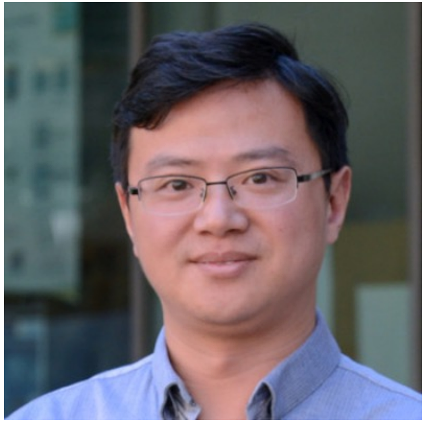
Welcome from the NDSS 2025 General Chairs

David Balenson

USC Information
Sciences Institute



Heng Yin

University of
California, Riverside

Welcome to the Wyndham San Diego Bayside!

Registered Attendees

NDSS 2025: 687 (+8.5%)
NDSS 2024: 633
NDSS 2023: 637
NDSS 2022: 579
NDSS 2021: 770 (virtual)

https://symphony.cdn.tambourine.com/wyndham-san-diego-bayside/media/cache/wyndham-sandiego-homepage-hero-5cc099fddff02-1500x640.webp

Organizing Committee

General Chairs
David Balenson, USC Information Sciences Institute
Heng Yin, University of California, Riverside

Program Chairs
Christina Pöpper, NYU Abu Dhabi
Hamed Okhravi, MIT Lincoln Laboratory

Artifact Evaluation Committee Chairs
Daniele Cono D'Elia, Sapienza University
Mathy Vanhoef, KU Leuven

Workshops Chairs
Jelena Mirkovic, USC Information Sciences Institute
Sébastien Bardin, CEA LIst

Poster Session Chairs
Tianshi Li, Northeastern University
Kaushal Kafle, University of South Florida

Student Support Committee
Tingting Chen, Cal Poly Pomona (Chair)
Eric Chan-Tin, Loyola University Chicago
Younghee Park, San Jose State University
Huirong Fu, Oakland University
Lei Yu, Rensselaer Polytechnic Institute

Publicity Chair
Yue Xiao, Indiana University Bloomington

Publications Chairs
Mridula Singh, CISPA
Hyungsub Kim, Indiana University Bloomington

Local Arrangements Chair
Tom Hutton, San Diego Supercomputer Center

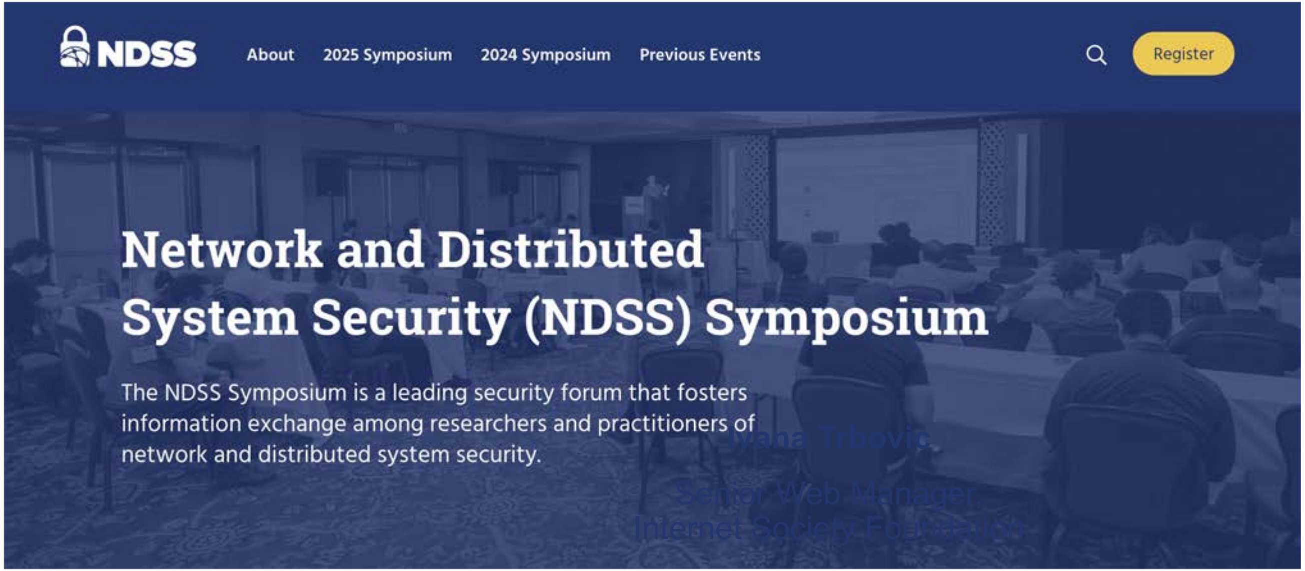
Sponsorship Coordinators
Yongdae Kim, KAIST
Heng Yin, University of California, Riverside
Mauro Conti, University of Padua

The Internet Society/Foundation Staff
Raquel Kroich, Event Manager
Sally Harvey, Sponsorships
Robin Wilton, Program Liaison
Robbie Mitchell, Publicity
Ivana Trbovic, Website Manager`

Steering Group

Yongdae Kim, KAIST (Chair)
Robin Wilton, Internet Society (Co-chair)
Christopher Kruegel, UC Santa Barbara
Michael Reiter, Duke University
Wenyuan Xu, Zhejiang University
Gene Tsudik, UC Irvine
Gabriela Ciocarlie, University of Texas at San Antonio
Lorenzo Cavallaro, University College London
Daphne Yao, Virginia Tech
Anita Nikolich, UIUC
Ahmad-Reza Sadeghi, TU Darmstadt

NDSS Website



Network and Distributed System Security (NDSS) Symposium

The NDSS Symposium is a leading security forum that fosters information exchange among researchers and practitioners of network and distributed system security.

Ivana Trbovic

Senior Web Manager,
Internet Society Foundation

A Special Thanks!

"An unsung hero is someone who makes a significant impact or contribution but does not receive the recognition or praise they deserve. These individuals often work behind the scenes, quietly making a difference without seeking attention or acknowledgment."
-ChatGPT

Ivana Trbović

Senior Web Manager,
Internet Society Foundation

Program Highlights

211 Technical Papers

63 Evaluated Artifacts

37 Posters

Two Keynotes:

- Dr. Johanna Sepúlveda, Airbus Defence and Space
- Dr. Kathleen Fisher, DARPA/I2O

Eight co-located events:

- Monday: FutureG, SDIoTSec, SpaceSec, USEC, WOSOC
- Friday: BAR, IMPACT, MADWeb

31 ISOC NDSS Fellows

And X BoFs …

Birds-of-a-Feather Sessions (BoFs)

Wednesday, 26 February, 16:30-17:45

Meeting spaces are available for informal gatherings of people interested in a topic (or you can use hotel spaces, like the pool area)

Opportunity for attendees to share ideas, discuss challenges, and network in an informal setting

Please reach out to Heng Yin <heng.yin@ucr.edu> if you're interested in organizing and holding a BOF

Thank You to Our Sponsors

Gold Sponsor	TikTok
Coffee Break Sponsor	Google
Silver Sponsors	ANT GROUP amazon | science FUTUREWEI Technologies paloalto NETWORKS
Lanyard Sponsor	Qualcomm
MADWeb 2025 Best Paper	paloalto NETWORKS

Housekeeping

Meetings Rooms

- **Paper tracks**: Pacific Ballroom, Coast Ballroom, Porthole, and Embarcadero
- **Posters and Lunches:** Loma Vista Terrace and Harborside
- **Breakfast & Breaks:** Pacific Ballroom D

Slack Channels

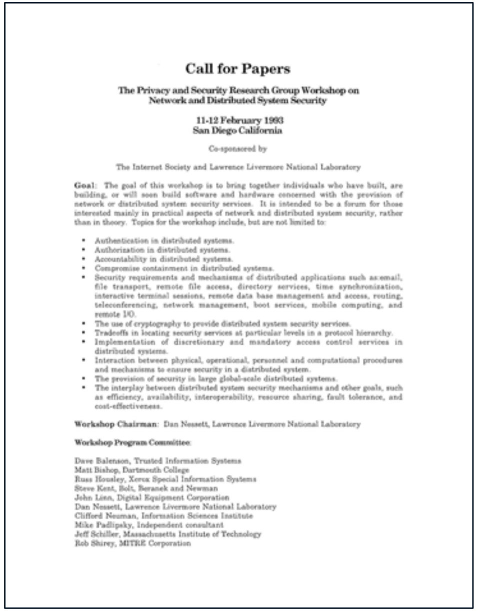
- Join workspace at https://ndss-2025.slack.com/
- One channel per track for Q&A
- One channel for event staff

1993 PSRG Workshop on Network and Distributed System Security (NDSS)

NDSS 1993 Call for Papers

Goal: The goal of this workshop is to bring together individuals who have built, are building, or will soon build software and hardware concerned with the provision of network or distributed system security services. It is intended to be a forum for those interested mainly in practical aspects of network and distributed system security, rather than in theory. Topics for the workshop include, but are not limited to:

- Authentication in distributed systems.
- Authorization in distributed systems.
- Accountability in distributed systems.
- Compromise containment in distributed systems.
- Security requirements and mechanisms of distributed applications such as email, file transport, remote file access, directory services, time synchronization, interactive terminal sessions, remote data base management and access, routing, teleconferencing, network management, boot services, mobile computing, and remote I/O.
- The use of cryptography to provide distributed system security services.
- Tradeoffs in locating security services at particular levels in a protocol hierarchy.
- Implementation of discretionary and mandatory access control services in distributed systems.
- Interaction between physical, operational, personnel and computational procedures and mechanisms to ensure security in a distributed system.
- The provision of security in large global-scale distributed systems.
- The interplay between distributed system security mechanisms and other goals, such as efficiency, availability, interoperability, resource sharing, fault tolerance, and cost-effectiveness.



Call for Papers

The Privacy and Security Research Group Workshop on Network and Distributed System Security

11-12 February 1993
San Diego California

Co-sponsored by

The Internet Society and Lawrence Livermore National Laboratory

Goal: The goal of this workshop is to bring together individuals who have built, are building, or will soon build software and hardware concerned with the provision of network or distributed system security services. It is intended to be a forum for those interested mainly in practical aspects of network and distributed system security, rather than in theory. Topics for the workshop include, but are not limited to:

- Authentication in distributed systems.
- Authorization in distributed systems.
- Accountability in distributed systems.
- Compromise containment in distributed systems.
- Security requirements and mechanisms of distributed applications such as email, file transport, remote file access, directory services, time synchronization, interactive terminal sessions, remote data base management and access, routing, teleconferencing, network management, boot services, mobile computing, and remote I/O.
- The use of cryptography to provide distributed system security services.
- Tradeoffs in locating security services at particular levels in a protocol hierarchy.
- Implementation of discretionary and mandatory access control services in distributed systems.
- Interaction between physical, operational, personnel and computational procedures and mechanisms to ensure security in a distributed system.
- The provision of security in large global-scale distributed systems.
- The interplay between distributed system security mechanisms and other goals, such as efficiency, availability, interoperability, resource sharing, fault tolerance, and cost-effectiveness.

Workshop Chairman: Dan Nessett, Lawrence Livermore National Laboratory

Workshop Program Committee:

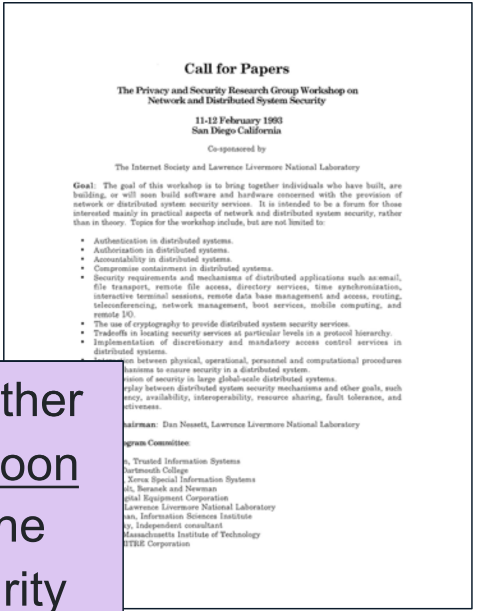
Dave Balenson, Trusted Information Systems
Matt Bishop, Dartmouth College
Russ Housley, Xerox Special Information Systems
Steve Kent, Bolt, Beranek and Newman
John Linn, Digital Equipment Corporation
Dan Nessett, Lawrence Livermore National Laboratory
Clifford Neuman, Information Sciences Institute
Mike Padlipsky, Independent consultant
Jeff Schiller, Massachusetts Institute of Technology
Rob Shirey, MITRE Corporation

NDSS 1993 Call for Papers

Goal: The goal of this workshop is to bring together individuals who have built, are building, or will soon build software and hardware concerned with the provision of network or distributed system security services. It is intended to be a forum for those interested mainly in practical aspects of network and distributed system security, rather than in theory. Topics for the workshop include, but are not limited to:

- Authentication in
- Authorization in d
- Accountability in
- Compromise cont
- Security requirem
  remote file access
  remote data base r
  boot services, mol
- The use of cryptog
- Tradeoffs in locat
- Implementation o
- Interaction betwee e
  security in a distri
- The provision of security in large global-scale distributed systems.
- The interplay between distributed system security mechanisms and other goals, such as efficiency, availability, interoperability, resource sharing, fault tolerance, and cost-effectiveness.

Goal: The goal of this workshop is to bring together individuals who have built, are building, or will soon build software and hardware concerned with the provision of network or distributed system security services. It is intended to be a forum for those interested mainly in practical aspects of network and distributed system security, rather than in theory.



