2025 IEEE/ACM 3rd International Workshop on Software Vulnerability Management (SVM 2025)

Ottawa, Ontario, Canada
3 May 2025

IEEE Catalog Number: CFP25IZ4-POD
ISBN: 979-8-3315-1469-3

Copyright © 2025 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:	CFP25IZ4-POD
ISBN (Print-On-Demand):	979-8-3315-1469-3
ISBN (Online):	979-8-3315-1468-6

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

2025 IEEE/ACM 3rd International Workshop on Software Vulnerability Management (SVM)

SVM 2025

Table of Contents

SVM 2025

Edge-Based Detection of Label Flipping Attacks in Federated Learning Using Explainable AI 1
Nourah Saad AlOtaibi (King Fahd University of Petroleum and Minerals, Saudi Arabia), Muhamad Felemban (King Fahd University of Petroleum and Minerals, Saudi Arabia), and Sajjad Mahmood (King Fahd University of Petroleum and Minerals, Saudi Arabia)

Understanding the Changing Landscape of Automotive Software Vulnerabilities: Insights from a Seven-Year Analysis 9
Srijita Basu (Chalmers University of Technology and University of Gothenburg) and Miroslaw Staron (Chalmers University of Technology and University of Gothenburg)

A Multi-Dimensional Visual Analytics Tool for the Security Posture of Open-Source Software.......... 17
Tianyu Li (KU Leuven, Belgium), Chaomeng Lu (KU Leuven, Belgium), and Bert Lagaisse (KU Leuven, Belgium)

"Just Use Rust": A Best-Case Historical Study of Open Source Vulnerabilities in C 25
Andrew Meneely (Rochester Institute of Technology), Aiden Green (Rochester Institute of Technology), Tyler Jaafari (Rochester Institute of Technology), Matthew Fluet (Rochester Institute of Technology), and Brandon Keller (Rochester Institute of Technology)

An Exploratory Study of Security Vulnerabilities in Machine Learning Deployment Projects 33
Akond Rahman (Auburn University), Anthony Skjellum (Tennessee Tech University), and Yue Zhang (Auburn University)

A Landscape Study of Open-Source Tools for Software Bill of Materials (SBOM) and Supply Chain Security 37
Derek Garcia (University of Hawaii, USA), Mehdi Tarrit Mirakorhli (University of Hawaii, USA), Schuyler Dillon (Rochester Institute of Technology, USA), Kevin Laporte (Rochester Institute of Technology, USA), Matthew Morrison (Rochester Institute of Technology, USA), Henry Lu (Rochester Institute of Technology, USA), Viktoria Koscinski (Rochester Institute of Technology, USA), Christopher Enoch (Rochester Institute of Technology, USA), Mohamad Fazelnia (University of Hawaii, USA), and Roger Chen (University of Hawaii, USA)

Author Index **47**