Welcome to ACSAC 2023!

Message from the Program Committee Chairs

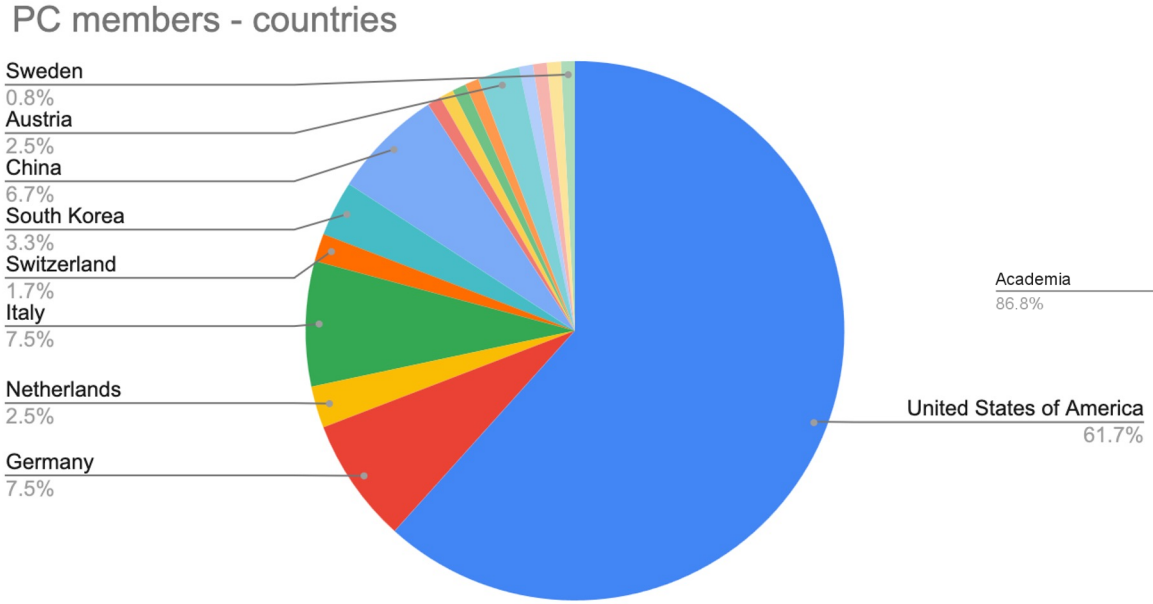
Roberto Perdisci
Professor
University of Georgia

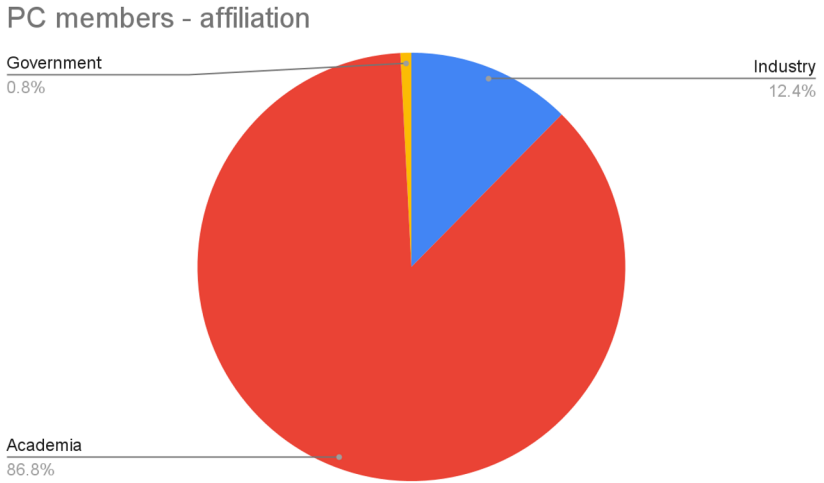
Martina Lindorfer
Associate Professor
TU Wien

Thank you to the PC members!

