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
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

| Title                                                                 | Page |
|----------------------------------------------------------------------|------|
| KRATOS: Multi-User Multi-Device-Aware Access Control System for the Smart Home | 1    |
| Amit Kumar Sikder, Leonardo Babun (Florida International University); Z. Berkay Celik (Purdue University); Abbas Acar, Hidayet Aksu (Florida International University); Patrick McDaniel (Penn State University); Engin Kirda (Northeastern University); Selcuk Uluagac (Florida International University) |      |
| Hacksaw: Biometric-Free Non-Stop Web Authentication in an Emerging World of Wearables | 13   |
| Prakash Shrestha, Nitesh Saxena (University of Alabama at Birmingham) |      |
| ivPair: Context-Based Fast Intra-Vehicle Device Pairing for Secure Wireless Connectivity | 25   |
| Kyuin Lee (University of Wisconsin-Madison); Neil Klingensmith (Loyola University Chicago); Dong He, Suman Banerjee, Younghyun Kim (University of Wisconsin-Madison) |      |
| Acoustic Integrity Codes: Secure Device Pairing Using Short-Range Acoustic Communication | 31   |
| Florentin Putz, Flor Álvarez, Jiska Classen (TU Darmstadt, Germany) |      |
| GNSS Spoofing Detection via Opportunistic IRIDIUM Signals | 42    |
| Gabriele Oligeri (Hamad Bin Khalifa University - College of Science and Engineering - Division of Information and Computing Technology); Savio Sciancalepore (Hamad Bin Khalifa University - College of Science and Engineering); Roberto Di Pietro (Hamad Bin Khalifa University (HBKU) - College of Science and Engineering (CSE)) |      |
| MAVPro: ADS-B Message Verification for Aviation Security with Minimal Numbers of On-Ground Sensors | 53    |
| Ala' Darabseh, Hoda AlKhzaimi, Christina Pöpper (New York University Abu Dhabi) |      |
| SVM: Secure Vehicle Motion Verification with a Single Wireless Receiver | 65    |
| Mingshun Sun, Yanmao Man, Ming Li (The University of Arizona); Ryan Gerdes (Virginia Tech) |      |
| Zigator: Analyzing the Security of Zigbee-Enabled Smart Homes | 77    |
| Dimitrios-Georgios Akestoridis, Madhumitha Harishankar, Michael Weber (Carnegie Mellon University); Patrick Tague (CMU) |      |
| Truncate after Preamble: PHY-based Starvation Attacks on IoT Networks | 89    |
| Stefan Gvozdenovic, Johannes K. Becker, John Mikulskis, David Starobinski (Boston University) |      |
| Countering Cross-technology Jamming Attack | 99    |
| Zicheng Chi, Yan Li, Xin Liu, Wei Wang, Yao Yao, Ting Zhu (University of Maryland Baltimore County); Yanchao Zhang (Arizona State University) |      |
| MagicPairing: Apple's Take on Securing Bluetooth Peripherals | 111   |
| Dennis Heinze, Jiska Classen (TU Darmstadt, SEEMOO); Felix Rohrbach (TU Darmstadt, Cryptoplexity) |      |
| BaseSAFE: Baseband SAnitized Fuzzing through Emulation | 122   |
| Dominik Maier, Lukas Seidel, Shinjo Park (TU Berlin) |      |
| Analyzing the Attack Landscape of Zigbee-enabled IoT Systems and Reinstating Users’ Privacy | 133   |
| Weicheng Wang, Fabrizio Cicala, Syed Rafiul Hussain, Elisa Bertino, Ninghui Li (Purdue University) |      |
An Empirical Study of Potentially Malicious Third-Party Libraries in Android Apps
Zicheng Zhang, Wenrui Diao, Chengyu Hu, Shanqing Guo (Shandong University); Chaoshun Zuo (Ohio State University); Li Li (Monash University)

Protecting Wi-Fi Beacons from Outsider Forgeries
Mathy Vanhoef (New York University Abu Dhabi); Prasant Adhikari (New York University); Christina Pöpper (New York University Abu Dhabi)

Practical Operation Extraction from Electromagnetic Leakage for Side-Channel Analysis and Reverse Engineering
Pieter Robyns, Mariano Di Martino (Hasselt University - tUL - Expertise Centre for Digital Media); Dennis Giese (Northeastern University); Wim Lamotte (Hasselt University - tUL - Expertise Centre for Digital Media); Peter Quax (Hasselt University - tUL - Flanders Make - EDM); Guevara Noubir (Northeastern University)

Secure and User-Friendly Over-the-Air Firmware Distribution in a Portable Faraday Cage
Martin Striegel, Florian Jakobsmeier, Johann Heyszl (Fraunhofer AISEC); Yacov Matveev, Georg Sigl (Technical University of Munich)

Lost and Found: Stopping Bluetooth Finders from Leaking Private Information
Mira Weller, Jiska Classen, Fabian Ullrich, Denis Wassmann, Erik Tews (Technical University of Darmstadt, Germany)

iRyP: A Purely Edge-based Visual Privacy-Respecting System for Mobile Cameras
Yuanyi Sun, Shiqing Chen, Sencun Zhu (The Pennsylvania State University); Yu Chen (SUNY at Binghamton)

Peek-a-Boo: I see your smart home activities, even encrypted!
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); Mauro Conti (University of Padua); Ahmad-Reza Sadeghi (Technical University of Darmstadt); Selcuk Uluagac (Florida International University)

Process Skew: Fingerprinting the Process for Anomaly Detection in Industrial Control Systems
Chuadhry Mujeeb Ahmed (Singapore University of Technology and Design); Jay Prakash (SUTD, SINGAPORE); Rizwan Qadeer (GCL Technologies Luxembourg); Anand Agrawal (NYU Abu Dhabi); Jianying Zhou (SUTD)