Call for Papers

The Privacy and Security Research Group Workshop on
Network and Distributed System Security

11-12 February 1993
San Diego California

Co-sponsored by

The Internet Society and Lawrence Livermore National Laboratory

Goal: The goal of this workshop is to bring together individuals who have built, are building, or will soon build software and hardware concerned with the provision of network or distributed system security services. It is intended to be a forum for those interested mainly in practical aspects of network and distributed system security, rather than in theory. Topics for the workshop include, but are not limited to:

- Authentication in distributed systems.
- Authorization in distributed systems.
- Accountability in distributed systems.
- Compromise containment in distributed systems.
- Security requirements and mechanisms of distributed applications such as email, file transport, remote file access, directory services, time synchronization, interactive terminal sessions, remote data base management and access, routing, teleconferencing, network management, boot services, mobile computing, and remote I/O.
- The use of cryptography to provide distributed system security services.
- Tradeoffs in locating security services at particular levels in a protocol hierarchy.
- Implementation of discretionary and mandatory access control services in distributed systems.
- Interaction between physical, operational, personnel and computational procedures
  chanisms to ensure security in a distributed system.
  vision of security in large global-scale distributed systems.
  rplay between distributed system security mechanisms and other goals, such
  ency, availability, interoperability, resource sharing, fault tolerance, and
  ctiveness.

hairman: Dan Nessett, Lawrence Livermore National Laboratory

gram Committee:

n, Trusted Information Systems
Dartmouth College
, Xerox Special Information Systems
olt, Beranek and Newman
gital Equipment Corporation
Lawrence Livermore National Laboratory
nan, Information Sciences Institute
ky, Independent consultant
Massachusetts Institute of Technology
ITRE Corporation

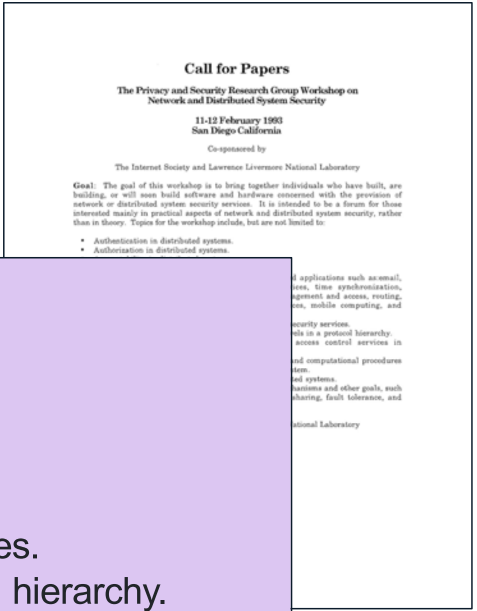
NDSS 1993 Call for Papers

Goal: The goal of this workshop is to bring together individuals who have built, are building, or will soon build software and hardware concerned with the provision of network or distributed system secu
aspects of n
include, bu

- Authenti
- Authoriz
- Account
- Compro
- Security
  remote f
  remote d
  boot ser
- The use
- Tradeof
- Impleme
- Interacti
  security
- The prov
- The inte
  interope

Topics for the workshop include, but are not limited to:

- Authentication in distributed systems.
- Authorization in distributed systems.
- Accountability in distributed systems.
- Compromise containment in distributed systems.
- Security requirements and mechanisms of distributed applications
- The use of cryptography to provide distributed system security services.
- Tradeoffs in locating security services at particular levels in a protocol hierarchy.
- Implementation of DAC and MAC services in distributed systems.
- Interaction between physical, operational, personnel and computational procedures and mechanisms
- The provision of security in large global-scale distributed systems.
- The interplay between distributed system security mechanisms and other goals, such as efficiency, availability, interoperability, resource sharing, fault tolerance, and cost-effectiveness.



Call for Papers

The Privacy and Security Research Group Workshop on Network and Distributed System Security

11-12 February 1993
San Diego California

Co-sponsored by

The Internet Society and Lawrence Livermore National Laboratory

Goal: The goal of this workshop is to bring together individuals who have built, are building, or will soon build software and hardware concerned with the provision of network or distributed system security services. It is intended to be a forum for those interested mainly in practical aspects of network and distributed system security, rather than in theory. Topics for the workshop include, but are not limited to:

- Authentication in distributed systems.
- Authorization in distributed systems.

d applications such as email,
ices, time synchronization,
agement and access, routing,
ces, mobile computing, and

ecurity services.
els in a protocol hierarchy.
access control services in

nd computational procedures
tem.
ted systems.
hanisms and other goals, such
sharing, fault tolerance, and

tional Laboratory

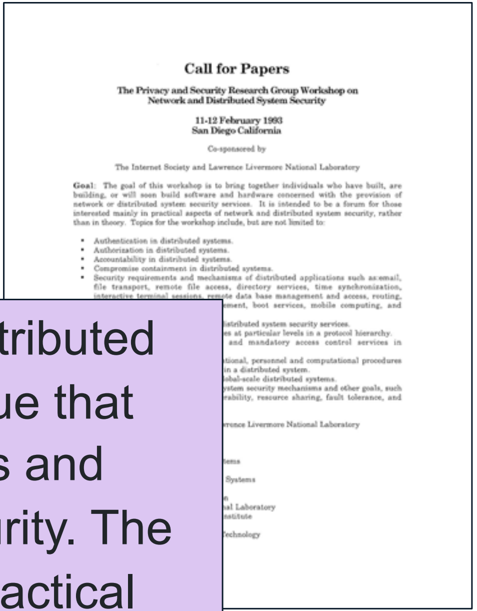
NDSS 1993 Call for Papers

Goal: The goal of this workshop is to bring together individuals who have built, are building, or will soon build software and hardware concerned with the provision of network or distributed system security services. It is intended to be a forum for those interested mainly in practical aspects of ne

include, but a

- Authentic
- Authoriza
- Accountab
- Comprom
- Security r
  remote fil
  remote da
  boot servi
- The use o
- Tradeoffs
- Implemen
- Interaction
  security i
- The provis
- The interp
  interoperability, resource sharing, fault tolerance, and cost-effectiveness.

NDSS 2025 Call for Papers: The Network and Distributed System Security Symposium (NDSS) is a top venue that fosters information exchange among researchers and practitioners of network and distributed system security. The target audience includes everyone interested in practical aspects of network and distributed system security, with a focus on system design and implementation. A major goal is to encourage and enable the Internet community to apply, deploy, and advance the state of practical security technologies.



Call for Papers

The Privacy and Security Research Group Workshop on
Network and Distributed System Security

11-12 February 1993
San Diego California

Co-sponsored by

The Internet Society and Lawrence Livermore National Laboratory

Goal: The goal of this workshop is to bring together individuals who have built, are building, or will soon build software and hardware concerned with the provision of network or distributed system security services. It is intended to be a forum for those interested mainly in practical aspects of network and distributed system security, rather than in theory. Topics for the workshop include, but are not limited to:

- Authentication in distributed systems.
- Authorization in distributed systems.
- Accountability in distributed systems.
- Compromise containment in distributed systems.
- Security requirements and mechanisms of distributed applications such as email, file transport, remote file access, directory services, time synchronization, interactive terminal sessions, remote data base management and access, routing, ement, boot services, mobile computing, and

istributed system security services.
es at particular levels in a protocol hierarchy.
and mandatory access control services in

tional, personnel and computational procedures
in a distributed system.
lobal-scale distributed systems.
ystem security mechanisms and other goals, such
rability, resource sharing, fault tolerance, and

rence Livermore National Laboratory

tems

Systems

n
al Laboratory
nstitute

Technology

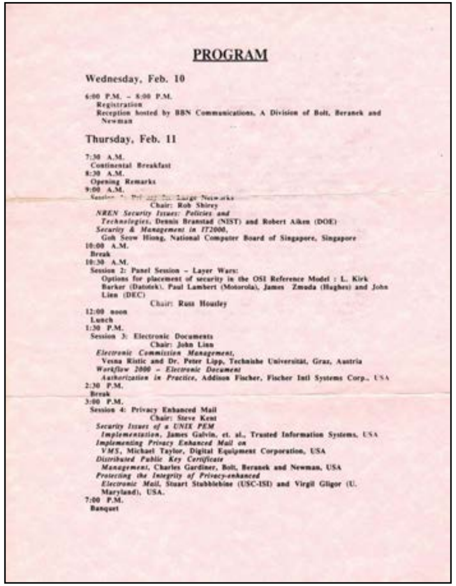
NDSS 1993 Program

Four paper sessions

- Privacy for Large Networks
- Electronic Documents
- Privacy Enhanced Mail
- Distributed Systems

Four panel sessions

- Layer Wars
- Exportable Algorithms – Promise or Pandora
- Network Security using Smart Cards
- Should Security be Legislated?



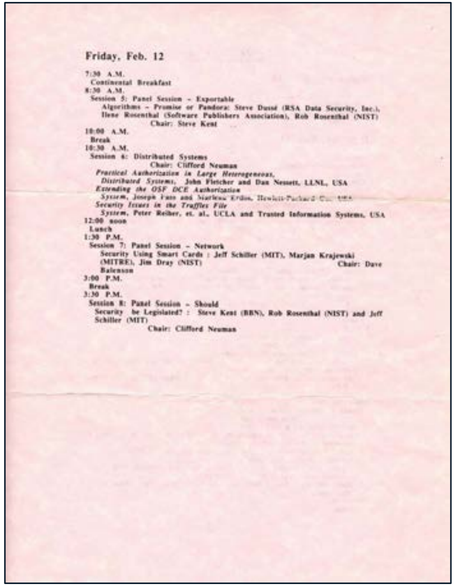
PROGRAM

Wednesday, Feb. 10

6:00 P.M. – 8:00 P.M.
Registration
Reception hosted by BBN Communications, A Division of Bolt, Beranek and Newman

Thursday, Feb. 11

7:30 A.M.
Continental Breakfast
8:30 A.M.
Opening Remarks
9:00 A.M.
Session 1: Privacy for Large Networks
Chair: Rob Shirey
NREN Security Issues: Policies and Technologies, Dennis Branstad (NIST) and Robert Aiken (DOE)
Security & Management in IT2000, Goh Seow Hiong, National Computer Board of Singapore, Singapore
10:00 A.M.
Break
10:30 A.M.
Session 2: Panel Session – Layer Wars:
Options for placement of security in the OSI Reference Model : L. Kirk Barker (Datotek), Paul Lambert (Motorola), James Zmuda (Hughes) and John Linn (DEC)
Chair: Russ Housley
12:00 noon
Lunch
1:30 P.M.
Session 3: Electronic Documents
Chair: John Linn
Electronic Commission Management, Vesna Ristic and Dr. Peter Lipp, Technishe Universität, Graz, Austria
Workflow 2000 – Electronic Document Authorization in Practice, Addison Fischer, Fischer Intl Systems Corp., USA
2:30 P.M.
Break
3:00 P.M.
Session 4: Privacy Enhanced Mail
Chair: Steve Kent
Security Issues of a UNIX PEM Implementation, James Galvin, et. al., Trusted Information Systems, USA
Implementing Privacy Enhanced Mail on VMS, Michael Taylor, Digital Equipment Corporation, USA
Distributed Public Key Certificate Management, Charles Gardiner, Bolt, Beranek and Newman, USA
Protecting the Integrity of Privacy-enhanced Electronic Mail, Stuart Stubblebine (USC-ISI) and Virgil Gligor (U. Maryland), USA.
7:00 P.M.
Banquet



Friday, Feb. 12

7:30 A.M.
Continental Breakfast
8:30 A.M.
Session 5: Panel Session – Exportable Algorithms – Promise or Pandora: Steve Dussé (RSA Data Security, Inc.), Ilene Rosenthal (Software Publishers Association), Rob Rosenthal (NIST)
Chair: Steve Kent
10:00 A.M.
Break
10:30 A.M.
Session 6: Distributed Systems
Chair: Clifford Neuman
Practical Authorization in Large Heterogeneous, Distributed Systems, John Fletcher and Dan Nessett, LLNL, USA
Extending the OSF DCE Authorization System, Joseph Fass and Marlena Erdos, Hewlett-Packard Co., USA
Security Issues in the Truffles File System, Peter Reiher, et. al., UCLA and Trusted Information Systems, USA
12:00 noon
Lunch
1:30 P.M.
Session 7: Panel Session – Network Security Using Smart Cards : Jeff Schiller (MIT), Marjan Krajewski (MITRE), Jim Dray (NIST)
Chair: Dave Balenson
3:00 P.M.
Break
3:30 P.M.
Session 8: Panel Session – Should Security be Legislated? : Steve Kent (BBN), Rob Rosenthal (NIST) and Jeff Schiller (MIT)
Chair: Clifford Neuman

NDSS 1993 Program

Four paper sessions

- Privacy for Large Networks
- El
- Pr
- Di

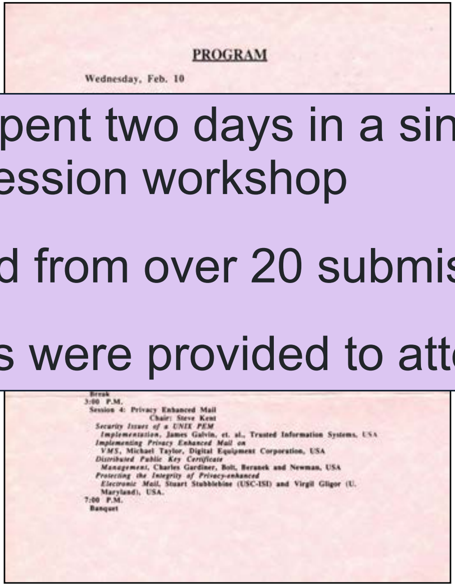
Four

- La
- Ex
  Promise of Pandora
- Network Security using Smart Cards
- Should Security be Legislated?