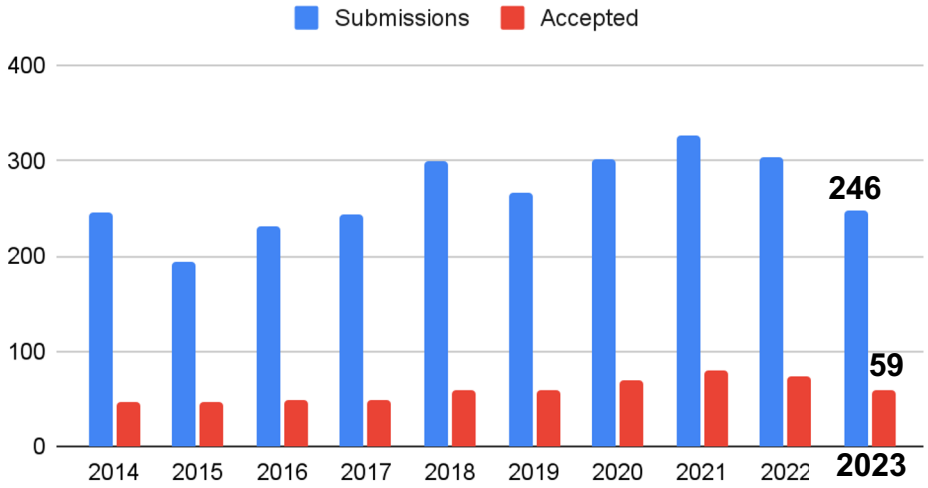
Acar Tamersoy, Gen Digital
Adrian Dabrowski, CISPA Helmholtz Center for Information Security
Adwait Nadkarni, William & Mary
Aisha Ali-Gombe, Louisiana State University
Alberto Dainotti, Georgia Institute of Technology
Amin Kharraz, Florida International University
Andrea Continella, University of Twente
Andrea Lanzi, University of Milan
Andrea Mambretti, IBM Research Europe - Zurich
Andreas Peter, University of Oldenburg
Anita Nikolich, UIUC
Antonio Bianchi, Purdue University
Anupam Das, North Carolina State University
Aravind Machiry, Purdue University
Aurore Fass, CISPA Helmholtz Center for Information Security
Baris Coskun, Amazon AWS
Bo Chen, Michigan Technological University
Brendan Saltaformaggio, Georgia Institute of Technology
Byoungyoung Lee, Seoul National University
Chenglin Miao, Iowa State University
Chenxiong Qian, The University of Hong Kong
Chia-Che Tsai, Texas A&M University
Christian Wressnegger, Karlsruhe Institute of Technology (KIT)
Christophe Hauser, Information Sciences Institute, University of Southern California
Daniel Arp, TU Berlin
Dave (Jing) Tian, Purdue University
Davide Maiorca, University of Cagliari, Italy
Ding Wang, Nankai University
Eleonora Losiouk, University of Padua
Elias Athanasopoulos, University of Cyprus
Elisa Bertino, Purdue University
Eugene Vasserman, Kansas State University
Evangelos Markatos, FORTH and University of Crete
Fabian Monrose, Georgia Institute of Technology
Federico Maggi, Amazon AWS
Fengjun Li, University of Kansas
Fengwei Zhang, Southern University of Science and Technology (SUSTech)
Gang Wang, UIUC
Giancarlo Pellegrino, CISPA Helmholtz Center for Information Security
Gianluca Stringhini, Boston University
Giorgio Giacinto, University of Cagliari, Italy
Giovanni Apruzzese, University of Liechtenstein
Guangliang Yang, Fudan University
Hongxin Hu, University at Buffalo
Hussain Almohri, Kuwait University
Hyungjoon (Kevin) Koo, Sungkyunkwan University
Jaewoo Lee, University of Georgia
Jialong Zhang, Tencent Security
Jie Yang, Florida State University
Jin-Hee Cho, Virginia Tech
Jinpeng Wei, University of North Carolina at Charlotte
Johanna Ullrich, SBA Research/University of Vienna
Johannes Kinder, LMU Munich
Kang Li, CertiK
Kapil Singh, IBM T.J. Watson Research Center
Karthika Subramani, Georgia Institute of Technology
Katsunari Yoshioka, Yokohama National University
Kaveh Razavi, ETH Zurich
Kevin Borgolte, Ruhr University Bochum
Konrad Rieck, TU Berlin
Kun Sun, George Mason University
Kyu Hyung Lee, University of Georgia
Lannan (Lisa) Luo, George Mason University
Le Guan, University of Georgia
Leigh Metcalf, CERT
Lejla Batina, Radboud University
Long Cheng, Clemson University
Lorenzo Cavallaro, UCL
Lorenzo De Carli , University of Calgary
Magnus Almgren, Chalmers University of Technology
Man-Ki Yoon, North Carolina State University
Manos Antonakakis, Georgia Institute of Technology
Marco Balduzzi, Trend Micro
Marco Squarcina, TU Wien
Marcus Botacin, Texas A&M University
Martin Johns, TU Braunschweig
Maura Pintor, University of Cagliari
Maverick Woo, Carnegie Mellon University
Michalis Polychronakis, Stony Brook University
Mu Zhang, University of Utah
Nick Nikiforakis, Stony Brook University
Ning Zhang, Washington University in St. Louis
Nitesh Saxena, Texas A&M University
Oleksii Starov, Palo Alto Networks
Omar Alrawi, Georgia Tech
Phani Vadrevu, University of New Orleans
Qi Li, Tsinghua University
Ram Krishnan, University of Texas at San Antonio
Sang Kil Cha, KAIST
Sangho Lee, Microsoft Research
Sarah Chmielewski, MIT Lincoln Laboratory
Savio Sciancalepore, Technische Universiteit Eindhoven (TU/e)
Selcuk Uluagac, Florida International University
Seungwon Shin, KAIST
Shagufta Mehnaz, Penn State University
Shanchieh (Jay) Yang, Rochester institute of Technology
Shuang Hao, University of Texas at Dallas
Stefano Calzavara, Università Ca' Foscari Venezia
Stefano Traverso, Ermes Cyber Security SRL
Stefano Zanero, Politecnico di Milano
Thang Hoang, Virginia Tech
Tuba Yavuz, University of Florida
Vasileios Kemerlis, Brown University
Vinod Yegneswaran, SRI International
Wei Meng, The Chinese University of Hong Kong
Wenwen Wang, University of Georgia
William Melicher, Palo Alto Networks
Xiaojing Liao, Indiana University Bloomington
Xiaoyan Sun, California State University, Sacramento
Xiapu Luo, The Hong Kong Polytechnic University
Yao Liu, University of South Florida
Yingying Chen, Rutgers University
Yinzhi Cao, Johns Hopkins University
Yue Duan, Illinois Institute of Technology
Yuzhe Tang, Syracuse University
Zachary Tudor, Idaho National Laboratory
Zhaoyan Xu, Bytedance US
Zhen Huang, DePaul University
Zhiqiang Lin, Ohio State University

