37th Annual Computer Security Applications Conference (ACSAC 2021)

December 6-10, 2021 · Austin, TX, USA

Statement on COVID-19

We are constantly monitoring the COVID-19 status and we are hopeful that by December travel restrictions will be lifted. If that is not the case or only partial restrictions are lifted or due to health concerns, we will accommodate remote presenters in case any accepted authors are unable to travel to the venue.

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 23~~ June 28, 23:59:59 (AoE – UTC-12)
- Notification to authors: August 19 (Early reject notification: July 25)

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.

Ethical Considerations

If human subjects are involved in the submission, authors need to discuss in the paper how the ethical concerns are addressed. If an impactful vulnerability is reported in the paper, the author should discuss their plan for responsible disclosure. The chairs will contact the authors in case of major concerns and may reject a submission if ethical concerns are not sufficiently addressed.

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. For those who decide to submit artifacts, please indicate your willingness of artifact submission (by ticking the appropriate checkbox) during the paper submission. **Authors are encouraged to submit artifacts (with proper anonymization) early, immediately after their papers advance to the second round.** Good artifacts will contribute positively to the paper evaluation. However, authors can still choose to submit artifacts after their papers get accepted. The PC will provide more details about artifact submission in due time.

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. Authors with ACM Artifact Evaluated badges are especially encouraged to submit to the *ACM DTRAP* special issue.

Program Committee

Heng Yin, UC Riverside (Program Chair)
Gabriela Ciocarlie, Elpha Secure (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, Penn State University
Aisha Ali-Gombe, Towson University
Qi Alfred Chen, UC Irvine
Andrea Lanzi, University of Milan
Andrew Paverd, Microsoft Research Cambridge
Anna Squicciarini, Penn State University
Anupam Das, North Carolina State University
Aravind Prakash, Binghamton University
Attilla Altay Yavuz, University of South Florida
Behnaz Hassanshahi, Oracle Labs Australia
Benjamin E. Ujcich, Georgetown University
Berkay Celik, Purdue University
Bimal Viswanath, Virginia Tech
Brendan Saltaformaggio, Georgia Tech
Carrie Gates, Bank of America
Christophe Hauser, University of Southern California/ISI
Dave (Jing) Tian, Purdue University
Ding Wang, Nankai University
Dolière Francis Somé, CISPA
Elena Ferrari, University of Insubria
Elias Athanasopoulos, University of Cyprus
Elizabeth Stobert, Carleton University
Eugene Vasserman, Kansas State University
Evangelos Markatos, FORTH and University of Crete
Lannan (Lisa) Luo, University of South Carolina
Lejla Batina, Radboud University
Lingwei Chen, Penn State University
Long Cheng, Clemson University
Magnus Almgren, Chalmers University of Technology
Manuel Egele, Boston University
Martin Johns, TU Braunschweig
Maverick Woo, Carnegie Mellon University
Michel van Eeten, TU Delft
Min Xu, Mastercard
Ming Li, University of Arizona
Mu Zhang, University of Utah
Neil Gong, Duke University
Nitesh Saxena, University of Alabama at Birmingham
Patrick Schaumont, Worcester Polytechnic Institute
Qi Li, Tsinghua University
Qian Feng, Baidu USA
Roberto Perdisci, University of Georgia
Sang Kil Cha, KAIST
Sangho Lee, Microsoft Research
Sarah Chmielewski, MIT Lincoln Laboratory
Sébastien Bardin, CEA, France
Seungwon Shin, KAIST
Sooel Son, KAIST
Shagufta Mehnaz, Dartmouth College

Fabian Yamaguchi, ShiftLeft
Fengjun Li, University of Kansas
Fengwei Zhang, Southern University of Science and Technology
Gang Wang, University of Illinois at Urbana-Champaign
Giancarlo Pellegrino, CISPA
Gianluca Stringhini, Boston University
Haya Shulman, Fraunhofer SIT
Hayawardh Vijayakumar, Samsung Research America
Hongxin Hu, University at Buffalo, SUNY
Hussain Almohri, Kuwait University
Jarilyn Hernández, MIT Lincoln Laboratory
Jeyavijayan Rajendran, Texas A&M University
Jialong Zhang, ByteDance
Jie Yang, Florida State University
Jin-Hee Cho, Virginia Tech
Juan Tapiador, Universidad Carlos III de Madrid
Julie Haney, National Institute of Standards and Technology
Katsunari Yoshioka, Yokohama National University
Kevin Alejandro Roundy, NortonLifelock Research Group
Kun Sun, George Mason University
Vasileios Kemerlis, Brown University
Wendy (Hui) Wang, Stevens Institute of Technology
Xiaojing Liao, Indiana University Bloomington
Xiaokui Shu, IBM Research
Xiaoyan Sun, California State University, Sacramento
Xiapu Luo, The Hong Kong Polytechnic University
Yanfang (Fanny) Ye, Case Western Reserve University
Yanick Fratantonio, Cisco Talos
Yao Liu, University of South Florida
Yingying Chen, Rutgers University
Yonghwi Kwon, University of Virginia
Yousra Aafer, University of Waterloo
Yuan Tian, University of Virginia
Yue Duan, Illinois Institute of Technology
Yuval Yarom, University of Adelaide and Data61
Zachary Tudor, Idaho National Laboratory
Zhaoyan Xu, Bytedance
Zhiqiang Lin, Ohio State University
Shanchieh (Jay) Yang, Rochester Institute of Technology
Thang Hoang, Virginia Tech