

2017 IEEE Symposium on Security and Privacy (SP 2017)

**San Jose, California, USA
22-26 May 2017**

Pages 1-556



**IEEE Catalog Number: CFP17020-POD
ISBN: 978-1-5090-5534-0**

**Copyright © 2017 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:	CFP17020-POD
ISBN (Print-On-Demand):	978-1-5090-5534-0
ISBN (Online):	978-1-5090-5533-3
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

2017 IEEE Symposium on Security and Privacy

SP 2017

Table of Contents

Message from the General Chair.....	xi
Message from the Program Committee Co-Chairs.....	xv
Organizing Committee.....	xvi
Program Committee.....	xvii
External Reviewers	xix

Session #1: Privacy and Learning

Membership Inference Attacks Against Machine Learning Models	3
<i>Reza Shokri, Marco Stronati, Congzheng Song, and Vitaly Shmatikov</i>	
SecureML: A System for Scalable Privacy-Preserving Machine Learning	19
<i>Payman Mohassel and Yupeng Zhang</i>	
Towards Evaluating the Robustness of Neural Networks	39
<i>Nicholas Carlini and David Wagner</i>	
Is Interaction Necessary for Distributed Private Learning?	58
<i>Adam Smith, Abhradeep Thakurta, and Jalaj Upadhyay</i>	
Pyramid: Enhancing Selectivity in Big Data Protection with Count Featurization	78
<i>Mathias Lecuyer, Riley Spahn, Roxana Geambasu, Tzu-Kuo Huang, and Siddhartha Sen</i>	

Session #2: Getting Security Right

SoK: Science, Security and the Elusive Goal of Security as a Scientific Pursuit	99
<i>Cormac Herley and P. C. van Oorschot</i>	
Stack Overflow Considered Harmful? The Impact of Copy&Paste on Android Application Security	121
<i>Felix Fischer, Konstantin Böttinger, Huang Xiao, Christian Stransky, Yasemin Acar, Michael Backes, and Sascha Fahl</i>	
Obstacles to the Adoption of Secure Communication Tools	137
<i>Ruba Abu-Salma, M. Angela Sasse, Joseph Bonneau, Anastasia Danilova, Alena Naiakshina, and Matthew Smith</i>	

Comparing the Usability of Cryptographic APIs	154
<i>Yasemin Acar, Michael Backes, Sascha Fahl, Simson Garfinkel, Doowon Kim, Michelle L. Mazurek, and Christian Stransky</i>	

SoK: Cryptographically Protected Database Search	172
<i>Benjamin Fuller, Mayank Varia, Arkady Yerukhimovich, Emily Shen, Ariel Hamlin, Vijay Gadepally, Richard Shay, John Darby Mitchell, and Robert K. Cunningham</i>	

Session #3: Attacks

IoT Goes Nuclear: Creating a ZigBee Chain Reaction	195
<i>Eyal Ronen, Adi Shamir, Achi-Or Weingarten, and Colin O'Flynn</i>	

SoK: Exploiting Network Printers	213
<i>Jens Müller, Vladislav Mladenov, Juraj Somorovsky, and Jörg Schwenk</i>	

How They Did It: An Analysis of Emission Defeat Devices in Modern Automobiles	231
<i>Moritz Contag, Guo Li, Andre Pawlowski, Felix Domke, Kirill Levchenko, Thorsten Holz, and Stefan Savage</i>	

The Password Reset MitM Attack	251
<i>Nethanel Gelernter, Senia Kalma, Bar Magnezi, and Hen Porcilan</i>	

An Experimental Security Analysis of an Industrial Robot Controller	268
<i>Davide Quarta, Marcello Pogliani, Mario Polino, Federico Maggi, Andrea Maria Zanchettin, and Stefano Zanero</i>	

Session #4: Systems Security and Authentication

Protecting Bare-Metal Embedded Systems with Privilege Overlays	289
<i>Abraham A. Clements, Naif Saleh Almakhdhub, Khaled S. Saab, Prashast Srivastava, Jinkyu Koo, Saurabh Bagchi, and Mathias Payer</i>	

NORAX: Enabling Execute-Only Memory for COTS Binaries on AArch64	304
<i>Yaohui Chen, Dongli Zhang, Ruowen Wang, Rui Qiao, Ahmed M. Azab, Long Lu, Hayawardh Vijayakumar, and Wenbo Shen</i>	

Securing Augmented Reality Output	320
<i>Kiron Lebeck, Kimberly Ruth, Tadayoshi Kohno, and Franziska Roesner</i>	

SysPal: System-Guided Pattern Locks for Android	338
<i>Geumhwan Cho, Jun Ho Huh, Junsung Cho, Seongyeol Oh, Youngbae Song, and Hyoungshick Kim</i>	

