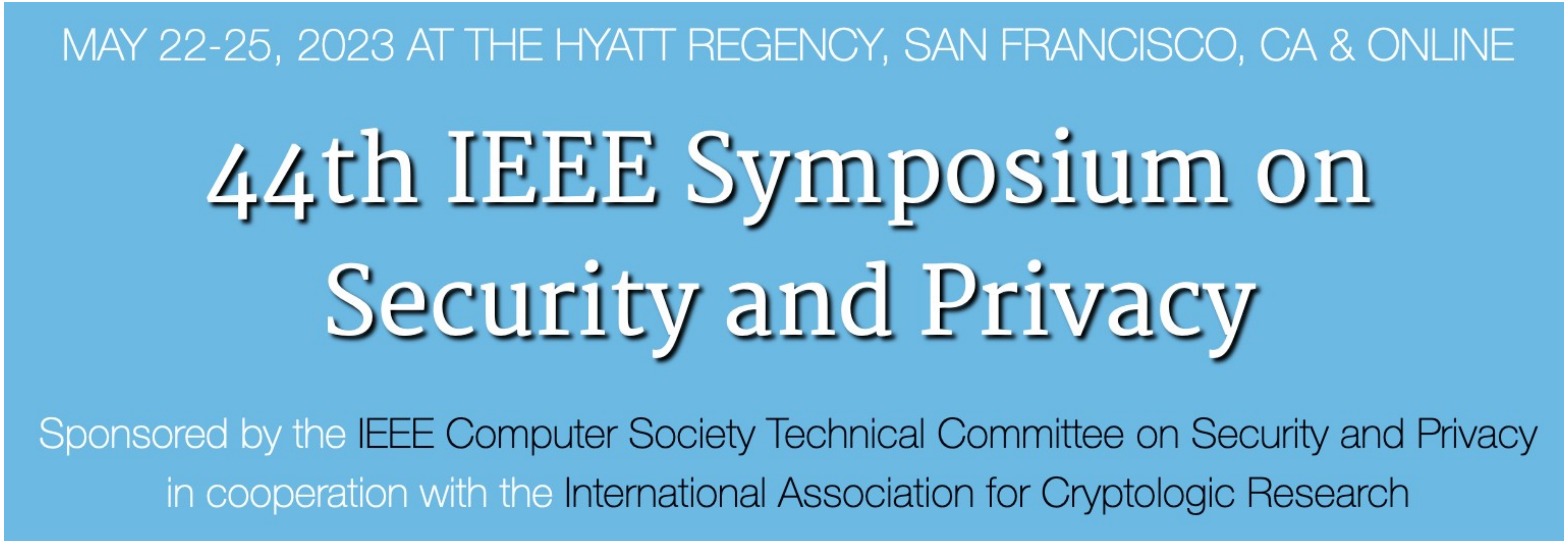
# Program Chairs’ Welcome



MAY 22-25, 2023 AT THE HYATT REGENCY, SAN FRANCISCO, CA & ONLINE

44th IEEE Symposium on Security and Privacy

Sponsored by the IEEE Computer Society Technical Committee on Security and Privacy in cooperation with the International Association for Cryptologic Research

