

General Chair Opening Remarks

MAY 18-21, 2026 AT THE HILTON SAN FRANCISCO UNION SQUARE, SAN
FRANCISCO, CA

47th IEEE Symposium on Security and Privacy

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

Alina Oprea
Northeastern University,
Boston, MA, USA

Welcome to S&P 2026!

- Flagship security conference
- At the Hilton San Francisco Union Square



**IEEE
COMPUTER
SOCIETY**



S&P 2026

At a Glance

254 papers in
conference

4 tracks
3 days

10-minute
talks

Keynote
speaker

2 IEEE award
speakers

40 posters

7 workshops

707
participants

32 student
travel grants
(\$46.5K)

8 sponsors
(\$64.5K)

Highlights:
Monday,
May 18

Opening Remarks

Best Paper Awards and ToT Awards

3 technical sessions, 4 tracks each

Poster Reception

Plaza A/B, 5-7pm

Mentoring Session

Golden Gate 6&7, 5:45-7pm

Highlights: Tuesday, May 19

IEEE Award Session ▼

Continental 4+5

10:45 AM – 12:00 PM

IEEE Internet Award

David Clark: "A Look Back: The Early History of (Not) Securing the Internet"

IEEE Innovation in Societal Infrastructure Award 2026

Moti Yung: "Security, Privacy, and Society."

IEEE Cybersecurity Award for Practice



TC Meeting

Continental 5

5:00 PM – 6:00 PM

PC Chairs "Ask Me Anything"

Continental 5

6:00 PM – 7:00 PM

Highlights: Wednesday, May 20

Keynote ▼

Continental 4+5

10:45 AM – 12:00 PM



Marta Kwiatkowska (University of Oxford)

Provable Robustness Guarantees for Artificial Intelligence: Progress and Challenges

Artificial intelligence powered by neural networks has made significant advances in the past few years and its deployment is accelerating. However, neural network models are susceptible to adversarial perturbations of inputs, such as imperceptible manipulations of images or structural perturbations of graph data that can drastically change the network output. Beyond inference, data errors or poisoning attacks that inject malicious data into the training process can result in wrong or harmful model predictions, and in multi-agent reinforcement learning strategic manipulations can steer the learned policy towards undesirable goals. Undetected, such issues pose a significant risk to the safety and security of high-stakes applications. Formal methods, and particularly formal verification techniques, have become indispensable components of rigorous software engineering methodologies and are well placed to provide the needed assurance in the form of provable robustness guarantees on model predictions. Using illustrative examples, this lecture will overview recent progress and future challenges in research aimed at developing provably robust and strategyproof AI systems.

Highlights: Thursday, May 21

LangSec: The 12th Workshop on Language-theoretic Security

Golden Gate 3

8:30 AM – 5:05 PM

CyberBio: First International Workshop on Cyberbiosecurity

Golden Gate 4

8:30 AM – 5:00 PM

ArtSec: Workshop on Artwork Security and Provenance in the Age of AI

Golden Gate 5

9:00 AM – 4:45 PM

SAGAI: Secure Agents for Generative Artificial Intelligence

Golden Gate 1-2

8:30 AM – 4:45 PM

ConPro: Workshop on Technology and Consumer Protection

Golden Gate 6

8:40 AM – 4:45 PM

MetaCRiSP: Workshop on Meta-Science and Critical Reflections in Security & Privacy Research

Golden Gate 7

8:50 AM – 4:15 PM

Data4SoftSec: Workshop on Datasets for Software Security

Golden Gate 8

8:45 AM – 4:45 PM

Thanks to the Organizing Committee

Vice Chair

Adam Aviv

Program Chairs

Cristina Nita-Rotaru

Nicolas Papernot

Treasurer

Adwait Nadkarni

Workshop Chairs

Ziming Zhao

Ghada Almashaqbeh

Poster Chair

Syed Hussain

ToT Award Chair

Dongyan Xu

Web Chair

Andreas Brüggemann

Artifact Evaluation

Jelena Mirkovic

Chairs

Manuel Egele

Chair Emeritus

Marina Blanton

Publicity Chairs

Prajwal Panzade

Amit Seal Ami

Travel Grant Chair

Yupeng Zhang

Donations Chair

Zhou Li

Publication Chairs

Shagufta Mehnaz

Berkay Celik

Site Chairs

Maddie Bautista

Kate Todd

Registration Manager

Tyler Owens

Speaker Manager

Whitney Lawless

IEEE Liaison

Michelle Ocampo

Thanks to the Steering Committee and TCSP

Steering Committee

Thorsten Holz
Alvaro Cardenas
Sean Peisert
Alina Oprea
Michael Reiter
Gregory Shannon
Carmela Troncoso
Hovav Shacham
Christopher Kruegel

IEEE Technical Community on Security and Privacy Officers

Thorsten Holz (Chair)
Alvaro Cardenas (Vice Chair)
Yong Guan (Treasurer)
Hilarie Orman (Cipher Newsletter Editor)

Thanks to Our Sponsors

Gold



Silver



ANT
RESEARCH

Bronze



Remembering Peter G. Neumann



Announcements

- Network access
 - Wifi network: Hilton Events
 - Password: IEEE2026
- Paper access
 - <https://www.computer.org/csdl/proceedings/sp/2026/2bojuokAJK8>
- Lunch
 - Plated lunch on Monday, Tuesday, Wednesday; boxed lunch on Thu
 - Dietary restrictions taken into account
- Code of conduct: <https://sp2026.ieee-security.org/codeofconduct.html>

Welcome from the PC Chairs

MAY 18-21, 2026 AT THE HILTON SAN FRANCISCO UNION SQUARE, SAN
FRANCISCO, CA

47th IEEE Symposium on Security and Privacy

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

Cristina Nita-Rotaru
Northeastern University

Nicolas Papernot
University of Toronto and Vector
Institute and Google DeepMind

Thank you to the S&P '26 Team!

- 16 Associate Chairs (from 10 in 2025)
- 320 PC members (from 219 in 2025)
- 2 REC Chairs: Blase Ur and Sofia Celi
- Webchair: Andreas Brüggemann
- HotCRP Support: Ivan Liang
- Publications Chairs: Shagufta Mehnaz and Berkay Celik
- General Chair: Alina Oprea
- IEEE CS TCSP chair (current/next): Thorsten Holz and Alvaro Cardenas

Associate Chairs (16)

Adwait Nadkarni (William & Mary)

Amir Houmansadr (UMass)

Andrew Paverd (Microsoft)

Catalin Hritcu (MPI-SP)

Christina Garman (Purdue University)

Daniele Cono D'Elia (Sapienza University)

David Barrera (Carleton University)

Florian Tramer (ETH Zurich)

Katerina Mitrokotsa (U. of St Gallen)

Mathias Lecuyer (U. of British Columbia)

Sara Rampazzi (University of Florida)

Sascha Fahl (CISPA)

Stephanie Roos (Kaiserslautern-Landau)

Varun Chandrasekaran (UIUC)

William Robertson (Northeastern Univ)

Ziming Zhao (Northeastern Univ.)

Program Committee (320)

