VehicleSec '27: 5th USENIX Symposium on Vehicle Security and Privacy

August 9–10, 2027, Denver, CO, USA

Sponsored by USENIX, the Advanced Computing Systems Association

The 5th USENIX Symposium on Vehicle Security and Privacy (VehicleSec '27) will take place on August 9–10, 2027, and is co-located with the 36th USENIX Security Symposium in Denver, CO, USA.

Important Dates

Cycle 1

- Paper submissions due: Tuesday, December 15, 2026, 23:59 AoE (Anywhere on Earth) time
- Notification of paper acceptance: Tuesday, February 2, 2027
- Final papers due: Tuesday, June 22, 2027

Cycle 2

- Paper submissions due: Thursday, March 11, 2027, 23:59 AoE (Anywhere on Earth) time
- Notification of paper acceptance: Tuesday, April 27, 2027
- Final papers due: Tuesday, June 22, 2027

Artifacts

- Artifact registration deadline for Cycle 1 papers: Tuesday, March 16, 2027
- Artifact registration deadline for Cycle 2 papers: Tuesday, May 4, 2027
- Artifact submission deadline: Tuesday, May 11, 2027
- Discussion period: Tuesday, May 25–Tuesday, June 8, 2027
- Badge notification to authors: Tuesday, June 15, 2027

Demo/Poster/Lightning Talk/Tutorial

- Submissions due: Tuesday, May 4, 2027
- Notification of acceptance: Tuesday, May 25, 2027
- Final abstracts due: Thursday, June 3, 2027

Overview

A vehicle is a machine that transports people and/or goods in one or more physical domains, such as on the ground (e.g., cars, bicycles, motorcycles, trucks, buses, scooters, trains), in the air (e.g., drones, airplanes, helicopters), in the water (e.g., ships, submarine), and in space (e.g., spacecraft). Due to their safety and mission-critical nature, the security and privacy of vehicles can pose direct threats to passengers, owners, operators, and the infrastructure. Recent improvements in vehicle autonomy and connectivity (e.g., autonomous driving, uncrewed aerial vehicles (UAVs), vehicle-to-everything (V2X) communication, intelligent transportation systems, swarm robotics, and small satellites) have also served to exacerbate security and privacy challenges and thus require urgent attention from academia, industry, and policy-makers. To meet this critical need, VehicleSec aims to bring together an audience of university researchers, scientists, industry professionals, and government representatives to contribute new theories, technologies, and systems on any security/privacy issues related to vehicles (e.g., ground, aerial, in/on water, space), their sub-systems (e.g., in-vehicle networks, autonomy, connectivity, human-machine interfaces), supporting infrastructures (e.g., transportation infrastructure, charging station, ground control station), and related fundamental technologies (e.g., sensing, control, AI/ML/DNN/LLM, wireless communication, real-time computing, edge computing, location service, simulation, digital twin, multi-agent protocol/system design, and human-machine interaction).

Demo/Poster Session

VehicleSec will feature a demo/poster session to allow academic, governmental, and industry participants to share demonstrations and/or present posters of their latest practical attacks, defenses, and security/privacy tools or systems related to vehicles.

Tutorial Session

The symposium will also feature a tutorial session with an in-depth learning experience on one or more state-of-the-art topics in vehicle privacy and security presented by researchers or practitioners within the field. A tutorial should focus on its topic in detail and include references to the "must-read" papers or materials within its domain. Tutorials in which participants actively engage in exercises or hands-on work are particularly welcome. We encourage tutorials to include hands-on elements, live demonstrations, or interactive discussions. Each tutorial will be allocated a one-hour slot. Proposals should clearly indicate the format of the tutorial, prerequisites for participating in the tutorial (e.g., background knowledge, program languages), required materials (e.g., hardware, datasets, virtual machine images, wifi access), including (if any) material provided by the applicant (e.g., hardware, documentation).

Lightning Talks Session

The symposium will feature a Lightning Talks session with short and engaging 5-minute in-person presentations on any topics that can be worth a timely shout-out to the VehicleSec community, which include but are not limited to emerging hot topics, preliminary research results, practical problems encountered, lessons learned, the introduction of tutorials and education materials, tips and tricks, simulators/simulations, data and visualizations (e.g., autonomous driving datasets), or other (interdisciplinary) topics related to vehicles.

