**ACSAC 2023**
December 4–8, 2023 · Austin, Texas, USA

# Welcome to ACSAC 39!!

https://www.acsac.org/

- Welcome
  - Guofei Gu, Conference Chair
- Technical Program and Distinguished Paper Awards
  - Roberto Perdisci and Martina Lindorfer, Program Co-Chairs
- Distinguished Paper with Artifacts Awards
  - Adwait Nadkarni and Xiaojing Liao, AE Co-Chairs
- SWSIS Scholarship Presentations
  - Gabriela Ciocarlie, ACSA Senior Fellow
- Keynote
  - Nicholas Carlini, Research Scientist, Google DeepMind

# About ACSAC

- Core mission: Investigate practical solutions for computer and network security technology

- A broad cross-section of security professionals drawn from academia, industry, and government

- Fun fact: ACSAC is among the oldest computer security conferences! (strong tradition)
  - ACSAC started from 1985
  - ACM CCS started from 1993
  - USENIX Security started from 1988
  - NDSS started from 1994
  - IEEE S&P started from 1980

# Wi-Fi Access

- The hotel provides Wi-Fi access from the meeting rooms

**The account is UTguest and no password required.**

# Program At-a-Glance (Wednesday)

- Breakfast
- **Welcome and Awards**
- **Distinguished Practitioner Keynote**
- Break
- **Multi-track Sessions**
- Lunch
- **Multi-track Sessions**
- Break
- **Multi-track Sessions**
- Conference Dinner

# Program At-a-Glance (Thursday)

- Breakfast
- **Test of Time Paper Awards**
- **Cybersecurity Artifacts Impact Awards and Presentations**
- Break
- **Multi-track Sessions**
- Lunch
- **Multi-track Sessions**
- Break
- **Multi-track Sessions**
- **ACSAC: The Next Forty Years – Open Community Discussion**
- **Poster & Work in Progress Session w/ Light Refreshments**

# Program At-a-Glance (Friday)

- Breakfast
- **Multi-track Sessions**
- Break
- **Multi-track Sessions**
- Closing with Prize Giveaway

- Optional Social Even
  - Lone Star River Boat Cruise (with Lunch)

# Panels & National Interest Track

**Wednesday**

- Panel: Cybersecurity Across Diverse Industries -- It's Not Just Attack/Defend
- Panel: National Cybersecurity Research Directions

**Thursday**

- NITRD Panel: 2023 Federal Cybersecurity R&D Strategic Plan
- Panel: Securing the Nexus: Cybersecurity Meets AI

**Friday**

- Panel: ACSAC - Accessibility of Cyber Interfaces as a Priority

# Case Studies

**Wednesday**

- Template Engines: A Methodology for Assessing Server-Side Code Execution Vulnerabilities. Lorenzo Pisu, University of Cagliari; Giorgio Giacinto, University of Cagliari
- Generative AI: A Security Case Study for Regulated Financial Service Organizations. Dennis Moreau, Intel

**Thursday**

- Working Towards Least Privilege in the Cloud. Kevin Roundy, Andromeda Security
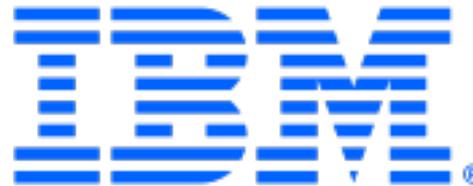- Beyond the XBOM: A Holistic Approach to Cyber Supply Chain Risk. Munish Walther-Puri, Exiger

# Test of Time Paper Awards

- Recognize and honor selected papers from the first 20+ years (1985-2007) that have had a significant impact
  - Led to a major change in the field
  - Are used commercially
  - Have been well cited
  - Are well known as strong papers



https://www.wabisabilearning.com/blog/13-educational-tools-test-time

# Cybersecurity Artifacts Competition and Impact Awards

- **Importance of Cybersecurity Artifacts**
- Introduced last year, this year we continue the Artifacts Competition
  - Broadly open to cybersecurity artifacts previously published in all peer-reviewed venues (conferences, journals), both in academia and industry.
- Example of "Impact"
  - The artifact has been reused and cited in subsequent research publications presented in academic or industry venues.
  - The artifact has been released as open-source software and has received demonstrable appreciation by the security community (e.g., in the form of "stars," "forks," or other types of citations).
  - The artifact has been successfully transitioned to a commercial technology.
  - The artifact consists of an online service that is open to the public or to researchers and demonstrates a significant number of users benefiting from it.
  - The artifact has become a de facto benchmark for one or more use cases.

