

Network and Distributed System Security Symposium 2018

San Diego, California, USA
18 – 21 February 2018

Volume 1 of 2

ISBN: 978-1-7138-2195-3

Printed from e-media with permission by:

Curran Associates, Inc.
57 Morehouse Lane
Red Hook, NY 12571



Some format issues inherent in the e-media version may also appear in this print version.

Copyright© (2018) by The Internet Society
All rights reserved.

Printed with permission by Curran Associates, Inc. (2020)

For permission requests, please contact The Internet Society
at the address below.

The Internet Society
11710 Plaza America Drive, Suite 400
Reston, VA 20190
U.S.A.

Phone: (703) 439-2120
Fax: (703) 326-9881

www.internetsociety.org

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
Email: curran@proceedings.com
Web: www.proceedings.com

TABLE OF CONTENTS

VOLUME 1

SESSION 1A: IOT

IOTFUZZER: DISCOVERING MEMORY CORRUPTIONS IN IOT THROUGH APP-BASED FUZZING.	1
<i>Jiongyi Chen , Wenrui Diao , Qingchuan Zhao , Chaoshun Zuo , Zhiqiang Lin , Xiaofeng Wang , Wing Cheong Lau , Menghan Sun , Ronghai Yang , Kehuan Zhang</i>	
FEAR AND LOGGING IN THE INTERNET OF THINGS.	16
<i>Qi Wang , Wajih Ul Hassan , Adam Bates, Carl Gunter</i>	
DECENTRALIZED ACTION INTEGRITY FOR TRIGGER-ACTION IOT PLATFORMS.	31
<i>Earlence Fernandes , Amir Rahmati , Jaeyeon Jung, Atul Prakash</i>	
WHAT YOU CORRUPT IS NOT WHAT YOU CRASH: CHALLENGES IN FUZZING EMBEDDED DEVICES.	47
<i>Marius Muench , Jan Stijohann , Frank Kargl , Aurelien Francillon, Davide Balzarotti</i>	

SESSION 1B: ATTACKS AND VULNERABILITIES

DIDN'T YOU HEAR ME? – TOWARDS MORE SUCCESSFUL WEB VULNERABILITY NOTIFICATIONS.	62
<i>Ben Stock , Giancarlo Pellegrino , Frank Li , Michael Backes, Christian Rossow</i>	
EXPOSING CONGESTION ATTACK ON EMERGING CONNECTED VEHICLE BASED TRAFFIC SIGNAL CONTROL.	77
<i>Qi Alfred Chen , Yucheng Yin , Yiheng Feng , Z Morley Mao, Henry X Liu</i>	
REMOVING SECRETS FROM ANDROID'S TLS.	92
<i>Jaeho Lee , Dan S Wallach</i>	
RTCAPTCHA: A REAL-TIME CAPTCHA BASED LIVENESS DETECTION SYSTEM.	107
<i>Erkam Uzun , Simon Pak Ho Chung , Irfan Essa, Wenke Lee</i>	

SESSION 2A: NETWORK SECURITY/CELLULAR NETWORKS

AUTOMATED ATTACK DISCOVERY IN TCP CONGESTION CONTROL USING A MODEL-GUIDED APPROACH.	122
<i>Samuel Jero , Endadul Hoque , David Choffnes , Alan Mislove, Cristina Nita-Rotaru</i>	
PREVENTING (NETWORK) TIME TRAVEL WITH CHRONOS.	137
<i>Omer Deutsch , Neta Rozen Schiff , Danny Dolev, Michael Schapira</i>	
LTEINSPECTOR: A SYSTEMATIC APPROACH FOR ADVERSARIAL TESTING OF 4G LTE.	152
<i>Syed Rafiul Hussain , Omar Chowdhury , Shagufta Mehnaz, Elisa Bertino</i>	
GUTI REALLOCATION DEMYSTIFIED: CELLULAR LOCATION TRACKING WITH CHANGING TEMPORARY IDENTIFIER.	167
<i>Byeongdo Hong , Sangwook Bae, Yongdae Kim</i>	

SESSION 2B: CRYPTO

MIND YOUR KEYS? A SECURITY EVALUATION OF JAVA KEYSTORES.....	182
<i>Riccardo Focardi , Francesco Palmarini , Marco Squarcina , Graham Steel, Mauro Tempesta</i>	
A SECURITY ANALYSIS OF HONEYWORDS.....	197
<i>Ding Wang , Haibo Cheng , Ping Wang , Jeff Yan, Xinyi Huang</i>	
REVISITING PRIVATE STREAM AGGREGATION: LATTICE-BASED PSA.....	212
<i>Daniela Becker , Jorge Guajardo, Karl-Heinz Zimmermann</i>	
ZEROTRACE : OBLIVIOUS MEMORY PRIMITIVES FROM INTEL SGX.	229
<i>Sajin Sasy , Sergey Gorbunov, Christopher W Fletcher</i>	

