2019 IEEE European Symposium on Security and Privacy (EuroS&P 2019)

Stockholm, Sweden
17 – 19 June 2019

IEEE Catalog Number: CFP19C75-POD
ISBN: 978-1-7281-1149-0

Copyright © 2019 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:	CFP19C75-POD
ISBN (Print-On-Demand):	978-1-7281-1149-0
ISBN (Online):	978-1-7281-1148-3

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

2019 IEEE European Symposium on Security and Privacy (EuroS&P)

EuroSP 2019

Table of Contents

Message from the General Chairs xi

Message from the Program Chairs xiii

Organizing Committee xv

Steering Committee xvi

Program Committee xvii

Sub Reviewers xix

Smartphones and Embedded Systems

False Sense of Security: A Study on the Effectivity of Jailbreak Detection in Banking Apps 1
Ansgar Kellner (Institute of System Security, TU Braunschweig), Micha Horlboge (Institute of System Security, TU Braunschweig), Konrad Rieck (Institute of System Security, TU Braunschweig), and Christian Wressnegger (Institute of System Security, TU Braunschweig)

Up-To-Crash: Evaluating Third-Party Library Updatability on Android 15
Jie Huang (CISPA Helmholtz Center for Information Security), Nataniel Borges (CISPA Helmholtz Center for Information Security), Sven Bugiel (CISPA Helmholtz Center for Information Security), and Michael Backes (CISPA Helmholtz Center for Information Security)

Challenges in Designing Exploit Mitigations for Deeply Embedded Systems 31
Ali Abbasi (Ruhr-University Bochum), Jos Wetzels (Eindhoven University of Technology), Thorsten Holz (Ruhr-University Bochum), and Sandro Etalle (Eindhoven University of Technology)

DroidEvolver: Self-Evolving Android Malware Detection System 47
Ke Xu (Singapore Management University), Yingjiu Li (Singapore Management University), Robert Deng (Singapore Management University), Kai Chen (Institute of Information Engineering, Chinese Academy of Sciences. School of Cyber Security, University of Chinese Academy of Sciences), and Jiayun Xu (Singapore Management University)

Programming Languages and Flow Control

Programming with Flow-Limited Authorization: Coarser is Better 63
Mathias Vorreiter Pedersen (Aarhus University) and Stephen Chong (Harvard University)

Information-Flow Control for Database-Backed Applications .79
Marco Guarnieri (IMDEA Software Institute), Musard Balliu (KTH Royal Institute of Technology), Daniel Schoepe (Chalmers University of Technology), David Basin (ETH Zurich), and Andrei Sabelfeld (Chalmers University of Technology)

Adaptive Call-Site Sensitive Control Flow Integrity .95
Mustakimur Khandaker (Florida State University), Abu Naser (Florida State University), Wenqing Liu (Florida State University), Zhi Wang (Florida State University), Yajin Zhou (Zhejiang University), and Yueqiang Cheng (Baidu X-lab)

STEROIDS for DOPed Applications: A Compiler for Automated Data-Oriented Programming .111
Jannik Pewny (Horst Görtz Institute, Ruhr University Bochum), Philipp Koppe (Horst Görtz Institute, Ruhr University Bochum), and Thorsten Holz (Horst Görtz Institute, Ruhr University Bochum)

Trusted Systems

A Symbolic Analysis of ECC-Based Direct Anonymous Attestation .127
Jorden Whitefield (University of Surrey), Liqun Chen (University of Surrey), Ralf Sasse (ETH Zurich), Steve Schneider (University of Surrey), Helen Treharne (University of Surrey), and Stephan Wesemeyer (University of Surrey)

SgxPectre: Stealing Intel Secrets from SGX Enclaves Via Speculative Execution .142
Guoxing Chen (The Ohio State University), Sanchuan Chen (The Ohio State University), Yuan Xiao (The Ohio State University), Yinqian Zhang (The Ohio State University), Zhiqiang Lin (The Ohio State University), and Ten H. Lai (The Ohio State University)

ReplicaTEE: Enabling Seamless Replication of SGX Enclaves in the Cloud .158
Claudio Soriente (NEC Labs Europe), Ghassan Karame (NEC Labs Europe), Wenting Li (NEC Labs Europe), and Sergey Fedorov (NEC Labs Europe)

Cryptocurrency, Blockchain and Cybercrime

Deanonymization and Linkability of Cryptocurrency Transactions Based on Network Analysis .172
Alex Biryukov (University of Luxembourg) and Sergei Tikhomirov (University of Luxembourg)