Aaron Johnson, Aarushi Goel, Aashish Kolluri, AbdelRahman Abdou, Abhiram Kothapalli, Adam Oest, Adam Dziedzic, Adil Ahmad, Adrien Koutsos, Ahmad-Reza Sadeghi, Alejandro Russo, Alesia Chernikova, Alessandro Brighente, Alexander Viand, Alexander Hoover, Alexandre Debant, Alexios Voulimeneas, Ali Abbasi, Alin Tomescu, Alvaro Cardenas, Amit Kumar Sikder, Amrita Roy Chowdhury, Anca Jurecut, Andrei Sabelfeld, Andrew Cullen, Andrew Kwong, Ang Chen, Angelos Stavrou, Anshuman Suri, Antonio Bianchi, Anwar Hithnawi, Aravind Machiry, Arslan Khan, Arthur Gervais, Arthur Azevedo de Amorim, Ashwinee Panda, Atul Prakash, Aviv Yaish, Awais Rashid, Aysajan Abidin, Bailey Kacsmar, Bart Copens, Ben Weintraub, Ben Zhao, Benjamin Beurdouche, Benjamin Dowling, Benny Pinkas, Bijeeta Pal, Bimal Viswanath, Binghui Wang, Bo Chen, Bogdan Carbunar, Boris Köpf, Brendan Saltaformaggio, Byoungyoung Lee, Carrie Gates, Cas Cremers, Changyu Dong, Chaowei Xiao, Chawin Sitawarin, Chengyu Song, Christian Wressnegger, Christof Ferreira Torres, Christopher A. Choquette-Choo, Clara Schneidewind, Claudio Soriente, Cristian-Alexandru Staicu, Dana Drachler Cohen, Daniel Genkin, Daniel Jost, Daniele Antonioli, Dario Pasquini, Dave Tian, David Heath, David Zage, Deepak Garg, Dimitris Kolonelos, Dominik Wermke, Doreen Riepel, Eleonora Losiouk, Elisa Bertino, Elisaweta Masserova, Emiliano De Cristofaro, Emily Wenger, Emma Dauterman, Eric Pauley, Eugene Bagdasarian, Evgenios Kornaropoulos, Eyal Ronen, Eysa Lee, Fabian Monrose, Fabio De Gaspari, Fabio Pierazzi, Faysal Hossain Shezan, Feargus Pendlebury, Fengwei Zhang, Fengyuan Xu, Florian Kerschbaum, FNU Suva, Frank Li, Frank Piessens, Franziska Boenisch, Gang Tan, Gautam Akiwate, Ghada Almashaqbeh, Ghassan Karame, Giorgio Severi, Giovanni Camurati, Grant Ho, Guan hong Tao, Habiba Farrukh, Haipeng Cai, Hans Hanley, Hanshen Xiao, Hao Chen, Haya Schulmann, Heather Zheng, Heng Yin, Hervé Debar, Hieu Le, Hiraku Morita, Hongxin Hu, Hugo Lefeuve, Hyungsub Kim, Ian Miers, Ilia Shumailov, Imtiaz Karim, Insu Yun, Ioana Boureanu, Ioannis Demertzis, Ivan Evtimov, Ivan De Oliveira Nunes, Jamie Hayes, Jana Hofmann, Jason Nieh, Jay Bosamiya, Jean-Luc Watson, Jean-Philippe Monteui, Jeremiah Blocki, Jianliang Wu, Jingxuan He, Jinyuan Jia, Jiska Classen, John Mitchell, Jon McCune, Jonas Hielscher, Jonathan Katz, Joseph Lallemand, Joshua Gancher, Julia Len, Kari Kostiaainen, Karthikeyan Bhargavan, Kartik Nayak, Kasper Rasmussen, Kassem Fawaz, Kathrin Grosse, Kaushal Kafle, Keewoo Lee, Kelsey Fulton, Kentrell Owens, Kexin Pei, Klaus v. Gleissenthall, Konrad Rieck, Lachlan Gunn, Lea Schönherr, Lenka Mareková, Lesly-Ann Daniel, Liang Wang, Lianying Zhao, Limin Jia, Lorenzo Cavallaro, Lorenzo De Carli, Lucianna Kiffer, Lujo Bauer, Lydia Zakyntinou, Mahak Pancholi, Mahmood Sharif, Man-Ki Yoon, Marco Squarcina, Marco Guarnieri, Marcus Botacin, Mario D'Onghia, Martin Henze, Marzieh Bitaab, Matthew Jones, Matthew Lentz, Matthew Jagielski, Maura Pintor, Mauro Conti, Meera Sridhar, Michael Hicks, Michelle Mazurek, Milad Nasr, Miuyin Yong Wong, Mohannad Alhanahnah, Moritz Schloegel, Morley Mao, Mridula Singh, Mu Zhang, Muhammad Ikram, Muoi Tran, Murtuza Jadhwal, Muslum Ozgur Ozmen, Nader Sehatbakhsh, Natalia Stakhanova, Nathan Malkin, Neil Gong, Nguyen Phong Hoang, Nidhi Hegde, Nikita Borisov, Nils Lukas, Ning Zhang, Ning Luo, Ninghui Li, Nuno Santos, Olya Ohrimenko, Om Thakkar, Omar Chowdhury, Orfeas Thyfronitis Litos, Pedro Moreno-Sanchez, Peng Gao, Phani Vadrevu, Piyush Kumar Sharma, Pratik Sarkar, Pratyush Mishra, Priyanka Nanayakkara, Qiben Yan, Raouf Kerkouche, Ravishankar Borgaonkar, Reethika Ramesh, Rei Safavi-Naini, Rex Fernando, Rohit Sinha, Ryan Sheatsley, Saeed Mahloujifar, Sahar Abdelnabi, Saikrishna Badrinarayanan, Sajin Sasy, Sam Kumar, Saman Zonouz, Samuel Marchal, Sandra Siby, Sanghyun Hong, Santiago Zanella-Beguelin, Santiago Torres-Arias, Sarbartha Banerjee, Sathvik Prasad, Sebastian Angel, Sebastian Szyller, Sebastien Gambs, Sébastien Bardin, Shagufa Mehnaz, Shih-Wei Li, Shima Ahmed, Shuang Song, Shweta Shinde, Siddharth Garg, Simon Oya, Sisi Duan, Song Li, Soteris Demetriou, Sourav Das, Srdjan Capkun, Stéphanie Delaune, Stephen Herwig, Steve Kremer, Sunil Manandhar, Sven Bugiel, Swarn Priya, Syed Rafiul Hussain, Sze Yiu Chau, Tahina Ramananandro, Tapti Palit, Teodora Baluta, Thang Hoang, Thomas Ristenpart, Thomas Pasquier, Thomas Nyman, Thorsten Holz, Thorsten Eisenhofer, Tiago Heinrich, Tianhao Wang, Tiantian Gong, Ting Wang, Tobias Fiebig, Ulfar Erlingsson, Urs Hengartner, Varun Madathil, Vincent Laporte, Vladimir Kolesnikov, Wajih Ul Hassan, Wanrong Zhang, Weilin Xu, Wenbo Guo, Wenhai Sun, Wenjing Lou, Wenke Lee, Xavier de Carné de Carnavalet, Xiao Wang, Yigitcan Kaya, Yiling He, Yinzhao Cao, Yizheng Chen, Yongdae Kim, Yossi Oren, Yousra Aafer, Yu Ding, Yuan Tian, Yuan Hong, Yuchen Yang, Yunang Chen, Yunming Xiao, Yupeng Zhang, Yuzhe Tang, Z. Berkay Celik, Zahra Ghodsi, Zhiqiang Lin, Zhuotao Liu, Zimo Chai, Ziqi Yang

Research Ethics Committee (REC)

- Blase Ur (senior co-chair) and Sofia Celi (junior co-chair)
- Members: Bogdan Carbunar, Emily Wenger, Jiska Classen, Julia Len, Michelle Mazurek, Sven Bugiel
- 149 submissions reviewed by the REC (76 in Cycle 1, 73 in Cycle 2)
- Common topics of REC review:
 - Experimentation on live systems
 - Responsible disclosure
 - Experimentation on human subjects
 - Weighing potential benefits and harms

How The Program Was Made

- 2 submission cycles
 - Continued Meta Reviews instead of resubmissions from 2024
 - 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
 - Ratings
 - Accept w/ Meta Review
 - Accept w/ Noteworthy Concerns in Meta Review
 - Weak Reject (Can Be Convinced By Champion)
 - Reject
 - All papers were assigned a shepherd

Challenges

- Continued growth:
 - Increase the PC and the AC
 - Cap limit at 6 per cycle for a total of 12
- Late reviews & their impact on decision making for submissions
- The LLM Usage:
 - Introduced an LLM Policy
- New ethics challenges:
 - Introduced an ethics consideration section
- Maintaining the integrity of the review process:
 - Introduced the use of ORCID and detailed COI policy

Distinguished Reviewer Awards

- Thomas Nyman
- Keewoo Lee
- Arslan Khan
- Mahak Pancholi
- Benjamin Dowling
- Amit Kumar Sikder
- Awais Rashid
- Abhiram Kothapalli
- Yongdae Kim
- Jon McCune
- Antonio Bianchi
- Adil Ahmad

- Thorsten Eisenhofer
- David Heath
- Shih-Wei Li
- Michelle Mazurek
- Alexander Hoover
- Franziska Boenisch
- Marzieh Bitaab
- Yinzhi Cao
- Qiben Yan
- Florian Kerschbaum
- Varun Madathil
- Changyu Dong



Ask Me Anything Session with PC Chairs !