Multi-touch Authentication Using Hand Geometry and Behavioral Information	357
<i>Yunpeng Song, Zhongmin Cai, and Zhi-Li Zhang</i>	

Session #5: Bitcoin and Distributed Systems

Hijacking Bitcoin: Routing Attacks on Cryptocurrencies	375
<i>Maria Apostolaki, Aviv Zohar, and Laurent Vanbever</i>	
Catena: Efficient Non-equivocation via Bitcoin	393
<i>Alin Tomescu and Srinivas Devadas</i>	
IKP: Turning a PKI Around with Decentralized Automated Incentives	410
<i>Stephanos Matsumoto and Raphael M. Reischuk</i>	
Augur: Internet-Wide Detection of Connectivity Disruptions	427
<i>Paul Pearce, Roya Ensafi, Frank Li, Nick Feamster, and Vern Paxson</i>	
Scalable Bias-Resistant Distributed Randomness	444
<i>Ewa Syta, Philipp Jovanovic, Eleftherios Kokoris Kogias, Nicolas Gailly, Linus Gasser, Ismail Khoffi, Michael J. Fischer, and Bryan Ford</i>	

Session #6: TLS Session Security

Implementing and Proving the TLS 1.3 Record Layer	463
<i>Antoine Delignat-Lavaud, Cedric Fournet, Markulf Kohlweiss, Jonathan Protzenko, Aseem Rastogi, Nikhil Swamy, Santiago Zanella-Beguelin, Karthikeyan Bhargavan, Jianyang Pan, and Jean Karim Zinzindohoue</i>	
Verified Models and Reference Implementations for the TLS 1.3 Standard	
Candidate	483
<i>Karthikeyan Bhargavan, Bruno Blanchet, and Nadim Kobeissi</i>	
SymCerts: Practical Symbolic Execution for Exposing Noncompliance in X.509	
Certificate Validation Implementations	503
<i>Sze Yiu Chau, Omar Chowdhury, Endadul Hoque, Huangyi Ge, Aniket Kate, Cristina Nita-Rotaru, and Ninghui Li</i>	
HVLearn: Automated Black-Box Analysis of Hostname Verification in SSL/TLS	
Implementations	521
<i>Suphannee Sivakorn, George Argyros, Kexin Pei, Angelos D. Keromytis, and Suman Jana</i>	
CRLite: A Scalable System for Pushing All TLS Revocations to All Browsers	539
<i>James Larisch, David Choffnes, Dave Levin, Bruce M. Maggs, Alan Mislove, and Christo Wilson</i>	

Session #7: Software Security

Finding and Preventing Bugs in JavaScript Bindings	559
<i>Fraser Brown, Shravan Narayan, Riad S. Wahby, Dawson Engler, Ranjit Jhala, and Deian Stefan</i>	
Skyfire: Data-Driven Seed Generation for Fuzzing	579
<i>Junjie Wang, Bihuan Chen, Lei Wei, and Yang Liu</i>	
UDDY: A Scalable Approach for Vulnerable Code Clone Discovery	595
<i>Seulbae Kim, Seunghoon Woo, Heejo Lee, and Hakjoo Oh</i>	
NEZHA: Efficient Domain-Independent Differential Testing	615
<i>Theofilos Petsios, Adrian Tang, Salvatore Stolfo, Angelos D. Keromytis, and Suman Jana</i>	
Backward-Bounded DSE: Targeting Infeasibility Questions on Obfuscated Codes	633
<i>Sébastien Bardin, Robin David, and Jean-Yves Marion</i>	

Session #8: Information-Flow Channel Security

Leakage-Abuse Attacks against Order-Revealing Encryption	655
<i>Paul Grubbs, Kevin Sekniqi, Vincent Bindschaedler, Muhammad Naveed, and Thomas Ristenpart</i>	
Side-Channel Attacks on Shared Search Indexes	673
<i>Liang Wang, Paul Grubbs, Jiahui Lu, Vincent Bindschaedler, David Cash, and Thomas Ristenpart</i>	
From Trash to Treasure: Timing-Sensitive Garbage Collection	693
<i>Mathias V. Pedersen and Aslan Askarov</i>	
Verifying and Synthesizing Constant-Resource Implementations with Types	710
<i>Van Chan Ngo, Mario Dehesa-Azuara, Matthew Fredrikson, and Jan Hoffmann</i>	
CoSMedis: A Distributed Social Media Platform with Formally Verified Confidentiality Guarantees	729
<i>Thomas Bauereiß, Armando Pesenti Gritti, Andrei Popescu, and Franco Raimondi</i>	

