Cybersecurity Artifacts Competition and Impact Awards
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
angr: A Powerful and User-friendly Binary Analysis Platform

Yan Shoshitaishvili, Ruoyu Wang, Audrey Dutcher, Christopher Kruegel, and Giovanni Vigna

Guofei Gu
GUOFEI GU
GENERAL CHAIR

Roberto Perdisci
ROBERTO PERDISCI
PC CHAIR
SGX-Step: An Open-Source Framework for Precise Dissection and Practical Exploitation of Intel SGX Enclaves

Jo Van Bulck and Frank Piessens

Guofei Gu
GUOFEI GU
GENERAL CHAIR

Roberto Perdisci
ROBERTO PERDISCI
PC CHAIR