July 8–10, 2020 Linz (Virtual Event), Austria



Association for Computing Machinery

Advancing Computing as a Science & Profession

WiSec'20

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

Sponsored by: ACM SIGSAC in cooperation with ACM SIGMOBILE

Supported by: Johannes Kepler University Linz, Institute of Networks and Security



Association for Computing Machinery

Advancing Computing as a Science & Profession

The Association for Computing Machinery 2 Penn Plaza, Suite 701 New York, New York 10121-0701

Copyright © 2020 by the Association for Computing Machinery, Inc. (ACM). Permission to make digital or hard copies of portions of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyright for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permission to republish from permissions@acm.org or Fax +1212 869-0481.

For other copying of articles that carry a code at the bottom of the first or last page, copying is permitted provided that the per-copy fee indicated in the code is paid through www.copyright.com.

Notice to Past Authors of ACM-Published Articles

ACM intends to create a complete electronic archive of all articles and/or other material previously published by ACM. If you have written a work that has been previously published by ACM in any journal or conference proceedings prior to 1978, or any SIG Newsletter at any time, and you do NOT want this work to appear in the ACM Digital Library, please inform permissions@acm.org, stating the title of the work, the author(s), and where and when published.

ISBN: 978-1-4503-8006-5

Additional copies may be ordered prepaid from: ACM Order Department PO Box 30777 New York, NY 10087-0777, USA

Phone: +1 800 342-6626 (USA and Canada) +1 212 626-0500 (Global) Fax: +1 212 944-1318 Email: acmhelp@acm.org Hours of Operation: 8:30 am-4:30 pm ET

Message from the Chairs

We are very pleased to welcome you to the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks. This year's WiSec marks the first virtual WiSec conference and we are both excited to try out this conference format and regretful to not be able to welcome you in the beautiful city of Linz, Austria, due to the ongoing SARS-CoV-2 pandemic. ACM WiSec 2020 continues to be the premier venue for research dedicated to all aspects of security and privacy in wireless and mobile networks, their systems, and their applications. The program will be presented online in a single track, along with a poster and demonstration session. WiSec 2020 will be open at no extra cost to everyone and we are trying out new formats such as a mixture of live streams, pre-recorded talks, and interactive Q/A sessions.

The technical program this year features 30 outstanding papers: 27 full and 3 short papers, that cover a wide variety of security and privacy problems relating to wireless networking, mobile networks, wearables, user interactions, cyber physical systems, vehicles and transportation, jamming, smart devices, and emerging applications. We continue with the replicability label and have some 7 papers that successfully applied and made all artefacts available that are required to reproduce the work.

Our call for papers attracted 104 qualified submissions from across the globe, which demonstrates the continuous growth of this topic area. These were carefully reviewed by 57 technical program committee (TPC) members from academia, industrial research labs, and federal organizations, along with a selected group of external experts. The TPC was formed with the goal of covering diverse research expertise as well as diverse perspectives and approaches.

The paper review process was double-blind, and the vast majority (85) of the papers received four or more reviews. The review period was accompanied by thorough online discussions. Despite the ongoing SARS-CoV-2 pandemic we managed to stick to our original timeline with tight time constraints on the review process, arriving at decisions some six weeks after the paper submission deadline. This is among the fastest turnaround times for any conference or journal; receiving high quality peer reviews in a short time frame is a great asset for authors, but it means considerable effort for the program committee, which deserves an extra thank you to our dedicated TPC members.

WiSec's exciting technical program is enriched by two keynote talks delivered by distinguished leaders in the field of wireless and mobile security and privacy: Prof. Panos Papadimitratos from

the KTH Royal Institute of Technology in Stockholm and Richard Grisenthwaite, Chief Architect & Fellow at Arm Limited. Warm thanks to both keynote speakers for joining us.

With moving virtual, this year, the WiSec Posters & Demos session gets an upgrade. It will feature three parallel sessions of three/four slots each. Authors will prepare a short video to be shown at the beginning of their slot. The accepted eleven posters/demos provide early results and exciting practical prototypes.