Ekiden: A Platform for Confidentiality-Preserving, Trustworthy, and Performant Smart Contracts .185
Raymond Cheng (UC Berkeley, Oasis Labs), Fan Zhang (Cornell Tech), Jernej Kos (Oasis Labs), Warren He (UC Berkeley, Oasis Labs), Nicholas Hynes (UC Berkeley, Oasis Labs), Noah Johnson (UC Berkeley, Oasis Labs), Ari Juels (Cornell Tech), Andrew Miller (UIUC, Oasis Labs), and Dawn Song (UC Berkeley, Oasis Labs)

Understanding eWhoring .201
Alice Hutchings (University of Cambridge) and Sergio Pastrana (Universidad Carlos III de Madrid)

Crypto 1: Schemes and Protocols

Key-Insulated and Privacy-Preserving Signature Scheme with Publicly Derived Public Key 215
Zhen Liu (Shanghai Jiao Tong University), Guomin Yang (University of Wollongong), Duncan S. Wong (CryptoBLK and Abelian Foundation), Khoa Nguyen (Nanyang Technological University), and Huaxiong Wang (Nanyang Technological University)

A Mechanised Cryptographic Proof of the WireGuard Virtual Private Network Protocol 231
Benjamin Lipp (Inria Paris), Bruno Blanchet (Inria Paris), and Karthikeyan Bhargavan (Inria Paris)

More Protocols

The Case of Adversarial Inputs for Secure Similarity Approximation Protocols 247
Evgenios M. Kornaropoulos (Brown University) and Petros Efstathopoulos (Symantec Research Labs)

A Practical Attestation Protocol for Autonomous Embedded Systems 263
Florian Kohnhäuser (TU Darmstadt), Niklas Büscher (TU Darmstadt), and Stefan Katzenbeisser (TU Darmstadt)

IFAL: Issue First Activate Later Certificates for V2X 279
Eric Verheul (Radboud University Nijmegen), Christopher Hicks (University of Birmingham), and Flavio D. Garcia (University of Birmingham)

SAID: Reshaping Signal into an Identity-Based Asynchronous Messaging Protocol with Authenticated Ratcheting 294
Olivier Blazy (University of Limoges, XLIM, CNRS UMR 7252), Angèle Bossuat (Univ Rennes, CNRS, IRISA), Xavier Bultel (Univ Rennes, CNRS, IRISA), Pierre-Alain Fouque (Univ Rennes, CNRS, IRISA), Cristina Onete (University of Limoges, XLIM, CNRS UMR 7252), and Elena Pagnin (Aarhus University)

Benchmarking and Modelling

SoK: Benchmarking Flaws in Systems Security 310
Erik van der Kouwe (Leiden University), Gernot Heiser (Data61 (formerly NICTA) and UNSW), Dennis Andriesse (Vrije Universiteit Amsterdam), Herbert Bos (Vrije Universiteit Amsterdam), and Cristiano Giuffrida (Vrije Universiteit Amsterdam)

Tell Me You Fixed It: Evaluating Vulnerability Notifications via Quarantine Networks 326
Orçun Çetin (Delft University of Technology), Carlos Gañán (Delft University of Technology), Lisette Altena (Delft University of Technology), Samaneh Tajalizadehkhoob (Delft University of Technology), and Michel van Eeten (Delft University of Technology)

Discovering Correlations: A Formal Definition of Causal Dependency Among Heterogeneous Events 340
Charles Xosanavongsa (CentraleSupélec, Inria, Univ Rennes), Eric Totel (CentraleSupélec, Inria, Univ Rennes), and Olivier Bettan (Thales Six GTS France)

Noise Explorer: Fully Automated Modeling and Verification for Arbitrary Noise Protocols 356
Nadim Kobeissi (INRIA Paris, Symbolic Software), Georgio Nicolas (Symbolic Software), and Karthikeyan Bhargavan (INRIA Paris)

Crypto 2: Side Channels and Users

Degenerate Fault Attacks on Elliptic Curve Parameters in OpenSSL 371
Akira Takahashi (Aarhus University) and Mehdi Tibouchi (NTT Secure Platform Laboratories)

On Aggregation of Information in Timing Attacks 387
Itsaka Rakotonirina (INRIA Nancy Grand-Est, LORIA) and Boris Köpf (Microsoft Research)

In Encryption We Don't Trust: The Effect of End-to-End Encryption to the Masses on User Perception 401
Sergej Dechand (University of Bonn), Alena Naiakshina (University of Bonn), Anastasia Danilova (University of Bonn), and Matthew Smith (University of Bonn, Fraunhofer FKIE)

Privacy

Rethinking Location Privacy for Unknown Mobility Behaviors 416
Simon Oya (University of Vigo), Carmela Troncoso (EPFL), and Fernando Pérez-González (University of Vigo)

