ACM WiSec 2019

Call for Papers

12th ACM Conference on Security and Privacy in Wireless and Mobile Networks

https://wisec19.fiu.edu/

ACM WiSec 2019 will run from May 15 to May 17, 2019 in Miami beach, USA.

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, and 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:

- Security protocols for wireless networking
- Security & privacy for smart devices (e.g., smartphones)
- Security of mobile applications for smartphones and wearables
- Wireless and mobile privacy and anonymity
- Secure localization and location privacy
- Cellular network fraud and security
- Jamming attacks and defenses
- Key management (agreement or distribution) for wireless or mobile systems
- Theoretical and formal approaches for wireless and mobile security
- Physical layer and Information-theoretic security schemes for wireless systems
- Cryptographic primitives for wireless and mobile security
- NFC and smart payment applications
- Security and privacy for mobile sensing systems
- Wireless or mobile security for Cyber-Physical Systems (e.g, healthcare, smart grid, or IoT applications)
- Vehicular networks security (e.g., drones, automotive, avionics, autonomous driving)
- Physical tracking security and privacy
- Usable mobile security and privacy
- Economics of mobile security and privacy
- Mobile malware and platform security
- Security for cognitive radio and dynamic spectrum access systems

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

Important Dates

Abstract submission: January 18th (open until paper submission deadline)
Paper submission: January 25th
Author notification: March 1st
Camera ready: April 8th
WiSec conference: May 15th-17th

Full and short papers

Full paper submissions to ACM WiSec 2019 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, which describe mature work of a more succinct nature. All papers must be thoroughly anonymized for double-blind reviewing. Detailed submission instructions will appear on the conference website.

Opinion papers

ACM WiSec 2019 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:".

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.

Posters and Demos

WiSec also solicits submission of posters and demos. The instructions to submit posters/demos will be made available later on WiSec 2019 website.

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 Chair:

- Selcuk Uluagac, Florida International University

PC co-Chairs:

- Yingying (Jennifer) Chen, Rutgers University
- Aurélien Francillon, EURECOM

Program Committee

David Barrera, Polytechnique Montreal, CA
Ravi Borgaonkar, SINTEF Digital, Norway
Kevin Butler, University of Florida, USA
Bogdan Carbunar, Florida International University , USA
Mauro Conti, University of Padua, Italy
Mathieu Cunche, INSA Lyon, France
Sophia D'antoine, Trails of bits, USA
Roberto Di Pietro, Hamad Bin Khalifa University, USA
Adam Doupe , Arizona State University, USA
Karim Eldefrawy, SRI International, USA
William Enck, NC State University, USA
Yanick Fratantonio, EURECOM, France
Paolo Gasti, New York Institute of Technology, USA
Jun Han, National University of Singapore, Singapore
Matthias Hollick, Technical University Darmstadt , Germany
Yier Jin, University of Florida, USA
Sneha Kasera, University of Utah, USA
Nicola Laurenti, University of Padua, Italy
Loukas Lazos, University of Arizona, USA
Vincent Lenders, armasuisse, Switzerland
Ming (Fred) Li, University of Arizona, USA
Wenjing Lou, Virginia Tech, USA
Di Ma, University of Michigan, USA
Michail Maniatakos, New York University Abu Dhabi, UAE
Ivan Martinovic, University of Oxford, UK
Collin Mulliner , Cruise Automation, USA
Divya Muthukumaran, Imperial College London, UK
Adwait Nadkarni, William & Mary, USA
Guevara Noubir, Northeastern University, USA
Christina Poepper, New York University Abu Dhabi, UAE
Aanjhan Ranganathan, Northeastern University, USA
Kasper Bonne Rasmussen, University of Oxford, UK
Bradley Reaves, NC State University, USA
Ahmad-Reza Sadeghi, Technische Universität Darmstadt, Germany
Merve Sahin, SAP Labs, France
Nitesh Saxena, University of Alabama at Birmingham, USA
Jens Schmitt, TU Kaiserslautern, Germany
Matthias Schunter, Intel Lab , Germany
Claudio Soriente, NEC Labs, Spain
Patrick Tague, Carnegie Mellon University, USA
Nils Ole Tippenhauer, Cispa / CISPA Helmholtz Center for Information Security, Germany
Patrick Traynor, University of Florida, USA
Mathy Vanhoef, New York University Abu Dhabi, UAE
Jie Yang, Florida State University, USA