Awards

Accepted papers and demos will be considered for Best Paper Award and Best Demo Award. Accepted artifacts will be considered for the Distinguished Artifact Award.

Areas of Interest

Topics of interest include, but are not limited to:

- Embedded/sensor/analog/actuator security, privacy, and forensics in vehicle settings
- Vehicle-related malware/firmware analysis
- Secure/resilient/trustworthy/privacy-preserving perception, localization, planning, and control in autonomous/automated vehicles
- Security/safety/robustness verification related to vehicles
- Intra- and inter-vehicle network (e.g., CAN bus, V2X, remote operator channel) security
- Multi-vehicle coordination/cooperation (e.g., V2X, drone swarm) security
- Compliance with policies (e.g., legal, security, privacy, safety, and environmental policies)
- Secure integration of hardware and software systems for vehicles (e.g., ground, aerial)
- Secure software/hardware updates in vehicle settings (e.g., cars, drones, airplanes, spacecraft)
- Privacy challenges in vehicle settings (e.g., driver/passenger privacy, drone/car/robot spying, intellectual property stealing)
- Privacy-preserving data sharing and analysis in vehicle settings
- Security/privacy in electric, medium- and heavy-duty vehicle systems
- Security/privacy in Intelligent Transportation Systems (ITS) (e.g., intelligent traffic signals)
- Security/privacy for vehicle-related supporting infrastructure (e.g., charging)
- Secure vehicle-related software/hardware development process (e.g., debugging tools, simulators, testbed) and their own security/privacy
- Security/privacy of any vehicle-related fundamental technologies (e.g., sensing, control, AI, location service, IoT)
- Human factors, trust, humans in the loop, and usable security related to vehicles
- Security/privacy/resilience-related metrics and risk assessment for vehicles
- GenAI-enabled attacks on vehicles and corresponding defensive approaches
- GenAI tools and frameworks for the security of vehicles

Ethical Considerations

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 the rejection of a submission regardless of its quality and scientific value. Where relevant, 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. 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. Authors may wish to consult the USENIX Security '27 Ethics Guidelines (www.usenix.org/conference/usenixsecurity27/call-for-papers#ethics).

Human Subjects Research

If your submitted document relates to human subjects, analyzes data derived from human subjects, may put humans at risk, or might have other ethical implications or introduce legal issues of potential concern to the VehicleSec community, authors should disclose if an ethics review (e.g., IRB approval) was conducted, and discuss in the paper how ethical and legal concerns were addressed.

Vulnerability Disclosure

If your submitted document reports a potentially high-impact vulnerability, the authors should 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 chairs will contact the authors in case of concerns. The Program Committee reserves the right to reject a submission if insufficient evidence was presented that ethical or relevant legal concerns were appropriately addressed.

Conflicts of Interest

Authors and Program Committee members are required to indicate any conflict of interest and its nature. Advisors and those that they are advising, as well as authors and PC members with an institutional relationship, are considered to share a conflict of interest. Professional collaborations (irrespective of whether they resulted in publication or funding) that occurred in the past two years and close personal relationships equally constitute a conflict of interest. PC members, including chairs, who have a conflict of interest with a paper will be entirely excluded from the evaluation of that paper.

A Special Note on "Fake Conflicts": Declaring conflicts of interest to avoid certain (otherwise non-conflicting) PC members is not allowed and can constitute grounds for rejection. The PC Chairs reserve the right to request additional explanation for any declared conflict. If authors have concerns about the fair treatment of their submissions, they should instead contact the chairs and provide convincing arguments for any special consideration that they are requesting.

Publication Info

Publication Info

Publication Info

section will count towards the page limit). Please consult the VehicleSec Policy on the Use of Generative AI (www.usenix.org/conference/vehiclesec27/ai-policy) for the details.