Over 160 attendees spent two days in a single-track, eight session workshop

12 papers selected from over 20 submissions

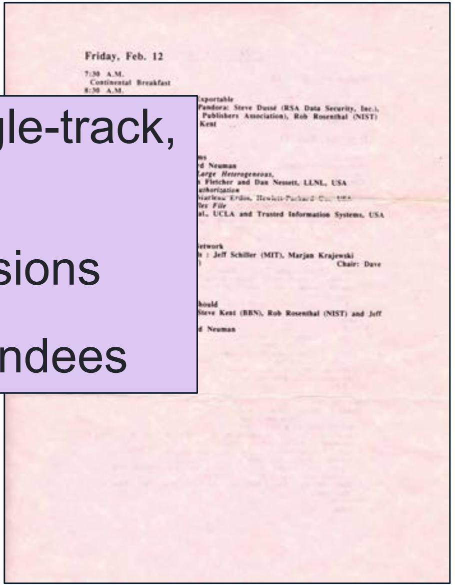
Printed proceedings were provided to attendees



PROGRAM

Wednesday, Feb. 10

Break
3:00 P.M.
Session 4: Privacy Enhanced Mail
Chair: Steve Kent
Security Issues of a UNIX PEM Implementation, James Galvin, et. al., Trusted Information Systems, USA
Implementing Privacy Enhanced Mail on VMS, Michael Taylor, Digital Equipment Corporation, USA
Distributed Public Key Certificate Management, Charles Gardiner, Bolt, Beranek and Newman, USA
Protecting the Integrity of Privacy-enhanced Electronic Mail, Stuart Stubblebine (USC-ISI) and Virgil Gligor (U. Maryland), USA.
7:00 P.M.
Banquet



Friday, Feb. 12

7:30 A.M.
Continental Breakfast
8:30 A.M.
Exportable
Pandora: Steve Dussé (RSA Data Security, Inc.),
Publishers Association), Rob Rosenthal (NIST)
Kent

ms
d Neuman
Large Heterogeneous,
Fletcher and Dan Nessett, LLNL, USA
uthorization
Marlena Erdos, Hewlett-Packard Co., USA
les File
al., UCLA and Trusted Information Systems, USA

etwork
: Jeff Schiller (MIT), Marjan Krajewski
)
Chair: Dave

hould
Steve Kent (BBN), Rob Rosenthal (NIST) and Jeff

d Neuman

Privacy and Security Research Group workshop on network and distributed system security: Proceedings. United States: 1993. Web. https://www.osti.gov/biblio/10147746

Presented by
Internet Society

NDSS SYMPOSIUM/2025

Program Chair Welcome

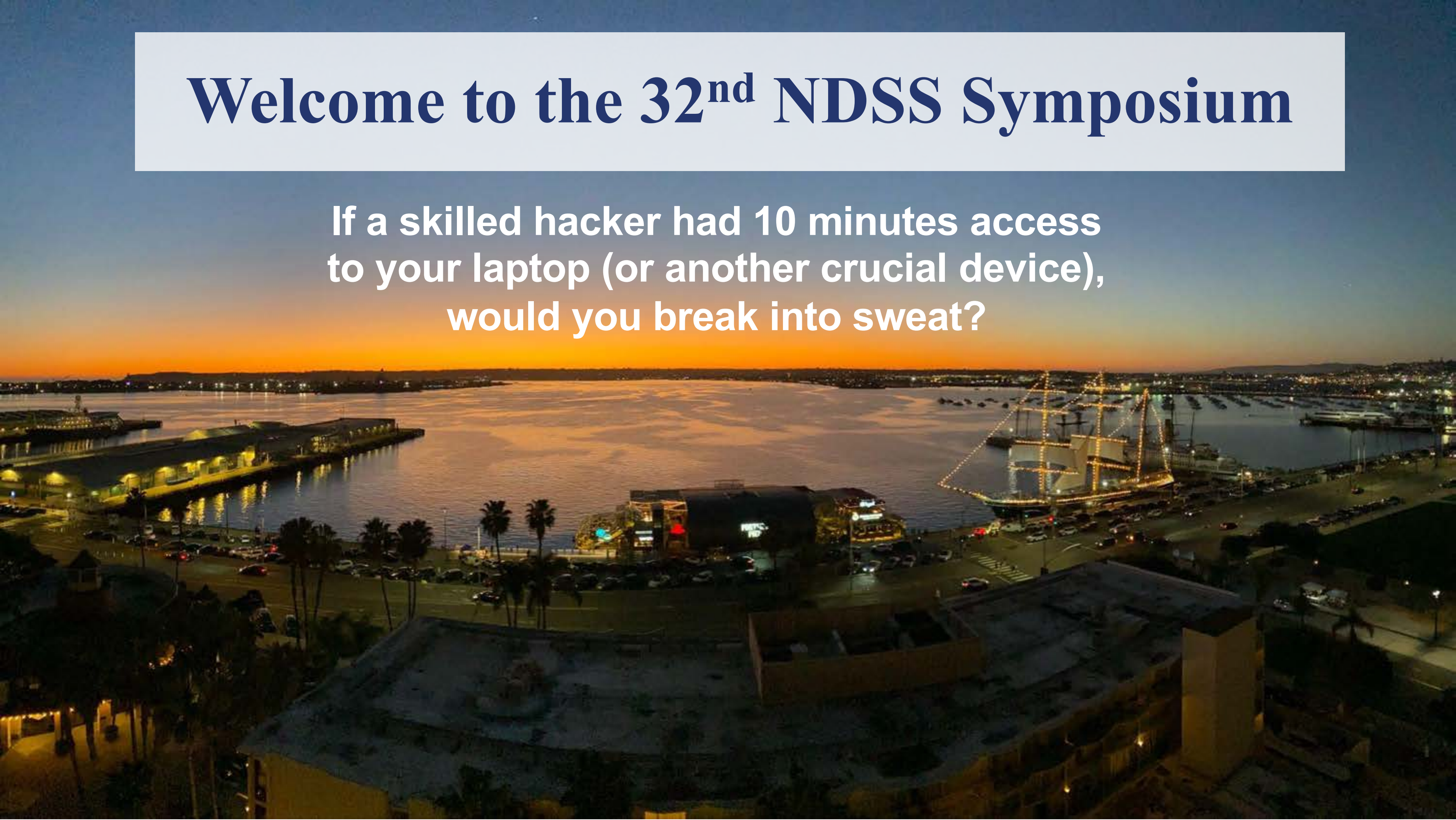
Opening Remarks Program Chairs

Christina Pöpper
New York University Abu Dhabi

Hamed Okhravi
MIT Lincoln Laboratory

Welcome to the 32nd NDSS Symposium

Welcome to the 32nd NDSS Symposium



If a skilled hacker had 10 minutes access to your laptop (or another crucial device), would you break into sweat?

NDSS’25 in Selected Numbers

NDSS SYMPOSIUM/2025

Presented by

Internet Society

#NDSSSymposium2025

Statistics

Accepted Papers: 211

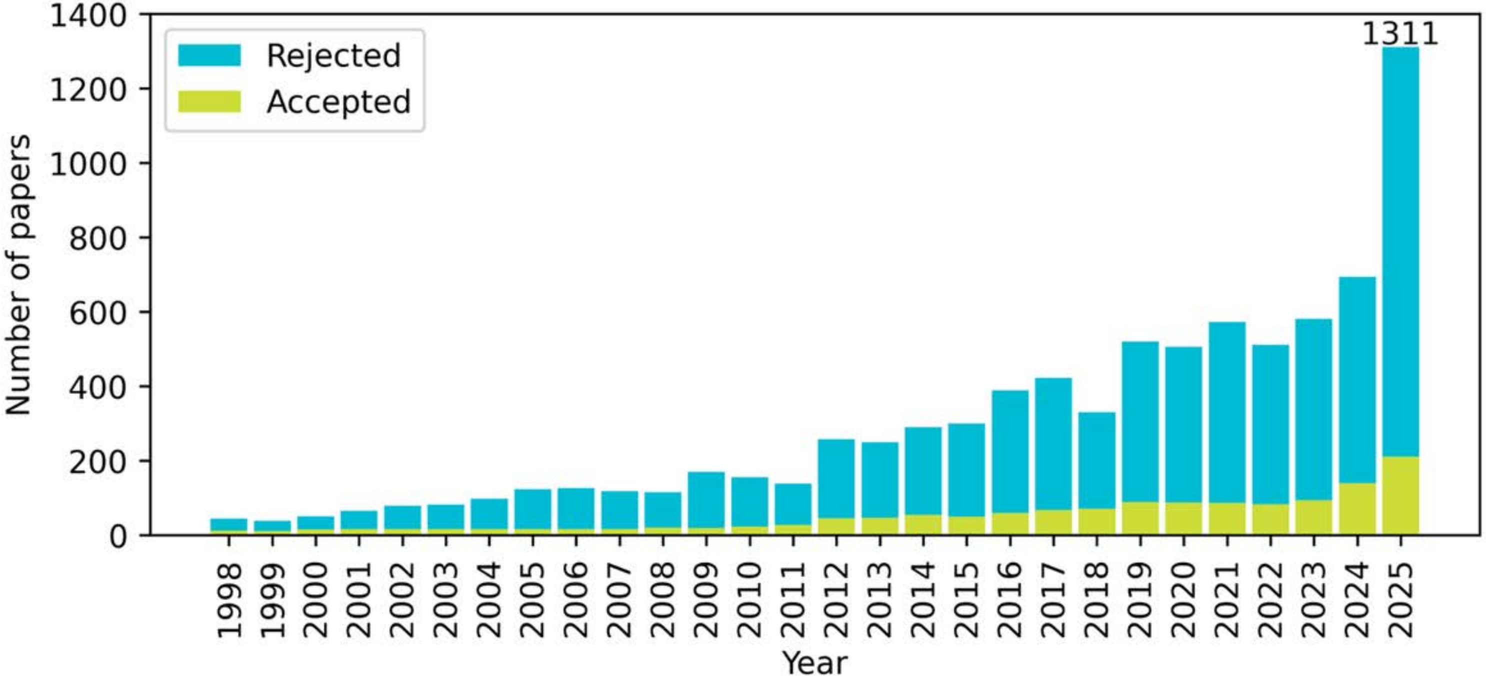
Submissions:

- Summer: 365 (+ 9 Desk Rejects)
- Fall: 946 (+ 49 Desk Rejects)