Session #9: Underground Economics

How to Learn Klingon without a Dictionary: Detection and Measurement of Black Keywords Used by the Underground Economy	751
<i>Hao Yang, Xiulin Ma, Kun Du, Zhou Li, Haixin Duan, Xiaodong Su, Guang Liu, Zhifeng Geng, and Jianping Wu</i>	
To Catch a Ratter: Monitoring the Behavior of Amateur DarkComet RAT Operators in the Wild	770
<i>Brown Farinholt, Mohammad Rezaeirad, Paul Pearce, Hitesh Dharmdasani, Haikuo Yin, Stevens Le Blond, Damon McCoy, and Kirill Levchenko</i>	

A Lustrum of Malware Network Communication: Evolution and Insights	788
<i>Chaz Lever, Platon Kotzias, Davide Balzarotti, Juan Caballero, and Manos Antonakakis</i>	
Under the Shadow of Sunshine: Understanding and Detecting Bulletproof Hosting on Legitimate Service Provider Networks	805
<i>Sumayah Alrwais, Xiaojing Liao, Xianghang Mi, Peng Wang, Xiaofeng Wang, Feng Qian, Raheem Beyah, and Damon McCoy</i>	
Your Exploit is Mine: Automatic Shellcode Transplant for Remote Exploits	824
<i>Tiffany Bao, Ruoyu Wang, Yan Shoshitaishvili, and David Brumley</i>	

Session #10: Cryptography

Optimized Honest-Majority MPC for Malicious Adversaries — Breaking the 1 Billion-Gate Per Second Barrier	843
<i>Toshinori Araki, Assi Barak, Jun Furukawa, Tamar Lichter, Yehuda Lindell, Ariel Nof, Kazuma Ohara, Adi Watzman, and Or Weinstein</i>	
vSQL: Verifying Arbitrary SQL Queries over Dynamic Outsourced Databases	863
<i>Yupeng Zhang, Daniel Genkin, Jonathan Katz, Dimitrios Papadopoulos, and Charalampos Papamanthou</i>	
A Framework for Universally Composable Diffie-Hellman Key Exchange	881
<i>Ralf Küsters and Daniel Rausch</i>	
One TPM to Bind Them All: Fixing TPM 2.0 for Provably Secure Anonymous Attestation	901
<i>Jan Camenisch, Liqun Chen, Manu Drijvers, Anja Lehmann, David Novick, and Rainer Urian</i>	
Cryptographic Function Detection in Obfuscated Binaries via Bit-Precise Symbolic Loop Mapping	921
<i>Dongpeng Xu, Jiang Ming, and Dinghao Wu</i>	

Session #11: Privacy

XHOUND: Quantifying the Fingerprintability of Browser Extensions	941
<i>Oleksii Starov and Nick Nikiforakis</i>	
Identifying Personal DNA Methylation Profiles by Genotype Inference	957
<i>Michael Backes, Pascal Berrang, Matthias Bieg, Roland Eils, Carl Herrmann, Mathias Humbert, and Irina Lehmann</i>	
Counter-RAPTOR: Safeguarding Tor Against Active Routing Attacks	977
<i>Yixin Sun, Anne Edmundson, Nick Feamster, Mung Chiang, and Prateek Mittal</i>	
Machine-Checked Proofs of Privacy for Electronic Voting Protocols	993
<i>Véronique Cortier, Constantin Cătălin Drăgan, François Dupressoir, Benedikt Schmidt, Pierre-Yves Strub, and Bogdan Warinschi</i>	

Spotless Sandboxes: Evading Malware Analysis Systems Using Wear-and-Tear Artifacts	1009
<i>Najmeh Miramirkhani, Mahathi Priya Appini, Nick Nikiforakis, and Michalis Polychronakis</i>	

Session #12: Authorization

Hardening Java's Access Control by Abolishing Implicit Privilege Elevation	1027
<i>Philipp Holzinger, Ben Hermann, Johannes Lerch, Eric Bodden, and Mira Mezini</i>	
Cloak and Dagger: From Two Permissions to Complete Control of the UI Feedback Loop	1041
<i>Yanick Fratantonio, Chenxiong Qian, Simon P. Chung, and Wenke Lee</i>	
SmarPer: Context-Aware and Automatic Runtime-Permissions for Mobile Devices	1058
<i>Katarzyna Olejnik, Italo Dacosta, Joana Soares Machado, Kévin Huguenin, Mohammad Emtiyaz Khan, and Jean-Pierre Hubaux</i>	
The Feasibility of Dynamically Granted Permissions: Aligning Mobile Privacy with User Preferences	1077
<i>Primal Wijesekera, Arjun Baokar, Lynn Tsai, Joel Reardon, Serge Egelman, David Wagner, and Konstantin Beznosov</i>	
IVD: Automatic Learning and Enforcement of Authorization Rules in Online Social Networks	1094
<i>Paul Marinescu, Chad Parry, Marjori Pomarole, Yuan Tian, Patrick Tague, and Ioannis Papagiannis</i>	

Author Index