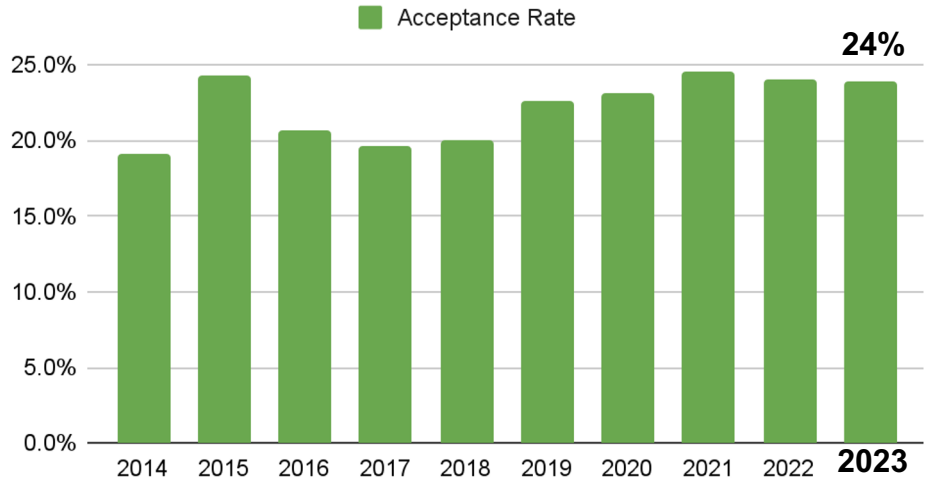
Program Committee: **121** members from **16** countries