  ⇒ 1311 Valid Submissions

167 PC members, 3629 Reviews, 9576 Discussion Comments

NDSS Growth



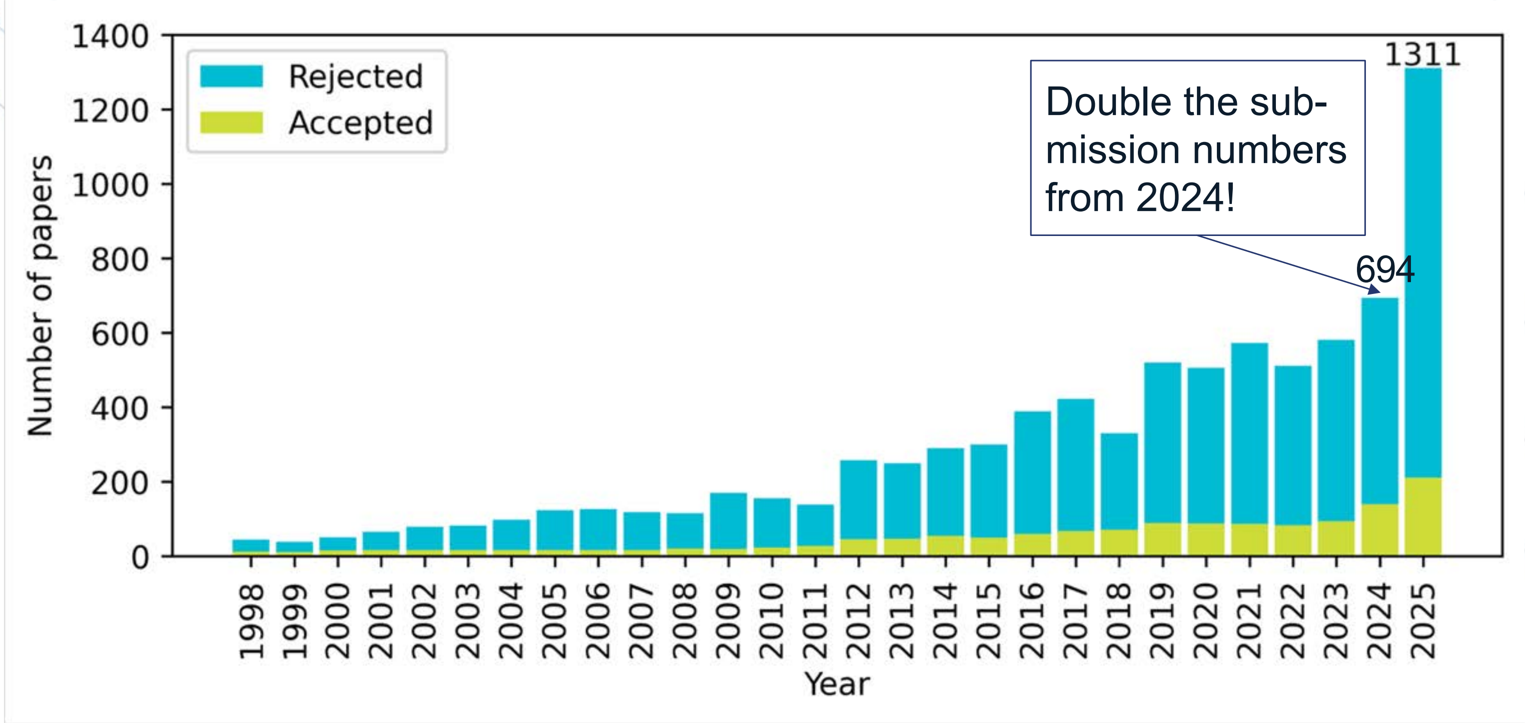
NDSS SYMPOSIUM/2025

Presented by

Internet Society

#NDSSSymposium2025

NDSS Growth



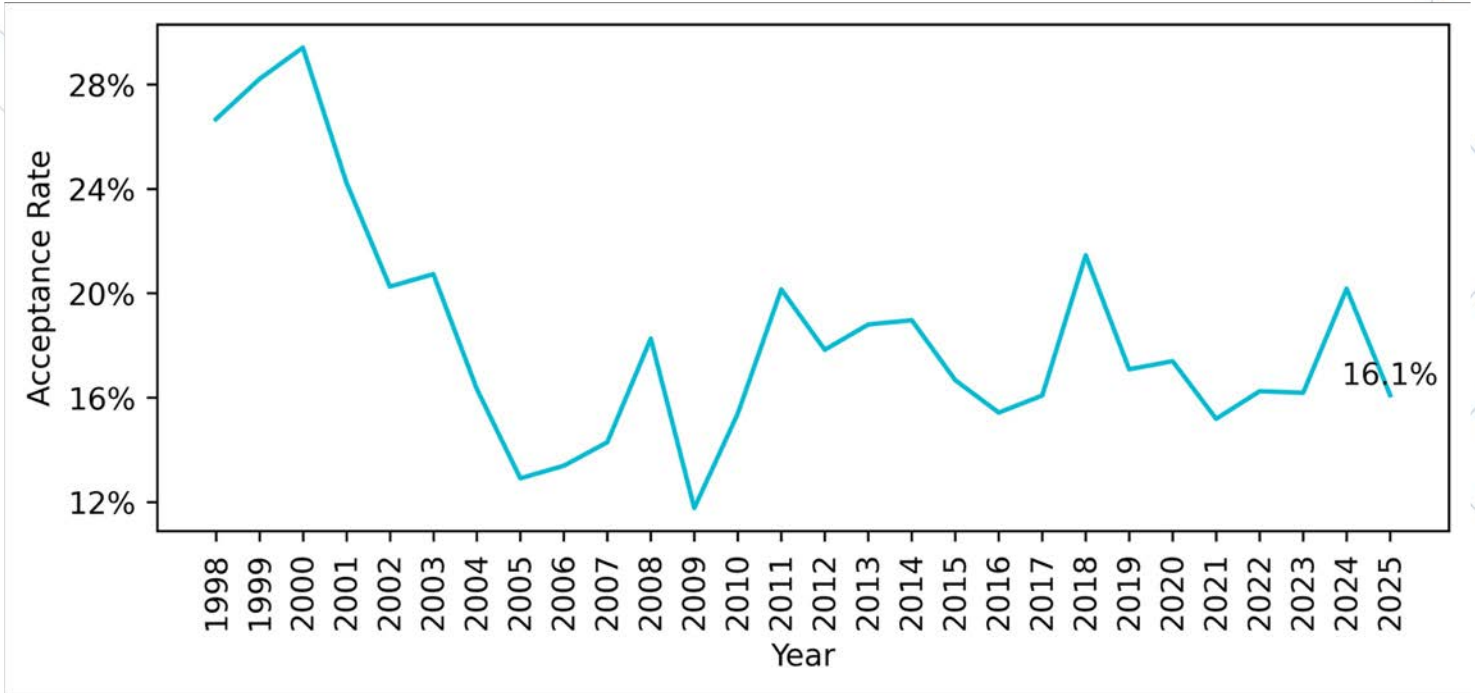
Double the submission numbers from 2024!

NDSS SYMPOSIUM/2025

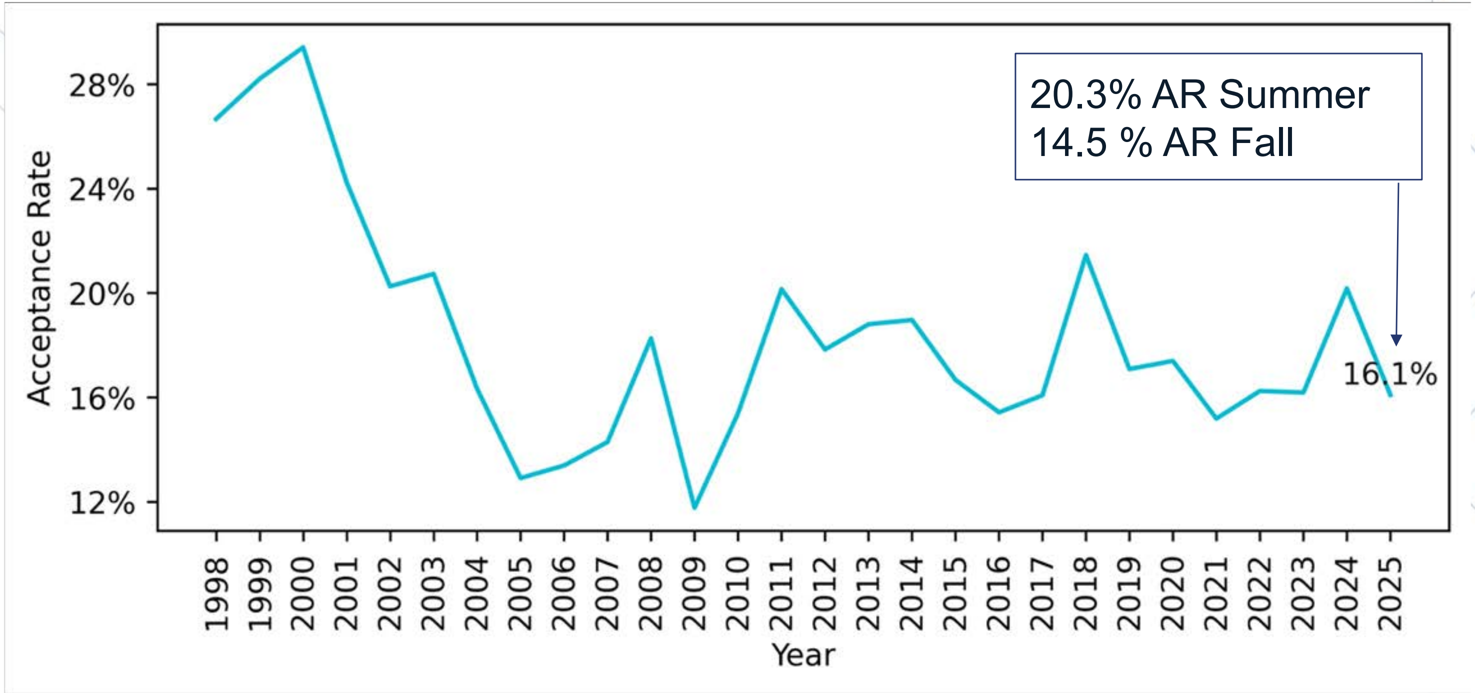
Presented by Internet Society

#NDSSSymposium2025

Historical Acceptance Rates



Historical Acceptance Rates

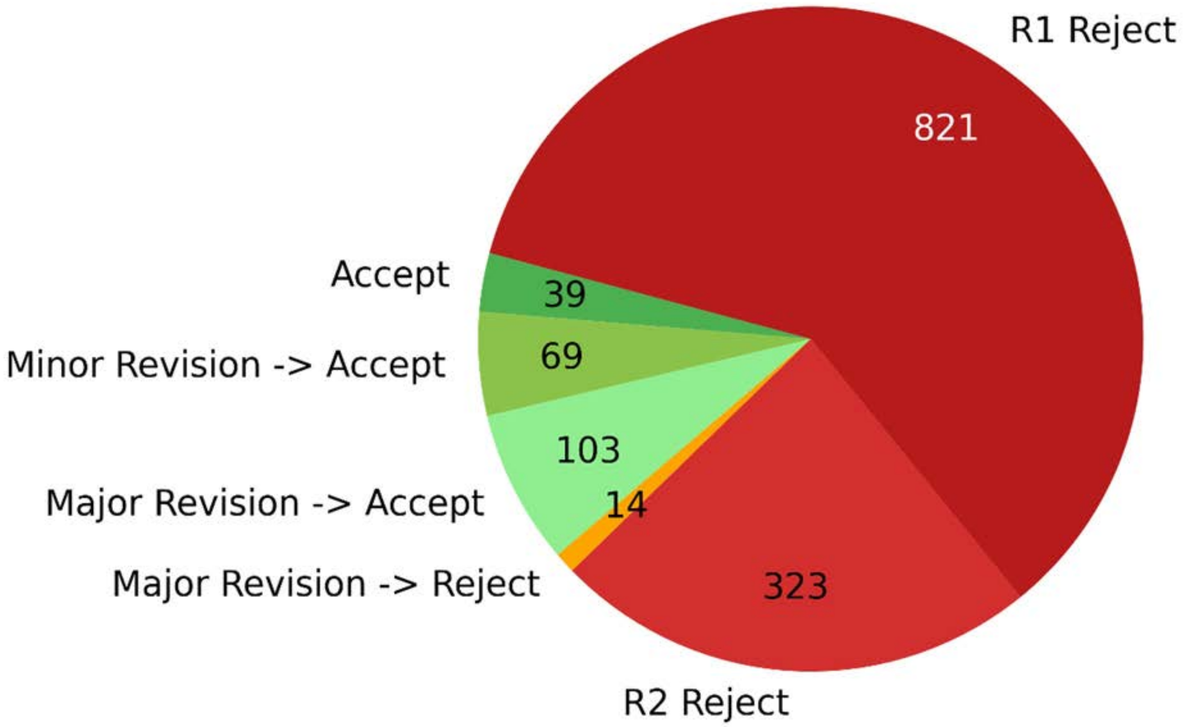


20.3% AR Summer
14.5 % AR Fall

Presented by

#NDSSSymposium2025

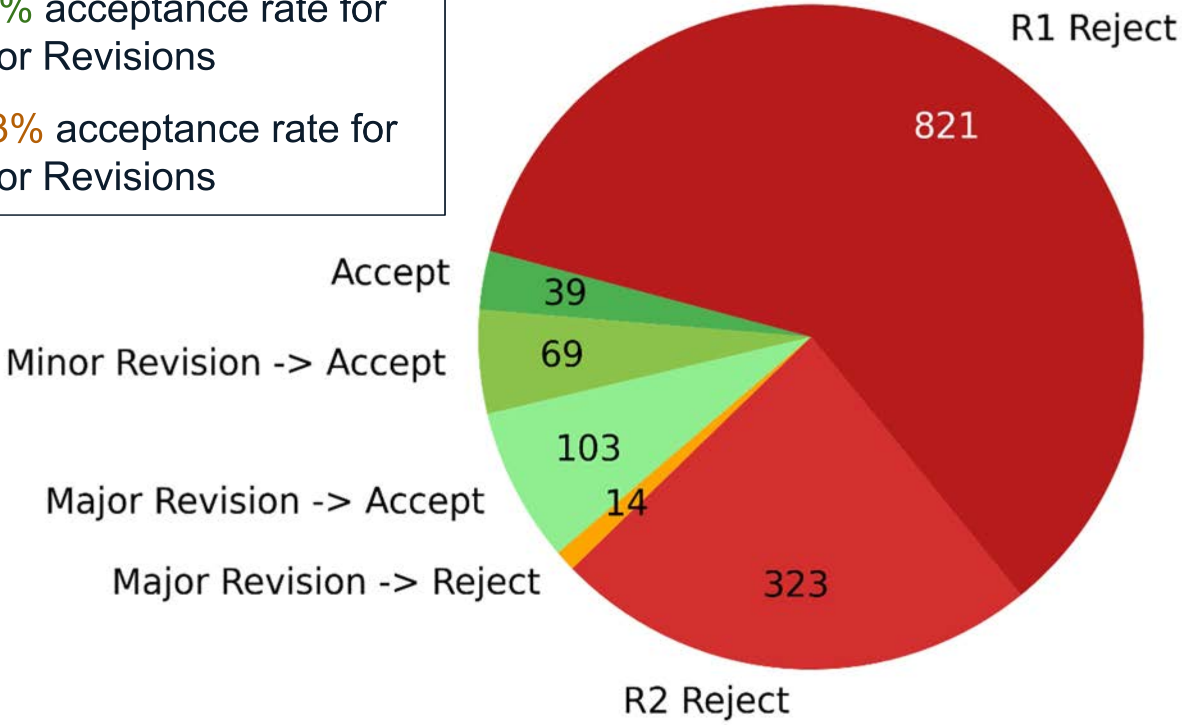
Paper Decisions During the Review Process



