

2018 IEEE Symposium on Security and Privacy (SP 2018)

**San Francisco, California, USA
21-23 May 2018**

Pages 1-546



**IEEE Catalog Number: CFP18020-POD
ISBN: 978-1-5386-4354-9**

**Copyright © 2018 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:	CFP18020-POD
ISBN (Print-On-Demand):	978-1-5386-4354-9
ISBN (Online):	978-1-5386-4353-2
ISSN:	1081-6011

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

2018 IEEE Symposium on Security and Privacy SP 2018

Table of Contents

Message from the General Chair	xiii
Message from the Program Chairs	xvii
Organizing Committee	xviii
Program Committee	xix
External Reviewers	xxii

Session #1: Machine Learning

AI2: Safety and Robustness Certification of Neural Networks with Abstract Interpretation	3
<i>Timon Gehr (ETH Zurich), Matthew Mirman (ETH Zurich), Dana Drachler-Cohen (ETH Zurich), Petar Tsankov (ETH Zurich), Swarat Chaudhuri (Rice University), and Martin Vechev (ETH Zurich)</i>	
Manipulating Machine Learning: Poisoning Attacks and Countermeasures for Regression Learning	19
<i>Matthew Jagielski (Northeastern University), Alina Oprea (Northeastern University), Battista Biggio (University of Cagliari), Chang Liu (University of California Berkeley), Cristina Nita-Rotaru (Northeastern University), and Bo Li (University of California Berkeley)</i>	
Stealing Hyperparameters in Machine Learning	36
<i>Binghui Wang (Iowa State University) and Neil Zhenqiang Gong (Iowa State University)</i>	
A Machine Learning Approach to Prevent Malicious Calls over Telephony Networks	53
<i>Huichen Li (Shanghai Jiao Tong University), Xiaojun Xu (Shanghai Jiao Tong University), Chang Liu (University of California, Berkeley), Teng Ren (TouchPal Inc.), Kun Wu (TouchPal Inc.), Xuezhi Cao (Shanghai Jiao Tong University), Weinan Zhang (Shanghai Jiao Tong University), Yong Yu (Shanghai Jiao Tong University), and Dawn Song (University of California)</i>	
Surveylance: Automatically Detecting Online Survey Scams	70
<i>Amin Kharraz (University of Illinois Urbana-Champaign), William Robertson (Northeastern University), and Engin Kirda (Northeastern University)</i>	

Session #2: Privacy

- Privacy Risks with Facebook's PII-Based Targeting: Auditing a Data Broker's Advertising Interface .89.....
Giridhari Venkatadri (Northeastern University), Athanasios Andreou (EURECOM), Yabing Liu (Northeastern University), Alan Mislove (Northeastern University), Krishna P. Gummadi (MPI-SWS), Patrick Loiseau (Univ. Grenoble Alpes), and Oana Goga (Univ. Grenoble Alpes)
- Anonymity Trilemma: Strong Anonymity, Low Bandwidth Overhead, Low Latency - Choose Two .108.....
Debajyoti Das (Purdue University), Sebastian Meiser (University College London), Esfandiar Mohammadi (ETH Zurich), and Aniket Kate (Purdue University)
- Locally Differentially Private Frequent Itemset Mining .127.....
Tianhao Wang (Purdue University), Ninghui Li (Purdue University), and Somesh Jha (University of Wisconsin-Madison)
- EyeTell: Video-Assisted Touchscreen Keystroke Inference from Eye Movements .144.....
Yimin Chen (Arizona State University), Tao Li (Arizona State University), Rui Zhang (University of Delaware), Yanchao Zhang (Arizona State University), and Terri Hedgpeth (Arizona State University)
- Understanding Linux Malware .161.....
Emanuele Cozzi (Eurecom), Mariano Graziano (Cisco Systems), Yanick Fratantonio (Eurecom), and Davide Balzarotti (Eurecom)