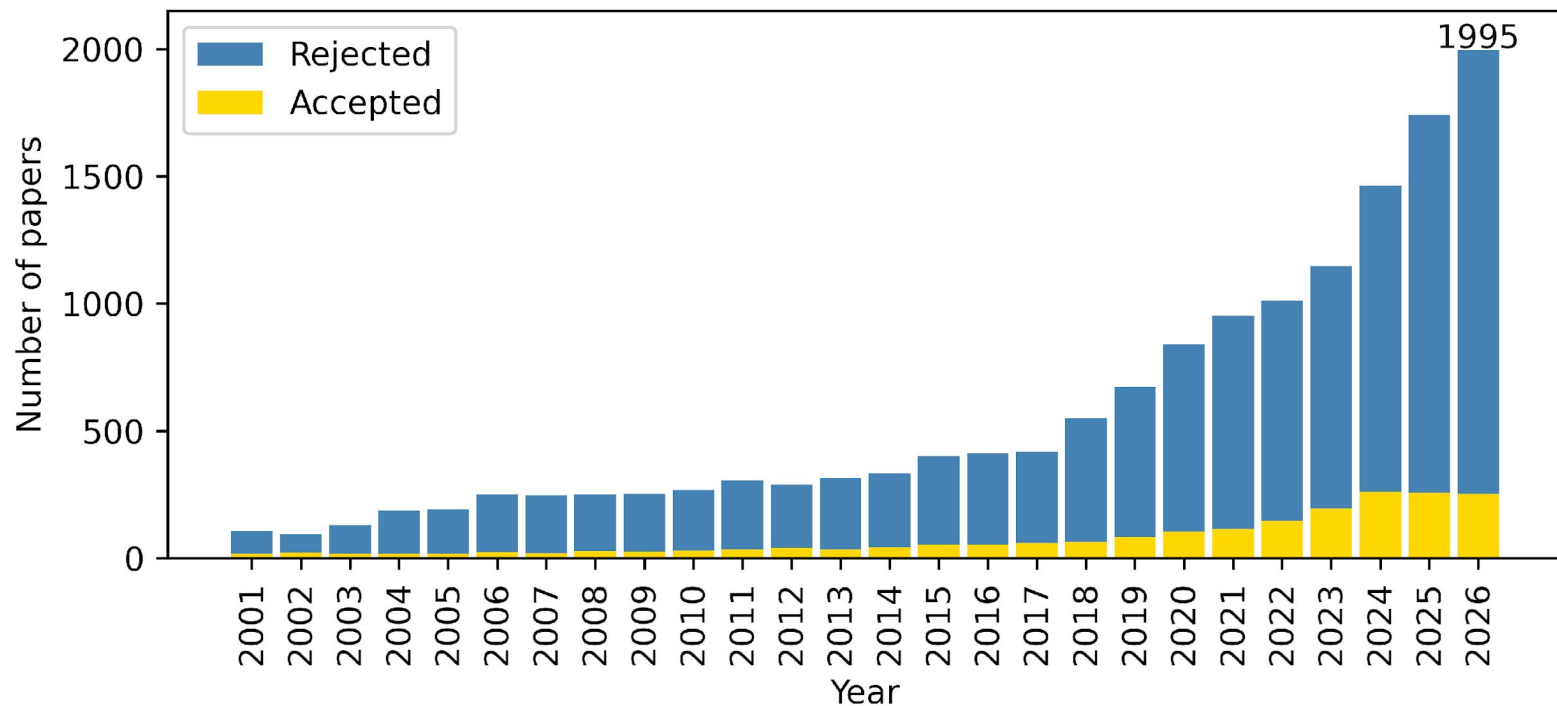
Tuesday May 19, Continental 5, 6 - 7PM

Session with the S&P PC Chairs and (former, current, future) PC Chairs from other security conference

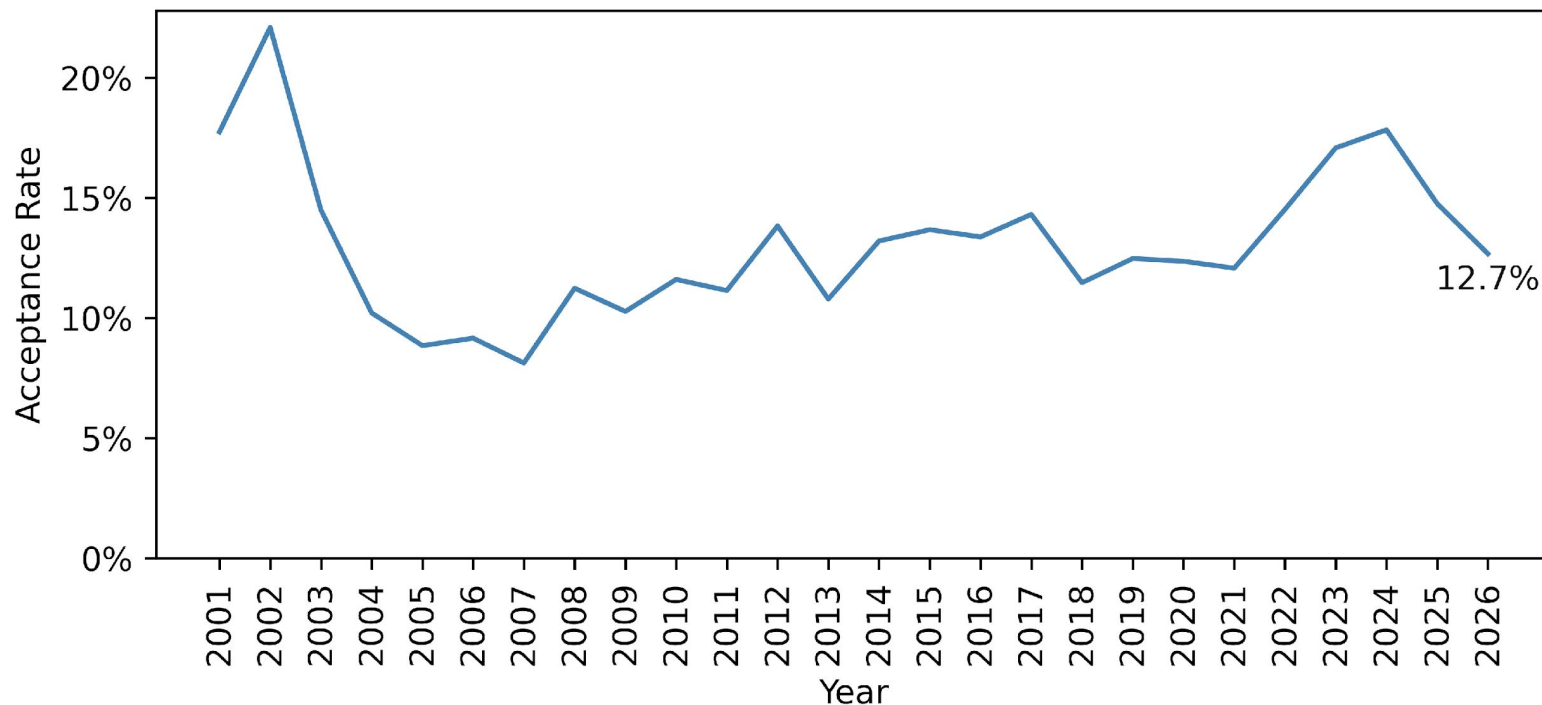
Selected Statistics

A big thank you to Mathias Payer & Will Enck for the scripts!

