2024 Annual Computer Security Applications Conference Workshops (ACSAC Workshops 2024)

Honolulu, Hawaii, USA
9-10 December 2024

IEEE

IEEE Catalog Number: CFP240C1-POD
ISBN: 979-8-3315-3282-6

****** 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:	CFP240C1-POD
ISBN (Print-On-Demand):	979-8-3315-3282-6
ISBN (Online):	979-8-3315-3281-9

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 Workshops (ACSAC Workshops)

ACSACW 2024

Table of Contents

Robustness, Privacy and Safety for ML Systems I

Robustness, Privacy and Safety for ML Systems II

Attack to ML Algorithms

ICSS

WAITI with IOT-SCTI

AI-Driven Cybersecurity Solutions for CTI, IoT and Software Infrastructures

Leveraging Large Language Models for Cybersecurity and Threat Intelligence

WEB3SEC