Session #3: Side Channels

- Racing in Hyperspace: Closing Hyper-Threading Side Channels on SGX with Contrived Data Races .178.....
Guoxing Chen (The Ohio State University), Wenhao Wang (Indiana University Bloomington & SKLOIS), Tianyu Chen (Indiana University Bloomington), Sanchuan Chen (The Ohio State University), Yinqian Zhang (The Ohio State University), XiaoFeng Wang (Indiana University Bloomington), Ten-Hwang Lai (The Ohio State University), and Dongdai Lin (SKLOIS)
- Grand Pwning Unit: Accelerating Microarchitectural Attacks with the GPU .195.....
Pietro Frigo (Vrije Universiteit Amsterdam), Cristiano Giuffrida (Vrije Universiteit Amsterdam), Herbert Bos (Vrije Universiteit Amsterdam), and Kaveh Razavi (Vrije Universiteit Amsterdam)
- SoK: Keylogging Side Channels .211.....
John Monaco (U.S. Army Research Laboratory)
- FPGA-Based Remote Power Side-Channel Attacks .229.....
Mark Zhao (Cornell University) and G. Edward Suh (Cornell University)
- Another Flip in the Wall of Rowhammer Defenses .245.....
Daniel Gruss (Graz University of Technology), Moritz Lipp (Graz University of Technology), Michael Schwarz (Graz University of Technology), Daniel Genkin (University of Pennsylvania and University of Maryland), Jonas Juffinger (Graz University of Technology), Sioli O'Connell (University of Adelaide), Wolfgang Schoechl (Graz University of Technology), and Yuval Yarom (University of Adelaide and Data61)

Session #4: Computing on Hidden Data

- EnclaveDB: A Secure Database Using SGX .264.....
Christian Priebe (Imperial College London), Kapil Vaswani (Microsoft Research), and Manuel Costa (Microsoft Research)
- Oblix: An Efficient Oblivious Search Index .279.....
Pratyush Mishra (UC Berkeley), Rishabh Poddar (UC Berkeley), Jerry Chen (UC Berkeley), Alessandro Chiesa (UC Berkeley), and Raluca Ada Popa (UC Berkeley)
- Improved Reconstruction Attacks on Encrypted Data Using Range Query Leakage .297.....
Marie-Sarah Lacharité (Royal Holloway), Brice Minaud (Royal Holloway), and Kenneth G. Paterson (Royal Holloway)
- Bulletproofs: Short Proofs for Confidential Transactions and More .315.....
Benedikt Bünz (Stanford University), Jonathan Bootle (University College London), Dan Boneh (Stanford University), Andrew Poelstra (Blockstream), Pieter Wuille (Blockstream), and Greg Maxwell (None)
- FuturesMEX: Secure, Distributed Futures Market Exchange .335.....
Fabio Massacci (University of Trento), Chan Nam Ngo (University of Trento), Jing Nie (University of International Business and Economics Beijing), Daniele Venturi (University of Rome "La Sapienza"), and Julian Williams (University of Durham)
- Implementing Conjunction Obfuscation Under Entropic Ring LWE .354.....
David Bruce Cousins (Raytheon BBN Technologies), Giovanni Di Crescenzo (Applied Communication Sciences / Vencore Labs), Kamil Doruk Gür (NJIT Cybersecurity Research Center), Kevin King (Massachusetts Institute of Technology), Yuriy Polyakov (NJIT Cybersecurity Research Center), Kurt Rohloff (NJIT Cybersecurity Research Center), Gerard W. Ryan (NJIT Cybersecurity Research Center), and Erkay Savas (NJIT Cybersecurity Research Center)

Session #5: Understanding Users

- Hackers vs. Testers: A Comparison of Software Vulnerability Discovery Processes .374.....
Daniel Votipka (University of Maryland), Rock Stevens (University of Maryland), Elissa Redmiles (University of Maryland), Jeremy Hu (University of Maryland), and Michelle Mazurek (University of Maryland)
- Towards Security and Privacy for Multi-user Augmented Reality: Foundations with End Users .392.....
Kiron Lebeck (University of Washington), Kimberly Ruth (University of Washington), Tadayoshi Kohno (University of Washington), and Franziska Roesner (University of Washington)
- Computer Security and Privacy for Refugees in the United States .409.....
Lucy Simko (University of Washington), Ada Lerner (Wellesley College), Samia Ibtasam (University of Washington), Franziska Roesner (University of Washington), and Tadayoshi Kohno (University of Washington)