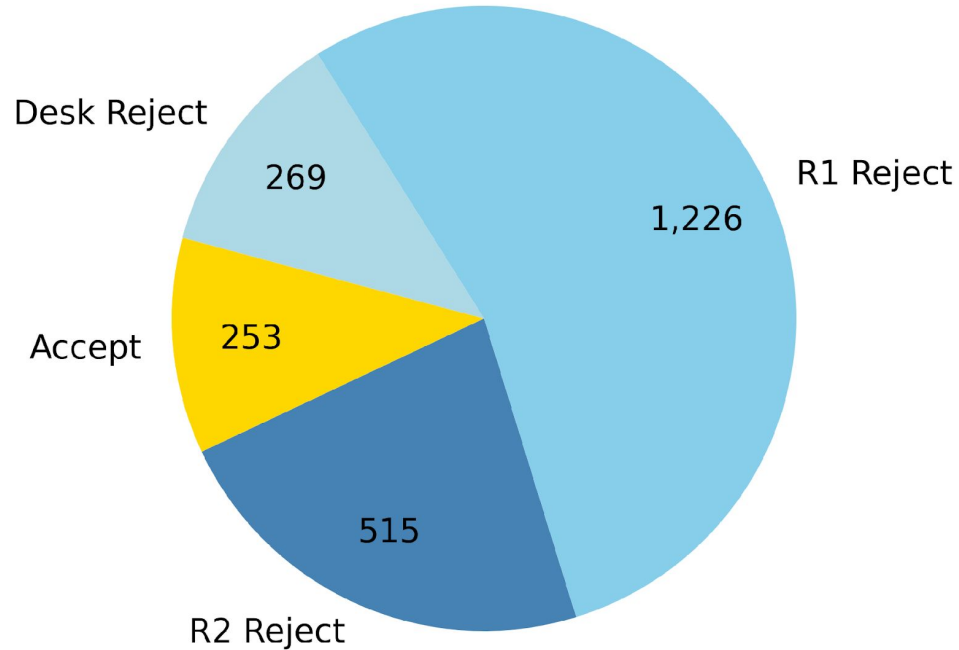
S&P Growth



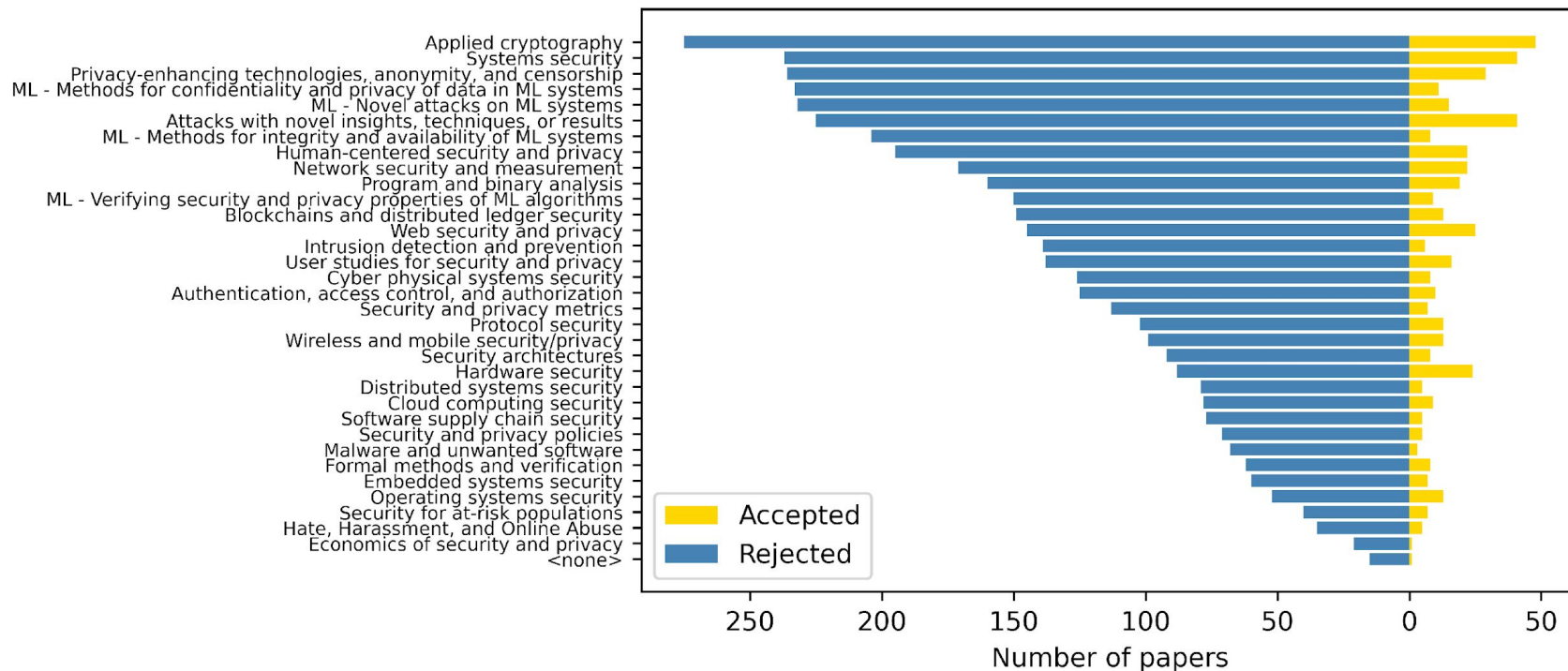
Historical Acceptance Rates



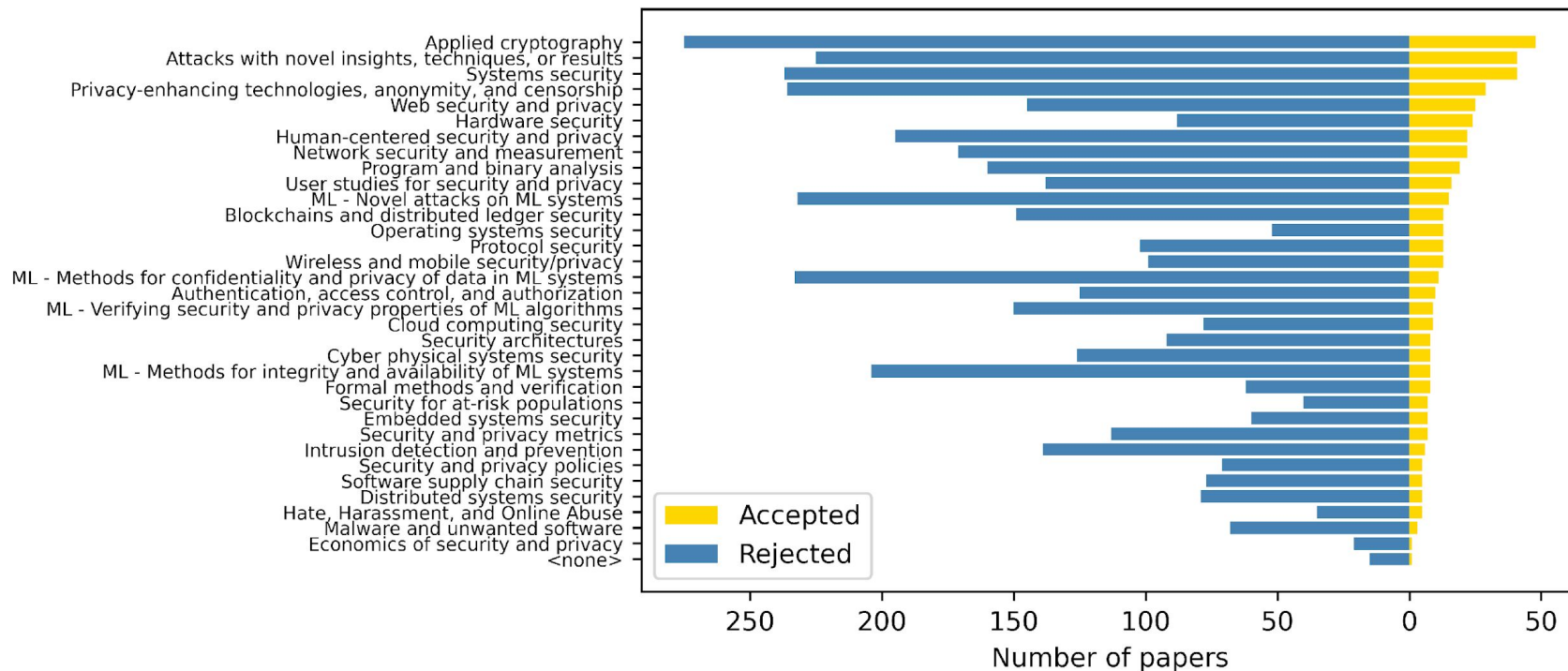
Paper Decisions During the Review Process



