

2020 IEEE European Symposium on Security and Privacy (EuroS&P 2020)

**Genoa, Italy
7 – 11 September 2020**



**IEEE Catalog Number: CFP20C75-POD
ISBN: 978-1-7281-5088-8**

**Copyright © 2020 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:	CFP20C75-POD
ISBN (Print-On-Demand):	978-1-7281-5088-8
ISBN (Online):	978-1-7281-5087-1

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

2020 IEEE European Symposium on Security and Privacy (EuroS&P) EuroSP 2020

Table of Contents

Message from the General Chairs .xi.....	
Message from the Euro S&P 2020 Program Chairs .xii.....	
Organizing Committee .xiv.....	
Program Committee .xv.....	
Steering Committee .xvii.....	

Session #1: Software Security

Quantitative Assessment on the Limitations of Code Randomization for Legacy Binaries .1.....	
<i>Pei Wang (Independent Researcher), Jinquan Zhang (The Pennsylvania State University), Shuai Wang (HKUST), and Dinghao Wu (The Pennsylvania State University)</i>	
Saffire: Context-sensitive Function Specialization against Code Reuse Attacks .17.....	
<i>Shachee Mishra (Stony Brook University) and Michalis Polychronakis (Stony Brook University)</i>	
Improving Fuzzing through Controlled Compilation .34.....	
<i>Laurent Simon (Samsung Research America) and Akash Verma (Samsung Research America)</i>	
VGraph: A Robust Vulnerable Code Clone Detection System Using Code Property Triplets .53....	
<i>Benjamin Bowman (George Washington University) and H. Howie Huang (George Washington University)</i>	

Session #2: Human Factors in Security and Privacy

Multi-country Study of Third Party Trackers from Real Browser Histories .70.....	
<i>Xuehui Hu Hu (King's College London), Guillermo Suarez de Tangil (King's College London), and Nishanth Sastry (University of Surrey)</i>	
X-Men: A Mutation-Based Approach for the Formal Analysis of Security Ceremonies .87.....	
<i>Diego Sempreboni (King's College London, UK) and Luca Viganò (King's College London, UK)</i>	
Anyone Else Seeing this Error?: Community, System Administrators, and Patch Information .105	
<i>Adam Jenkins (University of Edinburgh), Pieris Kalligeros (University of Edinburgh), Kami Vaniea (University of Edinburgh), and Maria Wolters (University of Edinburgh)</i>	

User Attitudes on Direct-to-Consumer Genetic Testing .120.....
Debjani Saha (University of Maryland), Anna Chan (University of Maryland), Brook Stacy (University of Maryland), Kiran Javkar (University of Maryland), Sushant Patkar (University of Maryland; National Cancer Institute, NIH), and Michelle L. Mazurek (University of Maryland)

Session #3: Security of AI

Jekyll: Attacking Medical Image Diagnostics Using Deep Generative Models .139.....
Neal Mangaokar (Virginia Tech), Jiameng Pu (Virginia Tech), Parantapa Bhattacharya (University of Virginia), Chandan K. Reddy (Virginia Tech), and Bimal Viswanath (Virginia Tech)

Evaluating Explanation Methods for Deep Learning in Security .158.....
Alexander Warnecke (TU Braunschweig), Daniel Arp (TU Braunschweig), Christian Wressnegger (Karlsruhe Institute of Technology), and Konrad Rieck (TU Braunschweig)

Bypassing Backdoor Detection Algorithms in Deep Learning .175.....
Te Juin Lester Tan (National University of Singapore) and Reza Shokri (National University of Singapore)

Biometric Backdoors: A Poisoning Attack against Unsupervised Template Updating .184.....
Giulio Lovisotto (University of Oxford), Simon Eberz (University of Oxford), and Ivan Martinovic (University of Oxford)

DLA: Dense-Layer-Analysis for Adversarial Example Detection .198.....
Philip Sperl (Fraunhofer Institute for Applied and Integrated Security), Ching-Yu Kao (Fraunhofer Institute for Applied and Integrated Security), Peng Chen (Fraunhofer Institute for Applied and Integrated Security), Xiao Lei (Fraunhofer Institute for Applied and Integrated Security), and Konstantin Böttinger (Fraunhofer Institute for Applied and Integrated Security)

Session #4: Blockchain and Crypto Protocol Security

Ordinos: A Verifiable Tally-Hiding E-Voting System .216.....
Ralf Küsters (University of Stuttgart), Julian Liedtke (University of Stuttgart), Johannes Müller (SnT/University of Luxembourg), Daniel Rausch (University of Stuttgart), and Andreas Vogt (FHNW, Switzerland)

Accountability in a Permissioned Blockchain: Formal Analysis of Hyperledger Fabric .236.....
Mike Graf (University of Stuttgart), Ralf Küsters (University of Stuttgart), and Daniel Rausch (University of Stuttgart)

