35th Annual Computer Security Applications Conference (ACSAC 2019)

December 9-13, 2019 • San Juan, Puerto Rico, 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/.

Important Dates:

- Paper submission deadline: June 8, 23:59:59 (anywhere)
- Early reject notification: July 24
- Notification to authors: August 23

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. This year, ACSAC 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 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, ACSAC encourages authors of accepted papers to submit software and data artifacts and make them publicly available to the entire community. These artifacts are **not** part of the paper evaluation. Their submission is strictly optional and occurs only after a paper has been accepted. Authors who decide to

participate in this program will interact with a special committee dedicated to verifying 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 want to submit (software, data, or both) and the verification procedure 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 *for a minimum period* of three months between October and December 2019. We plan to reward authors who participate in this program with a special mention during the conference and on the ACSAC webpage, a stamp of reproducibility on their papers, and (if enough authors participate to the program) by reserving a Distinguished Paper Award for this group.

Program Committee

Guofei Gu, Texas A&M University (Program Chair)
Danfeng (Daphne) Yao, Virginia Tech (Program Co-Chair)
Roberto Perdisci, University of Georgia (Artifact Evaluation Chair)

Yousra Aafer, Purdue University
Ehab Al-Shaer, UNC Charlotte
Magnus Almgren, Chalmers University of Technology
Elias Athanasopoulos, University of Cyprus
Adam Aviv, U.S. Naval Academy
Tiffany Bao, Arizona State University
Leyla Bilge, Symantec Research Lab
Lorenzo Cavallaro, King's College London
Yingying Chen, Rutgers University
Sarah Chmielewski, MIT Lincoln Laboratory
Jin-Hee Cho Virginia Tech
Cristina Cifuentes, Oracle Labs Australia
Adam Doupe, Arizona State University
Manuel Egele, Boston University
William Enck, North Carolina State University
Yanick Fratantonio, Eurecom
Carrie Gates, Securelytix
Neil Gong, Iowa State University
Christophe Hauser, University of Southern California
Amir Houmansadr, University of Massachussetts, Amherst
Hongxin Hu, Clemson University
Martin Johns, SAP
Alexandros Kapravelos, North Carolina State University
Vasileios Kemerlis, Brown University
Florian Kerschbaum, University of Waterloo
Yonghwi Kwon, University of Virginia
Andrea Lanzi, University of Milan
Sangho Lee, Microsoft Research
Fengjun Li, University of Kansas
Qi Li, Tsinghua University
Xiaojing Liao, Indiana University Bloomington
Zhiqiang Lin, Ohio State
Martina Lindorfer, TU Wien
Lannan (Lisa) Luo, University of South Carolina
Xiapu Luo, The Hong Kong Polytechnic University
Di Ma, University Michigan - Dearborn
Morley Mao, University of Michigan
Evangelos Markatos, FORTH
Collin Mulliner, Cruise Automation
Giancarlo Pellegrino, Saarland University
Chunyi Peng, Purdue University
Roberto Perdisci, University of Georgia
Christina Popper, NYU Abu Dhabi
Jeyavijayan Rajendran, Texas A&M University
Konrad Rieck, Technische Universität Braunschweig,
Kevin Alejandro Roundy, Symantec Research Labs
Nitesh Saxena, University of Alabama at Birmingham
Patrick Schaumont, Virginia Tech
Kent Seamons, Brigham Young University
Seungwon Shin, KAIST, Korea
Xiaokui Shu, IBM Research
Claudio Soriente, NEC Labs Europe
Anna Squicciarini, Penn State University
Ben Stock, CISPA Helmholtz Center i.G.
Gianluca Stringhini, University College London
Kun Sun, George Mason University
Xiaoyan Sun, California State University, Sacramento
Yixin Sun, Princeton University
Juan Tapiador, Universidad Carlos III de Madrid
Michel van Eeten, Delft University of Technology
Hayawardh Vijayakumar, Samsung Research America
Bimal Viswanath, Virginia Tech
Cong Wang, City University of Hong Kong
Gang Wang, Virginia Tech
Hui (Wendy) Wang, Stevens Institute of Technology
Maverick Woo, Carnegie Mellon University
Charles Wright, Portland State University
Xinyu Xing, Penn State University
Zhaoyan Xu, Palo Alto Networks
Fabian Yamaguchi, ShiftLeft
Attilla Altay Yavuz, University of South Florida
Yanfang (Fanny), Ye West Virginia University
Ting-Fang Yen, DataVisor
Heng Yin, UC Riverside
Katsunari Yoshioka, Yokohama National University
Daniel Zappala, Brigham Young University
Fengwei Zhang, Wayne State University
Jialong Zhang, ByteDance AI Lab
Yupeng Zhang, Texas A&M University

The full version of this CFP is available at https://www.acsac.org/2019/cfp/.
For additional information please contact program@acsac.org.