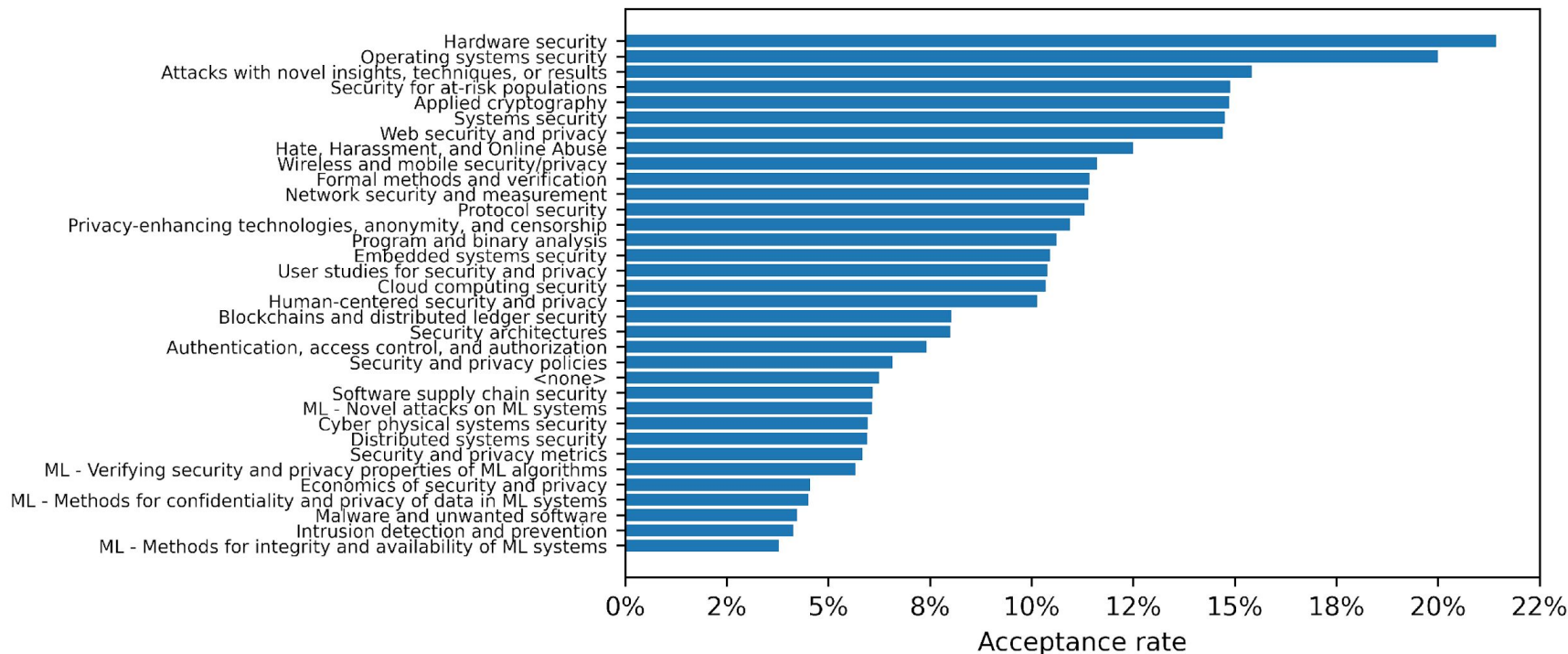
Rejected Papers by Topic



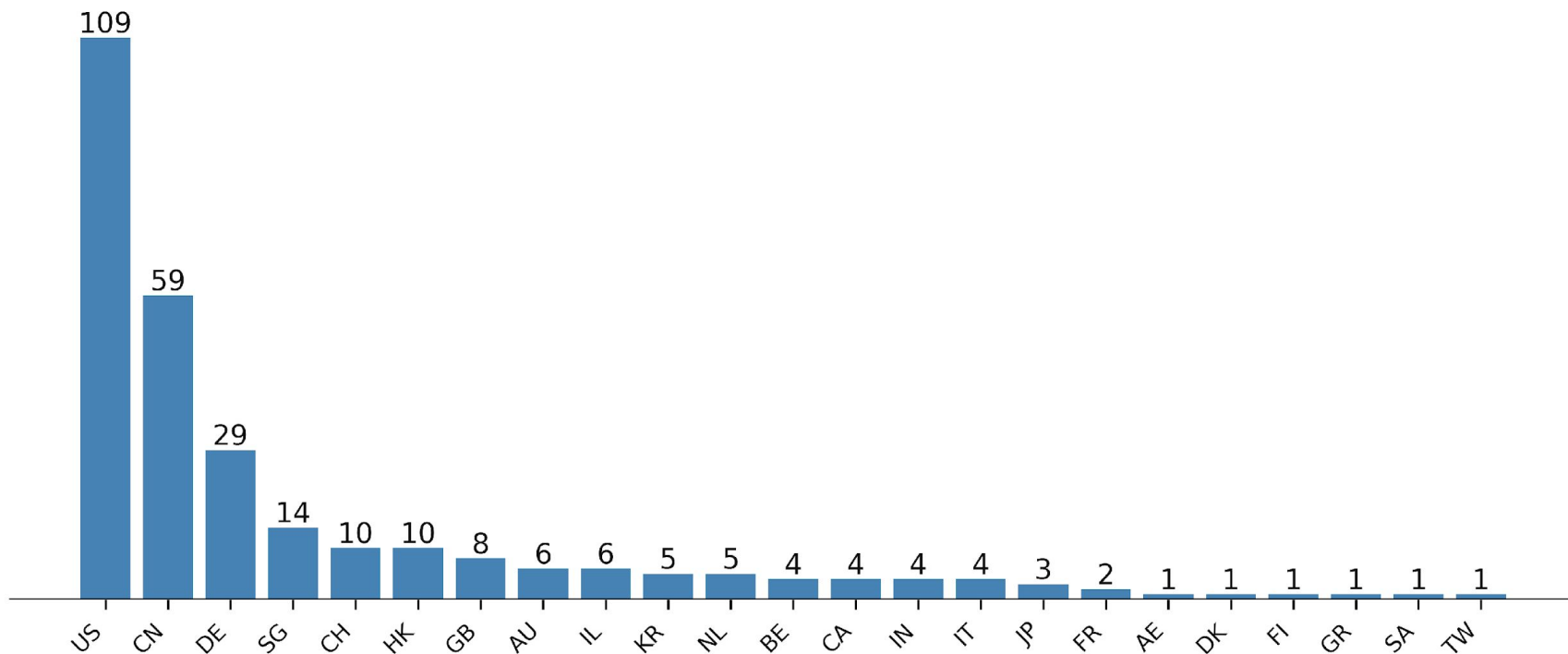
Accepted Papers by Topic



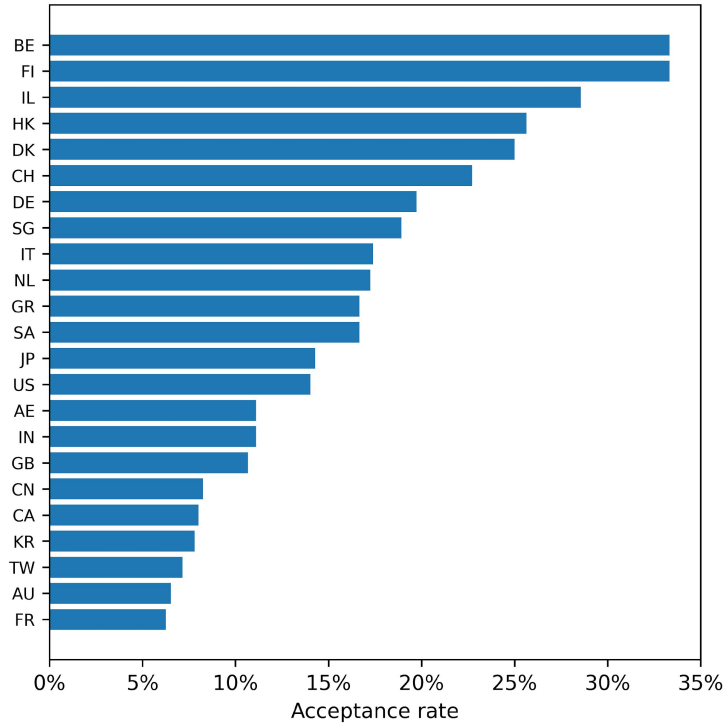
Acceptance Rate by Topic



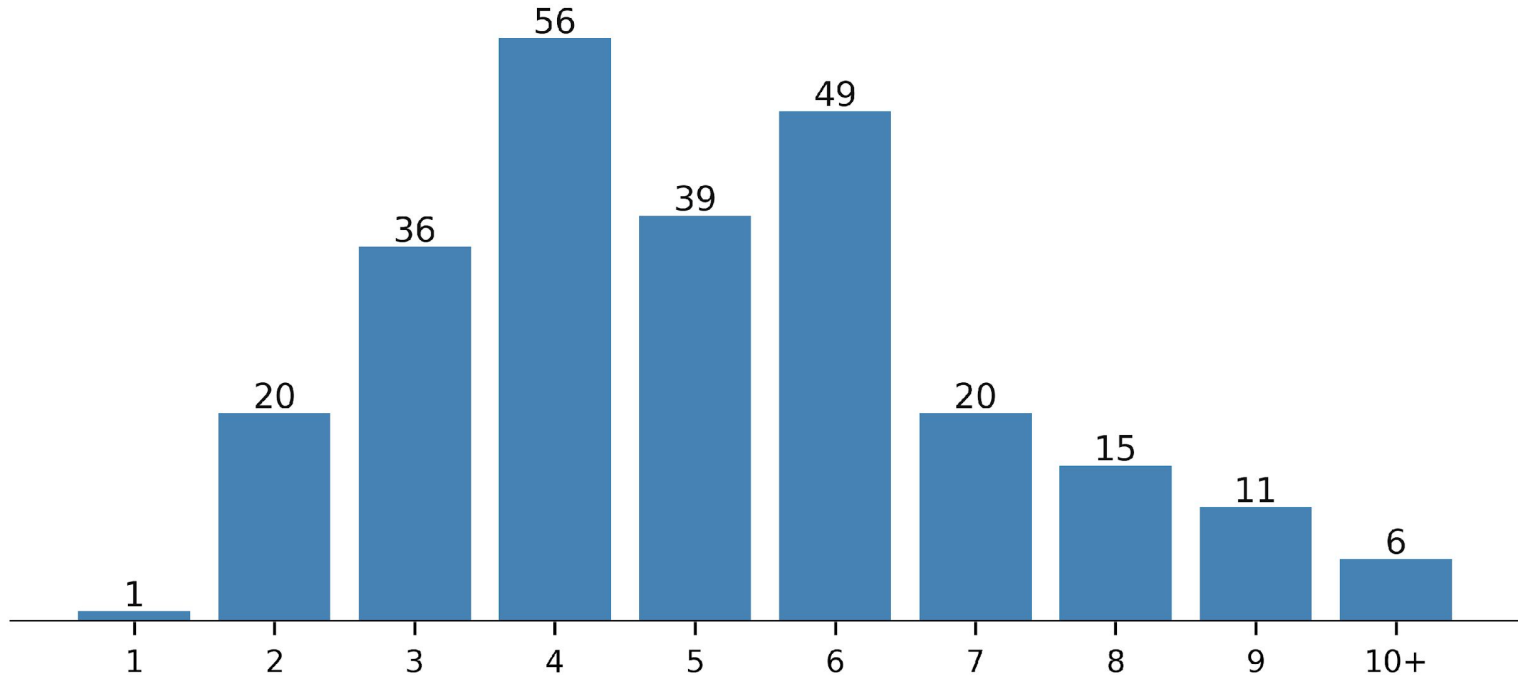
Accepted Papers by Country