Selection of ACSAC 2023 Papers

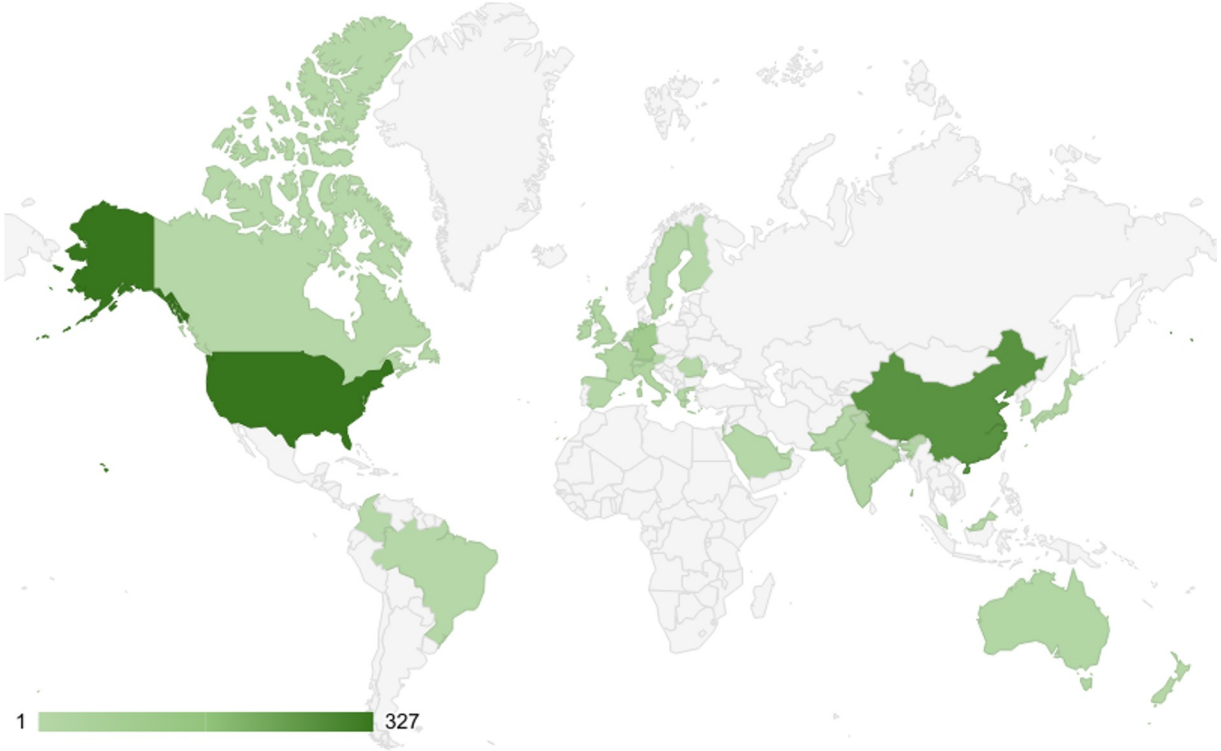




- 246 valid submission
- 2 Review Rounds – 143 (58%) advanced to Round 2
- 59 Accepted Papers – 24% acceptance rate
  - 30 conditionally accepted (minor revisions + shepherding)