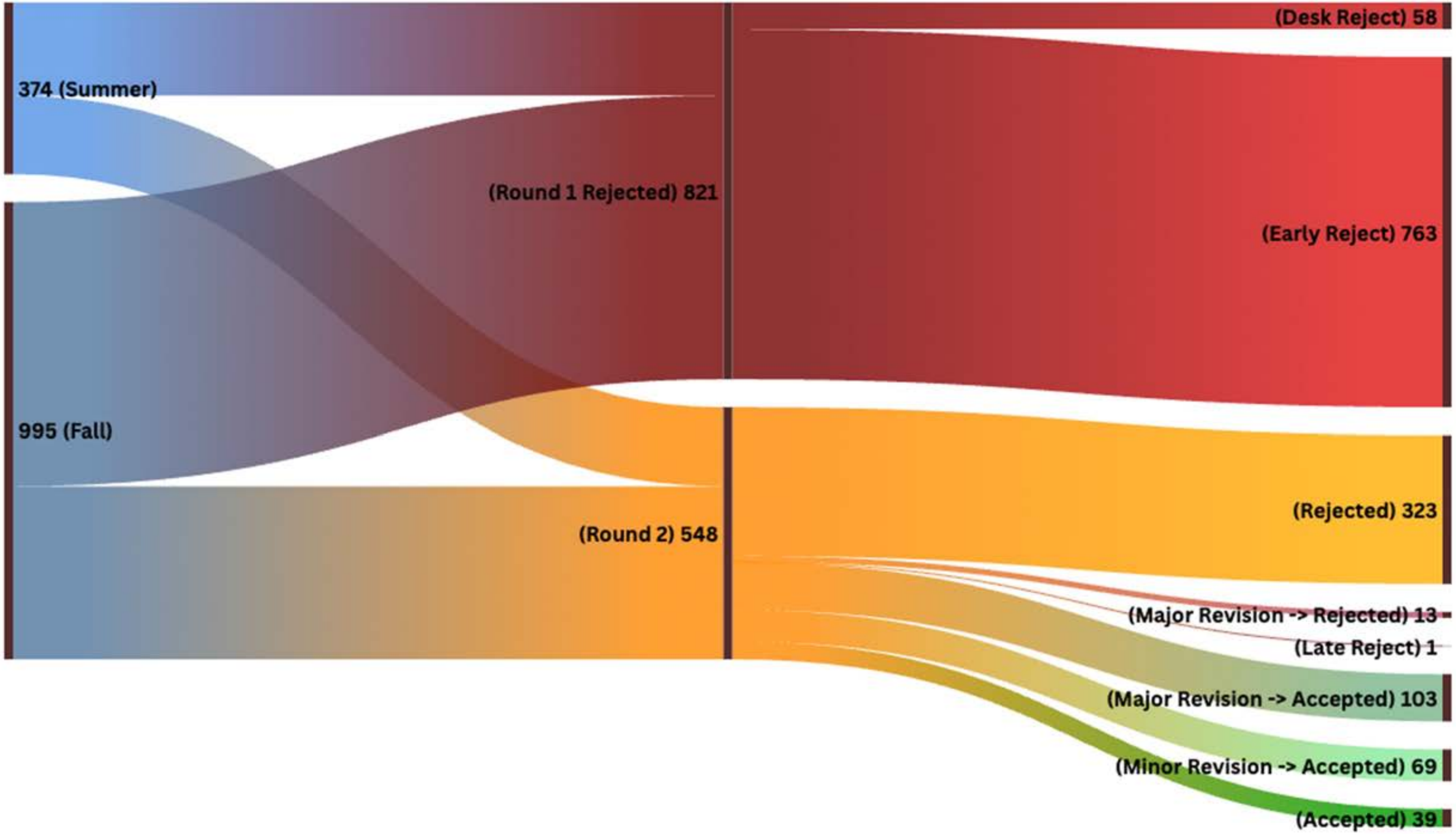
Paper Decisions During the Review Process

100% acceptance rate for Minor Revisions

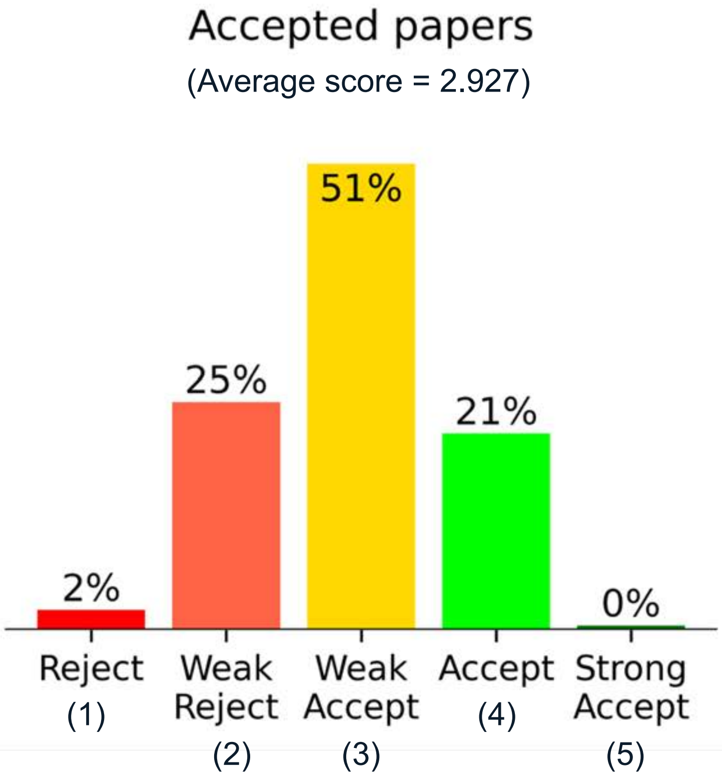
87.3% acceptance rate for Major Revisions