SESSION 3A: DEEP LEARNING AND ADVERSARIAL ML

AUTOMATED WEBSITE FINGERPRINTING THROUGH DEEP LEARNING.	244
<i>Vera Rimmer , Davy Preuveneers , Marc Juarez , Tom Van Goethem, Wouter Joosen</i>	
VULDEEPECKER: A DEEP LEARNING-BASED SYSTEM FOR VULNERABILITY DETECTION.....	259
<i>Zhen Li , Deqing Zou , Shouhuai Xu , Xinyu Ou , Hai Jin , Sujuan Wang , Zhijun Deng, Yuyi Zhong</i>	
KITSUNE: AN ENSEMBLE OF AUTOENCODERS FOR ONLINE NETWORK INTRUSION DETECTION.....	274
<i>Yisroel Mirsky , Tomer Doitshman , Yuval Elovici, Asaf Shabtai</i>	
FEATURE SQUEEZING: DETECTING ADVERSARIAL EXAMPLES IN DEEP NEURAL NETWORKS.....	289
<i>Weilin Xu , David Evans, Yanjun Qi</i>	
TROJANING ATTACK ON NEURAL NETWORKS.....	304
<i>Yingqi Liu , Shiqing Ma , Yousra Aafer , Wen-Chuan Lee , Juan Zhai , Weihang Wang, Xiangyu Zhang</i>	

SESSION 3B: AUTHENTICATION

BROKEN FINGERS: ON THE USAGE OF THE FINGERPRINT API IN ANDROID.....	319
<i>Antonio Bianchi , Yanick Fratantonio , Aravind Machiry , Christopher Kruegel , Giovanni Vigna , Simon Pak Ho Chung, Wenke Lee</i>	
K-MEANS++ VS. BEHAVIORAL BIOMETRICS: ONE LOOP TO RULE THEM ALL.	334
<i>Parimarjan Negi , Prafull Sharma , Vivek Sanjay Jain, Bahman Bahmani</i>	
ABC: ENABLING SMARTPHONE AUTHENTICATION WITH BUILT-IN CAMERA.....	347
<i>Zhongjie Ba , Sixu Piao , Xinwen Fu , Dimitrios Koutsonikolas , Aziz Mohaisen, Kui Ren</i>	
DEVICE PAIRING AT THE TOUCH OF AN ELECTRODE.....	362
<i>Marc Roeschlin , Ivan Martinovic, Kasper B Rasmussen</i>	

FACE FLASHING: A SECURE LIVENESS DETECTION PROTOCOL BASED ON LIGHT REFLECTIONS.	377
<i>Di Tang , Zhe Zhou , Yinqian Zhang , Kehuan Zhang</i>	

SESSION 4A: MEASUREMENTS

A LARGE-SCALE ANALYSIS OF CONTENT MODIFICATION BY OPEN HTTP PROXIES.	392
<i>Giorgos Tsirantonakis , Panagiotis Ilia , Sotiris Ioannidis , Elias Athanasopoulos, Michalis Polychronakis</i>	

MEASURING AND DISRUPTING ANTI-ADBLOCKERS USING DIFFERENTIAL EXECUTION ANALYSIS.	407
<i>Shitong Zhu , Xunchao Hu , Zhiyun Qian , Zubair Shafiq, Heng Yin</i>	

TOWARDS MEASURING THE EFFECTIVENESS OF TELEPHONY BLACKLISTS.	422
<i>Sharbani Pandit , Roberto Perdisci , Mustaque Ahamad, Payas Gupta</i>	

THINGS YOU MAY NOT KNOW ABOUT ANDROID (UN)PACKERS: A SYSTEMATIC STUDY BASED ON WHOLE-SYSTEM EMULATION.	437
<i>Yue Duan , Mu Zhang , Abhishek Vasisht Bhaskar , Heng Yin , Xiaorui Pan , Tongxin Li , Xueqiang Wang, Xiaofeng Wang</i>	

SESSION 4B: SOFTWARE ATTACKS AND SECURE ARCHITECTURES

KEYDROWN: ELIMINATING SOFTWARE-BASED KEYSTROKE TIMING SIDE-CHANNEL ATTACKS.	452
<i>Michael Schwarz , Moritz Lipp , Daniel Gruss , Samuel Weiser , Clementine Maurice , Raphael Spreitzer, Stefan Mangard</i>	

SECURING REAL-TIME MICROCONTROLLER SYSTEMS THROUGH CUSTOMIZED MEMORY VIEW SWITCHING.	467
<i>Chung Hwan Kim , Taegy Kim , Hongjun Choi , Zhongshu Gu , Byoungyoung Lee , Xiangyu Zhang, Dongyan Xu</i>	