Submission Guidelines for Papers

We accept (1) **regular papers up to 13 pages** and (2) **short position papers or work-in-progress (WIP) papers up to 6 pages**, excluding references and appendices. Short papers are suitable for position papers or original works whose descriptions fit within 6 pages. WIP papers are suitable for original yet incomplete work that is looking for middle-stage feedback from the community. We also accept **Systemization of Knowledge (SoK) papers**; the length of SoK papers should be similar to regular papers. Note that reviewers are not required to read the appendices or any supplementary material. Once accepted, the camera-ready version of regular and SoK papers should be at most 18 pages, and short position papers or work-in-progress (WIP) papers should be at most 10 pages, including the bibliography and any appendices. Authors should not change the font or the margins of the USENIX format. **For regular papers, shorter papers won't be penalized; thus, authors are encouraged to submit papers of appropriate length based on the research contribution.** Submissions must follow the USENIX Conference Submissions Policy (www.usenix.org/conferences/author-resources/submissions-policy)

Submissions should be typeset in two-column format using 10-point type on 12-point (single-spaced) leading in a text block 7" wide x 9" deep, with .33" inter-column space, formatted for 8.5" x 11" paper. Authors must use the USENIX templates and style files (www.usenix.org/conferences/author-resources/paper-templates) when preparing their paper for submission. Failure to adhere to the page limit and formatting requirements can be grounds for rejection. Submissions must be in Portable Document Format (PDF). Authors should pay special attention to unusual fonts, images, and figures that might create problems for reviewers. Documents should render correctly in Adobe Reader when printed in black and white.

Submissions should be anonymized for review; no author names or affiliations may appear on the title page, and papers should avoid revealing authors' identities in the text. When referring to their previous work, authors are required to cite their papers in the third person without identifying themselves. Acceptance of final papers may be subject to shepherd approval.

Short, WIP, and SoK papers must have their respective prefix "Short:"/"WIP:"/"SoK:" in their titles and be submitted via the submission systems for their respecive cycle, which are linked from the VehicleSec '27 Call for Papers web page

Double and Concurrent Submissions

Technical papers must not substantially overlap with papers that have been published or that are simultaneously submitted to a journal or a conference/workshop with proceedings. Double-submission will result in immediate rejection. The Program Committee may share information with other conference chairs and journal editors so as to detect such cases.

Submission and Publication Process

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, or that do not have a clear application to vehicle security and privacy may be rejected without review. Papers accompanied by nondisclosure agreement forms will not be considered.

Accepted submissions will be treated as confidential prior to publication on the VehicleSec '27 website; rejected submissions will be permanently treated as confidential.

As part of USENIX's open-access policy, all papers will be available online before the conference. If your accepted paper should not be published prior to the event, please notify production@usenix.org after you submit your final accepted paper. 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 for the complete terms of publication.

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

Alternative arrangements can be made if there are justifiable difficulties in travel and will be allowed only on a case-by-case basis with permission from the Program Co-chairs. The proceedings will be published and archived by USENIX.

If you have any other questions related to the submission process, please email the program co-chairs at vehiclesec27chairs@usenix.org. Please reach out as soon as possible, as it may not be possible to answer late questions prior to the submission deadline.

Review Process Outcomes

The review process will result in one of three outcomes:

- Accepted: In this case, reviewers either see no need for any required edits—the paper could be published as is—or trust the authors to make any required edits.
- Major Revision: Papers in this category are considered promising but need additional work (e.g., new implementations, experiments, and/or proofs). Authors of Cycle 1 papers may choose to revise and resubmit such papers to the second submission cycle of VehicleSec '27. The revision and second review of "Major Revision" papers will be based on a list of "revision tasks" clearly specified by the original reviewers and conveyed to the authors upon notification by a shepherd. A revised paper will be accepted to VehicleSec '27 if it satisfactorily fulfills the revision tasks.
- Rejected: This outcome indicates that the paper is not currently appropriate for publication at VehicleSec '27.

Papers rejected from the first submission cycle cannot be submitted to the second submission cycle of VehicleSec '27.

Desk Rejection Policy

Program Committee (PC) chairs reserve the right to desk-reject submissions where the topic, contributions, or core substance of the paper are not sufficiently clear or fall outside

the scope of the symposium. This includes low-quality or AI-generated ("AI-slop") papers that lack rigor or genuine scientific contribution. To facilitate early identification, a Round 0 Check will be conducted where the Committee evaluates initial clarity and substance.