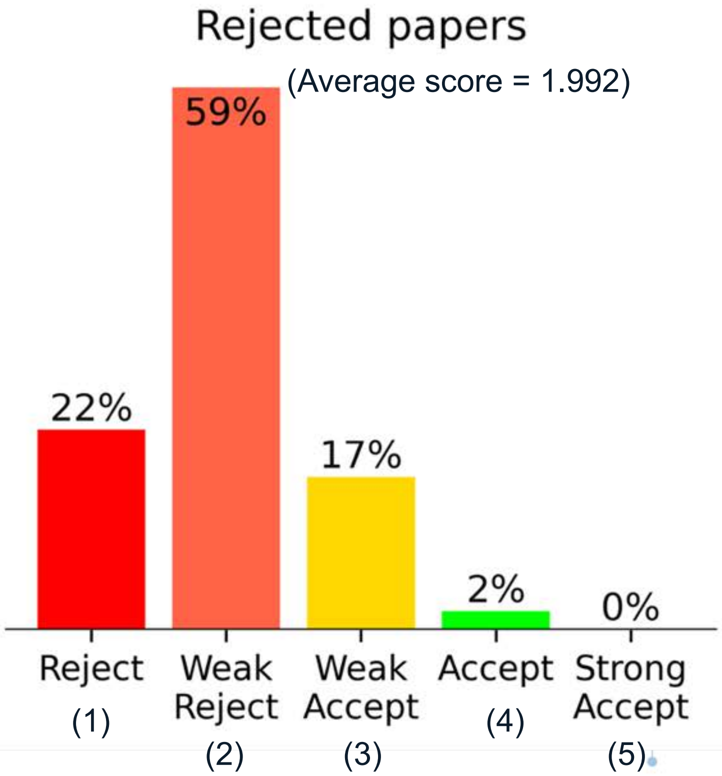


Paper Decisions During the Review Process

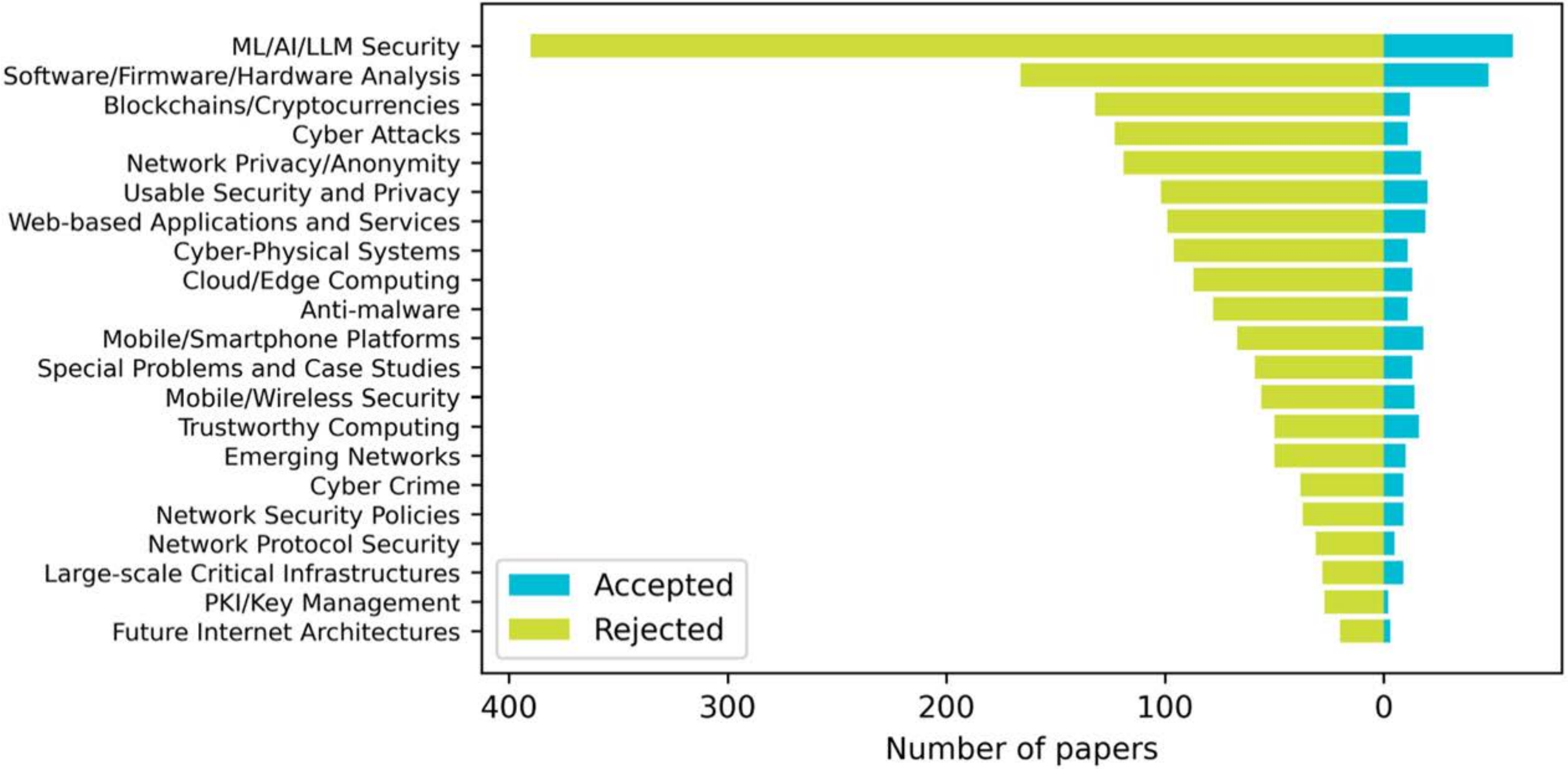


Review Scores for Accepted and Rejected Papers





Rejected Papers by Topic

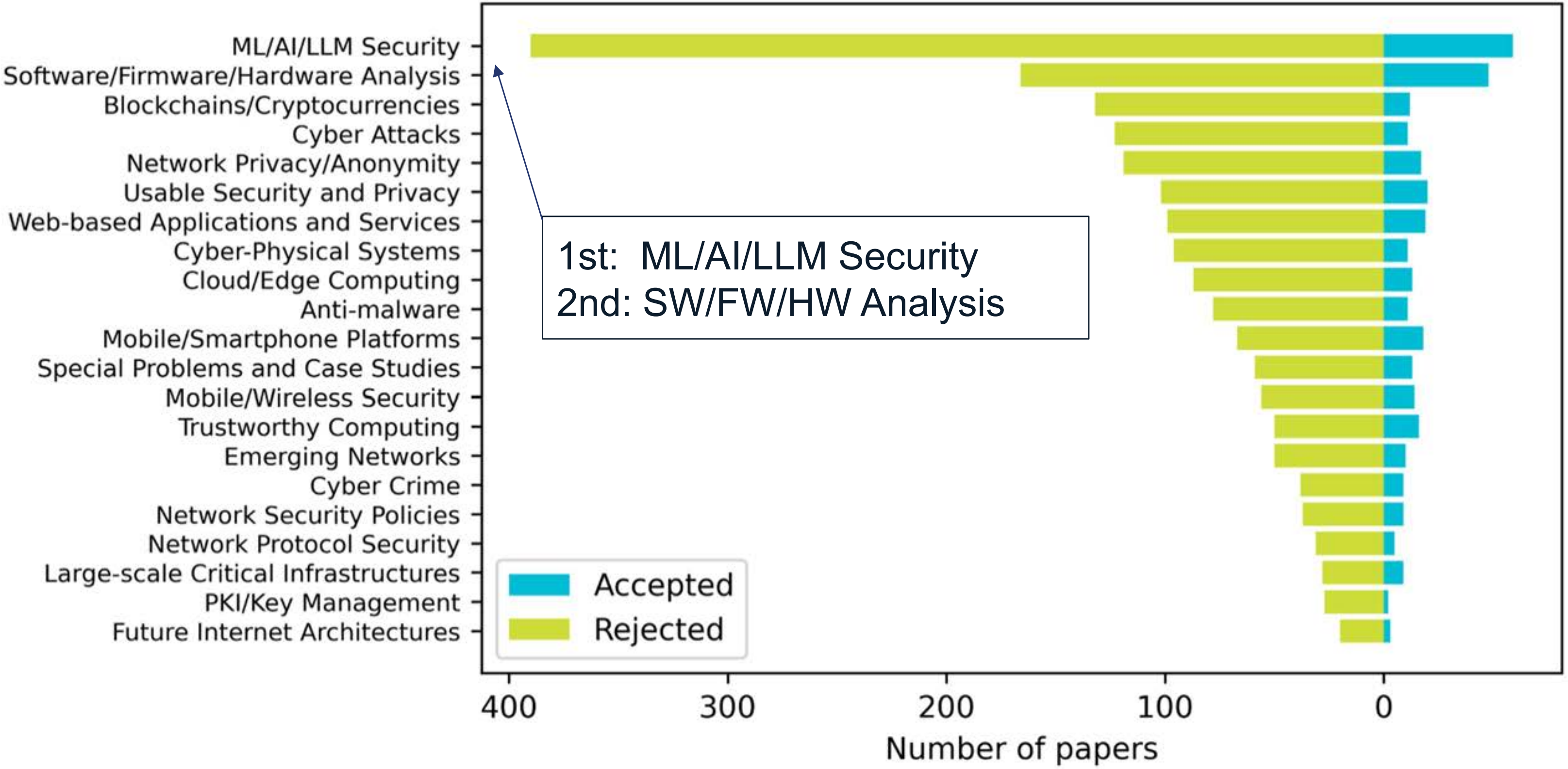


NDSS SYMPOSIUM/2025

Presented by Internet Society

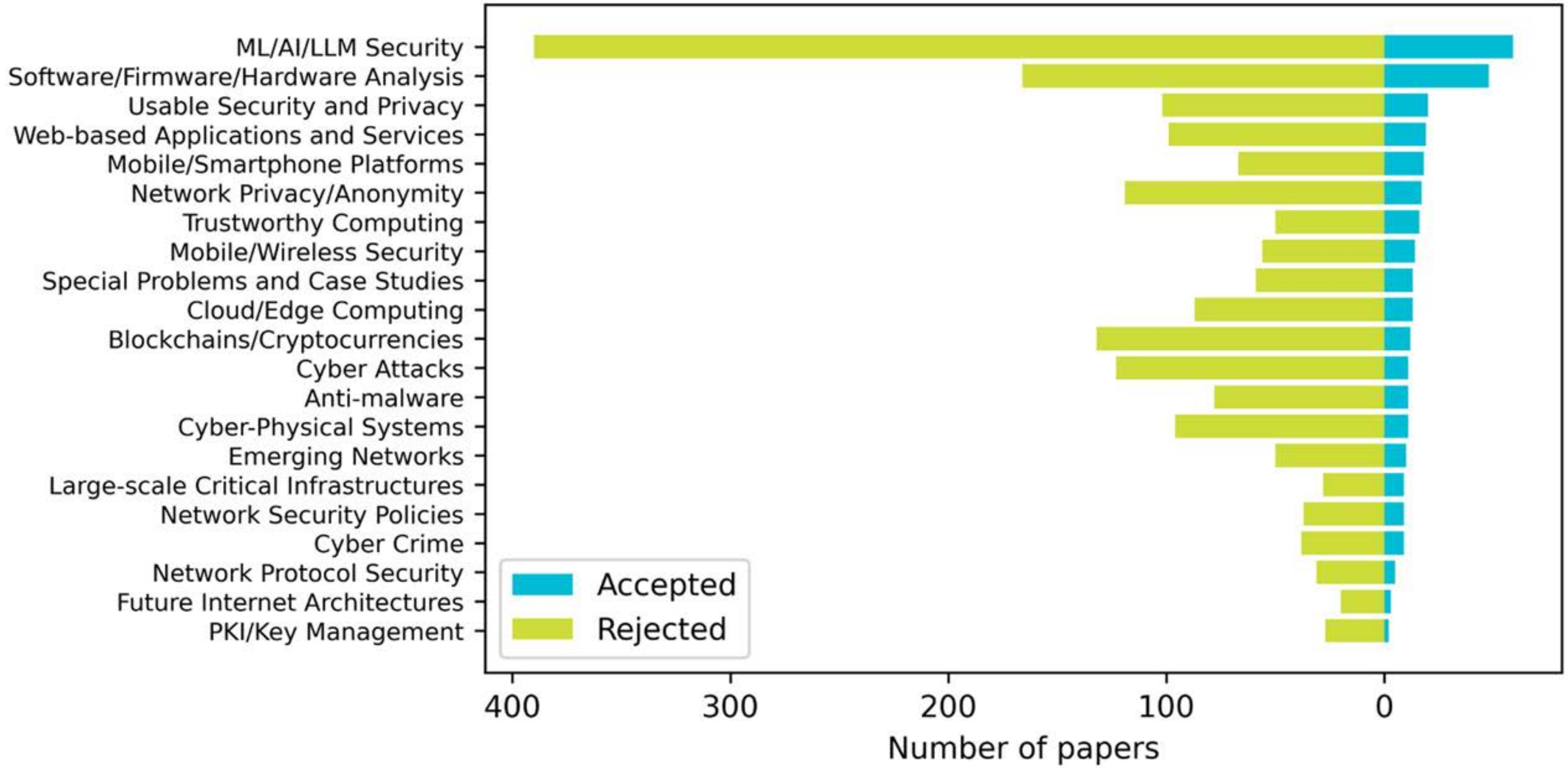
#NDSSSymposium2025

Rejected Papers by Topic



1st: ML/AI/LLM Security
2nd: SW/FW/HW Analysis

Accepted Papers by Topic



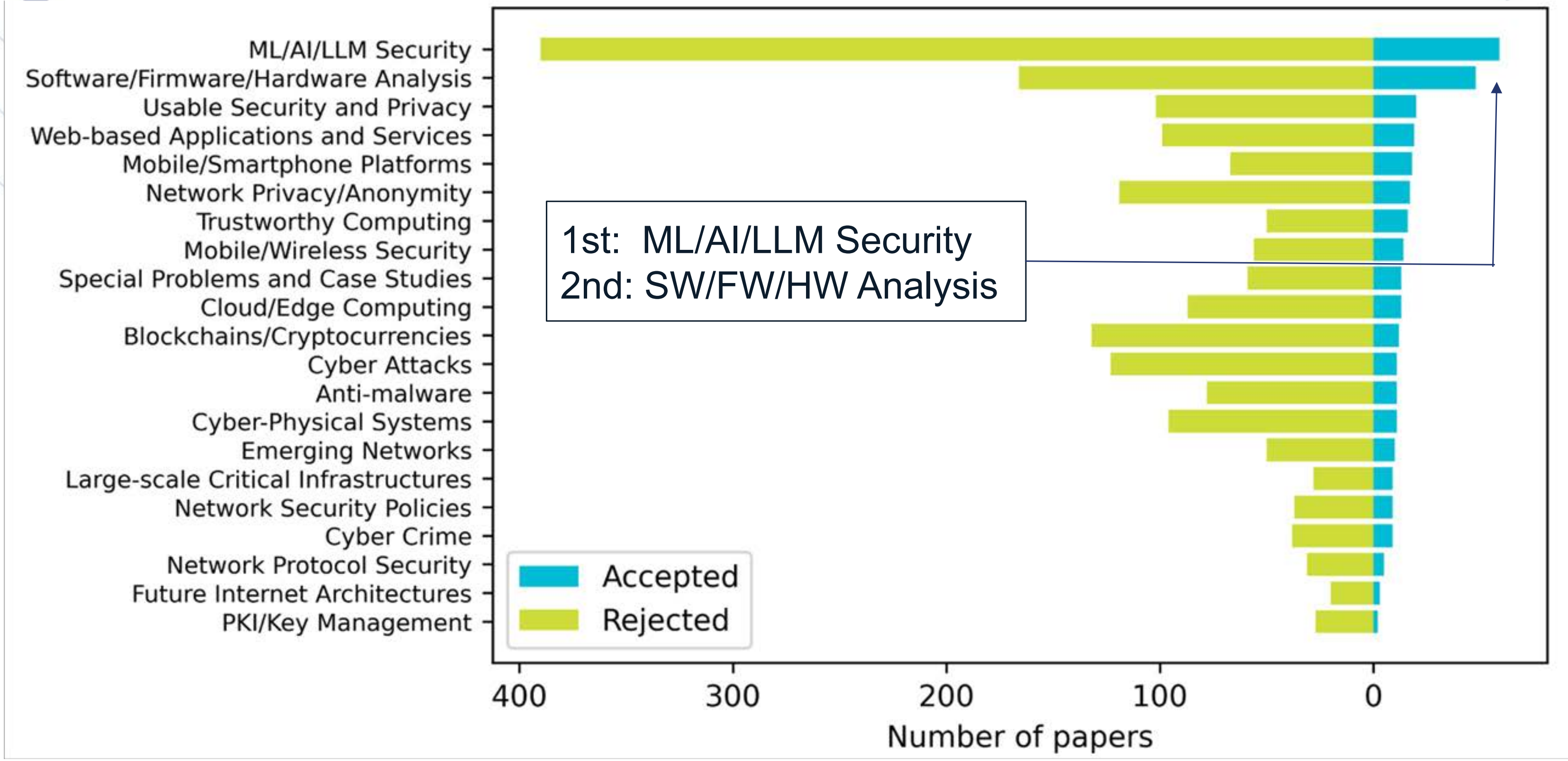
Presented by

Internet Society

NDSS SYMPOSIUM/2025

#NDSSSymposium2025

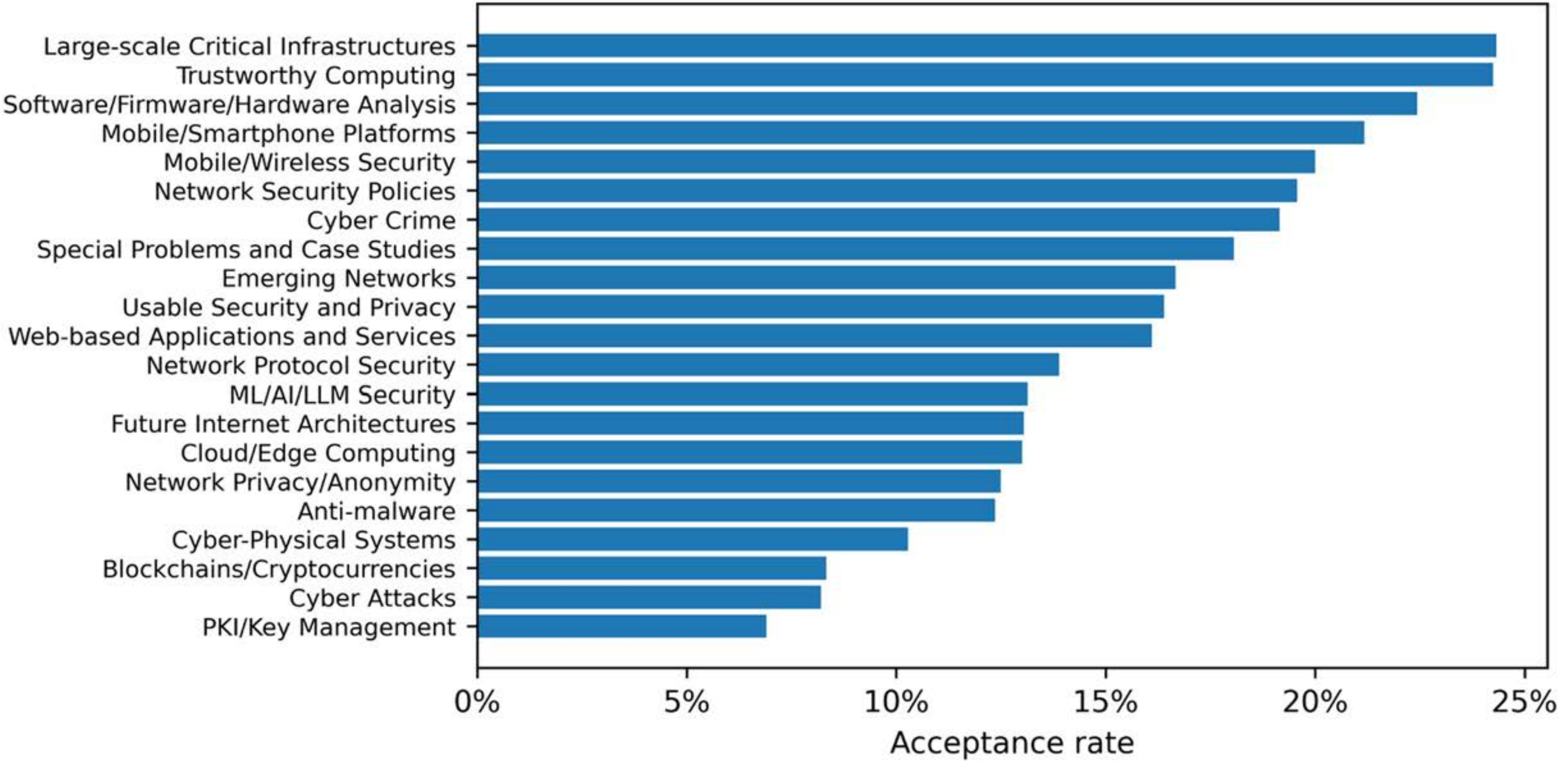
Accepted Papers by Topic



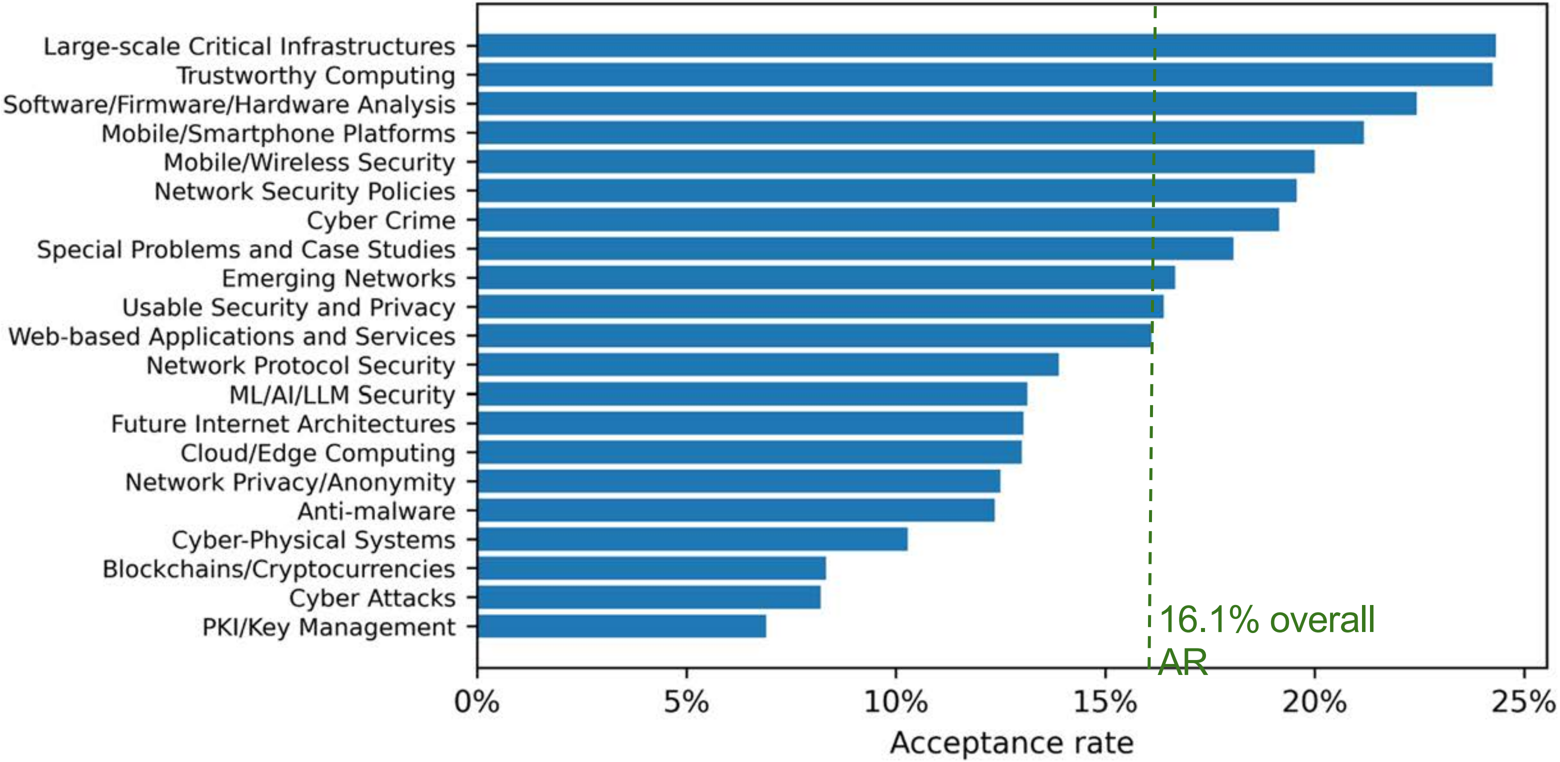
1st: ML/AI/LLM Security
2nd: SW/FW/HW Analysis