On Enforcing the Digital Immunity of a Large Humanitarian Organization .424.....	
	<i>Stevens Le Blond (École polytechnique fédérale de Lausanne), Alejandro Cuevas (École polytechnique fédérale de Lausanne), Juan Ramón Troncoso-Pastoriza (École polytechnique fédérale de Lausanne), Philipp Jovanovic (École polytechnique fédérale de Lausanne), Bryan Ford (École polytechnique fédérale de Lausanne), and Jean-Pierre Hubaux (École polytechnique fédérale de Lausanne)</i>
The Spyware Used in Intimate Partner Violence .441.....	
	<i>Rahul Chatterjee (Cornell Tech), Periwinkle Doerfler (NYU), Hadas Orgad (Technion), Sam Havron (Cornell University), Jackeline Palmer (Hunter College), Diana Freed (Cornell Tech), Karen Levy (Cornell University), Nicola Dell (Cornell Tech), Damon McCoy (NYU), and Thomas Ristenpart (Cornell Tech)</i>

Session #6: Programming Languages

Compiler-Assisted Code Randomization .461.....	
	<i>Hyungjoon Koo (Stony Brook University), Yaohui Chen (Northeastern University), Long Lu (Northeastern University), Vasileios P. Kemerlis (Brown University), and Michalis Polychronakis (Stony Brook University)</i>
Protecting the Stack with Metadata Policies and Tagged Hardware .478.....	
	<i>Nick Roessler (University of Pennsylvania) and André DeHon (University of Pennsylvania)</i>
Impossibility of Precise and Sound Termination-Sensitive Security Enforcements .496.....	
	<i>Minh Ngo (INRIA), Frank Piessens (imec-DistriNet), and Tamara Rezk (INRIA)</i>
Static Evaluation of Noninterference Using Approximate Model Counting .514.....	
	<i>Ziqiao Zhou (University of North Carolina at Chapel Hill), Zhiyun Qian (University of California), Michael K. Reiter (University of North Carolina), and Yinqian Zhang (The Ohio State University)</i>
DEEPSEC: Deciding Equivalence Properties in Security Protocols Theory and Practice .529.....	
	<i>Vincent Cheval (Inria Nancy & Loria), Steve Kremer (Inria Nancy & Loria), and Itsaka Rakotonirina (Inria Nancy & Loria)</i>

Session #7: Networked Systems

Distance-Bounding Protocols: Verification Without Time and Location .549.....	
	<i>Sjouke Mauw (CSC/SnT), Zach Smith (CSC), Jorge Toro-Pozo (CSC), and Rolando Trujillo-Rasua (SnT)</i>
Sonar: Detecting SS7 Redirection Attacks with Audio-Based Distance Bounding .567.....	
	<i>Christian Peeters (University of Florida), Hadi Abdullah (University of Florida), Nolen Scaife (University of Florida), Jasmine Bowers (University of Florida), Patrick Traynor (University of Florida), Bradley Reaves (North Carolina State University), and Kevin Butler (University of Florida)</i>

OmniLedger: A Secure, Scale-Out, Decentralized Ledger via Sharding .583.....
Eleftherios Kokoris-Kogias (EPFL), Philipp Jovanovic (EPFL), Linus Gasser (EPFL), Nicolas Gailly (EPFL), Ewa Syta (Trinity College), and Bryan Ford (EPFL)

Routing Around Congestion: Defeating DDoS Attacks and Adverse Network Conditions via Reactive BGP Routing .599.....
Jared M Smith (University of Tennessee) and Max Schuchard (University of Tennessee)

Tracking Ransomware End-to-end .618.....
Danny Yuxing Huang (Princeton University), Maxwell Matthaios Aliapoulios (New York University), Vector Guo Li (University of California), Luca Invernizzi (Google), Elie Bursztein (Google), Kylie McRoberts (Google), Jonathan Levin (Chainalysis), Kirill Levchenko (University of California), Alex C. Snoeren (University of California), and Damon McCoy (New York University)

Session #8: Program Analysis

The Rise of the Citizen Developer: Assessing the Security Impact of Online App Generators .634.....
Marten Oltrogge (CISPA), Erik Derr (CISPA), Christian Stransky (CISPA), Yasemin Acar (Leibniz University Hannover), Sascha Fahl (Leibniz University Hannover), Christian Rossow (CISPA), Giancarlo Pellegrino (CISPA), Sven Bugiel (CISPA), and Michael Backes (CISPA)

