhang, *Southern University of Science and Technology (SUSTech)*
Xiangyu Zhang, *Purdue University*
Yang Zhang, *CISPA Helmholtz Center for Information Security*
Yuan Zhang, *Fudan University*
Wenting Zheng, *Carnegie Mellon University*
Yajin Zhou, *Zhejiang University*
Haojin Zhu, *Shanghai Jiao Tong University*

Steering Committee

Michael Bailey, *University of Illinois at Urbana–Champaign*
Matt Blaze, *University of Pennsylvania*
Dan Boneh, *Stanford University*
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*
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, including but not limited to:

- 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
- Data-driven security and measurement studies
  - Measurements of fraud, malware, spam
  - Measurements of human behavior and security
- Privacy-enhancing technologies and anonymity
- 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

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.

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/usenixsecurity22/submission-policies-and-instructions for more information.

Artifact Evaluation

The Call for Artifacts will be available soon.

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, 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 sec22chairs@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 sec22it@usenix.org by February 1, 2022.

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, linked from the USENIX Security '22 Call for Papers web page, by July 6, 2022. Decisions will be made by July 13, 2022. 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/usenixsecurity22/publication-model-change.*

USENIX Security '22 submissions deadlines are as follows:

- **Summer Deadline:** Tuesday, June 8, 2021, 11:59 pm AoE
- **Fall Deadline:** Tuesday, October 12, 2021, 11:59 pm AoE
- **Winter Deadline:** Tuesday, February 1, 2022, 11:59 pm AoE

All papers that are accepted by the end of the winter submission reviewing cycle (February–May 2022) will appear in the proceedings for USENIX Security '22. All submissions will be made online via their respective web forms, linked from the USENIX Security '22 Call for Papers web page: Summer Deadline, Fall Deadline, Winter Deadline. Do not email submissions. Submissions should be finished, complete papers, and we may reject papers without review that have severe editorial problems (broken references, egregious spelling or grammar errors, missing figures, etc.) or are submitted in violation of the Submission Instructions outlined below.

All paper submissions, including Major Revisions, 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 so the paper should be self-contained without them. 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 '22 will be published and open and accessible to everyone without restrictions on the following dates:

- **Summer Deadline:** Tuesday, November 9, 2021
- **Fall Deadline:** Tuesday, April 5, 2022
- **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 10, 2022.

- **Summer Deadline:** Tuesday, November 2, 2021
- **Fall Deadline:** Tuesday, March 29, 2022
- **Winter Deadline:** Tuesday, July 12, 2022

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, (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 within the prior two years, (4) anyone who is serving as the sponsor or administrator of a grant that funds your research, or (5) close personal friendships. For other forms of conflict, authors must contact the chairs and explain the perceived conflict.

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.

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 double-blind. 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. Only blind the reference itself in the (unusual) case that a third-person reference is infeasible.
- 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 contain the authors' names or affiliations.

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.

Facebook 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 Facebook 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.

You may submit your USENIX Security '22 paper submission for consideration for the Prize as part of the regular submission process. Find out more about the Internet Defense Prize at www.internetdefenseprize.org.

Human Subjects and Ethical Considerations

Submissions that describe experiments on human subjects, that analyze data derived from human subjects (even anonymized data), or that otherwise may put humans at risk should:

1. Disclose whether the research received an approval or waiver from each of the authors' institutional ethics review boards (e.g., an IRB).
2. Discuss steps taken to ensure that participants and others who might have been affected by an experiment were treated ethically and with respect.

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). The same applies if the submission deals with personally identifiable information (PII) or other kinds of sensitive data. If a paper raises significant ethical and legal concerns, it might be rejected based on these concerns.

Contact the program co-chairs at sec22chairs@usenix.org if you have any questions.

Reviews from Prior Submissions

Drawn from the ACM CCS 2020 CFP, IEEE S&P 2021

For papers that were previously submitted to, and rejected from, another conference, 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. This includes withdrawn papers (if reviews were received) as well as papers whose last submission was at USENIX. Reviewers will be asked to complete their reviews before reading the provided supplementary material 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 contents) 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 resubmissions of Major Revisions, authors must submit a separate PDF that includes the verbatim Major Revision criteria, a list of changes to the paper, and a statement of how the changes address the review comments. While not required, authors are strongly encouraged to submit as part of the PDF a "PDF 'diff'" to assist reviewers in identifying your modifications. 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 sec22chairs@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 at www.usenix.org/submissions-policy for details.

Note that under the changes to the USENIX Security publication model, papers that have received a decision of Major Revisions from USENIX Security are still considered to be under review for the following two review cycles after notification; authors must formally withdraw their paper if they wish to submit to another venue. See USENIX Security Publication Model Changes at www.usenix.org/conference/usenixsecurity22/publication-model-change for details. For submissions that received Reject or Reject and Resubmit decisions from USENIX Security '21, resubmissions must follow the rules laid out for when they can be resubmitted (i.e., not in the next deadline for Reject and Resubmit, and not in the next two deadlines for Reject).

Questions? Contact your program co-chairs, sec22chairs@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.

Each accepted submission may be assigned a member of the program committee to act as its shepherd through the preparation of the final paper. The assigned member will act as a conduit for feedback from the committee to the authors.

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 for deadlines.

Specific questions about submissions may be sent to the program co-chairs at sec22chairs@usenix.org. The chairs will respond to individual questions about the submission process if contacted at least a week before the submission deadline.