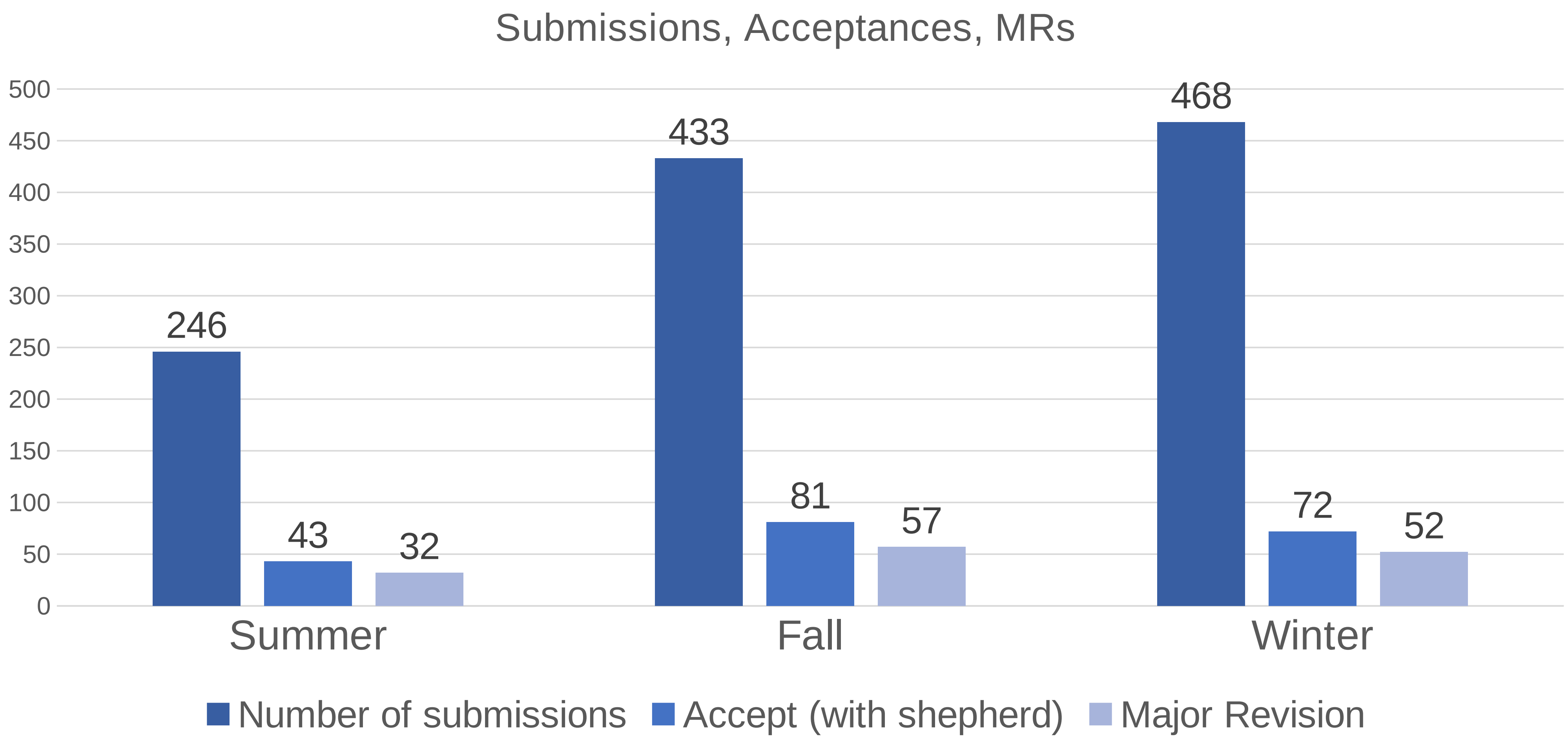
Thomas Ristenpart
Cornell Tech

Patrick Traynor
University of Florida

# How the program came to be

- 3 submission cycles (Spring, Summer, Winter)
    - Resubmissions accepted from some 2022 and earlier 2023 deadlines
    - R1 review (2 reviews per paper)
        - Early reject of many papers for which we saw no path towards acceptance
    - R2 reviews (2+ additional reviews per paper)
        - Research Ethics Committee (REC) review after R1 decisions
    - Author rebuttal and interaction period
    - Decisions (Accept, Conditional Accept, Major Revision, Reject)