AUTOMATED GENERATION OF EVENT-ORIENTED EXPLOITS IN ANDROID HYBRID APPS.	482
<i>Guangliang Yang , Jeff Huang, Guofei Gu</i>	

TIPPED OFF BY YOUR MEMORY ALLOCATOR: DEVICE-WIDE USER ACTIVITY SEQUENCING FROM ANDROID MEMORY IMAGES.	497
<i>Rohit Bhatia , Brendan Saltaformaggio , Seung Jei Yang , Aisha Ali-Gombe , Xiangyu Zhang , Dongyan Xu, Golden G Richard III</i>	

SESSION 5A: SOFTWARE SECURITY

K-MINER: UNCOVERING MEMORY CORRUPTION IN LINUX.	512
<i>David Gens , Simon Schmitt , Lucas Davi, Ahmad-Reza Sadeghi</i>	

VOLUME 2

CFIXX: OBJECT TYPE INTEGRITY FOR C++.	527
<i>Nathan Burow , Derrick McKee , Scott A Carr, Mathias Payer</i>	

BACK TO THE EPILOGUE: EVADING CONTROL FLOW GUARD VIA UNALIGNED TARGETS.....	541
<i>Andrea Biondo , Mauro Conti, Daniele Lain</i>	
SUPERSET DISASSEMBLY: STATICALLY REWRITING X86 BINARIES WITHOUT HEURISTICS.....	556
<i>Erick Bauman , Zhiqiang Lin, Kevin Hamlen</i>	
ENHANCING MEMORY ERROR DETECTION FOR LARGE-SCALE APPLICATIONS AND FUZZ TESTING.	571
<i>Wookhyun Han , Byungill Joe , Byoungyoung Lee , Chengyu Song, Insik Shin</i>	

SESSION 5B: PRIVACY IN MOBILE

FINDING CLUES FOR YOUR SECRETS: SEMANTICS-DRIVEN, LEARNING-BASED PRIVACY DISCOVERY IN MOBILE APPS.....	586
<i>Yuhong Nan , Zheming Yang , Xiaofeng Wang , Yuan Zhang , Donglai Zhu, Min Yang</i>	
BUG FIXES, IMPROVEMENTS, ... AND PRIVACY LEAKS – A LONGITUDINAL STUDY OF PII LEAKS ACROSS ANDROID APP VERSIONS.....	601
<i>Jingjing Ren , Martina Lindorfer , Daniel J Dubois , Ashwin Rao , David Choffnes, Narseo Vallina-Rodriguez</i>	
APPS, TRACKERS, PRIVACY, AND REGULATORS: A GLOBAL STUDY OF THE MOBILE TRACKING ECOSYSTEM.....	616
<i>Abbas Razaghpanah , Rishab Nithyanand , Narseo Vallina-Rodriguez , Srikanth Sundaresan , Mark Allman , Christian Kreibich, Phillipa Gill</i>	
OS-LEVEL SIDE CHANNELS WITHOUT PROCFS: EXPLORING CROSS-APP INFORMATION LEAKAGE ON IOS.	631
<i>Xiaokuan Zhang , Xueqiang Wang , Xiaolong Bai , Yinqian Zhang, Xiaofeng Wang</i>	
KNOCK KNOCK, WHO’S THERE? MEMBERSHIP INFERENCE ON AGGREGATE LOCATION DATA.....	646
<i>Apostolos Pyrgelis , Carmela Troncoso, Emiliano De Cristofaro</i>	

SESSION 6A: CLOUD

REDUCED COOLING REDUNDANCY: A NEW SECURITY VULNERABILITY IN A HOT DATA CENTER.	661
<i>Xing Gao , Zhang Xu , Haining Wang , Li Li, Xiaorui Wang</i>	
OBLIVATE: A DATA OBLIVIOUS FILESYSTEM FOR INTEL SGX.....	676
<i>Adil Ahmad , Kyungtae Kim , Muhammad Ihsanulhaq Sarfaraz, Byoungyoung Lee</i>	
MICROARCHITECTURAL MINEFIELDS: 4K-ALIASING COVERT CHANNEL AND MULTI-TENANT DETECTION IN IAAS CLOUDS.....	691
<i>Dean Sullivan , Orlando Arias , Travis Meade, Yier Jin</i>	
CLOUD STRIFE: MITIGATING THE SECURITY RISKS OF DOMAIN-VALIDATED CERTIFICATES.	705
<i>Kevin Borgolte , Tobias Fiebig , Shuang Hao , Christopher Kruegel, Giovanni Vigna</i>	