Reward Sharing Schemes for Stake Pools .256.....
Lars Bruenjes (IOHK), Aggelos Kiayias (University of Edinburgh and IOHK), Elias Koutsoupias (University of Oxford), and Aikaterini-Panagiota Stouka (University of Edinburgh and IOHK)

Modular Security Analysis of OAuth 2.0 in the Three-Party Setting .276.....
Xinyu Li (TCA Laboratory, Institute of Software, Chinese Academy of Sciences, China; State Key Laboratory of Cryptology, China; University of Chinese Academy of Sciences, China), Jing Xu (TCA Laboratory, Institute of Software, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Zhenfeng Zhang (TCA Laboratory, Institute of Software, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China), Xiao Lan (Cybersecurity Research Institute, Sichuan University, China), and Yuchen Wang (TCA Laboratory, Institute of Software, Chinese Academy of Sciences, China; University of Chinese Academy of Sciences, China)

Session #5: System Security

Replay Attacks and Defenses against Cross-shard Consensus in Sharded Distributed Ledgers .294
Alberto Sonnino (University College London & chainspace.io), Shehar Bano (University College London & chainspace.io), Mustafa Al-Bassam (University College London & chainspace.io), and George Danezis (University College London & chainspace.io)

TagBleed: Breaking KASLR on the Isolated Kernel Address Space Using Tagged TLBs .309.....
Jakob Koschel (Vrije Universiteit Amsterdam), Cristiano Giuffrida (Vrije Universiteit Amsterdam), Herbert Bos (Vrije Universiteit Amsterdam), and Kaveh Razavi (ETH Zürich)

Chameleons' Oblivion: Complex-Valued Deep Neural Networks for Protocol-Agnostic RF Device Fingerprinting .322.....
Ioannis Agadakos (SRI International), Nikolaos Agadakos (University of Illinois at Chicago), Jason Polakis (University of Illinois at Chicago), and Mohamed R. Amer (Robust AI)

DARIA: Designing Actuators to Resist Arbitrary Attacks against Cyber-Physical Systems .339....
Jairo Giraldo (University of Utah), Sahand Hadizadeh Kafash (University of Texas at Dallas), Justin Ruths (University of Texas at Dallas), and Alvaro A. Cardenas (University of California, Santa Cruz)

Session #6: Privacy 1

Practical Volume-Based Attacks on Encrypted Databases .354.....
Rishabh Poddar (UC Berkeley), Stephanie Wang (UC Berkeley), Jianan Lu (Princeton University), and Raluca Ada Popa (UC Berkeley)

On Deploying Secure Computing: Private Intersection-Sum-with-Cardinality .370.....
Mihaela Ion (Google LLC), Ben Kreuter (Google LLC), Ahmet Nergiz (Google LLC), Sarvar Patel (Google LLC), Shobhit Saxena (Google LLC), Karn Seth (Google LLC), Mariana Raykova (Google LLC), David Shanahan (Google LLC), and Moti Yung (Google LLC)

Differentially Private Two-Party Set Operations .390.....	
	<i>Bailey Kacsmar (University of Waterloo), Basit Khurram (University of Waterloo), Nils Lukas (University of Waterloo), Alexander Norton (University of Waterloo), Masoumeh Shafieinejad (University of Waterloo), Zhiwei Shang (University of Waterloo), Yaser Baseri (University of Waterloo), Maryam Sepehri (Universita degli studi di Milano), Simon Oya (University of Waterloo), and Florian Kerschbaum (University of Waterloo)</i>
Zone Encryption with Anonymous Authentication for V2V Communication .405.....	
	<i>Jan Camenisch (DFINITY), Manu Drijvers (DFINITY), Anja Lehmann (Hasso-Plattner-Institute – University of Potsdam), Gregory Neven (DFINITY), and Patrick Towa (IBM Research – Zurich / ENS and PSL Research University)</i>

Session #7: Security of Autonomous Vehicles and IoT

Extensive Security Verification of the LoRaWAN Key-Establishment: Insecurities and Patches.425	
	<i>Stephan Wesemeyer (University of Surrey, Surrey Center for Cyber Security), Ioana Boureanu (University of Surrey, Surrey Center for Cyber Security), Zach Smith (University of Luxembourg), and Helen Treharne (University of Surrey, Surrey Center for Cyber Security)</i>
AVGuardian: Detecting and Mitigating Publish-Subscribe Overprivilege for Autonomous Vehicle Systems .445.....	
	<i>David Ke Hong (University of Michigan), John Kloosterman (University of Michigan), Yuqi Jin (University of Michigan), Yulong Cao (University of Michigan), Qi Alfred Chen (University of California, Irvine), Scott Mahlke (University of Michigan), and Z. Morley Mao (University of Michigan)</i>
A Vehicular DAA Scheme for Unlinkable ECDSA Pseudonyms in V2X .460.....	
	<i>Christopher Hicks (University of Birmingham) and Flavio D. Garcia (University of Birmingham)</i>
IoTfinder: Efficient Large-Scale Identification of IoT Devices via Passive DNS Traffic Analysis .474.....	
	<i>Roberto Perdisci (University of Georgia and Georgia Institute of Technology), Thomas Papastergiou (Georgia Institute of Technology), Omar Alrawi (Georgia Institute of Technology), and Manos Antonakakis (Georgia Institute of Technology)</i>