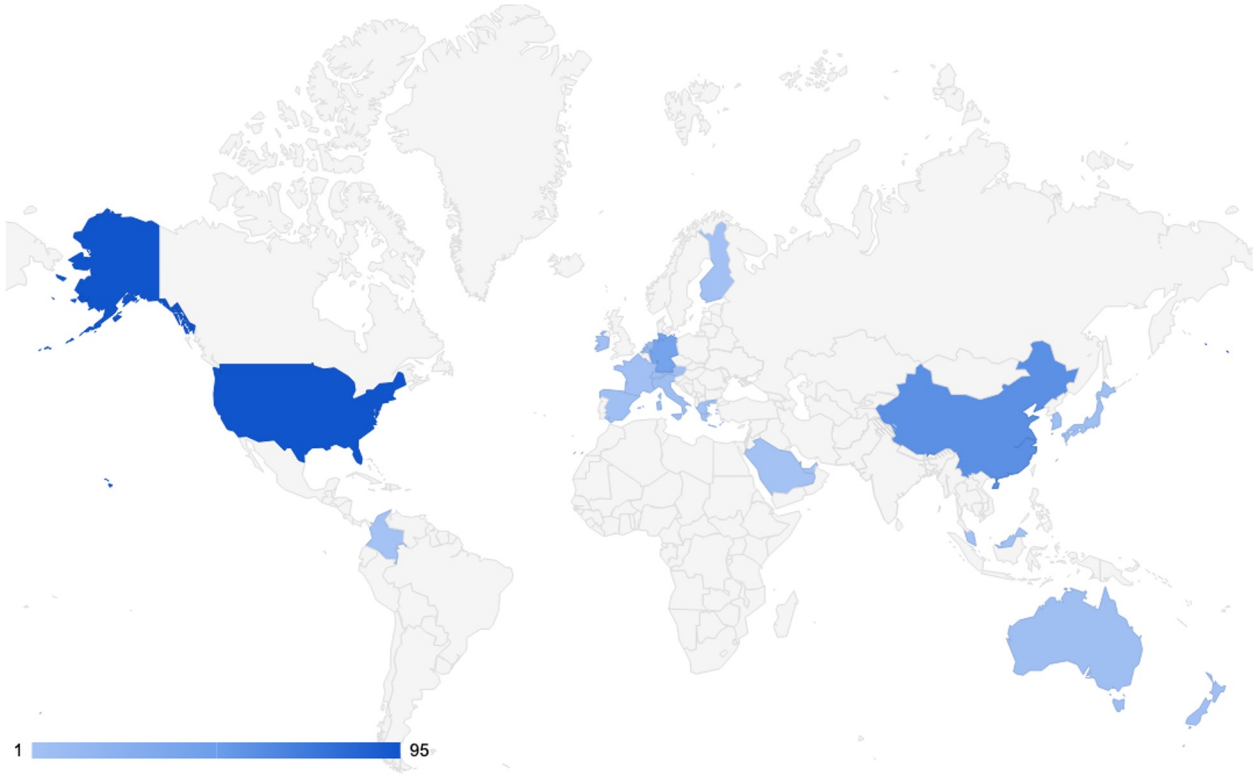
More than **1100** submission authors from **34** countries

```
327 United States
266 China
 94 Germany
 26 Italy
 23 India
 22 Netherlands
 21 France
 17 Singapore
 15 South Korea
 13 Australia
 12 United Kingdom
 11 Japan
  8 Ireland
  7 Switzerland
  7 Austria
  6 Sweden
  6 Israel
  …
```