AI PAPERS:
MOST ACCEPTED
&
& MOST REJECTED!
AI PAPERS
AI PAPERS
REJECTED
REJECTED
REJECTED
REJECTED!
REJECTED
REJECTED
REJECTED
REJECTED
REJECTD
REJECTD
AIL

Acceptance Rate by Topic

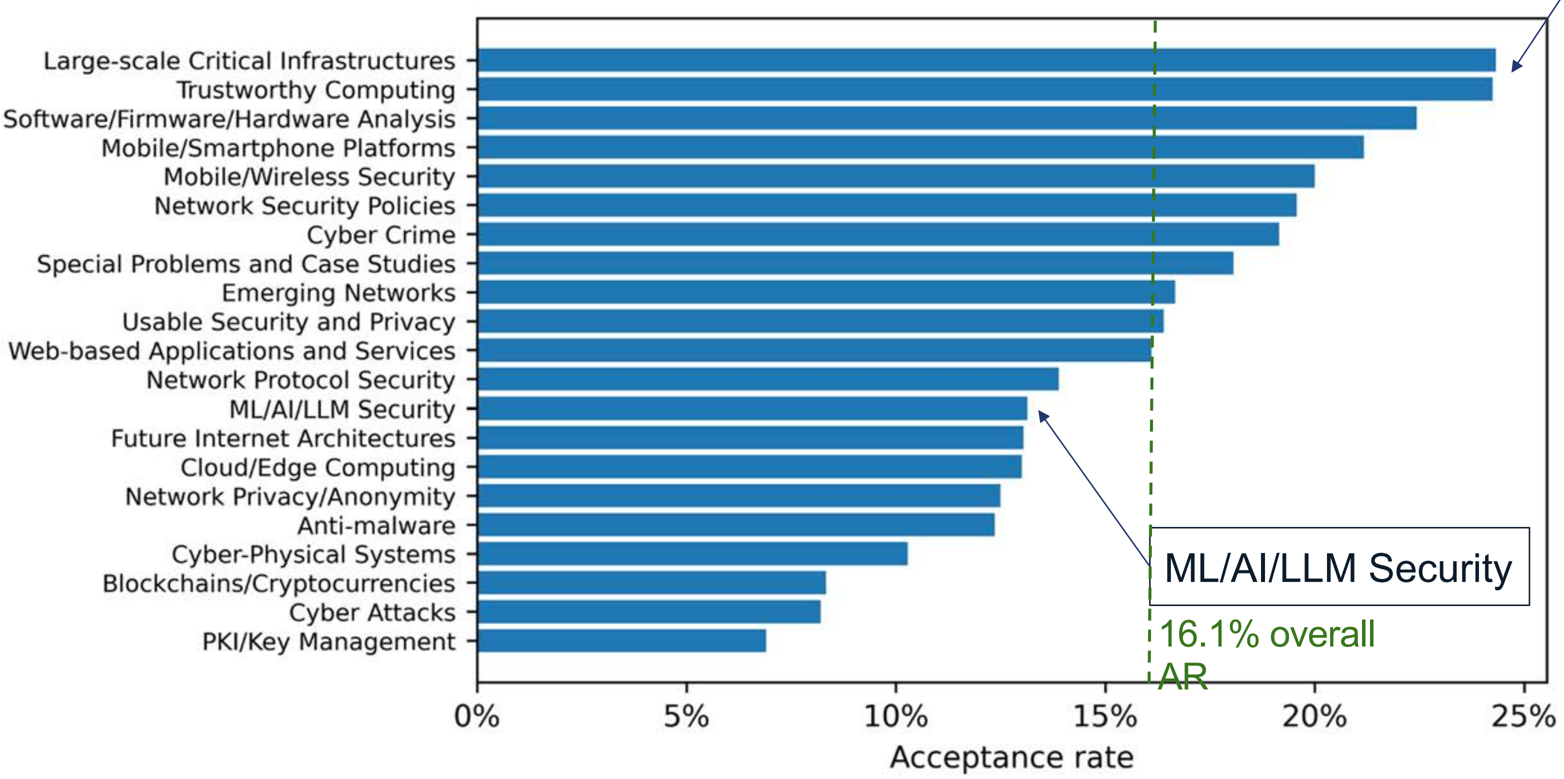


Acceptance Rate by Topic



Acceptance Rate by Topic

1st Large-Scale Critical Infrastructures
2nd Trustworthy Computing



ML/AI/LLM Security

16.1% overall AR

NDSS’25 Review Process Insights

NDSS SYMPOSIUM/2025

Presented by

Internet Society

#NDSSSymposium2025

TPC Members - Thank You

Abhishta Abhishta, University of Twente
Adam Bates University of Illinois at Urbana-Champaign
Adwait Nadkarni, William & Mary
Ahmad-Reza Sadeghi, TU Darmstadt
Alessandro Sorniotti, IBM Research Europe
Alexandra Dmitrienko, University of Wuerzburg
Ali Abbasi, CISPA Helmholtz Center for Information Security
Alvaro Cardenas, University of California, Santa Cruz
Amy Babay, University of Pittsburgh
Ang Li, The University of Michigan-Dearborn
Angelos Stavrou, Virginia Tech
Antonio Villani, Retooling
Aolin Ding, Accenture Labs
Aravind Machiry, Purdue University
Awais Rashid, University of Bristol
Bahruz Jabiyev, Dartmouth College
Bart Coppens, Ghent University
Ben Stock, CISPA Helmholtz Center for Information Security
Benjamin Ujcich, Georgetown University
Benjamin Andow, Google
Binbin Zhao, Georgia Institute of Technology
Brendan Saltaformaggio, Georgia Institute of Technology
Christine Utz, Radboud University
Christof Ferreira Torres, ETH Zurich
Christophe Hauser, Dartmouth College
Christopher Kruegel, UC Santa Barbara
Claudio Soriente, NEC Laboratories Europe
Coby Wang, Visa Research
Daniel Gruss, Graz University of Technology
Daniele Cono D'Elia, Sapienza University of Rome
Daoyuan Wu, Hong Kong University of Science and Techn.
David Mohaisen, University of Central Florida
Derrick McKee, MIT Lincoln Laboratory
Derui Wang, CSIRO's Data61
Ding Wang, Nankai University
Doowon Kim, University of Tennessee, Knoxville
Eleonora Losiouk, University of Padua
Erik van der Kouwe Vrije, Universiteit Amsterdam
Faysal Hossain Shezan, University of Texas at Arlington
Fengwei Zhang, Southern University of Science and Techn.

Flavio Toffalini, EPFL
Gang Qu, University of Maryland
Gary Tan, Pennsylvania State University
Ghassan Karame, Ruhr University Bochum
Giovanni Apruzzese, University of Liechtenstein
Guangdong Bai, The University of Queensland
Fengwei Zhang, Southern University of Science and Techn.
Flavio Toffalini, EPFL
Gang Qu, University of Maryland
Gary Tan, Pennsylvania State University
Ghassan Karame, Ruhr University Bochum
Giovanni Apruzzese, University of Liechtenstein
Guangdong Bai, The University of Queensland
Guofei Gu, Texas A&M University
Habiba Farrukh, University of California, Irvine
Haibin Zhang, Yangtze Delta Region Institute of Tsinghua U.
Haipeng Cai, Washington State University
Han Qiu, Tsinghua University
Haojin Zhu, Shanghai Jiao Tong University
Hong Hu, Pennsylvania State University
Hongxin Hu, University at Buffalo
Hossein Fereidooni, KOBIL GmbH
Houman Homayoun, University of California Davis
Hyungsub Kim, Purdue University & Indiana University
Imtiaz Karim, Purdue University
Insu Yun, KAIST
Ivan Martinovic, University of Oxford
Jason (Minhui) Xue, CSIRO's Data61
Jianjun Chen, Tsinghua University
Juan Tapiador, Carlos III University of Madrid
Jun Xu, University of Utah
Juraj Somorovsky, Paderborn University
JV Rajendran, Texas A&M University
Kai Li, San Diego State University
Kaihua Qin, Yale University
Kaushal Kafle, University of Florida
Kevin Borgolte, Ruhr University Bochum
Kevin Leach, Vanderbilt University
Kun Sun, George Mason University
Kyungtae Kim, Dartmouth College
Lannan Lisa Luo, George Mason University
Le Guan, University of Georgia
Lejla Batina, Radboud University
Lingyu Wang, Concordia University
Lorenzo Cavallaro, University College London
Manuel Egele, Boston University
Marcus Botacin, Texas A&M University

Marcus Peinado, Microsoft Research
Marko Vukolic, ConsensusLab
Martin Strohmeier, Cyber-Defence Campus, armasuisse
Martin Henze, RWTH Aachen University & Fraunhofer FKIE
Martin Johns, TU Braunschweig
Mathias Payer, EPFL
Matteo Grosse-Kampmann, Rhine-Waal University / AWARE7 GmbH
Meng Luo, Zhejiang University
Meng Xu, University of Waterloo
Michael Schwarz, CISPA Helmholtz Center for Information Security
Mihalis Maniatakos, NYU Abu Dhabi
Min Suk Kang, KAIST
Ming Li, The University of Texas at Arlington
Minghong Fang, Duke University
Mingxue Zhang Zhejiang University
Mitsuaki Akiyama, NTT
Mohammad Islam, University of Texas at Arlington
Mu Zhang, University of Utah
Murtuza Jadliwala, University of Texas at San Antonio
Nader Sehatbakhsh, UCLA
Nadim Kobeissi, Cure53, Symbolic Software
Nathan Burow, MIT Lincoln Laboratory
Neil Gong, Duke University
Nick Nikiforakis, Stony Brook University
Nidhi Rastogi, Rochester Institute of Technology
Ning Wang, University of South Florida
Omar Chowdhury, Stony Brook University
Paria Shirani, University of Ottawa
Peng Gao, Virginia Tech
Per Larsen, Immunant, Inc.
Phani Vadrevu, Louisiana State University
Prashast Srivastava, Columbia University
Qi Li, Tsinghua University
Qiang Tang, The University of Sydney
Qiben Yan, Michigan State University
Qingchuan Zhao, City University of Hong Kong
Qiushi Wu, IBM Research
Rachel Greenstadt, New York University
Raghavendran Ramakrishnan, Snowflake Inc
Rajvardhan Oak, University of California Davis / Microsoft Corporation
René Mayrhofer, Johannes Kepler University Linz
Rob Cunningham, University of Pittsburgh
Ruoyu "Fish" Wang, Arizona State University
Saman Zonouz, Georgia Institute of Technology

Samuel Jero, MIT Lincoln Laboratory
Sandra Siby, Imperial College London
Sang Kil Cha, KAIST
Santosh Nagarakatte, Rutgers University
Sebastian Köhler, University of Oxford
Sébastien Bardin, CEA List, Université Paris Saclay
Shagufta Mehnaz, Pennsylvania State University
Shahin Tajik, Worcester Polytechnic Institute
Sherman S. M. Chow, Chinese University of Hong Kong
Shweta Shinde, ETH Zurich
Sisi Duan, Tsinghua University
Soheil Salehi, The University of Arizona
Srdjan Čapkun, ETH Zurich
Stephen Herwig, William & Mary
Stjepan Picek, Radboud University
Suryadipta Majumdar, Concordia University
Syed Rafiul Hussain, Pennsylvania State University
Takuya Watanabe, Deloitte Tohmatsu Cyber LLC
Tatsuya Mori, Waseda University
Theodor Schnitzler, Maastricht University
Tianhao Wang, University of Virginia
Ting Wang, Stony Brook University
Tuba Yavuz, University of Florida
Veelasha Moonsamy, Ruhr University Bochum
Wajih Ul Hassan, University of Virginia
Wenke Lee, Georgia Institute of Technology
William Robertson, Northeastern University
Xiaokuan Zhang, George Mason University
Xingliang Yuan, The University of Melbourne
Xinwen Fu, University of Massachusetts Lowell
Xinyang Ge, Databricks
Xinyu Xing, Northwestern University
Yang Zhang, CISPA Helmholtz Center for Information Security
Yongdae Kim, KAIST
Yonghwi Kwon, University of Maryland
Yuan Hong, University of Connecticut
Yue Zhang, Drexel University
Yuzhe Tang, Syracuse University
Z. Berkay Celik, Purdue University
Zephyr Yao, New Jersey Institute of Technology
Zhikun Zhang, Stanford & CISPA
Zhiyun Qian, University of California, Riverside
Zhou Li, University of California, Irvine

TPC Members - Thank You

167 PC members

Max # of reviews: 27

Avg # of reviews: 22

Abhishta Abhishta, University of Twente
Adam Bates University of Illinois at Urbana-Champaign
Adwait Nadkarni, William & Mary
Ahmad-Reza Sadeghi, TU Darmstadt
Alessandro Sorniotti, IBM Research Europe
Alexandra Dmitrienko, University of Wuerzburg
Ali Abbasi, CISPA Helmholtz Center for Information Security
Alvaro Cardenas, University of California, Santa Cruz
Amy Babay, University of Pittsburgh
Ang Li, The University of Michigan-Dearborn
Angelos Stavrou, Virginia Tech
Antonio Villani, Retooling
Aolin Ding, Accenture Labs
Aravind Machiry, Purdue University
Awais Rashid, University of Bristol
Bahruz Jabiyev, Dartmouth College
Bart Coppens, Ghent University
Ben Stock, CISPA Helmholtz Center for Information Security
Benjamin Ujcich, Georgetown University
Benjamin Andow, Google
Binbin Zhao, Georgia Institute of Technology
Brendan Saltaformaggio, Georgia Institute of Technology
Christine Utz, Radboud University
Christof Ferreira Torres, ETH Zurich
Christophe Hauser, Dartmouth College
Christopher Kruegel, UC Santa Barbara
Claudio Soriente, NEC Laboratories Europe
Coby Wang, Visa Research
Daniel Gruss, Graz University of Technology
Daniele Cono D'Elia, Sapienza University of Rome
Daoyuan Wu, Hong Kong University of Science and Techn.
David Mohaisen, University of Central Florida
Derrick McKee, MIT Lincoln Laboratory
Derui Wang, CSIRO's Data61
Ding Wang, Nankai University
Doowon Kim, University of Tennessee, Knoxville
Eleonora Losiouk, University of Padua
Erik van der Kouwe Vrije, Universiteit Amsterdam
Faysal Hossain Shezan, University of Texas at Arlington
Fengwei Zhang, Southern University of Science and Techn.

