# 2024 Annual Computer Security Applications Conference (ACSAC 2024)

## Honolulu, Hawaii, USA
## 9-13 December 2024

## Pages 1-635

IEEE Catalog Number: CFP24393-POD
ISBN: 979-8-3315-2089-2

**Copyright © 2024 by the Institute of Electrical and Electronics Engineers, Inc.**
**All Rights Reserved**

*Copyright and Reprint Permissions*: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

****** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

| | |
|---|---|
| IEEE Catalog Number: | CFP24393-POD |
| ISBN (Print-On-Demand): | 979-8-3315-2089-2 |
| ISBN (Online): | 979-8-3315-2088-5 |
| ISSN: | 1063-9527 |

**Additional Copies of This Publication Are Available From:**

Curran Associates, Inc
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: (845) 758-0400
Fax: (845) 758-2633
E-mail: curran@proceedings.com
Web: www.proceedings.com

# 2024 Annual Computer Security Applications Conference (ACSAC)

# ACSAC 2024

## Table of Contents



## Generative AI (for) Security

## Virtualization and Cloud Security

## Web Security and Privacy



## Cyber-Physical Systems Security

## Passwords and Authentication



## Microarchitectural Attacks and Side-Channels

## Cryptocurrency and Payment Security



## System Security

## IoT and Smart Home Security



## Privacy Enhancing Technologies

## Machine Learning Security I: Federated Learning

## Malware and Intrusion Detection

## Machine Learning Security II: Backdoors & Attacks



## (Autonomous) Vehicle Security

## Application Security



## Network Security

## Machine Learning Security III: Potpourri

**Author Index**