Session #8: Privacy 2

Generalized Iterative Bayesian Update and Applications to Mechanisms for Privacy Protection .490.....	
	<i>Ehab ElSalamouny (INRIA, France and Suez Canal University, Egypt) and Catuscia Palamidessi (INRIA and LIX, E´cole Polytechnique, France)</i>

Membership Inference against DNA Methylation Databases .508.....	
	<i>Inken Hagestedt (CISPA Helmholtz Center for Information Security), Mathias Humbert (Cyber-Defence Campus, armasuisse S+T), Pascal Berrang (CISPA Helmholtz Center for Information Security), Irina Lehmann (Helmholtz Centre for Environmental Research Leipzig, UFZ), Roland Eils (Berlin Institute of Health), Michael Backes (CISPA Helmholtz Center for Information Security), and Yang Zhang (CISPA Helmholtz Center for Information Security)</i>
A Pragmatic Approach to Membership Inferences on Machine Learning Models .521.....	
	<i>Yunhui Long (University of Illinois at Urbana-Champaign), Lei Wang (Indiana University Bloomington), Diyue Bu (Indiana University Bloomington), Vincent Bindschaedler (University of Florida), Xiaofeng Wang (Indiana University Bloomington), Haixu Tang (Indiana University Bloomington), Carl Gunter (University of Illinois at Urbana-Champaign), and Kai Chen (SKLOIS, Institute of Information Engineering, Chinese Academy of Sciences; School of Cyber Security, University of Chinese Academy of Sciences)</i>
Chorus: A Programming Framework for Building Scalable Differential Privacy Mechanisms .535	
	<i>Noah Johnson (UC Berkeley), Joseph Near (University of Vermont), Joseph Hellerstein (UC Berkeley), and Dawn Song (UC Berkeley)</i>

Session #9: Web Security and Privacy

Detecting Malware Injection with Program-DNS Behavior .552.....	
	<i>Yixin Sun (University of Virginia), Kangkook Jee (University of Texas at Dallas), Suphanee Sivakorn (Rajamangala University of Technology Tawan-ok), Zhichun Li (Stellar Cyber), Cristian Lumezanu (NEC Labs America), Lauri Korts-Parn (Cyber Defense Institute), Zhenyu Wu (Google), Junghwan Rhee (NEC Labs America), Chung Hwan Kim (NEC Laboratories America), Mung Chiang (Purdue University), and Prateek Mittal (Princeton University)</i>
SecurePay: Strengthening Two-Factor Authentication for Arbitrary Transactions .569.....	
	<i>Radhesh Krishnan Konoth (Vrije Universiteit Amsterdam), Björn Fischer (Vrije Universiteit Amsterdam), Wan Fokkink (Vrije Universiteit Amsterdam), Elias Athanasopoulos (University of Cyprus), Kaveh Razavi (ETH Zürich), and Herbert Bos (Vrije Universiteit Amsterdam)</i>
PESTO: Proactively Secure Distributed Single Sign-On, or How to Trust a Hacked Server .587...	
	<i>Carsten Baum (Aarhus University), Tore Frederiksen (The Alexandra Institute), Julia Hesse (IBM Research - Zurich), Anja Lehmann (Hasso Plattner Institute, University of Potsdam), and Avishay Yanai (VMware Research)</i>
COMAR: Classification of Compromised versus Maliciously Registered Domains .607.....	
	<i>Sourena Maroofi (Univ. Grenoble Alpes, CNRS, Grenoble INP, LIG), Maciej Korczynski (Univ. Grenoble Alpes, CNRS, Grenoble INP, LIG), Cristian Hesselman (SIDN Labs), Benoît Ampeau (AFNIC Labs), and Andrzej Duda (Univ. Grenoble Alpes, CNRS, Grenoble INP, LIG)</i>

SoK: Delegation and Revocation, the Missing Links in the Web's Chain of Trust .624.....
*Laurent Chuat (ETH Zurich), AbdelRahman Abdou (Carleton University),
Ralf Sasse (ETH Zurich), Christoph Sprenger (ETH Zurich), David Basin
(ETH Zurich), and Adrian Perrig (ETH Zurich)*

Author Index 639