Learning from Mutants: Using Code Mutation to Learn and Monitor Invariants of a Cyber-Physical System .648.....
Yuqi Chen (Singapore University of Technology and Design), Christopher M. Poskitt (Singapore University of Technology and Design), and Jun Sun (Singapore University of Technology and Design)

Precise and Scalable Detection of Double-Fetch Bugs in OS Kernels .661.....
Meng Xu (Georgia Institute of Technology), Chenxiang Qian (Georgia Institute of Technology), Kangjie Lu (University of Minnesota), Michael Backes (CISPA Helmholtz Center i.G.), and Taesoo Kim (Georgia Institute of Technology)

CollAFL: Path Sensitive Fuzzing .679.....
Shuitao Gan (State Key Laboratory of Mathematical Engineering and Advanced Computing), Chao Zhang (Tsinghua University), Xiaojun Qin (State Key Laboratory of Mathematical Engineering and Advanced Computing), Xuwen Tu (State Key Laboratory of Mathematical Engineering and Advanced Computing), Kang Li (Cyber Immunity Lab), Zhongyu Pei (Tsinghua University), and Zuoning Chen (National Research Center of Parallel Computer Engineering and Technology)

T-Fuzz: Fuzzing by Program Transformation .697.....
Hui Peng (Purdue University), Yan Shoshitaishvili (Arizona State University), and Mathias Payer (Purdue University)

Angora: Efficient Fuzzing by Principled Search .711.....
Peng Chen (ShanghaiTech University) and Hao Chen (University of California, Davis)

Session #9: Web

- FP-STALKER: Tracking Browser Fingerprint Evolutions .728.....
Antoine Vastel (University of Lille / INRIA), Pierre Laperdrix (INSA / INRIA), Walter Rudametkin (University of Lille / INRIA), and Romain Rouvoy (University of Lille / INRIA)
- Study and Mitigation of Origin Stripping Vulnerabilities in Hybrid-postMessage Enabled Mobile Applications .742.....
Guangliang Yang (Texas A&M University), Jeff Huang (Texas A&M University), Guofei Gu (Texas A&M University), and Abner Mendoza (Texas A&M University)
- Mobile Application Web API Reconnaissance: Web-to-Mobile Inconsistencies & Vulnerabilities .756.....
Abner Mendoza (Texas A&M University) and Guofei Gu (Texas A&M University)
- Enumerating Active IPv6 Hosts for Large-Scale Security Scans via DNSSEC-Signed Reverse Zones .770.....
Kevin Borgolte (University of California Santa Barbara), Shuang Hao (University of Texas at Dallas), Tobias Fiebig (Delft University of Technology), and Giovanni Vigna (University of California Santa Barbara)
- Tracking Certificate Misissuance in the Wild .785.....
Deepak Kumar (University of Illinois), Zhengping Wang (University of Illinois), Matthew Hyder (University of Illinois), Joseph Dickinson (University of Illinois), Gabrielle Beck (University of Michigan), David Adrian (University of Michigan), Joshua Mason (University of Illinois), Zakir Durumeric (University of Michigan), J. Alex Halderman (University of Michigan), and Michael Bailey (University of Illinois)
- A Formal Treatment of Accountable Proxying Over TLS .799.....
Karthikeyan Bhargavan (INRIA de Paris), Ioana Boureanu (Univ. of Surrey), Antoine Delignat-Lavaud (Microsoft Research), Pierre-Alain Fouque (Univ. of Rennes 1), and Cristina Onete (Univ. of Limoges)

Session #10: Authentication

- Secure Device Bootstrapping Without Secrets Resistant to Signal Manipulation Attacks .819.....
Nirnimesh Ghose (University of Arizona), Loukas Lazos (University of Arizona), and Ming Li (University of Arizona)
- Do You Feel What I Hear? Enabling Autonomous IoT Device Pairing Using Different Sensor Types .836.....
Jun Han (Carnegie Mellon University), Albert Jin Chung (Carnegie Mellon University), Manal Kumar Sinha (Carnegie Mellon University), Madhumitha Harishankar (Carnegie Mellon University), Shijia Pan (Carnegie Mellon University), Hae Young Noh (Carnegie Mellon University), Pei Zhang (Carnegie Mellon University), and Patrick Tague (Carnegie Mellon University)
- On the Economics of Offline Password Cracking .853.....
Jeremiah Blocki (Purdue University), Benjamin Harsha (Purdue University), and Samson Zhou (Purdue University)