Flavio Toffalini, EPFL
Gang Qu, University of Maryland
Gary Tan, Pennsylvania State University
Ghassan Karame, Ruhr University Bochum
Giovanni Apruzzese, University of Liechtenstein
Guangdong Bai, The University of Queensland
Fengwei Zhang, Southern University of Science and Techn.
Flavio Toffalini, EPFL
Gang Qu, University of Maryland
Gary Tan, Pennsylvania State University
Ghassan Karame, Ruhr University Bochum
Giovanni Apruzzese, University of Liechtenstein
Guangdong Bai, The University of Queensland
Guofei Gu, Texas A&M University
Habiba Farrukh, University of California, Irvine
Haibin Zhang, Yangtze Delta Region Institute of Tsinghua U.
Haipeng Cai, Washington State University
Han Qiu, Tsinghua University
Haojin Zhu, Shanghai Jiao Tong University
Hong Hu, Pennsylvania State University
Hongxin Hu, University at Buffalo
Hossein Fereidooni, KOBIL GmbH
Houman Homayoun, University of California Davis
Hyungsub Kim, Purdue University & Indiana University
Imtiaz Karim, Purdue University
Insu Yun, KAIST
Ivan Martinovic, University of Oxford
Jason (Minhui) Xue, CSIRO's Data61
Jianjun Chen, Tsinghua University
Juan Tapiador, Carlos III University of Madrid
Jun Xu, University of Utah
Juraj Somorovsky, Paderborn University
JV Rajendran, Texas A&M University
Kai Li, San Diego State University
Kaihua Qin, Yale University
Kaushal Kafle, University of Florida
Kevin Borgolte, Ruhr University Bochum
Kevin Leach, Vanderbilt University
Kun Sun, George Mason University
Kyungtae Kim, Dartmouth College
Lannan Lisa Luo, George Mason University
Le Guan, University of Georgia
Lejla Batina, Radboud University
Lingyu Wang, Concordia University
Lorenzo Cavallaro, University College London
Manuel Egele, Boston University
Marcus Botacin, Texas A&M University

Marcus Peinado, Microsoft Research
Marko Vukolic, ConsensusLab
Martin Strohmeier, Cyber-Defence Campus, armasuisse
Martin Henze, RWTH Aachen University & Fraunhofer FKIE
Martin Johns, TU Braunschweig
Mathias Payer, EPFL
Matteo Grosse-Kampmann, Rhine-Waal University / AWARE7 GmbH
Meng Luo, Zhejiang University
Meng Xu, University of Waterloo
Michael Schwarz, CISPA Helmholtz Center for Information Security
Mihalis Maniatakos, NYU Abu Dhabi
Min Suk Kang, KAIST
Ming Li, The University of Texas at Arlington
Minghong Fang, Duke University
Mingxue Zhang Zhejiang University
Mitsuaki Akiyama, NTT
Mohammad Islam, University of Texas at Arlington
Mu Zhang, University of Utah
Murtuza Jadliwala, University of Texas at San Antonio
Nader Sehatbakhsh, UCLA
Nadim Kobeissi, Cure53, Symbolic Software
Nathan Burow, MIT Lincoln Laboratory
Neil Gong, Duke University
Nick Nikiforakis, Stony Brook University
Nidhi Rastogi, Rochester Institute of Technology
Ning Wang, University of South Florida
Omar Chowdhury, Stony Brook University
Paria Shirani, University of Ottawa
Peng Gao, Virginia Tech
Per Larsen, Immunant, Inc.
Phani Vadrevu, Louisiana State University
Prashast Srivastava, Columbia University
Qi Li, Tsinghua University
Qiang Tang, The University of Sydney
Qiben Yan, Michigan State University
Qingchuan Zhao, City University of Hong Kong
Qiushi Wu, IBM Research
Rachel Greenstadt, New York University
Raghavendran Ramakrishnan, Snowflake Inc
Rajvardhan Oak, University of California Davis / Microsoft Corporation
René Mayrhofer, Johannes Kepler University Linz
Rob Cunningham, University of Pittsburgh
Ruoyu "Fish" Wang, Arizona State University
Saman Zonouz, Georgia Institute of Technology

Samuel Jero, MIT Lincoln Laboratory
Sandra Siby, Imperial College London
Sang Kil Cha, KAIST
Santosh Nagarakatte, Rutgers University
Sebastian Köhler, University of Oxford
Sébastien Bardin, CEA List, Université Paris Saclay
Shagufta Mehnaz, Pennsylvania State University
Shahin Tajik, Worcester Polytechnic Institute
Sherman S. M. Chow, Chinese University of Hong Kong
Shweta Shinde, ETH Zurich
Sisi Duan, Tsinghua University
Soheil Salehi, The University of Arizona
Srdjan Čapkun, ETH Zurich
Stephen Herwig, William & Mary
Stjepan Picek, Radboud University
Suryadipta Majumdar, Concordia University
Syed Rafiul Hussain, Pennsylvania State University
Takuya Watanabe, Deloitte Tohmatsu Cyber LLC
Tatsuya Mori, Waseda University
Theodor Schnitzler, Maastricht University
Tianhao Wang, University of Virginia
Ting Wang, Stony Brook University
Tuba Yavuz, University of Florida
Veelasha Moonsamy, Ruhr University Bochum
Wajih Ul Hassan, University of Virginia
Wenke Lee, Georgia Institute of Technology
William Robertson, Northeastern University
Xiaokuan Zhang, George Mason University
Xingliang Yuan, The University of Melbourne
Xinwen Fu, University of Massachusetts Lowell
Xinyang Ge, Databricks
Xinyu Xing, Northwestern University
Yang Zhang, CISPA Helmholtz Center for Information Security
Yongdae Kim, KAIST
Yonghwi Kwon, University of Maryland
Yuan Hong, University of Connecticut
Yue Zhang, Drexel University
Yuzhe Tang, Syracuse University
Z. Berkay Celik, Purdue University
Zephyr Yao, New Jersey Institute of Technology
Zhikun Zhang, Stanford & CISPA
Zhiyun Qian, University of California, Riverside
Zhou Li, University of California, Irvine

TPC Subcommittees - Special Thanks

Topic-Concern Assessment Committee

- Lorenzo Cavallaro, Ghassan Karame, Ivan Martinovic, Mathias Payer, Stjepan Picek, William Robertson, Ben Stock
- Assessed 101 papers we had flagged for possible topic concerns
- 34 papers desk rejected

Ethics Review Board

- Srdjan Capkun (Chair), Rachel Greenstadt, Aravind Machiry, René Mayrhofer, William Robertson, Juan Tapiador
- Assessed 49 papers with Ethical Concerns
- Interactive process with the authors to address concerns

Distinguished Paper Selection Committee → More tomorrow

Ethics

NDSS promotes, upholds, & defends professional conduct + ethical academic behavior

Zero tolerance for

- Simultaneous submission to other conferences → rejection from both venues
- Borderline double submission in Summer and Fall Cycle
  → early reject of Fall submission
- Unethical attempts of author(s) to interfere with the review process (Author-Reviewer Favoritism & Disclosure of Reviewer Identities)
  → late paper reject after acceptance

Ethics

NDSS promotes, upholds, & defends professional conduct + ethical academic behavior

Zero tolerance for

- Simultaneous submission to other conferences → rejection from both venues
- Borderline double submission in Summer and Fall Cycle
  → early reject of Fall submission
- Unethical attempts of author(s) to interfere with the review process (Author-Reviewer Favoritism & Disclosure of Reviewer Identities)
  → late paper reject after acceptance

Further case-by-case investigations

- Suspicion of AI-generated text in papers and reviews
- Suspicion of plagiarism
- Suspicion of retaliation
- Benefits vs. Risks of security research (such as attacking real-world systems)

Ethics

https://www.sigsac.org/protect/

Cross-Conference Response: NDSS is part of ACM SIGSAC PROTECT

- PROTECT = SIGSAC Committee on Preserving Professional Conduct and Academic Ethics), established in Fall 2024
- NDSS TPC Co-Chairs & Steering Committee Representative
- Coordination with PC chairs of all first-tier security conferences
- Continuous discussion of protection mechanisms (manual reviewer bidding vs. automatic assignments, restrictive reviewer identity sharing vs. anonymous reviewer discussions, etc.)

Current status:

- Single allegation: in dubio pro reo | Accumulated evidence: Strict reaction
- Focus on prevention / defense mechanisms rather than punishment
- Report unethical behavior in reviews of computer security conferences: https://forms.gle/bcCfB5TmCvSiXnsf7 → ~10 cases submitted / under investigation

Committee

- Somesh Jha
- Ninghui Li
- Christina Pöpper
- Zhiqiang Lin
- Lujo Bauer
- Véronique Cortier
- William Enck
- Thorsten Holz
- Trent Jaeger
- Engin Kirda
- David Lie
- Cristina Nita-Rotaru
- Hamed Okhravi
- Mathias Payer
- Giancarlo Pellegrino
- Michael Reiter
- Yinqian Zhang

Further Thanks go to …

David Balenson - Organizing Committee Chair

Mridula Singh and Hyungsub Kim for handling the Proceedings

Robin Wilton from ISOC - bridge between Program Co-Chairs, Organizing Committee and ISOC

External reviewers (we needed your expert knowledge!)

All **authors** who submitted papers (you keep pushing boundaries!)

All of you for coming (you will make the next big breakthrough!)

Good Security …

… is like good health - You only realize how bad yours is when it is too late.

ENJOY
NDSS
2025

Artifact Evaluation Chair Welcome

NDSS SYMPOSIUM/2025

Presented by

Internet Society

#NDSSSymposium2025

Artifact Evaluation

Established with NDSS 2024, the initiative promotes reproducibility of results and dissemination of well-packaged artifacts for our peers

Very positive response

- 63 evaluated artifacts (+79% on 2024)
- More badges requested
- 100+ applications for AE committee

Run by Daniele Cono D’Elia (Sapienza) & Mathy Vanhoef (KU Leuven)

Evaluation Process

Three badges: Available, Functional, Reproduced

9-week evaluation period. Each submission had 3+ reviews

Workflow

- Continuous interactions between authors and evaluators
- Authors receive preliminary reviews so they can work on minor enduring issues
- Evaluators check amendments and converge on a decision

Highlights

68 submissions. 63 met the evaluation requirements (vs. 38 in 2024)

Badges awarded

- 61 artifacts were made **Available** (100% of requested)
- 59 artifacts deemed **Functional** (96.72% of requested)
- 45 artifacts with results **Reproduced** (90% of requested)

Evaluators worked tirelessly to ensure thorough evaluations, helping authors polish their claims and amend clerical errors in their results

Received help from SPHERE project for some CPU-intensive artifacts

The Ones Who Made It Possible

Advije Rizvani
Ahmed Lekssays
Alessandro Erba
Amit Samanta
Andrew Roberts
Aolin Ding
Ayomide Akinsanya
Cen Zhang
CheolJun Park
Christoph Sendner
Cristian Assaiante
Dipsy Desai
Dongwei Xiao
Evangelos Bitsikas
Felix Lange
Fuman Xie
Gertjan Franken
Guangjing Wang
Hao Cui
Héloïse Gollier
Hengkai Ye
Hongyan Chang
Jan Jancar
Jeroen Robben
Jessy Ayala
Jiahao Yu
Jing Liu
Kelly Kaoudis
Marc Damie
Marton Bognar
Matteo Marini
Mir Masood Ali
Nico Heitmann
Naman Gupta
Niklas Niere
Paul Staat
Pedro Bernardo
Prajwal Panzade
Qifan Zhang
Rajrup Ghosh
Rishit Saiya
Ryan Vrecenar
Salvatore Signorello
Shaofeng Li
Shenghan Zheng
Steven Ngo
Tillson Galloway
Tolga Atalay
Torsten Krauß
Tristan Benoit
Vik Vanderlinden
Vinny Adjibi
Xu He
Xuan Xie
Xuesong Bai
Yi Liu
Yiming Zhang
Yirui He
Yu Nong
Yujin Huang
Zheng Yu
Zhengxiong Luo
Zilong Lin