2022 IEEE 7th European Symposium on Security and Privacy (EuroS&P 2022)

Genoa, Italy
6 – 10 June 2022

IEEE Catalog Number: CFP22C75-POD
ISBN: 978-1-6654-1615-3

**Copyright © 2022 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:	CFP22C75-POD
ISBN (Print-On-Demand):	978-1-6654-1615-3
ISBN (Online):	978-1-6654-1614-6

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

CURRAN ASSOCIATES INC.
proceedings
.com

2022 IEEE 7th European Symposium on Security and Privacy (EuroS&P)

EuroSP 2022

Table of Contents

Message from the EuroS&P 2022 General Chairs x
Message from the EuroS&P 2022 Program Committee Co-Chairs xi
Organizing Committee of EuroS&P 2022 xii
Program Committee of EuroS&P 2022 xiii

ML for Security

Modelling Direct Messaging Networks with Multiple Recipients for Cyber Deception 1
Kristen Moore (Data61, CSIRO, Australia; Cyber Security Cooperative Research Centre Australia), Cody James Christopher (Data61, CSIRO, Australia; Cyber Security Cooperative Research Centre Australia), David Liebowitz (Penten Pty Ltd, Australia; UNSW, Australia), Surya Nepal (Data61, CSIRO, Australia; Cyber Security Cooperative Research Centre Australia), and Renee Selvey (Data61, CSIRO, Australia; Cyber Security Cooperative Research Centre Australia)

SoK: The Impact of Unlabelled Data in Cyberthreat Detection 20
Giovanni Apruzzese (University of Liechtenstein), Pavel Laskov (University of Liechtenstein), and Aliya Tastemirova (University of Liechtenstein)

SIERRA: Ranking Anomalous Activities in Enterprise Networks 44
*Jehyun Lee (Trustwave), Farren Tang (Trustwave), Phyo May Thet (A*STAR I2R), Desmond Yeoh (Shopee), Mitch Rybczynski (Trustwave), and Dinil Mon Divakaran (Trustwave)*

Investigating Graph Embedding Methods for Cross-Platform Binary Code Similarity Detection . 60
Victor Cochard (Cyber-Defence Campus, armasuisse S+T, Switzerland), Damian Pfammatter (Cyber-Defence Campus, armasuisse S+T, Switzerland), Chi Thang Duong (DISL, EPFL, Switzerland), and Mathias Humbert (University of Lausanne, Switzerland)

Illuminati: Towards Explaining Graph Neural Networks for Cybersecurity Analysis 74
Haoyu He (The George Washington University), Yuede Ji (University of North Texas), and H. Howie Huang (The George Washington University)

Encrypted Computation

SoK: Cryptanalysis of Encrypted Search with LEAKER - A Framework for LEakage AttacK Evaluation on Real-World Data 90
Seny Kamara (Brown University), Abdelkarim Kati (Mohammed-VI Polytechnic University), Tarik Moataz (Aroki Systems), Thomas Schneider (TU Darmstadt), Amos Treiber (TU Darmstadt), and Michael Yonli (TU Darmstadt)

EZEE: Epoch Parallel Zero Knowledge for ANSI C 109
Yibin Yang (Georgia Institute of Technology, USA), David Heath (Georgia Institute of Technology, USA), Vladimir Kolesnikov (Georgia Institute of Technology, USA), and David Devecsery (Facebook; Work done at Georgia Tech, USA)

SoK: Privacy-Preserving Computing in the Blockchain Era 124
Ghada Almashaqbeh (University of Connecticut) and Ravital Solomon (Sunscreen)

CostCO: An Automatic Cost Modeling Framework for Secure Multi-party Computation 140
Vivian Fang (UC Berkeley), Lloyd Brown (UC Berkeley), William Lin (UC Berkeley), Wenting Zheng (CMU), Aurojit Panda (NYU), and Raluca Ada Popa (UC Berkeley)

Network and Web Security

HyperLogLog: Exponentially Bad in Adversarial Settings 154
Kenneth G. Paterson (ETH Zurich) and Mathilde Raynal (EPFL)

Trampoline Over the Air: Breaking in IoT Devices Through MQTT Brokers 171
Huikai Xu (Tsinghua University), Miao Yu (Tsinghua University), Yanhao Wang (Qi An Xin Technology Research Institute), Yue Liu (Southeast University; Qi An Xin Technology Research Institute), Qinsheng Hou (Shandong University; Qi An Xin Technology Research Institute), Zhenbang Ma (Qi An Xin Technology Research Institute), Haixin Duan (Tsinghua University; Qi An Xin Technology Research Institute), Jianwei Zhuge (Tsinghua University), and Baojun Liu (Tsinghua University)