# Optional Social Outing - Lone Star River Boat Cruise

- Stay for the Friday closing so you don't miss our rockin' giveaways with Emcee Z, then embark on the Lone Star River Boat Cruise for lunch and an afternoon social
- Friday noon
- **Check at REGISTRATION DESK if interested**

Mobile Program

https://www.openconf.org/acsac2023/mobile

# Conference Proceedings

- Via ACM Digital Library

  https://dl.acm.org/conference/acsac
  https://dl.acm.org/doi/proceedings/10.1145/3627106

- Via ACSAC website

  https://www.acsac.org/2023/program/papers/

ICPS

Published by ACM

# Organizing Committee

- **Conference Chair**
  Guofei Gu, Texas A&M University
- **Program Chair**
  Roberto Perdisci, University of Georgia and Georgia Tech
- **Program Co-Chair**
  Martina Lindorfer, TU Wien
- **Artifacts Evaluation Co-Chairs**
  Adwait Nadkarni, William & Mary
  Xiaojing Liao, Indiana University Bloomington
- **Case Studies Chair**
  David Ott, VMware
- **National Interest Track Chair**
  Tomas Vagoun, NITRD
- **Panels Chair**
  Daniel Faigin, Aerospace Corporation
  Beth Scruggs, Aerospace Corporation
- **Posters & Works-in-Progress Co-Chairs**
  Yonghwi Kwon, University of Virginia
  Chung Hwan Kim, University of Texas at Dallas (UTD)
- **Workshops Chair**
  Harvey Rubinovitz, MITRE
  Hongxin Hu, University of Buffalo
- **Test of Time Award Committee Chair**
  William Robertson, Northeastern University

- **Knowledge Coordinator**
  Dan Thomsen, SIFT
- **Local Arrangements Coordinator**
  Chia-Che Tsai, Texas A&M University
  Zain Shamsi, Applied Research Lab, UT Austin
- **Proceedings Coordinator**
  Giorgio Giacinto, University of Cagliari, Italy
- **Publicity Co-Coordinators**
  Peter Mayer, Karlsruhe Institute of Technology
  Hamed Okhravi, MIT Lincoln Laboratory
  Xiapu Luo, Hong Kong Polytechnic University
- **Registration Coordinators**
  Karen Davis
  Daniel Faigin, Aerospace Corporation
- **Sponsorship chair**
  Kapil Singh, IBM
- **Student Conferenceship Coordinators**
  Jinpeng Wei, University of North Carolina at Charlotte
  Tyson Bailey, Sandia National Lab
- **Treasurer**
  David Balenson, USC Information Sciences Institute
- **Web Advisor**
  Robert H'obbes' Zakon, Zakon Group

# Steering Committee

- David Balenson, USC Information Sciences Institute
- Kevin Butler, University of Florida
- Juan Caballero, IMDEA Software Institute
- Gabriela Ciocarlie, The University of Texas at San Antonio
- Jeremy Epstein, NSF*
- Daniel Faigin, Aerospace Corporation
- Carrie Gates, Bank of America
- Guofei Gu, Texas A&M University
- Ann Marmor-Squires, The Sq Group
- Charles Payne, Adventium Labs

- William Robertson, Northeastern University
- Steve Rome
- Harvey Rubinovitz, MITRE
- Stephen Schwab, USC-ISI
- Cristina Serban, AT&T Security Research Center (Ret.)
- Dan Thomsen, SIFT
- Danfeng (Daphne) Yao, Virginia Tech
- Heng Yin, UC Riverside
- Robert H'obbes' Zakon, Zakon Group LLC

# Keep Up with ACSAC on Social Media

Twitter
- @ACSAC_Conf
- https://twitter.com/ACSAC_Conf

Facebook
- https://www.facebook.com/acsaconf/
- https://www.facebook.com/groups/acsacattendees/

LinkedIn
- https://www.linkedin.com/in/acsac-chair/

# Program Chair Opening Remarks

# SWSIS Scholarship

# Keynotes

# Distinguished Practitioner Keynote

**Computer Security in the Age of Large Language Models Abstract**

**Nicholas Carlini**

Research Scientist
Google DeepMind

# Enjoy the conference!