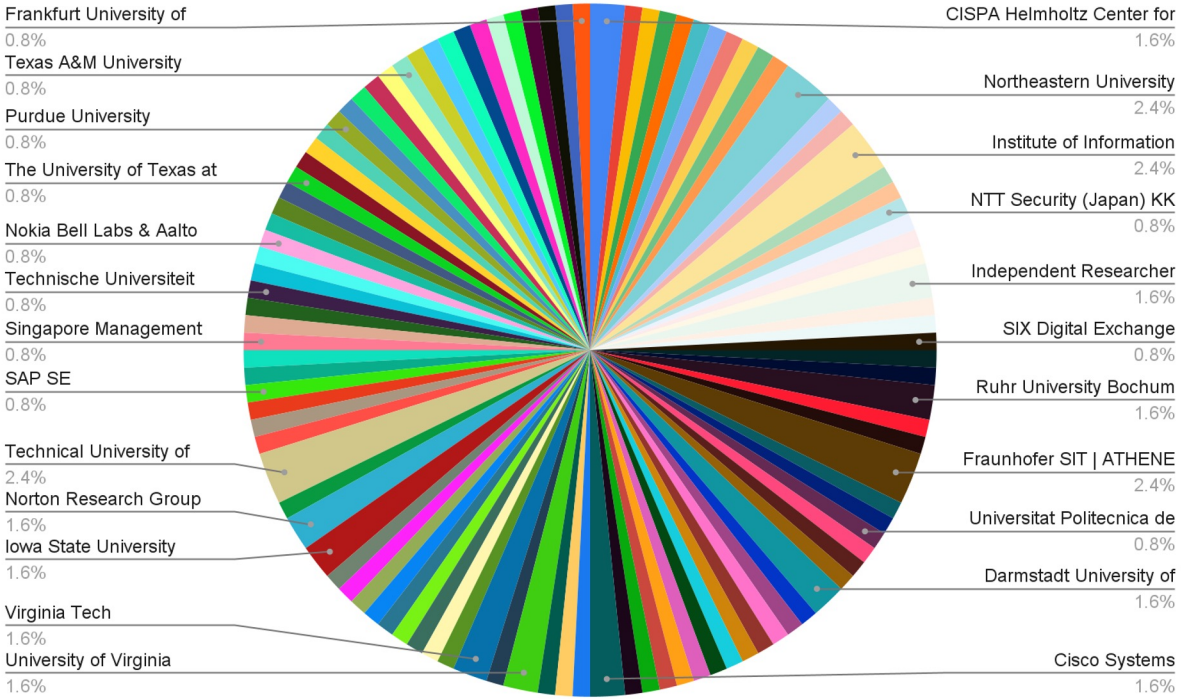


More than **270** accepted authors from **23** countries

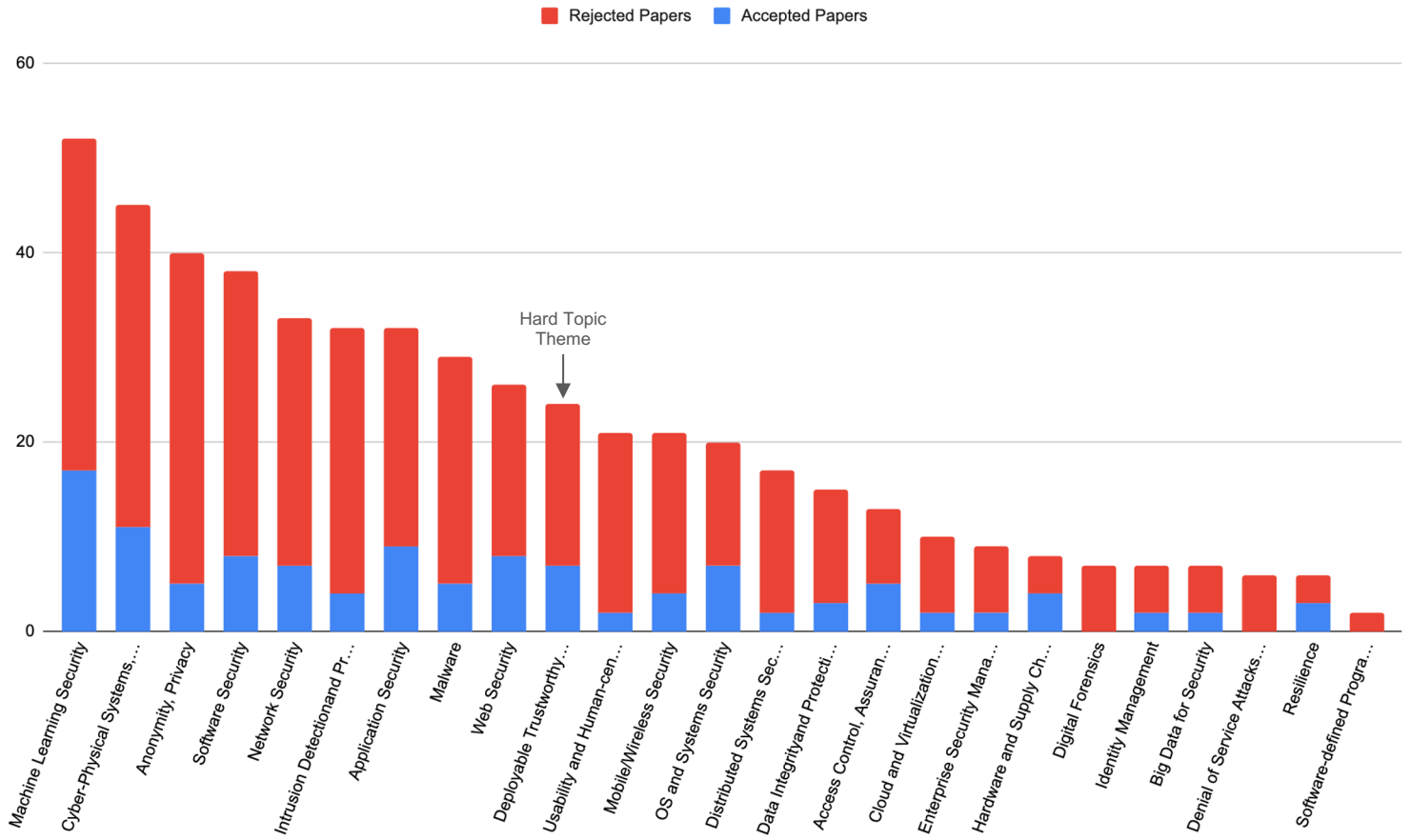
95 United States
57 China
41 Germany
 9 Netherlands
 5 Switzerland
 5 Singapore
 5 Italy
 5 Austria
 5 Australia
 4 Spain
 4 South Korea
 4 Japan
 …



More than 100 affiliations for accepted papers



Submission topics



Distinguished Paper Award

Distinguished Paper Award

- PC Chairs selected 10 top papers based on reviews
- PC members voted to select the best among these 10
- PC Chairs made the final decision

- This year we selected 2 best papers for award

First Distinguished Paper Award goes to...

Protecting Your Voice from Speech Synthesis Attacks

Zihao Liu, Yan Zhang, Chenglin Miao

Iowa State University

Second Distinguished Paper Award goes to...