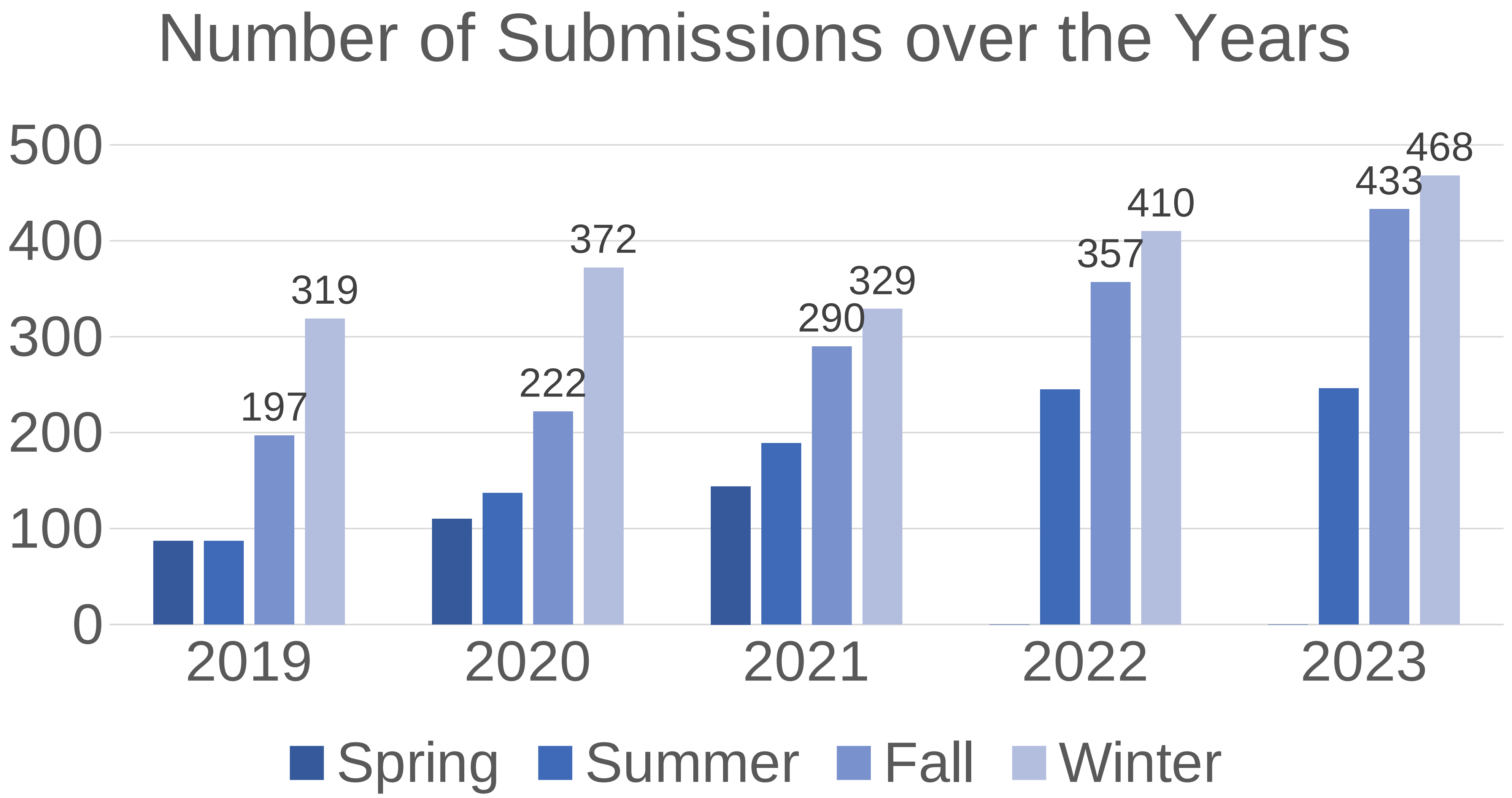
- Obviously, execution sometimes messier, and many corner cases
    - Associate Chairs and Program Committee did a ton of work to try to make as smooth as possible
    - Program Chairs worked to “keep trains running” and deal with complex cases



Desk rejects: 23

Total Number of Submissions: **1,147**

Total accepted: **196**



~13% increase in submissions over 2022

# Acceptance rates

| Category | Number | Rate |
|---|---:|---:|
| Accepts (new) | 14 | 1.4% |
| Conditional Accepts (new) | 66 | 6.5% |
| Accepts (resubmission) | 83 | 62.9% |
| Conditional Accepts (resubmission) | 33 | 25.0% |
| **Overall accept rate** | **196** | **17.0%** |

**2022 overall accept rate: 14.5%**

66% won a Distinguished Paper Award (stay tuned!)

# Program committee did huge amount of work

- 205 PC members in Round 3 (including associate chairs)
  - Estimated to be **~2,300 reviews**
- **Keeping review quality high challenging**
  - Rely on reviewers, discussions, associate chairs to flag issues
  - As we scale, more difficulty ensuring issues (papers, bad reviews, etc.) don't slip through the cracks
- Small number of PC membership changes over the year
  - Handful of cases of removal by program chairs for poor performance
  - Some excused for life events
- Research Ethics Committee chaired by Srdjan Capkun
  - Almost exclusively provided feedback to authors asking for clarifications

# Associate Chairs make the process scale

| | |
|---|---|
| Henry Corrigan-Gibbs | MIT |
| Adam Doupe | Arizona State University |
| Sarah Meiklejohn | Google / UCL |
| Nicolas Papernot | University of Toronto and Vector Institute |
| Christina Poepper | NYU Abu Dhabi |
| Mariana Raykova | Google |
| Elissa Redmiles | MPI SWS |
| Andrei Sabelfeld | Chalmers University |
| Ben Stock | CISPA |
| Yuval Yarom | University of Adelaide |

Thank you!!!

