

2023 IEEE Security and Privacy Workshops (SPW 2023)

**San Francisco, California, USA
25 May 2023**



**IEEE Catalog Number: CFP23SPX-POD
ISBN: 979-8-3503-1237-9**

**Copyright © 2023 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:	CFP23SPX-POD
ISBN (Print-On-Demand):	979-8-3503-1237-9
ISBN (Online):	979-8-3503-1236-2
ISSN:	2639-7862

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

CURRAN ASSOCIATES INC.
proceedings
.com

2023 IEEE Security and Privacy Workshops (SPW) **SPW 2023**

Table of Contents

SecWeb 2023

HoneyKube: Designing and Deploying a Microservices-based Web Honeypot	1
<i>Chakshu Gupta (University of Twente, The Netherlands), Thijs van Ede (University of Twente, The Netherlands), and Andrea Continella (University of Twente, The Netherlands)</i>	
Evaluating Password Composition Policy and Password Meters of Popular Websites	12
<i>Kyungchan Lim (University of Tennessee, USA), Joshua H. Kang (University of Tennessee, USA), Matthew Dixon (University of Tennessee, USA), Hyungjoon Koo (Sungkyunkwan University, South Korea), and Doowon Kim (University of Tennessee, USA)</i>	

6th Deep Learning Security and Privacy Workshop

Is It Overkill? Analyzing Feature-Space Concept Drift in Malware Detectors	21
<i>Zhi Chen (University of Illinois at Urbana-Champaign), Zhenning Zhang (University of Illinois at Urbana-Champaign), Zeliang Kan (King's College London and University College London), Limin Yang (University of Illinois at Urbana-Champaign), Jacopo Cortellazzi (King's College London and University College London), Feargus Pendlebury (University College London), Fabio Pierazzi (King's College London), Lorenzo Cavallaro (University College London), and Gang Wang (University of Illinois at Urbana-Champaign)</i>	
Deep Bribe: Predicting the Rise of Bribery in Blockchain Mining with Deep RL	29
<i>Roi Bar-Zur (Technion, IC3), Danielle Dori (Technion), Sharon Vardi (Technion), Ittay Eyal (Technion, IC3), and Aviv Tamar (Technion)</i>	
On the Brittleness of Robust Features: An Exploratory Analysis of Model Robustness and Illusionary Robust Features	38
<i>Alireza Aghabagherloo (KU Leuven, Belgium), Rafa Gálvez (KU Leuven, Belgium), Davy Preuveneers (KU Leuven, Belgium), and Bart Preneel (KU Leuven, Belgium)</i>	
Benchmarking the Effect of Poisoning Defenses on the Security and Bias of Deep Learning Models	45
<i>Nathalie Baracaldo (IBM Research), Farhan Ahmed (IBM Research), Kevin Eykholt (IBM Research), Yi Zhou (IBM Research), Shriti Priya (IBM Research), Taesung Lee (IBM Research), Swanand Kahde (IBM Research), Mike Tan (The MITRE Corporation), Sridevi Polavaram (The MITRE Corporation), Sterling Suggs (Two Six Technologies), Yuyang Gao (Emory University), and David Slater (Two Six Technologies)</i>	

On the Pitfalls of Security Evaluation of Robust Federated Learning	57
<i>Momin Ahmad Khan (University of Massachusetts Amherst), Virat Shejwalkar (University of Massachusetts Amherst), Amir Houmansadr (University of Massachusetts Amherst), and Fatima M. Anwar (University of Massachusetts Amherst)</i>	
SafeFL: MPC-friendly Framework for Private and Robust Federated Learning	69
<i>Till Gehlhar (Technical University of Darmstadt), Felix Marx (Technical University of Darmstadt), Thomas Schneider (Technical University of Darmstadt), Ajith Suresh (Technical University of Darmstadt), Tobias Wehrle (Technical University of Darmstadt), and Hossein Yalame (Technical University of Darmstadt)</i>	
Membership Inference Attacks against Diffusion Models	77
<i>Tomoya Matsumoto (Osaka University), Takayuki Miura (Osaka University / NTT), and Naoto Yanai (Osaka University)</i>	
On Feasibility of Server-side Backdoor Attacks on Split Learning	84
<i>Behrad Tajalli (Radboud University, Netherlands), Oguzhan Ersoy (Radboud University, Netherlands), and Stjepan Picek (Radboud University, Netherlands)</i>	
Your Email Address Holds the Key: Understanding the Connection Between Email and Password Security with Deep Learning	94
<i>Etienne Salimbeni (EPFL, Switzerland), Nina Mainusch (EPFL, Switzerland), and Dario Pasquini (EPFL, Switzerland)</i>	

The Ninth Workshop on Language-Theoretic Security (LangSec)

A Survey of Parser Differential Anti-Patterns	105
<i>Sameed Ali (Dartmouth College) and Sean W. Smith (Dartmouth College)</i>	
PolyDoc: Surveying PDF Files from the PolySwarm network	117
<i>Prashant Anantharaman (Narf Industries), Robert Lathrop (Narf Industries), Rebecca Shapiro (Narf Industries), and Michael Locasto (Narf Industries)</i>	
Whole-Program Privilege and Compartmentalization Analysis with the Object-Encapsulation Model	135
<i>Yudi Yang (Rice University), Weijie Huang (Rice University), Kelly Kaoudis (Trail of Bits), and Nathan Dautenhahn (Rice University)</i>	
Unsupervised clustering of file dialects according to monotonic decompositions of mixtures.....	147
<i>Michael Robinson (American University, USA), Tate Altman (American University, USA), Denley Lam (BAE Systems FAST Labs, USA), and Letitia Li (BAE Systems FAST Labs, USA)</i>	
DISV: Domain Independent Semantic Validation of Data Files	163
<i>Ashish Kumar (Penn State University), Bill Harris (Galois, Inc.), and Gang Tan (Penn State University)</i>	
Blind Spots: Identifying Exploitable Program Inputs	175
<i>Henrik Brodin (Trail of Bits), Marek Surovič (Trail of Bits), and Evan Sultanik (Trail of Bits)</i>	

