CALL FOR PAPERS

ACM WiSec 2020

13th ACM Conference on Security and Privacy in Wireless and Mobile Networks

https://wisec2020.ins.jku.at/

The 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks (ACM WiSec 2020) will be held in **Linz, Austria** from **July 8 to July 10, 2020**.

ACM WiSec is the leading ACM and SIGSAC conference dedicated to all aspects of security and privacy in wireless and mobile networks and their applications. In addition to the traditional ACM WiSec topics of physical, link, and network layer security, we welcome papers focusing on the increasingly diverse range of mobile or wireless applications such as Internet of Things, Cyber-Physical Systems, as well as the security and privacy of mobile software platforms, usable security and privacy, biometrics, and cryptography.

The conference welcomes both theoretical as well as systems contributions. Topics of interest include, but are not limited to

- Cryptographic primitives for wireless and mobile security
- Data-driven security attacks and counter measures
- Economics of mobile security and privacy
- Jamming attacks and defenses
- Key management (agreement or distribution) for wireless or mobile systems
- Mobile malware and platform security
- NFC and smart payment applications
- Next generation cellular network fraud and security
- Physical tracking security and privacy
- Resilience and dependability for mobile and wireless networks

- Security and privacy for cognitive radio and dynamic spectrum access systems
- Security and privacy for mobile applications (e.g., mobile sensing systems)
- Security and privacy for smart devices (e.g., smartphones)
- Secure localization and location privacy
- Security protocols for wireless networking
- Theoretical and formal approaches for wireless and mobile security
- Usable mobile security and privacy
- Vehicular networks security (e.g., drones, automotive, avionics, autonomous driving)
- Wireless and mobile privacy and anonymization techniques
- Wireless or mobile security for cyber-physical systems (e.g, healthcare, smart grid) and IoT systems
- Wireless network security for critical infrastructures

The proceedings of ACM WiSec, sponsored by SIGSAC, will be published by the ACM.

Important dates

- Paper submission deadline: **EXTENDED: March 13, 2020 (23:59 AoE)**
  ~~February 28, 2020 (23:59 AoE)~~
- Author notification: April 24, 2020
- Camera-ready deadline: May 15, 2020 (23:59 AoE)
- WiSec conference: July 8 - 10, 2020

Full and short papers

Full paper submissions to ACM WiSec 2020 can be up to 10 pages in the ACM conference style excluding the bibliography and well-marked appendices, and up to 12 pages in total. ACM WiSec also encourages the submission of short papers with a length of up to 6 pages (including bibliography and appendices), which describe mature work of a more succinct nature. All papers must be thoroughly anonymized for double-blind reviewing. Detailed submission instructions are available on the WiSec 2020 website at https://wisec2020.ins.jku.at/submission-guidelines/.

Opinion papers

ACM WiSec 2020 invites papers (ACM conference style, up to 3 pages excluding references) that present personal perspectives on all aspects of security and privacy in wireless and mobile networks.

Opinion papers could also criticize previous research or research directions, as well as highlight possible promising research directions. The opinions expressed in these papers are expected to be anyway corroborated by theoretical foundations, experiments, or experiences. Like the

regular papers, the opinion papers will be reviewed by the WiSec Technical Program Committee. The selected opinion papers will be a part of the WiSec technical program and will be published in the conference proceedings. Opinion papers should be submitted using the same submission procedure adopted for the full papers. The title of these papers must have the prefix "OPINION: ".

Posters and demos

WiSec also solicits submission of posters and demos. The instructions to submit posters/ demos are available on the WiSec 2020 website at https://wisec2020.ins.jku.at/call-for-posters-and-demos/.

Replicability label

The goal of the replicability label is to support replicability in mobile and wireless security experimental research process and to increase the impact of mobile and wireless research, enable dissemination of research results, sharing of code and experiments setups, and to enable the research community to build on prior experimental results. WiSec will follow the ACM policy on artifact review and badging. Towards this goal, the WiSec replicability label recognizes papers whose results were replicated by an independent group of researchers. Authors of accepted papers can participate in this voluntary process by submitting their experiments according to the replicability evaluation instructions.

Authors are encouraged to plan ahead when running their experiments to minimize the overhead of applying for this label.

Double submissions

It is a policy of the ACM to disallow double submissions, where the same (or substantially similar) paper is concurrently submitted to multiple conferences/journals. Any double submissions detected will be immediately rejected from all conferences/journals involved.