# Distinguished Paper Awards

- Award committee consists of the program chairs and associate chairs
- Shortlist of 21 papers:
  - Straight accepts for fresh submissions (14 papers)
  - 2 votes for BPA (7 total across all cycles)
- Discussion plus voting by committee

- This year there were a lot of papers that people felt were deserving of an award, so we increased the number of awards to 12
  - 6% of accepted papers
  - 1% of submissions

# MEGA: Malleable Encryption Goes Awry

Matilda Backendal (ETH Zurich)
Miro Haller (ETH Zurich)
Kenneth Paterson (ETH Zurich)

# Practically-exploitable Cryptographic Vulnerabilities in Matrix

Martin R. Albrecht (Royal Holloway, University of London)
Sofía Celi (Brave Software)
Benjamin Dowling (University of Sheffield)
Daniel Jones (Royal Holloway, University of London)

# Weak Fiat-Shamir Attacks on Modern Proof Systems

Quang Dao (Carnegie Mellon University)
Jim Miller (Trail of Bits)
Opal Wright (Trail of Bits)
Paul Grubbs (University of Michigan)

# Typing High-Speed Cryptography against Spectre v1

Basavesh Ammanaghatta Shivakumar (MPI-SP)
Gilles Barthe (MPI-SP and IMDEA Software Institute)
Benjamin Grégoire (Inria and Université Côte d'Azur)
Vincent Laporte (Inria Nancy)
Tiago Oliviera (MPI-SP)
Swarn Priya (Inria and Université Côte d'Azur)
Peter Schwabe (MPI-SP & Radboud University)
Lucas Tabary-Maujean (ENS Paris-Saclay)

# Red Team vs. Blue Team: A Real-World Hardware Trojan Detection Case Study Across Four Modern CMOS Technology Generations

Endres Puschner (Max Planck Institute for Security and Privacy)
Thorben Moos (UCLouvain)
Christian Kison (Bundeskriminalamt)
Steffen Becker (Ruhr University Bochum & Max Planck Institute for Security and Privacy)
Amir Moradi (Ruhr University Bochum)
Christof Paar (Max Planck Institute for Security and Privacy)

# It's (DM) Clobbering Time: Attack Techniques, Prevalence, and Defenses

Soheil Khodayari (CISPA Helmholtz Center for Information Security)
Giancarlo Pellegrino (CISPA Helmholtz Center for Information Security)

# The Leaky Web: Automated Discovery of Cross-Site Information Leaks in Browsers and the Web

Jannis Rautenstrauch (CISPA Helmholtz Center for Information Security)
Giancarlo Pellegrino (CISPA Helmholtz Center for Information Security)
Ben Stock (CISPA Helmholtz Center for Information Security)

# WaVe:
# a verifiably secure WebAssembly sandboxing runtime

Evan Johnson (University of California San Diego)
Evan Laufer (Stanford University)
Zijie Zhao (University of Illinois Urbana-Champaign)
Shravan Narayan (University of California San Diego)
Stefan Savage (University of California San Diego)
Deian Stefan (University of California San Diego)
Fraser Brown (Carnegie Mellon University)

# Characterizing Everyday Misuse of Smart Home Devices

Phoebe Moh (University of Maryland)
Pubali Datta (University of Illinois Urbana-Champaign)
Noel Warford (University of Maryland)
Adam Bates (University of Illinois Urbana-Champaign)
Nathan Malkin (University of Maryland)
Michelle L. Mazurek (University of Maryland)

# Not Yet Another Digital ID: Privacy-preserving Humanitarian Aid Distribution

Boya Wang (EPFL)
Wouter Lueks (CISPA Helmholtz Center for Information Security)
Justinas Sukaitis (ICRC)
Vincent Graf Narbel (ICRC)
Carmela Troncoso (EPFL)

# “In Eighty Percent of the Cases, I Select the Password for Them”: Security and Privacy Challenges, Advice, and Opportunities at Cybercafes in Kenya

Collins W. Munyendo (The George Washington University)
Yasemin Acar (The George Washington University)
Adam J. Aviv (The George Washington University)

# Space Odyssey: An Experimental Software Security Analysis of Satellites

Johannes Willbold (Ruhr-Universität Bochum)
Moritz Schloegel (Ruhr-Universität Bochum)
Manuel Vögele (Ruhr-Universität Bochum)
Maximilian Gerhardt (Ruhr-Universität Bochum)
Thorsten Holz (CISPA Helmholtz Center for Information Security)
Ali Abbasi (CISPA Helmholtz Center for Information Security)

# Changes to the 2024 Procedures

- Major Revisions have been eliminated from the 2024 Conference.
- Instead, all papers will be published with meta-reviews, providing context for the acceptance of each paper.
- Please see the 2024 CFP for full details:

  https://www.ieee-security.org/TC/SP2024/cfpapers.html
- The community is faced with a wide range of challenges, and we hope that you actively engage in addressing them.