SePanner: Analyzing Semantics of Controller Variables in Industrial Control Systems based on Network Traffic

Jie Meng[*], Zeyu Yang[*], Zhenyong Zhang[+], Yangyang Geng[^], Ruilong Deng[*], Peng Cheng[*], Jiming Chen[*], Jianying Zhou[#]

[*]Zhejiang University, [+]Guizhou University, [^]Information Engineering University, and [#]Singapore University of Technology and Design

Top Reviewer Awards

Top Reviewers

- **Aurore Fass**, CISPA
- **Christian Wressnegger**, KIT
- **Giovanni Apruzzese**, University of Liechtenstein
- **Konrad Rieck**, TU Berlin
- **Marco Squarcina**, TU Wien
- **Marcus Botacin**, Texas A&M University
- **Magnus Almgren**, Chalmers University of Technology

Paper Artifacts Evaluation

Thanks to the Artifacts Evaluation Committee!

Xiaojing Liao
Assistant Professor
Indiana University Bloomington

Adwait Nadkarni
Associate Professor
William & Mary

Artifacts Evaluation

- Goal: foster reproducibility of cybersecurity research results
  - 3 ACM badges: **Functional**, **Results Reproduced**, and **Reusable** (*supersedes Functional*)
- **41 artifacts submissions** (69% of ACSAC accepted papers)
- The Artifact Committee included **23 mentors and 63 students**
  - Each artifact was assigned ~6 reviewers: 3 students and 3 mentors
- **The process:**
  - ACSAC AE Evaluator Guide (adapted from the USENIX'23 Evaluator Guide)
  - Initial *"Kick the tires"* period to prevent surprises later
  - Highly interactive evaluation that helped improve the artifacts: ***734 comments*** from authors and PC (~17/paper)
- 38/41 assigned at least one badge: **23 Reusable** *(supercedes Functional)*, **19 Results Reproduced**, and **14 Functional**

Distinguished Paper with Artifacts Award

(1/2)

Artemis: Defanging Software Supply Chain Attacks in Multi-repository Update Systems

Marina Moore,Trishank Kuppusamy, Justin Cappos

Distinguished Paper with Artifacts Award

(2/2)

Remote Attestation of Confidential VMs Using Ephemeral vTPMs

Vikram Narayanan, Claudio Carvalho, Angelo Ruocco, Gheorghe Almasi, James Bottomley, Mengmei Ye, Tobin Feldman-Fitzthum, Daniele Buono, Hubertus Franke, Anton Burtsev

Distinguished Artifact Reviewers

Leon Weiß
Ruhr University Bochum

Vinny Adjibi
Georgia Institute of Technology

Hongbo Chen
Indiana University Bloomington

Cybersecurity Artifacts Competition and Impact Award

- New initiative (since ACSAC 2022) 

- Competition Objectives:
  - Further promote reproducibility of cybersecurity research results
  - Acknowledge efforts of authors who contribute to real-world deployment/use of novel and reliable security solutions
  - Award artifacts that have had a **significant impact on cybersecurity research and applications**
  - Submissions open to cybersecurity artifacts **previously published in peer-reviewed venues** (conferences, journals), both in academia and industry (not only ACSAC)

Cybersecurity Artifacts Competition and Impact Award

- Co-Chairs:
  - Guofei Gu chair, Texas A&M University
  - Roberto Perdisci, University of Georgia
  - Martina Lindorfer, TU Wien

- Committee Members:
  - David Balenson, USC Information Sciences Institute
  - Gabriela Ciocarlie, The University of Texas at San Antonio
  - Gianluca Stringhini, Boston University
  - Phillip Porras, SRI
  - Jelena Mirkovic, USC Information Sciences Institute
  - Leigh Metcalf, CERT
  - Juan Caballero, IMDEA

Artifacts Competition Finalists

- 4 Finalists - Impact Award(s) will be announced on **Thursday 9-10am**
  - **SGX-Step: An Open-Source Framework for Precise Dissection and Practical Exploitation of Intel SGX Enclaves**
  - **DeterLab Testbed for Cybersecurity Experimentation**
  - **angr: A Powerful and User-friendly Binary Analysis Platform**
  - **Zipr: A High-Impact, Robust, Open-source, Multi-platform, Static Binary Rewriter**

Enjoy the conference!