36th Annual Computer Security Applications Conference (ACSAC 2020)

December 7-11, 2020 • 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/. ACSAC authors will be invited to submit an extended version of their work to a special issue of the *ACM Digital Threats: Research and Practice* (*DTRAP*) journal.

Important Dates:

- Paper submission deadline: June 12, 23:59:59 (AoE – UTC-12)
- Early reject notification: July 19
- Notification to authors: August 17

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. Like last year, ACSAC 2020 especially encourages submissions in the area of our hard topic theme of **Deployable and Impactful Security**. Submissions in this hard topic theme include research results and technologies that are more practical and applied, and can be potentially deployed, where they can have a direct impact on improving the quality of cybersecurity in real-world systems. Deployable and impactful security generally involves the development of defensive solutions, rather than simply exposing weaknesses and vulnerabilities. While ACSAC has always solicited work on applied security, by having it as a hard topic theme we hope to put greater emphasis on deployability and impactfulness. Deployable and impactful security needs to address key real-world challenges, which may include accuracy, runtime overhead, ground-truth labeling, human aspects, usability, and energy consumption. Deployable and impactful security does not necessarily mean building a complete system, which may not be realistic, particularly in an academic environment. However, the work needs to identify key deployment challenges, explain the deficiencies in state-of-the-art solutions, and experimentally demonstrate the effectiveness of the proposed approaches and (potential) impact to the real world. The work may involve prototyping, defining metrics, benchmark evaluation, and experimental comparison with state-of-the-art approaches in testbeds or real-world pilots, possibly with operational data. Having the deployability and impactfulness goal motivates one to focus on solving the most critical real-world challenges, which may otherwise be ignored by the fast-moving research community.

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

To help improve reproducibility in computer security research, ACSAC encourages authors of accepted papers to submit software and data artifacts and make them publicly available to the entire community. These artifacts will not be part of

the paper evaluation. Their submission is strictly optional and will occur only after a paper has been accepted. Authors of accepted papers who decide to participate in this program will interact with a special committee dedicated to reviewing the submitted artifacts (e.g., to test that source code compiles and runs correctly, or that datasets content match their description). Authors can decide what they would like to submit (software, data, or both). However, the submitted artifacts must contribute in some inherent way to the generation of the related paper's main results. To the extent possible, all components that are most relevant to the paper should be included.

The artifacts review process will take place in parallel with the preparation of the camera-ready version of the paper. 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 to the program) by reserving a Distinguished Paper Award for this group. Authors with ACM Artifact Evaluated badges are especially encouraged to submit to the *ACM DTRAP* special issue.

Program Committee

Daphne Yao, Virginia Tech (Program Chair)
Heng Yin, UC Riverside (Program Co-chair)
Roberto Perdisci, University of Georgia (Artifacts Evaluation Chair)

Yousra Aafer, *University of Waterloo*
Hussain Almohri, *Kuwait University*
Magnus Almgren, *Chalmers University of Technology*
Elias Athanasopoulos, *University of Cyprus*
Ezedin Barka, *United Arab Emirates University*
Sébastien Bardin, *CEA France*
Lejla Batina, *Radboud University*
Tiffany Bao, *Arizona State University*
Alfred Chen, *UC Irvine*
Yingying Chen, *Rutgers University*
Long Cheng, *Clemson University*
Sarah Chmielewski, *MIT Lincoln Laboratory*
Jin-Hee Cho, *Virginia Tech*
Martin Degeling, *Ruhr University Bochum*
Adam Doupé, *Arizona State University*
Manuel Egele, *Boston University*
William Enck, *North Carolina State University*
Yanick Fratantonio, *Eurecom*
Carrie Gates, *Bank of America*
François Gauthier, *Oracle Labs Australia*
Neil Gong, *Duke University*
Guofei Gu, *Texas A&M University*
Behnaz Hassanshahi, *Oracle Labs Australia*
Christophe Hauser, *University of Southern California/ISI*
Jarilyn Hernández, *MIT Lincoln Laboratory*
Amir Houmansadr, *UMASS Amherst*
Hongxin Hu, *Clemson University*
Martin Johns, *SAP*
Alexandros Kapravelos, *North Carolina State University*
Vasileios Kemerlis, *Brown University*
Yonghwi Kwon, *University of Virginia*
Andrea Lanzi, *University of Milan*
Sangho Lee, *Microsoft Research*
Fengjun Li, *University of Kansas*
Ming Li, *University of Arizona*
Qi Li, *Tsinghua University*
Xiaojing Liao, *Indiana University Bloomington*
Zhiqiang Lin, *Ohio State University*
Yao Liu, *University of South Florida*
Lannan (Lisa) Luo, *University of South Carolina*
Xiapu Luo, *The Hong Kong Polytechnic University*
Di Ma, *University Michigan - Dearborn*
Evangelos Markatos, *FORTH and University of Crete*
Andrew Paverd, *Microsoft Research Cambridge*
Giancarlo Pellegrino, *CISPA*
Roberto Perdisci, *University of Georgia*
Aravind Prakash, *Binghamton University*
Jeyavijayan Rajendran, *Texas A&M University*
Kevin Alejandro Roundy, *NortonLifelock Research Group*
Brendan Saltaformaggio, *Georgia Tech*
Nitesh Saxena, *University of Alabama at Birmingham*
Patrick Schaumont, *Worcester Polytechnic Institute*
Kent Seamons, *Brigham Young University*
Francis Dolière Somé, *CISPA*
Sooel Son, *KAIST*
Seungwon Shin, *KAIST*
Xiaokui Shu, *IBM Research*
Anna Squicciarini, *Penn State University*
Gianluca Stringhini, *Boston University*
Kun Sun, *George Mason University*
Xiaoyan Sun, *California State University, Sacramento*
Yixin Sun, *University of Virginia*
Juan Tapiador, *Universidad Carlos III de Madrid*
Michel van Eeten, *Delft University of Technology*
Eugene Vasserman, *Kansas State University*
Hayawardh Vijayakumar, *Samsung Research America*
Bimal Viswanath, *Virginia Tech*
Cong Wang, *City University of Hong Kong*
Ding Wang, *Nankai University*
Gang Wang, *University of Illinois at Urbana-Champaign*
Hui (Wendy) Wang, *Stevens Institute of Technology*
Maverick Woo, *Carnegie Mellon University*
Charles Wright, *Portland State University*
Xinyu Xing, *Penn State University*
Min Xu, *Mastercard*
Zhaoyan Xu, *Palo Alto Networks*
Fabian Yamaguchi, *ShiftLeft*
Attilla Altay Yavuz, *University of South Florida*
Yuval Yarom, *University of Adelaide and Data61*
Yanfang (Fanny) Ye, *Case Western Reserve University*
Ting-Fang Yen, *DataVisor*
Katsunari Yoshioka, *Yokohama National University*
Fengwei Zhang, *SUSTech*
Jialong Zhang, *ByteDance AI Lab*
Yupeng Zhang, *Texas A&M University*
Mary Ellen Zurko, *MIT Lincoln Laboratory*