Hide and Seek: Revisiting DNS-Based User Tracking 188
Deliang Chang (Tsinghua University), Joann Qiongna Chen (University of California, Irvine), Zhou Li (University of California, Irvine), and Xing Li (Tsinghua University)

SoK: All or Nothing - A Postmortem of Solutions to the Third-Party Script Inclusion Permission Model and a Path Forward 206
Steven Sprecher (Northeastern University), Christoph Kerschbaumer (Mozilla Corporation), and Engin Kirda (Northeastern University)

Lethe: Practical Data Breach Detection with Zero Persistent Secret State 223
Antreas Dionysiou (University of Cyprus) and Elias Athanasopoulos (University of Cyprus)

Software Security

Hand Sanitizers in the Wild: A Large-Scale Study of Custom JavaScript Sanitizer Functions 236
David Klein (Technische Universität Braunschweig), Thomas Barber (SAP Security Research), Souphiane Bensalim (SAP Security Research), Ben Stock (CISPA Helmholtz Center for Information Security), and Martin Johns (Technische Universität Braunschweig)

Lightweight, Multi-Stage, Compiler-Assisted Application Specialization 251
Mohannad Alhanahnah (University of Wisconsin-Madison, USA), Rithik Jain (University of Wisconsin-Madison, USA), Vaibhav Rastogi (University of Wisconsin-Madison, USA), Somesh Jha (University of Wisconsin-Madison, USA), and Thomas Reps (University of Wisconsin-Madison, USA)

LockedDown: Exploiting Contention on Host-GPU PCIe Bus for Fun and Profit 270
Mert Side (Texas Tech University, USA), Fan Yao (University of Central Florida, USA), and Zhenkai Zhang (Clemson University, USA)

Fuzzing with Data Dependency Information 286
Alessandro Mantovani (EURECOM), Andrea Fioraldi (EURECOM), and Davide Balzarotti (EURECOM)

Adversarial Machine Learning

Unrolling SGD: Understanding Factors Influencing Machine Unlearning 303
Anvith Thudi (University of Toronto), Gabriel Deza (University of Toronto), Varun Chandrasekaran (University of Wisconsin-Madison), and Nicolas Papernot (University of Toronto)

Transformer-Based Extraction of Deep Image Models 320
Verena Battis (Fraunhofer Institute SIT - ATHENE, Germany) and Alexander Penner (Fraunhofer Institute SIT - ATHENE, Germany)

DNN Model Architecture Fingerprinting Attack on CPU-GPU Edge Devices 337
Kartik Patwari (University of California, Davis, USA), Syed Mahbub Hafiz (University of California, Davis, USA), Han Wang (University of California, Davis, USA), Houman Homayoun (University of California, Davis, USA), Zubair Shafiq (University of California, Davis, USA), and Chen-Nee Chuah (University of California, Davis, USA)

Towards Fair and Robust Classification 356
Haipei Sun (Facebook Inc, USA), Kun Wu (Stevens Institute of Technology), Ting Wang (Penn State University, University Park, PA), and Wendy Hui Wang (Stevens Institute of Technology, Hoboken)

Users and Security

WatchAuth: User Authentication and Intent Recognition in Mobile Payments using a Smartwatch 377
Jack Sturgess (University of Oxford, UK), Simon Eberz (University of Oxford, UK), Ivo Sluganovic (University of Oxford, UK), and Ivan Martinovic (University of Oxford, UK)

Difficult for Thee, But Not for Me: Measuring the Difficulty and User Experience of Remediating Persistent IoT Malware 392
Elsa Rodríguez (Delft University of Technology), Max Fukkink (Delft University of Technology), Simon Parkin (Delft University of Technology), Michel van Eeten (Delft University of Technology), and Carlos Gañán (Delft University of Technology)

KGP Meter: Communicating Kin Genomic Privacy to the Masses 410
Mathias Humbert (University of Lausanne, Switzerland), Didier Dupertuis (EPFL, Switzerland), Mauro Cherubini (University of Lausanne, Switzerland), and Kévin Huguenin (University of Lausanne, Switzerland)

aaeCAPTCHA: The Design and Implementation of Audio Adversarial CAPTCHA 430
Md Imran Hossen (University of Louisiana at Lafayette, USA) and Xiali Hei (University of Louisiana at Lafayette, USA)

Information Flow

Dynamic Policies Revisited 448
Amir M. Ahmadian (KTH Royal Institute of Technology) and Musard Balliu (KTH Royal Institute of Technology)

Compositional Information Flow Monitoring for Reactive Programs 467
McKenna McCall (Carnegie Mellon University, USA), Abhishek Bichhawat (Indian Institute of Technology Gandhinagar, USA), and Limin Jia (Carnegie Mellon University, USA)

