38th Annual Computer Security Applications Conference (ACSAC 2022)

Dec 5-9, 2022 · Austin, TX, USA

Call for Submissions

ACSAC is an internationally recognized forum where practitioners, researchers, and developers in information system security meet to learn and to exchange practical ideas and experiences. If you are developing practical solutions to problems related to the protection of users, commercial enterprises, or countries' information infrastructures, consider submitting your work to the Annual Computer Security Applications Conference. For more information, see https://www.acsac.org/. Select ACSAC papers will be invited for submission of an extended version to a special issue of the ACM Digital Threats: Research and Practice (DTRAP) journal.

Important Dates:

- Paper submission deadline: June 29, 23:59:59 (AoE – UTC-12)
- Notification to authors: September 2nd (Early reject notification: August 1st)

Topics and Hard Topic Theme

We solicit papers offering novel contributions in any aspect of applied security, including the application of security technology, the implementation of systems, and the discussion of lessons learned. ACSAC 2022 especially encourages submissions in the area of our hard topic theme of **Deployable Trustworthy Systems**. Trustworthy systems generally involve the development of capabilities that offer security, safety, and reliability guarantees. ACSAC has always solicited work on applied security; with this hard topic, we hope to put great emphasize on deployable trustworthy systems.

The trustworthy systems topic is expended and includes but is not limited to approaches applied at the intersection of operation systems, formal methods, and programming languages; approaches applied at the architecture level; trustworthy artificial intelligence with emphasize on explainability, correctness, and robustness to attacks; zero-trust solutions that assume no implicit trust, but continually assess risk; and trustworthy systems form a user's perspective. The trustworthy systems topic does not necessarily mean building a complete solution, but the work needs to identify key challenges, explain the deficiencies in state-of-the-art solutions, and demonstrate the effectiveness of the proposed approaches and (potential) impact to the real world.

Ethical Considerations

Papers that might raise ethical concerns (e.g., papers that use human subjects or describe experiments related to vulnerabilities in software or systems) must include an Ethical Considerations section that properly describes what procedures have been followed to minimize potential harm. Such papers should discuss the steps taken to avoid negatively affecting any third-parties, whether an institutional ethics committee reviewed the research, or how the authors plan to responsibly disclose the vulnerabilities to the appropriate software/system vendors or owners before publication.

Submission Rules

Submitted papers must not substantially overlap with papers that have been published or are simultaneously under submission to a journal or a conference with proceedings. Please ensure that your submission is a PDF file of a maximum of 10 pages, excluding well-marked references and appendices limited to 5 pages. Committee members are not required to read the appendices. Submissions must be generated using the ACM acmart template available at https://www.acm.org/publications/proceedings-template, using the [sigconf, anonymous] options. All submissions must be anonymous (i.e., papers should not contain author names or affiliations, or obvious citations). Submissions violating any of the above constraints risk rejection without consideration of their merits. Submissions are to be made using the HotCRP system. Papers will be reviewed in two consecutive rounds, and early-reject notifications will be sent to authors after the first round, if a paper has received only strongly negative reviews. Appeals based on factual disagreements may be submitted to the Program Chairs, who may appoint an independent reviewer to decide the appeal. In any case, papers

cannot be re-submitted elsewhere until the authors are notified of acceptance or rejection, early or final, and until any appeal has been resolved.

Artifact Submission

During submission, authors of papers whose main contributions and experimental results rely primarily on new or reproduced artifacts (e.g., code and/or data) **should indicate** whether they will separately submit their artifacts for evaluation by the artifacts evaluation committee and make the artifacts publicly available, if their paper is accepted. This acknowledgement will be visible to the reviewers and may therefore be taken into consideration during the review process. Authors who **have justifiable reasons to not submit** their artifacts for evaluation (if their paper is accepted) should add a comment in the corresponding comment box in the submission form.

The authors of the submitted artifacts need to commit to keep them **available online on a publicly accessible website**. We plan to reward authors who participate in this program with a special mention during the conference and on the ACSAC webpage, an ACM Artifact Evaluated badge on their papers, and (if enough authors participate in the program) by reserving a Distinguished Paper Award for this group.