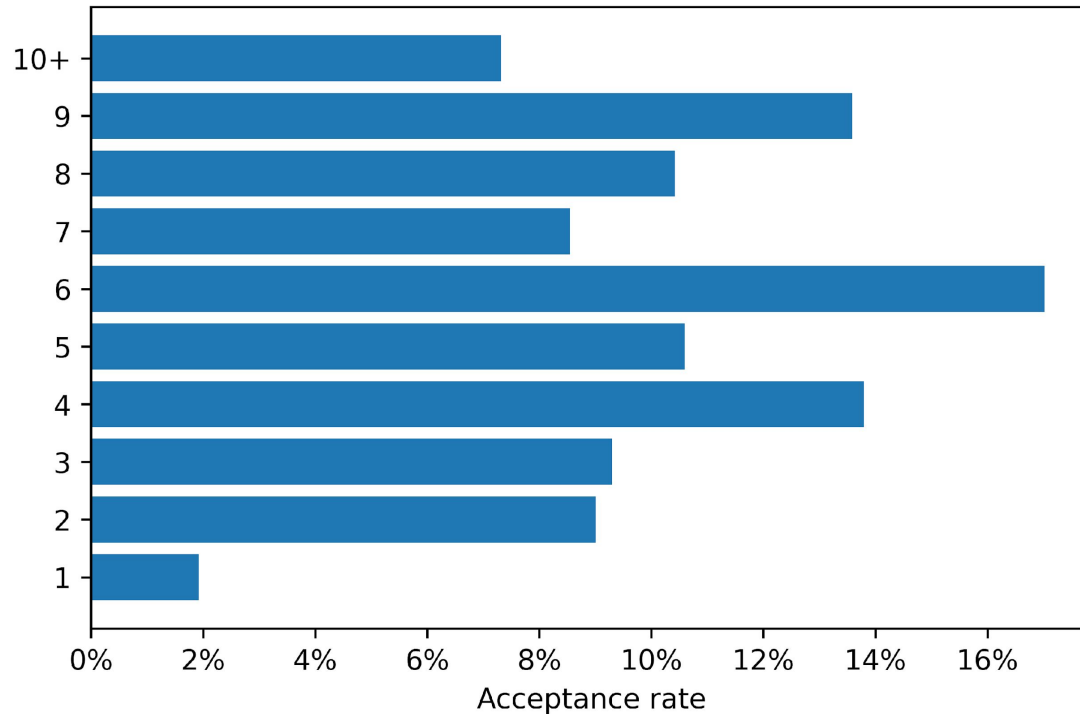
Acceptance Rate by Country



Accepted Papers by the Number of Authors



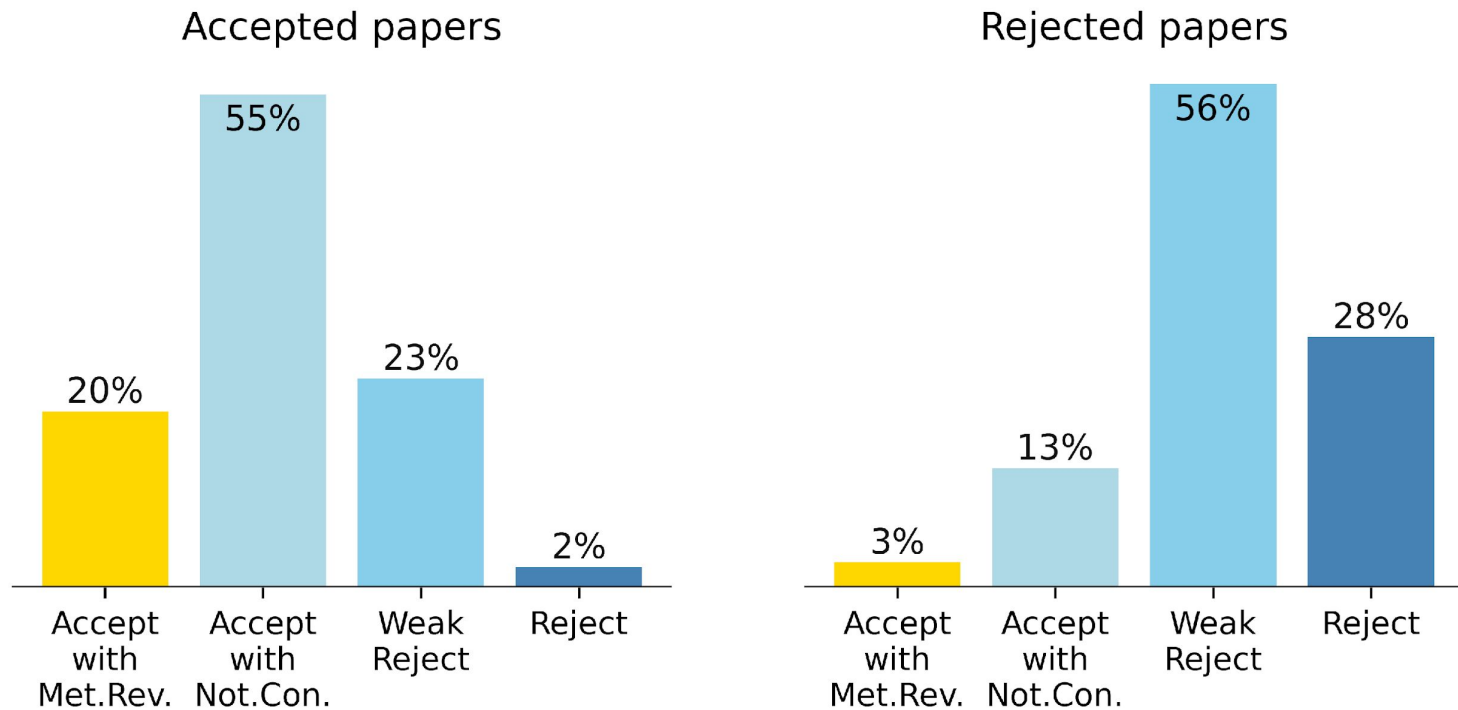
Acceptance Rate by the Number of Authors



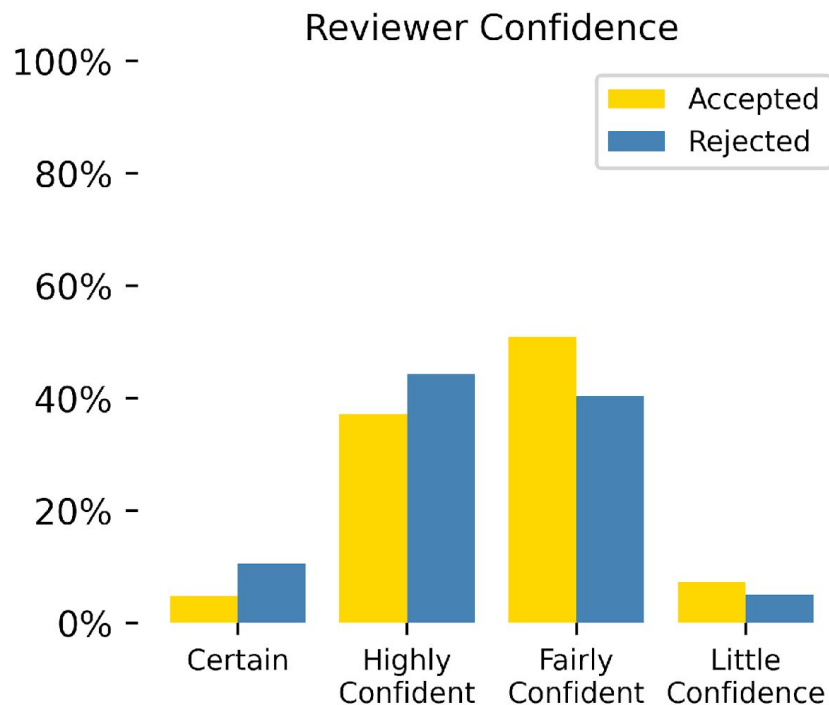
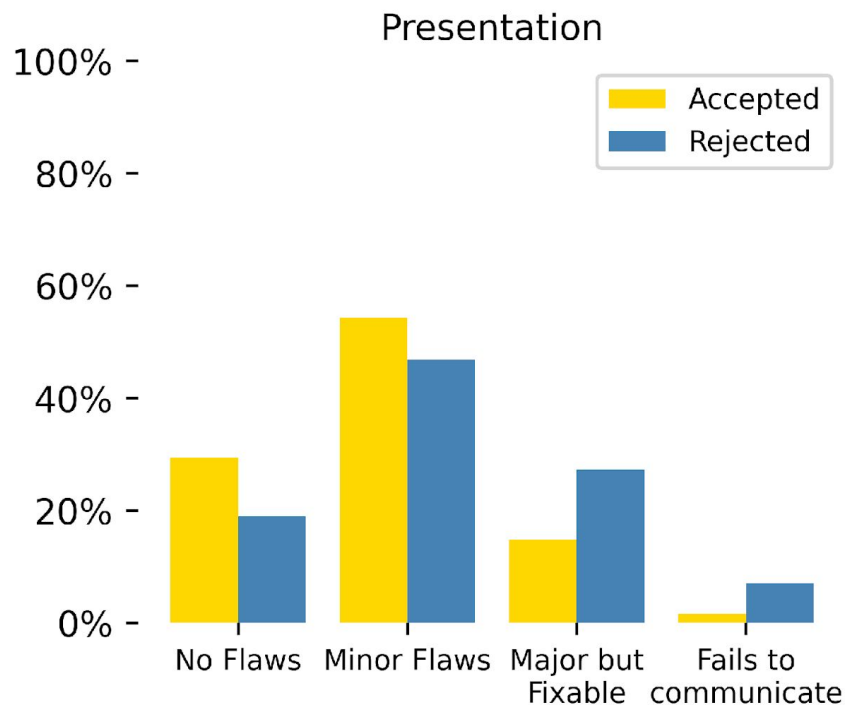
Conflicts of Interest