Authorship Policy

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

Optional Artifact Evaluation

A scientific paper consists of a constellation of artifacts that extend beyond the document itself: software, hardware, evaluation data and documentation, raw survey results, mechanized proofs, models, test suites, benchmarks, and so on. In some cases, the quality of these artifacts is as important as that of the paper itself. To emphasize the importance of such artifacts, the benefits to the authors and the community as a whole, and to promote the availability and reproducibility of experimental results, VehicleSec '27 runs an Artifact Evaluation. Authors of accepted papers are encouraged to submit their artifacts for availability, functionality, and reproducibility assessments. The Artifact Evaluation Committee (AEC) will review each submitted artifact and also grant the Distinguished Artifact Award to outstanding artifacts accepted to VehicleSec '27.

The Call for Artifacts will be available soon.

Submission Guidelines for Demos and Posters

We accept demos and posters of up to 2 pages, including references and appendices. Submissions should be typeset in two-column format using 10-point type on 12-point (single-spaced) leading in a text block 7" wide x 9" deep, with .33" inter-column space, formatted for 8.5" x 11" paper. Authors must use the USENIX templates and style files (www.usenix.org/conferences/author-resources/paper-templates) when preparing their demo and poster for submission. Submissions must be in Portable Document Format (PDF). Authors should pay special attention to unusual fonts, images, and figures that might create problems for reviewers. Documents should render correctly in Adobe Reader when printed in black and white.

Submissions can be anonymized for review, but it is not mandatory. Demo and Poster papers must have the prefix "Demo:" or "Poster:" in their titles and be submitted via the demos and posters submission form, which will be available on the Call for Papers webpage.

To allow attendees to better learn and experience practical vehicle-related attacks, defenses, and tools, VehicleSec will structurally encourage authors to submit Demos. Specifically, all accepted demos will be provided a demo table and a poster easel (so a superset of the setup for an accepted Poster, which will be provided only a poster easel). At the presentation time, each demo should have (1) exhibitions, slides, videos, and/or interactive/live demos to showcase on the table and (2) a poster presentation of the demo to be put on the easel. All the accepted demos will be considered for the Best Demo Award. Note that although at the presentation time, the setup of a Demo includes a Poster, authors only need to submit a Demo paper. For additional information regarding demos and posters, please do not hesitate to contact the Demo/Poster Chair at vehiclesec27-demos-posters-tutorials@usenix.org.

Submission Guidelines for Tutorials

We invite tutorial proposals to be a part of the tutorial sessions taking place during the symposium on August 9 and/or August 10, 2027. Tutorials aim to offer participants an in-depth and practical understanding of emerging topics in vehicle security and privacy, spanning research advancements, industry practices, and critical policy issues. We welcome proposals from researchers, practitioners, and educators in academia, industry, and government.

We encourage tutorials to include hands-on elements, live demonstrations, or interactive discussions. Each tutorial will be allocated in a one-hour slot. Proposals should clearly indicate the format of the tutorial and required materials.

We accept tutorial submissions of up to 2 pages, including references and appendices. Submissions should be typeset in two-column format following the Demo/Poster layout (please see Submission Guidelines for Demos and Posters above). Submissions can be anonymized for review, but it is not mandatory. Tutorial submissions must have the prefix "Tutorial:" in their titles and be submitted via the tutorial submission form, which will be available on the Call for Papers webpage.

Tutorial proposals must include:

- Title: A concise and descriptive title.
- Abstract: A brief summary (up to 500 words) outlining the tutorial's scope, objectives, and intended audience.
- Presenter(s): Names, affiliations, and a short bio (a maximum of 250 words each) highlighting relevant expertise and experience.
- Target Audience: Specify the expected audience, required prior knowledge, and estimated number of attendees.
- Content Outline: Detailed breakdown of topics to be covered and expected learning outcomes.
- Format and Duration: Proposed session length (one hour) and preferred mode of delivery (e.g., lecture, hands-on, hybrid).
- Special Requirements: Any technical or logistical needs (e.g., software, hardware, internet connectivity). Note that requirements will be reviewed along with the submission, and if accepted, submitters will be notified of what needs can and cannot be fulfilled.
- Supporting Material (optional): Any existing slides, reference materials, or prerequisites that will be provided by the tutorial presenters.