Organisation committee

General chairs

- René Mayrhofer, *Johannes Kepler University Linz, Linz, Austria*
- Michael Roland, *Johannes Kepler University Linz, Linz, Austria*

PC chairs

- Matthias Hollick, *Technische Universität Darmstadt, Darmstadt, Germany*
- Wenjing Lou, *Virginia Tech, Blacksburg, VA, USA*

Program committee

- Ravishankar Borgaonkar, *SINTEF Digital and University of Stavanger, Norway*
- Kevin Butler, *University of Florida, USA*
- Srdjan Capkun, *ETH Zurich, Switzerland*
- Bogdan Carbunar, *Florida International University, USA*
- Yimin Chen, *Virginia Tech, USA*
- Yingying Chen, *Rutgers University, USA*
- Mauro Conti, *University of Padua, Italy*
- Mathieu Cunche, *University of Lyon / Inria, France*
- Adrian Dabrowski, *University of California, Irvine, USA*
- Karim Eldefrawy, *SRI International, USA*
- William Enck, *North Carolina State University, USA*
- Yanick Fratantonio, *EURECOM, France*
- Ryan Gerdes, *Virginia Tech, USA*
- Jun Han, *National University of Singapore, Singapore*
- Matthias Hollick, *Technische Universität Darmstadt, Germany*
- Hongxin Hu, *Clemson University, USA*
- Yier Jin, *University of Florida, USA*
- Sneha Kumar Kasera, *University of Utah, USA*
- Nicola Laurenti, *University of Padua, Italy*
- Loukas Lazos, *University of Arizona, USA*
- Vincent Lenders, *armasuisse, Switzerland*
- Ming Li, *University of Arizona, USA*
- Wenjing Lou, *Virginia Tech, USA*
- Zhuo Lu, *University of South Florida, USA*
- Ivan Martinovic, *University of Oxford, UK*
- Aziz Mohaisen, *University of Central Florida, USA*
- Collin Mulliner, *cruise, USA*
- Adwait Nadkarni, *William & Mary, USA*
- Guevara Noubir, *Northeastern University, USA*
- Panos Papadimitratos, *KTH Royal Institute of Technology, Sweden*
- Roberto Di Pietro, *Hamad Bin Khalifa University, Qatar*
- Christina Poepper, *New York University Abu Dhabi, UAE*
- Aanjhan Ranganathan, *Northeastern University, USA*
- Kasper Rasmussen, *University of Oxford, UK*
- Brad Reaves, *North Carolina State University, USA*
- Ahmad-Reza Sadeghi, *Technische Universität Darmstadt, Germany*
- Merve Sahin, *SAP Security Research, France*
- Nitesh Saxena, *The University of Alabama at Birmingham, USA*
- Jens Schmitt, *TU Kaiserslautern, Germany*
- Matthias Schunter, *Intel Labs, USA*
- Claudio Soriente, *NEC Laboratories Europe, Germany*
- Angelos Stavrou, *George Mason University, USA*

- Wenhai Sun, *Purdue University, USA*
- Patrick Tague, *Carnegie Mellon University, USA*
- Nils Ole Tippenhauer, *CISPA – Helmholtz Center for Information Security, Germany*
- Patrick Traynor, *University of Florida, USA*
- Selcuk Uluagac, *Florida International University, USA*
- Mathy Vanhoef, *New York University Abu Dhabi, UAE*
- Jie Yang, *Florida State University, USA*
- Attila Yavuz, *University of South Florida, USA*
- Yves Younan, *Cisco Talos, USA*
- Kai Zeng, *George Mason University, USA*
- Fengwei Zhang, *Southern University of Science and Technology (SUSTech), China*
- Ning Zhang, *Washington University in St. Louis, USA*
- Rui Zhang, *University of Delaware, USA*
- Yanchao Zhang, *Arizona State University, USA*
- Zhenghao Zhang, *Florida State University, USA*
- Yao Zheng, *University of Hawai'i at Mānoa, USA*
- Ting Zhu, *University of Maryland, Baltimore County, USA*

Program committee – Posters and Demos

- Giovanni Camurati, *EURECOM, France*
- Merlin Chlosta, *Ruhr University Bochum, Germany*
- Célestin Matte, *Inria, France*
- Dario Nisi, *EURECOM, France*
- Pieter Robyns, *UHasselt – tUL / imec, Belgium*
- David Rupprecht, *Ruhr University Bochum, Germany*
- Domien Schepers, *Northeastern University, USA*
- Lennert Wouters, *COSIC, KU Leuven / imec, Belgium*