Revisiting User Privacy for Certificate Transparency 432
Daniel Kales (Graz University of Technology), Olamide Omolola (Graz University of Technology), and Sebastian Ramacher (Graz University of Technology)

PILOT: Practical Privacy-Preserving Indoor Localization Using OuTsourcing 448
Kimmo Järvinen (University of Helsinki), Helena Leppäkoski (Tampere University), Elena-Simona Lohan (Tampere University), Philipp Richter (Tampere University), Thomas Schneider (TU Darmstadt), Oleksandr Tkachenko (TU Darmstadt), and Zheng Yang (Singapore University of Technology and Design)

The 5G-AKA Authentication Protocol Privacy 464
Adrien Koutsos (LSV, CNRS, ENS Paris-Saclay, Université Paris-Saclay)

Machine Learning

Towards Understanding Limitations of Pixel Discretization Against Adversarial Attacks 480
Jiefeng Chen (University of Wisconsin-Madison), Xi Wu (Google), Vaibhav Rastogi (University of Wisconsin-Madison), Yingyu Liang (University of Wisconsin-Madison), and Somesh Jha (University of Wisconsin-Madison)

EzPC: Programmable and Efficient Secure Two-Party Computation for Machine Learning 496
Nishanth Chandran (Microsoft Research, India), Divya Gupta (Microsoft Research, India), Aseem Rastogi (Microsoft Research, India), Rahul Sharma (Microsoft Research, India), and Shardul Tripathi (IIT Delhi)

PRADA: Protecting Against DNN Model Stealing Attacks 512
Mika Juuti (Aalto University), Sebastian Szyller (Aalto University), Samuel Marchal (Aalto University), and N. Asokan (Aalto University)

Mitch: A Machine Learning Approach to the Black-Box Detection of CSRF Vulnerabilities .528....
Stefano Calzavara (Università Ca' Foscari Venezia), Mauro Conti (Università di Padova), Riccardo Focardi (Università Ca' Foscari Venezia), Alvise Rabitti (Università Ca' Foscari Venezia), and Gabriele Tolomei (Università di Padova)

Internet, Passwords and Malware

Domain Impersonation is Feasible: A Study of CA Domain Validation Vulnerabilities .544...........
Lorenz Schwittmann (University of Duisburg-Essen), Matthäus Wander (University of Duisburg-Essen), and Torben Weis (University of Duisburg-Essen)

TraffickStop: Detecting and Measuring Illicit Traffic Monetization Through Large-Scale DNS Analysis .560...
Baojun Liu (Tsinghua University; Beijing National Research Center for Information Science and Technology), Zhou Liu (University of California, Irvine), Peiyuan Zong (Institute of Information Engineering, Chinese Academy of Sciences), Chaoyi Lu (Tsinghua University; Beijing National Research Center for Information Science and Technology), Haixin Duan (Tsinghua University; Beijing National Research Center for Information Science and Technology; 360 Enterprise Security Group), Ying Liu (Tsinghua University; Beijing National Research Center for Information Science and Technology), Sumayah Alrwais (King Saud University), Xiaofeng Wang (Indiana University Bloomington), Shuang Hao (University of Texas at Dallas), Yaoqi Jia (Zilliqa Research), Yiming Zhang (Tsinghua University; Beijing National Research Center for Information Science and Technology), Kai Chen (Institute of Information Engineering, Chinese Academy of Sciences), and Zaifeng Zhang (360 Netlab)

StopGuessing: Using Guessed Passwords to Thwart Online Guessing .576.............................
Stuart Schechter (None), Yuan Tian (University of Virginia, Charlottesville, VA), and Cormac Herley (Microsoft Research, Redmond, WA, USA)

MALPITY: Automatic Identification and Exploitation of Tarpit Vulnerabilities in Malware .590.......
Walla Sebastian (CISPA Helmholtz Center for Information Security) and Christian Rossow (CISPA Helmholtz Center for Information Security)

Voting

Private Votes on Untrusted Platforms: Models, Attacks and Provable Scheme .606...................
Sergiu Bursuc (Inria Nancy-Grand'Est, LORIA, France), Constantin-Catalin Dragan (Department of Computer Science, University of Surrey, UK), and Steve Kremer (Inria Nancy-Grand'Est, LORIA, France)

Is Your Vote Overheard? A New Scalable Side-Channel Attack Against Paper Voting .621..........
Kristjan Krips (Cybernetica), Jan Willemson (Cybernetica), and Sebastian Värv (University of Tartu)

Improving Automated Symbolic Analysis of Ballot Secrecy for E-Voting Protocols: A Method Based on Sufficient Conditions .635..
Lucca Hirschi (Inria & LORIA) and Cas Cremers (CISPA Helmholtz Center for Information Security)

Author Index 651 . . . .