Putting together WiSec 2020 was a team effort. We express our sincere gratitude to many for their hard work and contributions. First, we thank all the authors who submitted their great research to the conference. We are truly grateful to all the TPC members and reviewers – their dedication and enthusiasm in the short-time review process were instrumental in constructing the strong technical program; some of them deserve additional thanks for accepting to act as session chairs. We also thank the entire WiSec 2020 organizing team, especially the Publication Co-Chairs Max Maass and Yao Zheng, the Poster/Demo Co-Chairs Merve Sahin and Mathy Vanhoef, the Replicability Committee and its Co-Chairs Aanjhan Ranganathan and Yao Zheng, the Web Chair Daniel Hofer, the Publicity Co-Chairs Kai Jansen and Feng Lin and all the volunteers of the local (now virtual) arrangements team for their tremendous support and behind-the-scenes effort. Finally, we extend our thanks and appreciation to the WiSec Steering Committee and past WiSec chairs for their guidance and wisdom.

Finally, many thanks go to Johannes Kepler University Linz and to the ACM, SIGSAC, and NSF for their continuing sponsorship and support, notably for student travel grants which would be extended to next year's conference. Again, welcome to WiSec 2020, the first online WiSec which brings leading researchers together to promote the exchange of thoughts and ideas on the latest advances in the area of security and privacy in wireless and mobile networks.

René Mayrhofer General Co-Chairs Johannes Kepler University Linz Linz, AT

Matthias Hollick, Program Co-Chairs

TU-Darmstadt Darmstadt, DE

Max Maaß

Publication Co-Chairs TU-Darmstadt Darmstadt, DE

Michael Roland

General Co-Chairs Johannes Kepler University Linz Linz, AT

Wenjing Lou Program Co-Chairs Virginia Tech

Blacksburg, US

Yao Zheng

Publication Co-Chairs University of Hawaii at Manoa Honolulu, US

Contents

KRATOS: Multi-User Multi-Device-Aware Access Control System for the Smart Home
Hacksaw: Biometric-Free Non-Stop Web Authentication in an Emerging World of Wearables 13 Prakash Shrestha, Nitesh Saxena (<i>University of Alabama at Birmingham</i>)
ivPair: Context-Based Fast Intra-Vehicle Device Pairing for Secure Wireless Connectivity 25 Kyuin Lee (<i>University of Wisconsin-Madison</i>); Neil Klingensmith (<i>Loyola University Chicago</i>); Dong He, Suman Banerjee, Younghyun Kim (<i>University of Wisconsin-Madison</i>)
Acoustic Integrity Codes: Secure Device Pairing Using Short-Range Acoustic Communication 31 Florentin Putz, Flor Álvarez, Jiska Classen (<i>TU Darmstadt, Germany</i>)
GNSS Spoofing Detection via Opportunistic IRIDIUM Signals
MAVPro: ADS-B Message Verification for Aviation Security with Minimal Numbers of On-Ground
Sensors53Ala' Darabseh, Hoda AlKhzaimi, Christina Pöpper (New York University Abu Dhabi)
SVM: Secure Vehicle Motion Verification with a Single Wireless Receiver
Zigator: Analyzing the Security of Zigbee-Enabled Smart Homes
Truncate after Preamble: PHY-based Starvation Attacks on IoT Networks
Countering Cross-technology Jamming Attack
MagicPairing: Apple's Take on Securing Bluetooth Peripherals
BaseSAFE: Baseband SAnitized Fuzzing through Emulation 122 Dominik Maier, Lukas Seidel, Shinjo Park (<i>TU Berlin</i>)
Analyzing the Attack Landscape of Zigbee-enabled IoT Systems and Reinstating Users' Privacy133Weicheng Wang, Fabrizio Cicala, Syed Rafiul Hussain, Elisa Bertino, Ninghui Li (Purdue University)133