BrokenStrokes: On the (in)Security of Wireless Keyboards
Gabriele Oligeri (Hamad Bin Khalifa University - College of Science and Engineering - Division of Information and Computing Technology); Savio Sciancalepore, Simone Raponi (Hamad Bin Khalifa University - College of Science and Engineering); Roberto Di Pietro (Hamad Bin Khalifa University (HBKU) - College of Science and Engineering (CSE))

Spotr: GPS Spoofing Detection via Device Fingerprinting
Mahsa Foruhandeh, Abdullah Zubair Mohammed, Gregor Kildow, Paul Burges, Ryan Gerdes (Virginia Tech)

Fingerprinting Encrypted Voice Traffic on Smart Speakers with Deep Learning
Chenggang Wang, Sean Kennedy, Haipeng Li, King Hudson, Gowtham Atluri (University of Cincinnati, Cincinnati, USA); Xuetao Wei (Southern University of Science and Technology, China); Wenhai Sun (Purdue University, West Lafayette, USA); Boyang Wang (University of Cincinnati, Cincinnati, USA)
Protecting Location Privacy from Untrusted Wireless Service Providers .......................... 266
Keen Sung, Brian Neil Levine (University of Massachusetts Amherst); Mariya Zheleva (University at Albany, SUNY)

Valkyrie: A Generic Framework for Verifying Privacy Provisions in Wireless Networks .......................... 278
Guillaume Celosia, Mathieu Cunche (Univ Lyon, INSA Lyon, Inria, CITI)

A Plug-n-Play Game Theoretic Framework for Defending Against Radio Window Attacks .......................... 284
Pruthuvi Maheshakya Wijewardena, Aditya Bhaskara, Sneha Kumar Kasera, Syed Ayaz Mahmud (University of Utah); Neal Patwari (Washington University in St. Louis)

Paging Storm Attacks against 4G/LTE Networks from Regional Android Botnets: Rationale, Practicality, and Implications .......................... 295
Kaiming Fang (Binghamton University); Guanhua Yan (Binghamton University, State University of New York)

ChirpOTLE: A Framework for Practical LoRaWAN Security Evaluation .......................... 306
Frank Hessel, Lars Almon, Flor Alvarez (TU Darmstadt, Germany)

Security in Terahertz WLANs with Leaky Wave Antennas ........................................... 317
Chia-Yi Yeh, Yasaman Ghasempour (Rice University); Yasith Amarasinghe, Daniel M. Mittleman (Brown University); Edward W. Knightly (Rice University)

DEMO: Attaching InternalBlue to the Proprietary macOS IOBluetooth Framework .......................... 328
Davide Toldo, Jiska Classen, Matthias Hollick (SEEMOO, TU Darmstadt)

DEMO: BTLEmap: Nmap for Bluetooth Low Energy ........................................... 331
Alexander Heinrich, Milan Stute, Matthias Hollick (Secure Mobile Networking Lab, Department of Computer Science, TU Darmstadt)

DEMO: ColoT: A Consent and Information assistant for the IoT ........................................... 334
Victor Morel, Mathieu Cunche (University of Lyon / Inria); Daniel Le Métayer (INRIA Grenoble Rhônes-Alpes)

DEMO: Extracting Physical-Layer BLE Advertisement Information from Broadcom and Cypress Chips ........................................... 337
Jiska Classen, Matthias Hollick (SEEMOO, TU Darmstadt)

Demo: iJam with Channel Randomization ........................................... 340
Jordan L. Melcher, Yao Zheng, Dylan Anthony, Matthew Troglia (University of Hawaii - Electrical Engineering Department); Yanjun Pan, Ming Li (University of Arizona); Thomas Yang, Alvin Yang, Samson Aggelopoulos (University of Hawaii - Electrical Engineering Department)

DEMO: RESCURE: Retrofit Security for Critical Infrastructures ........................................... 343
Mario Münzer, Stefan Ilic (Technikon Forschungs- und Planungsgesellschaft mbH); Georgios Selimis, Rui Wang (Intrinsic ID); Frans M. J. Willems, Lieneke Kusters (Eindhoven University of Technology)

DEMO: Venom: a Visual and Experimental Bluetooth Low Energy Tracking System ........................................... 346
Guillaume Celosia, Mathieu Cunche (Univ Lyon, INSA Lyon, Inria, CITI)
POSTER: AcousticPrint: Acoustic Signature based Open Set Drone Identification 349
Harini Kolamunna (University of Sydney); Junye Li (University of New South Wales); Thilini Dahanayaka (The University of Sydney); Suranga Seneviratne (The University of Sydney, Sydney, Australia); Kanchana Thilakaratna (Data61-CSIRO and The University of Sydney); Albert Zomaya (The University of Sydney); Aruna Seneviratne (UNSW)

Poster: AnaMPhy: Anonymity Assisted Secret Refreshment at the Physical Layer 351
Jay Prakash (Singapore University of Technology and Design, Singapore); Rajesh Pachigolla (Synopsys India Pvt Ltd., India); Aman Goyal (University of California San Diego, USA); Parthajit Mohapatra (Indian Institute of Technology Tirupati, India); Tony Q.S. Quek (Singapore University of Technology and Design, Singapore)

POSTER: SemperFi: A Spoofer Eliminating Standalone GPS Receiver 353
Harshad Sathaye, Aanjhan Ranganathan (Northeastern University)

POSTER: Unprotected geo-localisation data through ARGOS satellite signals: The risk of cyberpoaching 356
Jean Sebastien Finger, Aurelien Francillon (Eurecom)