Transparent DIFC: Harnessing Innate Application Event Logging for Fine-Grained Decentralized Information Flow Control 487
Jason Liu (University of Illinois at Urbana-Champaign, USA), Anant Kandikuppa (University of Illinois at Urbana-Champaign, USA), and Adam Bates (University of Illinois at Urbana-Champaign, USA)

xTag: Mitigating Use-After-Free Vulnerabilities via Software-Based Pointer Tagging on Intel x86-64 502
Lukas Bernhard (Ruhr University Bochum), Michael Rodler (University of Duisburg-Essen), Thorsten Holz (CISPA Helmholtz Center for Information Security), and Lucas Davi (University of Duisburg-Essen)

Systems & Hardware Security

HARM: Hardware-Assisted Continuous Re-Randomization for Microcontrollers 520
Jiameng Shi (University of Georgia), Le Guan (University of Georgia), Wenqiang Li (Institute of Information Engineering, CAS), Dayou Zhang (University of Georgia), Ping Chen (Fudan University), and Ning Zhang (Washington University in St. Louis)

Laser Meager Listener: A Scientific Exploration of Laser-Based Speech Eavesdropping in Commercial User Space 537
Payton Walker (Texas A&M University, USA) and Nitesh Saxena (Texas A&M University, USA)

SoK: Workerounds - Categorizing Service Worker Attacks and Mitigations 555
Karthika Subramani (University of Georgia), Jordan Jueckstock (North Carolina State University), Alexandros Kapravelos (North Carolina State University), and Roberto Perdisci (University of Georgia; Georgia Institute of Technology)

SAUSAGE: Security Analysis of Unix Domain Socket usAGE in Android 572
Mounir Elgharabawy (Concordia University, Canada), Blas Kojusner (University of Florida, USA), Mohammad Mannan (Concordia University, Canada), Kevin R. B. Butler (University of Florida, USA), Byron Williams (University of Florida, USA), and Amr Youssef (Concordia University, Canada)

Applied Cryptography

We Can Make Mistakes: Fault-Tolerant Forward Private Verifiable Dynamic Searchable Symmetric Encryption 587
Dandan Yuan (The University of Auckland), Shujie Cui (Monash University), and Giovanni Russello (The University of Auckland)

Cross Chain Atomic Swaps in the Absence of Time via Attribute Verifiable Timed Commitments... 606
Yacov Manevich (University of Haifa, Israel) and Adi Akavia (University of Haifa, Israel)

SoK: Oblivious Pseudorandom Functions 625
Sílvia Casacuberta (Harvard University), Julia Hesse (IBM Research Europe - Zurich), and Anja Lehmann (Hasso Plattner Institute & University of Potsdam)

Signature Correction Attack on Dilithium Signature Scheme 647
Saad Islam (Worcester Polytechnic Institute, USA), Koksal Mus (Worcester Polytechnic Institute, USA), Richa Singh (Worcester Polytechnic Institute, USA), Patrick Schaumont (Worcester Polytechnic Institute, USA), and Berk Sunar (Worcester Polytechnic Institute, USA)

Attacks on Machine Learning

GRAPHITE: Generating Automatic Physical Examples for Machine-Learning Attacks on Computer Vision Systems 664
Ryan Feng (University of Michigan), Neal Mangaokar (University of Michigan), Jiefeng Chen (University of Wisconsin, Madison), Earlence Fernandes (University of Wisconsin, Madison), Somesh Jha (University of Wisconsin, Madison), and Atul Prakash (University of Michigan)

TrojanZoo: Towards Unified, Holistic, and Practical Evaluation of Neural Backdoors 684
Ren Pang (Pennsylvania State University), Zheng Zhang (Pennsylvania State University), Xiangshan Gao (Zhejiang University), Zhaohan Xi (Pennsylvania State University), Shouling Ji (Zhejiang University), Peng Cheng (Zhejiang University), Xiapu Luo (The Hong Kong Polytechnic University), and Ting Wang (Pennsylvania State University)

Dynamic Backdoor Attacks Against Machine Learning Models 703
Ahmed Salem (Microsoft Research), Rui Wen (CISPA Helmholtz Center for Information Security), Michael Backes (CISPA Helmholtz Center for Information Security), Shiqing Ma (Rutgers University), and Yang Zhang (CISPA Helmholtz Center for Information Security)

Captcha me if you can: Imitation Games with Reinforcement Learning 719
Ilias Tsingenopoulos (imec-DistriNet, KU Leuven, Belgium), Davy Preuveneers (imec-DistriNet, KU Leuven, Belgium), Lieven Desmet (imec-DistriNet, KU Leuven, Belgium), and Wouter Joosen (imec-DistriNet, KU Leuven, Belgium)

Author Index **737**