- Thank you to Giancarlo Pellegrino for providing the initial code base.
- Number of corrections confirmed by authors is high:
 - ~1000 submissions with discrepancies flagged
 - ~475 missing conflicts were confirmed by the authors of ~350 papers and added on HotCRP
 - ~150 unnecessary conflicts were confirmed by the authors of ~100 papers and removed from HotCRP
- Co-authors should discuss conflicts prior to submitting (received contradicting explanations for discrepancies flagged to the authors)

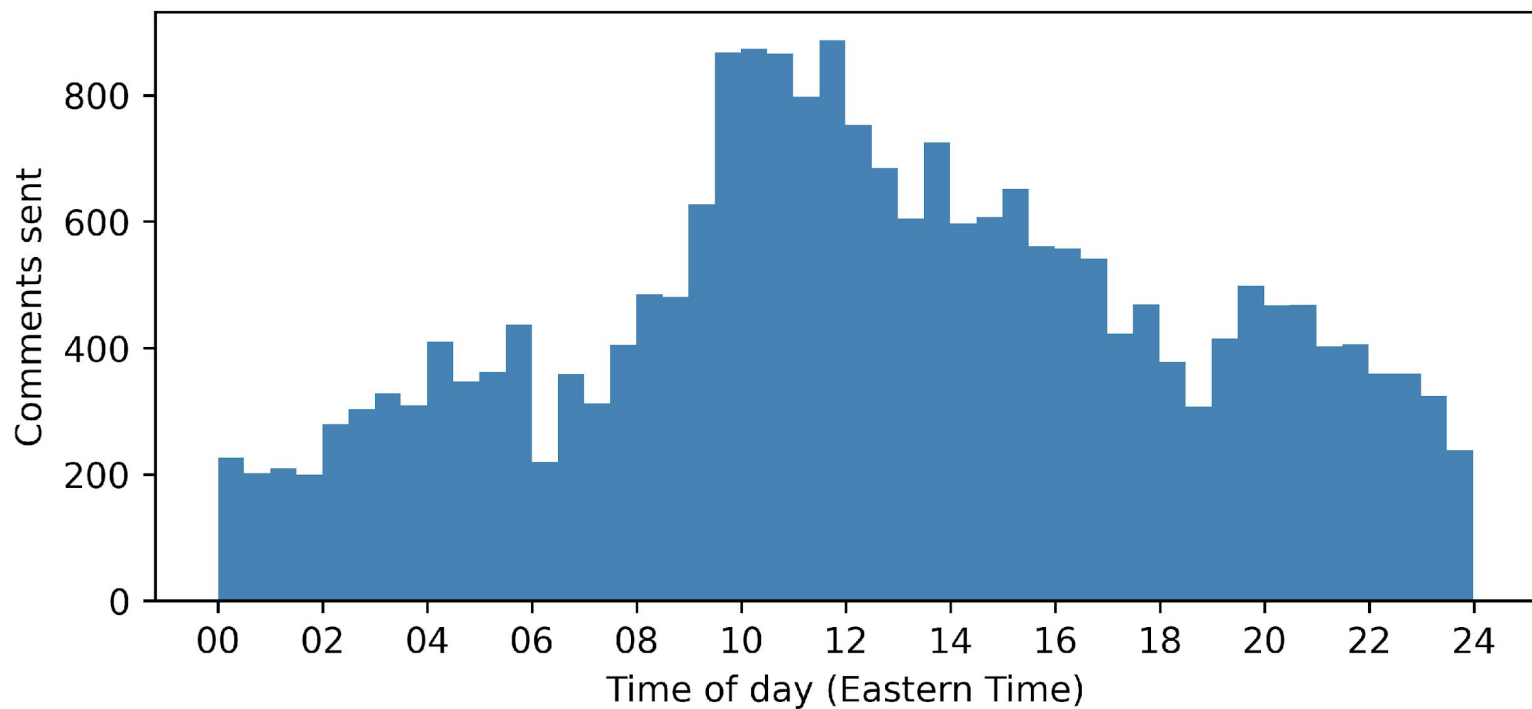
Reviews for Accepted and Rejected Papers



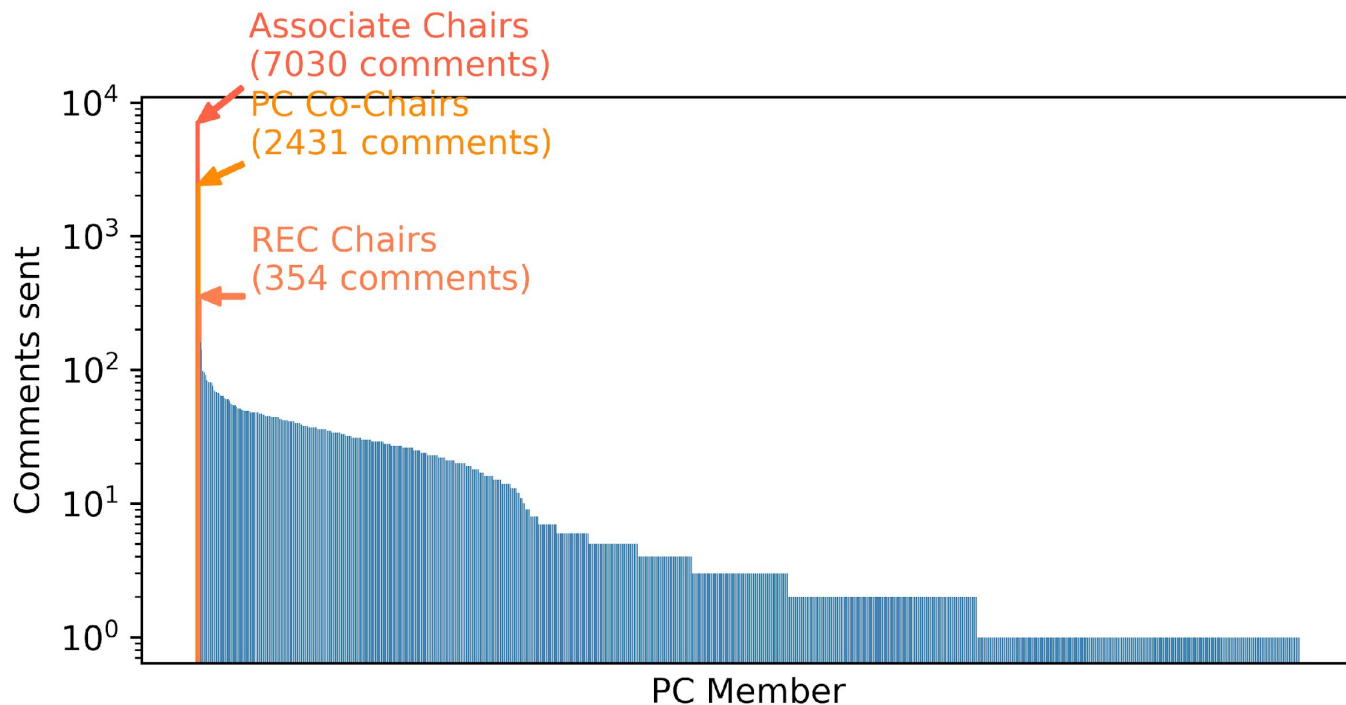
Writing Quality and Reviewer Confidence



HotCRP Comments By Time



HotCRP Comments By PC Member



16 Associate Chairs

2 REC co-Chairs

320 PC Members

Thank you very much for your help!