An Empirical Study of Potentially Malicious Third-Party Libraries in Android Apps 14 Zicheng Zhang, Wenrui Diao, Chengyu Hu, Shanqing Guo (<i>Shandong University</i>); Chaoshun Zuo (<i>Ohio State University</i>); Li Li (<i>Monash University</i>)	4
Protecting Wi-Fi Beacons from Outsider Forgeries	55
Practical Operation Extraction from Electromagnetic Leakage for Side-Channel Analysis and Revers Engineering	;e 51
Secure and User-Friendly Over-the-Air Firmware Distribution in a Portable Faraday Cage 17 Martin Striegel, Florian Jakobsmeier, Johann Heyszl (<i>Fraunhofer AISEC</i>); Yacov Matveev, Georg Sigl (<i>Technical University of Munich</i>)	73
Lost and Found: Stopping Bluetooth Finders from Leaking Private Information	34
iRyP: A Purely Edge-based Visual Privacy-Respecting System for Mobile Cameras 19 Yuanyi Sun, Shiqing Chen, Sencun Zhu (<i>The Pennsylvania State University</i>); Yu Chen (<i>SUNY at</i> <i>Binghamton</i>)) 5
Peek-a-Boo: I see your smart home activities, even encrypted! 20 Abbas Acar (Florida International University); Hossein Fereidooni, Tigist Abera (Technical University of Darmstadt); Amit Kumar Sikder (Florida International University); Markus Miettinen (Technical University of Darmstadt); Hidayet Aksu (Florida International University); Markus Oconti (University of Padua); Ahmad-Reza Sadeghi (Technical University of Darmstadt); Selcuk Uluagac (Florida International University) International University))7
Process Skew: Fingerprinting the Process for Anomaly Detection in Industrial Control Systems . 21 Chuadhry Mujeeb Ahmed (<i>Singapore University of Technology and Design</i>); Jay Prakash (<i>SUTD,</i> <i>SINGAPORE</i>); Rizwan Qadeer (<i>GCL Technologies Luxembourg</i>); Anand Agrawal (<i>NYU Abu Dhabi</i>); Jianying Zhou (<i>SUTD</i>)	9
BrokenStrokes: On the (in)Security of Wireless Keyboards	31
Spotr: GPS Spoofing Detection via Device Fingerprinting	1 2
Fingerprinting Encrypted Voice Traffic on Smart Speakers with Deep Learning 25 Chenggang Wang, Sean Kennedy, Haipeng Li, King Hudson, Gowtham Atluri (<i>University of Cincinnati,</i> <i>Cincinnati, USA</i>); Xuetao Wei (<i>Southern University of Science and Technology, China</i>); Wenhai Sun (<i>Purdue University, West Lafayette, USA</i>); Boyang Wang (<i>University of Cincinnati, Cincinnati, USA</i>)	;4

Protecting Location Privacy from Untrusted Wireless Service Providers	66
Valkyrie: A Generic Framework for Verifying Privacy Provisions in Wireless Networks 27 Guillaume Celosia, Mathieu Cunche (<i>Univ Lyon, INSA Lyon, Inria, CITI</i>)	78
A Plug-n-Play Game Theoretic Framework For Defending Against Radio Window Attacks 28 Pruthuvi Maheshakya Wijewardena, Aditya Bhaskara, Sneha Kumar Kasera, Syed Ayaz Mahmud (<i>University of Utah</i>); Neal Patwari (<i>Washington University in St. Louis</i>)	84
Paging Storm Attacks against 4G/LTE Networks from Regional Android Botnets: Rationale,Practicality, and Implications29Kaiming Fang (Binghamton University); Guanhua Yan (Binghamton University, State University of New York)	95
ChirpOTLE: A Framework for Practical LoRaWAN Security Evaluation	06
Security in Terahertz WLANs with Leaky Wave Antennas	317
DEMO: Attaching InternalBlue to the Proprietary macOS IOBluetooth Framework	28
DEMO: BTLEmap: Nmap for Bluetooth Low Energy	31
DEMO: ColoT: A Consent and Information assistant for the IoT	34
DEMO: Extracting Physical-Layer BLE Advertisement Information from Broadcom and Cypress Chips 33 Jiska Classen, Matthias Hollick (SEEMOO, TU Darmstadt)	37
Demo: iJam with Channel Randomization	40
DEMO: RESCURE: Retrofit Security for Critical Infrastructures	43
DEMO: Venom: a Visual and Experimental Bluetooth Low Energy Tracking System	46

POSTER: AcousticPrint: Acoustic Signature based Open Set Drone Identification	9
Poster: AnaMPhy: Anonymity Assisted Secret Refreshment at the Physical Layer	1
POSTER: SemperFi: A Spoofer Eliminating Standalone GPS Receiver	3
POSTER: Unprotected geo-localisation data through ARGOS satellite signals: The risk ofcyberpoaching	6