Tutorial proposals will be evaluated based on:

- Relevance to the symposium themes.
- Clarity and comprehensiveness of the proposal.
- Practicality and accessibility of the tutorial content.
- Presenter expertise and experience.

We encourage diversity in topics and presenters to provide participants with a broad range of learning opportunities. For additional information regarding tutorials, do not hesitate to contact the Tutorial Chair at vehiclesec27-demos-posters-tutorials@usenix.org.

Submission Guidelines for Lightning Talks

We will host a Lightning Talks session at the symposium. We solicit short and engaging 5-minute in-person presentations on any topics that can be worth a timely shout-out to the VehicleSec community, which include but are not limited to emerging hot topics, work-in-progress research ideas, and preliminary results, practical problems encountered, lessons learned, tips and tricks, simulators/simulations, data and visualizations (e.g., autonomous driving datasets), or other (interdisciplinary) topics related to vehicles.

Note that the lightning talks are not intended for self-promotion or commercial advertisement. Specifically, share concepts, methodologies, or findings that can be broadly applied or spark meaningful discussions. Focus on the work itself rather than promoting your product, service, or organization. Avoid sales pitches, advertisements, or excessive emphasis on personal or corporate achievements.

Please submit your Lightning Talk title and abstract (200 words or less) for full consideration via the Lightning Talk submission form, which will be available on the Call for Papers webpage. Lightning Talk abstracts will be published on the symposium website.

All lightning talk submissions must include the presenter's name, affiliation, and contact information. Please note that the presenter must make all submissions. Submissions from PR firms will be rejected without review. A time limit for lightning talks will be strictly enforced. For additional information regarding Lightning Talks, do not hesitate to contact the Lightning Talk Chair at vehiclesec27-talks@usenix.org.

Symposium Organizers

General Chairs

Sara Rampazzi, *University of Florida*
Qiben Yan, *Michigan State University*

Program Co-Chairs

Hyungsub Kim, *Indiana University*
Dario Stabili, *University of Modena and Reggio Emilia*