A Tale of Two Studies: The Best and Worst of YubiKey Usability .872.....
Joshua Reynolds (University of Illinois at Urbana-Champaign and Brigham Young University), Trevor Smith (Brigham Young University), Ken Reese (Brigham Young University), Luke Dickinson (Brigham Young University), Scott Ruoti (MIT Lincoln Laboratory), and Kent Seamons (Brigham Young University)

When Your Fitness Tracker Betrays You: Quantifying the Predictability of Biometric Features Across Contexts .889.....
Simon Eberz (University of Oxford), Giulio Lovisotto (University of Oxford), Andrea Patanè (University of Oxford), Marta Kwiatkowska (University of Oxford), Vincent Lenders (armasuisse), and Ivan Martinovic (University of Oxford)

Session #11: Cryptography

vRAM: Faster Verifiable RAM with Program-Independent Preprocessing .908.....
Yupeng Zhang (University of Maryland), Daniel Genkin (University of Maryland and University of Pennsylvania), Jonathan Katz (University of Maryland), Dimitrios Papadopoulos (Hong Kong University of Science and Technology), and Charalampos Papamanthou (University of Maryland)

Doubly-Efficient zkSNARKs Without Trusted Setup .926.....
Riad S. Wahby (Stanford University), Ioanna Tzialla (New York University), Abhi Shelat (Northeastern University), Justin Thaler (Georgetown University), and Michael Walfish (New York University)

xJsnark: A Framework for Efficient Verifiable Computation .944.....
Ahmed Kosba (University of Maryland), Charalampos Papamanthou (University of Maryland), and Elaine Shi (Cornell University)

PIR with Compressed Queries and Amortized Query Processing .962.....
Sebastian Angel (The University of Texas at Austin and New York University), Hao Chen (Microsoft Research), Kim Laine (Microsoft Research), and Srinath Setty (Microsoft Research)

Secure Two-party Threshold ECDSA from ECDSA Assumptions .980.....
Jack Doerner (Northeastern University), Yashvanth Kondi (Northeastern University), Eysa Lee (Northeastern University), and Abhi Shelat (Northeastern University)

Session #12: Devices

Speechless: Analyzing the Threat to Speech Privacy from Smartphone Motion Sensors .1000.....
S Abhishek Anand (University of Alabama at Birmingham) and Nitesh Saxena (University of Alabama at Birmingham)

Crowd-GPS-Sec: Leveraging Crowdsourcing to Detect and Localize GPS Spoofing Attacks .1018.....
Kai Jansen (Ruhr-University Bochum), Matthias Schäfer (University of Kaiserslautern), Daniel Moser (ETH Zurich), Vincent Lenders (armasuisse), Christina Pöpper (New York University Abu Dhabi), and Jens Schmitt (University of Kaiserslautern)

SoK: "Plug & Pray" Today – Understanding USB Insecurity in Versions 1 Through C	1032
<i>Jing Tian (University of Florida), Nolen Scaife (University of Florida), Deepak Kumar (University of Illinois at Urbana-Champaign), Michael Bailey (University of Illinois at Urbana-Champaign), Adam Bates (University of Illinois at Urbana-Champaign), and Kevin Butler (University of Florida)</i>	
Blue Note: How Intentional Acoustic Interference Damages Availability and Integrity in Hard Disk Drives and Operating Systems	1048
<i>Connor Bolton (University of Michigan), Sara Rampazzi (University of Michigan), Chaohao Li (Zhejiang University), Andrew Kwong (University of Michigan), Wenyuan Xu (Zhejiang University), and Kevin Fu (University of Michigan)</i>	
The Cards Aren't Alright: Detecting Counterfeit Gift Cards Using Encoding Jitter	1063
<i>Nolen Scaife (University of Florida), Christian Peeters (University of Florida), Camilo Velez (University of Florida), Hanqing Zhao (University of Florida), Patrick Traynor (University of Florida), and David Arnold (University of Florida)</i>	

Author Index