Automatically Detecting Variability Bugs Through Hybrid Control and Data Flow Analysis	187
<i>Kelly Kaoudis (Trail of Bits), Henrik Brodin (Trail of Bits), and Evan Sultanik (Trail of Bits)</i>	
Research Report: Synthesizing Intrusion Detection System Test Data from Open-Source Attack Signatures	198
<i>Jared Chandler (Tufts University, USA) and Adam Wick (Fastly, USA)</i>	
Corpus-wide Analysis of Parser Behaviors via a Format Analysis Workbench	209
<i>Walt Woods (Galois, Inc.) and Pottayil Harisanker Menon (Galois, Inc.)</i>	

17th IEEE Workshop on Offensive Technologies

Reflections on Trusting Docker: Invisible Malware in Continuous Integration Systems	219
<i>Florent Moriconi (EURECOM, AMADEUS, France), Axel Ilmari Neergaard (EURECOM, France, CUJO AI, Finland), Lucas Georget (EURECOM, EDF R&D, LAAS-CNRS, France), Samuel Aubertin (EURECOM, France), and Aurélien Francillon (EURECOM, France)</i>	
ROPfuscator: Robust Obfuscation with ROP	228
<i>Giulio De Pasquale (King's College London), Fukutomo Nakanishi (Toshiba Corporation), Daniele Ferla (Università di Bologna), and Lorenzo Cavallaro (University College London)</i>	
GPThreats-3: Is Automatic Malware Generation a Threat?	238
<i>Marcus Botacin (Texas A&M University)</i>	
Emoji shellcoding in RISC-V	255
<i>Hadrien Barral (Ecole Normale Supérieure), Georges-Axel Jaloyan (Ecole Normale Supérieure), and David Naccache (Ecole Normale Supérieure)</i>	
The ghost is the machine: weird machines in transient execution	264
<i>Ping-Lun Wang (Carnegie Mellon University, USA), Fraser Brown (Carnegie Mellon University, USA), and Riad S. Wahby (Carnegie Mellon University, USA)</i>	
Cryo-Mechanical RAM Content Extraction Against Modern Embedded Systems	273
<i>Yuanzhe Wu (Red Balloon Security, USA), Grant Skipper (Red Balloon Security, USA), and Ang Cui (Red Balloon Security, USA)</i>	
CustomProcessingUnit: Reverse Engineering and Customization of Intel Microcode	285
<i>Pietro Borrello (Sapienza University of Rome, Italy), Catherine Easdon (Dynatrace Research & Graz University of Technology, Austria), Martin Schwarzl (Graz University of Technology, Austria), Roland Czerny (Graz University of Technology, Austria), and Michael Schwarz (CISPA Helmholtz Center for Information Security, Germany)</i>	
The Little Seal Bug: Optical Sound Recovery from Lightweight Reflective Objects	298
<i>Ben Nassi (Ben-Gurion University of the Negev), Raz Swissa (Ben-Gurion University of the Negev), Jacob Shams (Ben-Gurion University of the Negev), Boris Zadov (Ben-Gurion University of the Negev), and Yuval Elovici (Ben-Gurion University of the Negev)</i>	
ESPwn32: Hacking with ESP32 System-on-Chips	311
<i>Romain Cayre (EURECOM), Damien Cauquil (Quarkslab), and Aurélien Francillon (EURECOM)</i>	

Fuzzing the Latest NTFS in Linux with Papora: An Empirical Study	326
<i>Edward Lo (Amber Group), Ningyu He (Peking University, China), Yuejie Shi (Amber Group), Jiajia Xu (Amber Group), Chiachih Wu (Amber Group), Ding Li (Peking University, China), and Yao Guo (Peking University, China)</i>	
Divergent Representations: When Compiler Optimizations Enable Exploitation	337
<i>Andreas D. Kellas (Columbia University), Alan Cao (Trail of Bits), Peter Goodman (Trail of Bits), and Junfeng Yang (Columbia University)</i>	
Go or No Go: Differential Fuzzing of Native and C Libraries	349
<i>Alessandro Sorniotti (IBM Research Europe -- Zürich), Michael Weissbacher (Block, Inc.), and Anil Kurmus (IBM Research Europe -- Zürich)</i>	
ASanItiy: On Bug Shadowing by Early ASan Exits	364
<i>Vincent Ulitzsch (Technische Universit at Berlin - SECT), Deniz Scholz (Technische Universit at Berlin - SECT), and Dominik Maier (Technische Universit at Berlin - SECT)</i>	
Scripted Henchmen: Leveraging XS-Leaks for Cross-Site Vulnerability Detection	371
<i>Tom Van Goethem (imec-DistriNet, KU Leuven), Iskander Sanchez-Rola (Norton Research Group), and Wouter Joosen (imec-DistriNet, KU Leuven)</i>	
Hakuin: Optimizing Blind SQL Injection with Probabilistic Language Models	384
<i>Jakub Pružinec (Nanyang Technological University, Singapore) and Quynh Anh Nguyen (Nanyang Technological University, Singapore)</i>	
Towards Simultaneous Attacks on Multiple Cellular Networks	394
<i>Alexander Ross (North Carolina State University) and Bradley Reaves (North Carolina State University)</i>	
Author Index	407