THANKS TO OUR PC

Distinguished Papers Awards

MAY 18-21, 2026 AT THE HILTON SAN FRANCISCO UNION SQUARE, SAN
FRANCISCO, CA

47th IEEE Symposium on Security and Privacy

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

Cristina Nita-Rotaru
Northeastern University

Nicolas Papernot
University of Toronto and Vector
Institute and Google DeepMind

Distinguished Paper Awards

- Award committee consists of the Associate Chairs
- Shortlist of 28 papers proposed by Associate Chairs
 - AC voted, they had 50 points to distribute
 - PC Chairs did not propose papers or vote
- 13 papers stood out above the others
 - <1% of submissions
- 1 paper accepted and voted Distinguished paper last year
 - Delayed because of vulnerability disclosure and patch issue



Enter, Exit, Page Fault, Leak: Testing Isolation Boundaries for Microarchitectural Leaks

Oleksii Oleksenko (Azure Research, Microsoft)

Flavien Solt (ETH Zurich)

Cédric Fournet (Azure Research, Microsoft)

Jana Hofmann (Azure Research, Microsoft)

Boris Köpf (Azure Research, Microsoft)

Stavros Volos (Azure Research, Microsoft)

Your Compiler is Backdooring Your Model: Understanding and Exploiting Compilation Inconsistency Vulnerabilities in Deep Learning Compilers

Simin Chen (Columbia University)

Jinjun Peng (Columbia University)

Yixin He (University of Southern California)

Junfeng Yang (Columbia University)

Baishakhi Ray (Columbia University)

Demystifying and Exploiting ASLR on NVIDIA GPUs

Ruofan Zhu (Zhejiang University)

Ganhao Chen (Zhejiang University)

Wenbo Shen (Zhejiang University)

Lyuye Zhang (Nanyang Technological University)

Dakun Shen (Zhejiang University)

Rui Chang (Zhejiang University)

Yanan Guo (University of Rochester)

Phoenix: Rowhammer Attacks on DDR5 with Self-Correcting Synchronization

Diego Meyer (ETH Zurich)

Patrick Jattke (ETH Zurich)

Michele Marazzi (ETH Zurich)

Salman Qazi (Google)

Daniel Moghimi (Google)

Kaveh Razavi (ETH Zurich)

Nebula: Proving machine executions via folding schemes

Arasu Arun (New York University)

Srinath Setty (Microsoft Research)

LLMs in the SOC: An Empirical Study of Human-AI Collaboration in Security Operations Centers

Ronal Singh (Data61, CSIRO)

Shahroz Tariq (Data61, CSIRO)

Fatemeh Jalalvand (Data61, CSIRO)

Mohan Baruwal Chhetri (Data61, CSIRO)

Surya Nepal (Data61, CSIRO)

Cecile Paris (Data61, CSIRO)

Martin Lochner (eSentire Inc)

Auditing Apple's DifferentialPrivacy.framework: Implementation Bugs, Misconfigurations, and Practical Risks

Rishav Chourasia (Betterdata.ai)

Ergute Bao (Mohamed bin Zayed University of Artificial Intelligence)

Uzair Javaid (Betterdata.ai)

Xiaokui Xiao (National University of Singapore)

Lost in Translation: Text Message Spoofing via Email

Sumanth Rao (UC San Diego)

Ye Shu (UC San Diego)

Stefan Savage (UC San Diego)

Aaron Schulman (UC San Diego)

Geoffrey M. Voelker (UC San Diego)

Enze Liu (CMU)

FASTION: Breaking AMD SEV-SNP by Hijacking Control over Interconnect

Philipp Giersfeld (ETH Zurich)
Benedict Schlüter (ETH Zurich)
Shweta Shinde (ETH Zurich)

Weighted Batched Threshold Encryption with Applications to Mempool Privacy

Amit Agarwal (Category Labs)

Kushal Babel (Category Labs)

Sourav Das (Category Labs)

Babak Poorebrahim Gilkalaye (Category Labs)

Arup Mondal (Ashoka University)

Benny Pinkas (Bar-Ilan University)

Peter Rindal (Category Labs)

Aayush Yadav (George Mason University)

TREVEX: A Black-Box Detection Framework For Data-Flow Transient Execution Vulnerabilities

Daniel Weber (CISPA Helmholtz Center for Information Security)

Fabian Thomas (CISPA Helmholtz Center for Information Security)

Leon Trampert (CISPA Helmholtz Center for Information Security)

Ruiyi Zhang (CISPA Helmholtz Center for Information Security)

Michael Schwarz (CISPA Helmholtz Center for Information Security)

GPUBreach: Privilege Escalation Attacks on GPUs using Rowhammer

Chris S. Lin (University of Toronto)

Yuqin Yan (University of Toronto)

Guozhen Ding (University of Toronto)

Joyce Qu (University of Toronto)

Joseph Zhu (University of Toronto)

David Lie (University of Toronto)

Gururaj Saileshwar (University of Toronto)

Responsible Disclosure is a Two-Way Street: Empirically Measuring the Responsible Disclosure Contract in the Firmware Ecosystem

Hui Jun Tay (Arizona State University)

Souradip Nath (Arizona State University)

Arvind S Raj (Arizona State University)

Abhay Bhat (Arizona State University)

Ishan Bansal (Arizona State University)

Audrey Dutcher (Arizona State University)

Moritz Schloegel (Arizona State University)

Adam Doupé (Arizona State University)

Tiffany Bao (Arizona State University)

Yan Shoshitaishvili (Arizona State University)

Ruoyu Wang (Arizona State University)

Goldilocks and the Three P-States: Mitigating Hertzbleed via Adaptive Frequency Control

Inwhan Chun (Carnegie Mellon University)

Christine Guo (Princeton University)

Riccardo Paccagnella (Carnegie Mellon University)

Artifact Evaluation

MAY 18-21, 2026 AT THE HILTON SAN FRANCISCO UNION SQUARE, SAN
FRANCISCO, CA

47th IEEE Symposium on Security and Privacy

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

Jelena Mirkovic
USC / ICI

Manuel Egele
Boston University

Artifact Evaluation

- First year at S&P – asked for specific metadata format and evaluation on public research infrastructure where possible
- Cycle 1
 - 27 artifacts submitted
 - 8 Available badges, 2 Functional, 17 Reproducible
- Cycle 2
 - 29 artifacts submitted
 - 2 Available badges, 7 Functional, 20 Reproducible
- 4 distinguished artifact and 4 distinguished evaluator awards

Distinguished Artifacts

- Daniel Weber, Fabian Thomas, Leon Trampert, Ruiyi Zhang, Michael Schwarz, “TREVEEX: A Black-Box Detection Framework For Generic Transient Execution Vulnerabilities”
- Tim Rausch, Sylvain Chatel, Wouter Lueks, “xDup: Privacy-Preserving Deduplication for Humanitarian Organizations using Fuzzy PSI”
- Gabriele Digregorio, Marco Di Gennaro, Stefano Zanero, Stefano Longari, Michele Carminati, “On the (In)Security of Loading Machine Learning Models”
- Bofan Li, Zhankai Ye, Weikuan Yu, Yongning Tang, Xin Liu, “2FiA: Towards WiFi Sensing-Based Authentication with Unique Biometrics”

Distinguished Evaluators

- Aritra Dasgupta, University of Florida
- Muhammad Danish, University of New Mexico
- Mohammad Jamshir Qureshi, Purdue University
- Jinseo Lee, KAIST

Test of Time Awards

MAY 18-21, 2026 AT THE HILTON SAN FRANCISCO UNION SQUARE, SAN
FRANCISCO, CA

47th IEEE Symposium on Security and Privacy

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

Dongyan Xu
Purdue University

S&P Test of Time (ToT) Award

- Honoring influential papers from the IEEE S&P Symposium that have made a lasting impact on computer security and privacy
- This year we expanded the eligibility scope to *all S&P papers published in 2016 and earlier*
 - Impacts may take more than 10-12 years to show
 - Papers will have unlimited (instead of three) chances to win
 - Approved by S&P Steering Committee Chair and S&P'26 General Chair
- ToT Award Committee
 - Lujo Bauer (CMU), Jeremy Epstein (GTRI), Adrian Perrig (ETH), Christina Pöpper (NYUAD), Daphne Yao (VT), Dongyan Xu (Purdue, Chair)

S&P Test of Time (ToT) Award

- Phase 1: Creating candidate pool
 - By **both** citation counts (IEEE Xplore) and committee nominations
 - 79 papers identified as candidates
- Phase 2: Selecting finalists
 - 14 finalists selected after committee discussion and recommendation
- Phase 3: (Ranked choice) voting to decide winners
 - 5 papers “made the cut”
- Conflicts of interest declared and avoided in the process
- **The winners are (in chronological order):**

S&P Test of Time (ToT) Award

“A Comparison of Commercial and Military Computer Security Policies”, *IEEE S&P 1987*

David D. Clark, David R. Wilson

For its fundamental and lasting impact in the area of security policies



S&P Test of Time (ToT) Award

“The Chinese Wall Security Policy”, *IEEE S&P*
1989

David F.C. Brewer, Michael J. Nash

*For its influential instantiation of practical security
models and policies*



S&P Test of Time (ToT) Award

“De-anonymizing Social Networks”, *IEEE S&P*
2009

Arvind Narayanan, Vitaly Shmatikov

*For its continued influence on social network
privacy research and practice*



S&P Test of Time (ToT) Award

“Dissecting Android Malware: Characterization and Evolution”, *IEEE S&P 2012*

Yajin Zhou, Xuxian Jiang

For its lasting impact on mobile app security research and practice



S&P Test of Time (ToT) Award

“The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes”, *IEEE S&P 2012*

Joseph Bonneau, Cormac Herley, Paul C. van Oorschot, Frank Stajano

For its lasting influence on research and systematization of knowledge in web authentication



Enjoy the Conference!



Agenda

- General Chair Opening Remarks (Alina Oprea): 10 minutes
- PC Chairs and award session (Cristina Nita-Rotaru and Nicolas Papernot): 40 minutes
 - Review process
 - Best paper awards
 - Best reviewer awards
- Artifact evaluation (Jelena Mirkovic): 5 minutes
- ToT award (Dongyan Xu): 20 minutes