Program Committee

Gabriela Ciocarlie, The University of Texas at San Antonio (Program Chair)
Roberto Perdisci, University of Georgia (Program Co-chair)
Martina Lindorfer, TU Vienna (Artifact Evaluation Co-chair)
Gianluca Stringhini, Boston University (Artifact Evaluation Co-chair)

Adwait Nadkarni, William & Mary
Aiping Xiong, The Pennsylvania State University
Aisha Ali-Gombe, Towson University
Alberto Dainotti, Georgia Institute of Technology
Alexandros Kapravelos, North Carolina State University
Ambra Demontis, University of Cagliari
Amin Kharraz, Florida International University
Anita Nikolich, University of Illinois - Urbana Champaign
Anna Squicciarini, Penn State University
Aravind Prakash, Binghamton University
Attila A Yavuz, University of South Florida
Baris Coskun, Amazon AWS
Benjamin E. Ujcich, Georgetown University
Bo Chen, Michigan Technological University
Brendan Saltaformaggio, Georgia Institute of Technology
Byoungyoung Lee, Seoul National University (SNU)
Christian Wressnegger, Karlsruhe Institute of Technology
Christophe Hauser, Information Sciences Institute, University of Southern California
Cong Wang, City University of Hong Kong
Dave (Jing) Tian, Purdue University
Davide Maiorca, University of Cagliari, Italy
Ding Wang, Nankai University
Dolière Francis Somé, CISPA Helmholtz Center for Information Security
Elias Athanasopoulos, University of Cyprus
Elisa Bertino, Purdue University
Andrea Continella, University of Twente
Amir Houmansadr, University of Massachusetts Amherst
Eugene Vasserman, Kansas State University
Evangelos Markatos, University of Crete and FORTH
Federico Maggi, Huawei Technologies
Fengwei Zhang, Southern University of Science and Technology (SUSTech)
Kevin Alejandro Roundy, Norton Research Group
Kun Sun, George Mason University
Kyu Hyung Lee, University of Georgia
Lannan Lisa Luo, University of South Carolina
Le Guan, University of Georgia
Leigh Metcalf, CERT Software Engineering Institute, CMU
Lejla Batina, Radboud University
Lingwei Chen, Wright State University
Long Cheng, Clemson University
Lorenzo De Carli, Worcester Polytechnic Institute
Magnus Almgren, Chalmers University of Technology
Man-Ki Yoon, Yale University
Manos Antonakakis, Georgia Tech
Manuel Egele, Boston University
Marco Balduzzi, Trend Micro Research
Martin Johns, TU Braunschweig
Martina Lindorfer, TU Wien
Maverick Woo, Carnegie Mellon University
Ming Li, University of Arizona
Mu Zhang, University of Utah
Mustakimur Rahman Khandaker, University of Georgia
Nick Nikiforakis, Stony Brook University
Nitesh Saxena, Texas A&M University
Oleksii Starov, Palo Alto Networks
Omar Alrawi, Georgia Institute of Technology
Patrick Schaumont, Worcester Polytechnic Institute
Phani Vadrevu, University of New Orleans
Qi Alfred Chen, University of California, Irvine
Qi Li, Tsinghua University
Qian Feng, Baidu USA
Ram Krishnan, University of Texas at San Antonio
Sang Kil Cha, KAIST
Sangho Lee, Microsoft Research
Sarah Chmielewski, MIT Lincoln Laboratory

François Gauthier, Oracle Labs
Giancarlo Pellegrino, CISPA Helmholtz Center for Information Security
Gianluca Stringhini, Boston University
Giorgio Giacinto, University of Cagliari, Italy
Guenevere (Qian) Chen, The University of Texas at San Antonio
Haya Shulman, Goethe-Universität Frankfurt and Fraunhofer SIT
Hayawardh Vijayakumar, Samsung Research America
Hongxin Hu, University at Buffalo
Hussain Almohri, Kuwait University
Jarilyn Hernandez Jimenez, MIT Lincoln Laboratory
Jeyavijayan Rajendran, Texas A&M University
Jie Yang, Florida state university
Jin-Hee Cho, Virginia Tech
Juan Caballero, IMDEA Software Institute
Kapil Singh, IBM T.J. Watson Research Center
Sébastien Bardin, Université Paris-Saclay, CEA LIST
Seungwon Shin, KAIST
Shanchieh (Jay) Yang, Rochester Institute of Technology
Sooel Son, KAIST
Stefano Calzavara, Università Ca' Foscari Venezia
Tamara Rezk, INRIA
Thang Hoang, Virginia Tech
Xiaojing Liao, Indiana University Bloomington
Xiapu Luo, The Hong Kong Polytechnic University
Yanfang (Fanny) Ye, University of Notre Dame
Yeongjin Jang, Oregon State University
Yinzhi Cao, Johns Hopkins University
Yonghwi Kwon, University of Virginia
Yousra Aafer, University of Waterloo
Yue Duan, Illinois Institute of Technology
Zachary Tudor, Idaho National Laboratory
Zhiqiang Lin, Ohio State University