Program Committee

Zeeshan Afzal, *Linköping University*
Daniele Antonioli, *EURECOM*
Md Armanuzzaman, *The University of Texas at El Paso*
Luca Arnaboldi, *University of Birmingham*
Dipkamal Bhusal, *Rochester Institute of Technology*
Gedare Bloom, *University of Colorado Colorado Springs*
Elias Bou-Harb, *Louisiana State University*
Zeb Bowden, *Virginia Tech Transportation Institute*
Alessandro Brighente, *University of Padua*
Divanilson R. Campelo, *Universidade Federal de Pernambuco*
Justin Cappos, *NYU*
Niusen Chen, *University of Nevada, Reno*
Yimin Chen, *University of Massachusetts Lowell*
Yueqi Chen, *University of Colorado Boulder*
Anastasija Collen, *HEG-Genève*
Mauro Conti, *University of Padua and Örebro University*
Qinrun Dai, *University of Colorado Boulder*
Jeremy Daily, *Colorado State University*
Marco De Vincenzi, *NYU*
Denis Donadel, *Fondazione Bruno Kessler*
Knut Eckstein, *European Space Agency*
Yiheng Feng, *Purdue University*
Clement Fung, *University of Maryland, Baltimore County*
Giovanni Gambigliani Zoccoli, *University of Modena and Reggio Emilia*
Rachel Gerdes, *Virginia Tech*
Zain Alabedin Haj Hammadeh, *German Aerospace Center (DLR)*
Mohammad Hamad, *Technische Universität Munich*
Xiali Hei, *University of Louisiana at Lafayette*
Bardh Hoxha, *Toyota Motor North America R&D*
Hongxin Hu, *University at Buffalo*
Shengtuo Hu, *Palo Alto Networks*
Shalabh Jain, *Center of Data for Public Good, Indian Institute of Science, Bangalore*
Ameer Kashani, *DENSO*
Chung Hwan Kim, *The University of Texas at Dallas*
Huy Kang Kim, *Korea University*
Seulbae Kim, *Pohang University of Science and Technology (POSTECH)*
Yongdae Kim, *Korea Advanced Institute of Science and Technology (KAIST)*
Sebastian Köhler, *University of Manchester*
Vireshwar Kumar, *Indian Institute of Technology Delhi*
Ming F. Li, *University of Arizona*
Peng Liu, *The Pennsylvania State University*
Stefano Longari, *Politecnico di Milano*
Efren Lopez Morales, *New Mexico State University*
Li Lu, *Zhejiang University*
Pedram Mohajeransari, *Clemson University*
Bassam Moussa, *University of Doha for Science and Technology*
Srinivasan Murali, *Texas A&M University–San Antonio*
Pal-Stefan Murvay, *Politehnica University of Timișoara*
Habeeb Olufowobi, *The University of Texas at Arlington*
Christos Papadopoulos, *University of Memphis*
Karthik Pattabiraman, *University of British Columbia*
James Pavur, *Istari Digital*
Mert D. Pesé, *Clemson University*
Sujan Rao, *Micron Technology*
Indrakshi Ray, *Colorado State University*
Anna Raymaker, *Georgia Institute of Technology*
Amir Salarpour, *Clemson University*
Mohsen Salehi, *University of British Columbia*
Krishna Sampigethaya, *Embry-Riddle Aeronautical University, Prescott*
Neetesh Saxena, *Cardiff University*
Md Hasan Shahriar, *University of Arkansas*
Shanghao Shi, *Washington University in St. Louis*
Mridula Singh, *CISPA Helmholtz Center for Information Security*
Ruoyu Song, *Purdue University*
David Starobinski, *Boston University*
Takeshi Sugawara, *The University of Electro-Communications*
Dean Sullivan, *University of New Hampshire*
Nils Ole Tippenhauer, *CISPA Helmholtz Center for Information Security*
Sadegh Torabi, *George Mason University*
Yazhou Tu, *Auburn University*
Maryna Veksler, *Virginia Commonwealth University*
Chenyi Wang, *University of Arizona*
Lan Wang, *University of Memphis*
Andre Weimerskirch, *Block Harbor Cybersecurity*
Johannes Willbold, *Variant Security*
Yang Xiao, *University of Kentucky*
Shouhuai Xu, *University of Colorado Colorado Springs*

Kun Yang, *Zhejiang University*
Doguhan Yeke, *Purdue University and Capital One*
Kentaro Yoshioka, *Keio University*
Qingzhao Zhang, *University of Arizona*
Xingli Zhang, *University of Louisiana at Lafayette*
Ce Zhou, *Missouri University of Science and Technology*
Xugui Zhou, *Louisiana State University*
Yi Zhu, *Wayne State University*

Invited Talks, Tutorials, and Lightning Talks Co-Chairs
Ameer Kashani, *DENSO International America, Inc.*
Hrushikesh Varma, *University of California, Irvine*

Poster/Demo Program Co-Chairs
Jinwen Wang, *University of Texas Dallas*
Qingzhao Zhang, *University of Arizona*

Poster/Demo Program Committee
TBA

Publicity Co-Chairs
Hanqing Guo, *Indiana University*
Zhiyuan Yu, *Texas A&M University*

Sponsorship Co-Chairs
Shaunak D. Bopardikar, *Michigan State University*
Karthik Pattabiraman, *University of British Columbia*

Steering Committee
Gail-Joon Ahn, *Arizona State University*
David Balenson, *USC Information Sciences Institute*
Alfred Chen, *University of California, Irvine*
Chunming Qiao, *University at Buffalo*
Kang Shin, *University of Michigan*
Mani Srivastava, *University of California, Los Angeles*
Gene Tsudik, *University of California, Irvine*
Dongyan Xu, *Purdue University*

Artifact Evaluation Committee Co-Chairs
Taegyu Kim, *The Pennsylvania State University*
Muslum Ozgur Ozmen, *Arizona State University*

Artifact Evaluation Committee
TBA