SESSION 6B: PRIVACY AND DE-ANONYMIZATION

CONSENSUAL AND PRIVACY-PRESERVING SHARING OF MULTI-SUBJECT AND INTERDEPENDENT DATA.....	720
<i>Alexandra-Mihaela Olteanu , Kevin Huguenin , Italo Dacosta, Jean-Pierre Hubaux</i>	
WHEN CODING STYLE SURVIVES COMPILATION: DE-ANONYMIZING PROGRAMMERS FROM EXECUTABLE BINARIES.....	735
<i>Aylin Caliskan , Fabian Yamaguchi , Edwin Dauber , Richard Harang , Konrad Rieck , Rachel Greenstadt, Arvind Narayanan</i>	
DE-ANONYMIZATION OF MOBILITY TRAJECTORIES: DISSECTING THE GAPS BETWEEN THEORY AND PRACTICE.....	750
<i>Huandong Wang , Chen Gao , Yong Li , Gang Wang , Depeng Jin, Jingbo Sun</i>	
VEIL: PRIVATE BROWSING SEMANTICS WITHOUT BROWSER-SIDE ASSISTANCE.	765
<i>Frank Wang , James Mickens, Nikolai Zeldovich</i>	

SESSION 7A: WEB SECURITY

GAME OF MISSUGGESTIONS: SEMANTIC ANALYSIS OF SEARCH-AUTOCOMPLETE MANIPULATIONS.	780
<i>Peng Wang , Xianghang Mi , Xiaojing Liao , Xiaofeng Wang , Kan Yuan , Feng Qian, Raheem Beyah</i>	
SYNODE: UNDERSTANDING AND AUTOMATICALLY PREVENTING INJECTION ATTACKS ON NODE.JS.....	795
<i>Cristian-Alexandru Staicu , Michael Pradel, Benjamin Livshits</i>	
JAVASCRIPT ZERO: REAL JAVASCRIPT AND ZERO SIDE-CHANNEL ATTACKS.	810
<i>Michael Schwarz , Moritz Lipp, Daniel Gruss</i>	
RIDING OUT DOMSDAY: TOWARDS DETECTING AND PREVENTING DOM CROSS-SITE SCRIPTING.	825
<i>William Melicher , Anupam Das , Mahmood Sharif , Lujo Bauer, Limin Jia</i>	

SESSION 7B: AUDIT LOGS

TOWARDS SCALABLE CLUSTER AUDITING THROUGH GRAMMATICAL INFERENCE OVER PROVENANCE GRAPHS.....	840
<i>Wajih Ul Hassan , Mark Lemay , Nuraini Aguse , Adam Bates, Thomas Moyer</i>	
MCI : MODELING-BASED CAUSALITY INFERENCE IN AUDIT LOGGING FOR ATTACK INVESTIGATION.	855
<i>Yonghwi Kwon , Fei Wang , Weihang Wang , Kyu Hyung Lee , Wen-Chuan Lee , Shiqing Ma , Xiangyu Zhang , Dongyan Xu , Somesh Jha , Gabriela Ciocarlie , Ashish Gehani, Vinod Yegneswaran</i>	
TOWARDS A TIMELY CAUSALITY ANALYSIS FOR ENTERPRISE SECURITY.....	870
<i>Yushan Liu , Mu Zhang , Ding Li , Kangkook Jee , Zhichun Li , Zhenyu Wu , Junghwan Rhee, Prateek Mittal</i>	

JSGRAPH: ENABLING RECONSTRUCTION OF WEB ATTACKS VIA EFFICIENT TRACKING OF LIVE IN-BROWSER JAVASCRIPT EXECUTIONS.....	885
<i>Bo Li , Phani Vadrevu , Kyu Hyung Lee, Roberto Perdisci</i>	

SESSION 8: ANDROID

ACEDROID: NORMALIZING DIVERSE ANDROID ACCESS CONTROL CHECKS FOR INCONSISTENCY DETECTION.....	900
<i>Yousra Aafer , Jianjun Huang , Yi Sun , Xiangyu Zhang , Ninghui Li, Chen Tian</i>	

INSTAGUARD: INSTANTLY DEPLOYABLE HOT-PATCHES FOR VULNERABLE SYSTEM PROGRAMS ON ANDROID.....	915
<i>Yaohui Chen , Yuping Li , Long Lu , Yueh-Hsun Lin , Haywardh Vijayakumar , Zhi Wang, Xinming Ou</i>	

BREAKAPP: AUTOMATED, FLEXIBLE APPLICATION COMPARTMENTALIZATION.....	930
<i>Nikos Vasilakis , Ben Karel , Nick Roessler , Nathan Dautenhahn , Andre Dehon, Jonathan M Smith</i>	

RESOLVING THE PREDICAMENT OF ANDROID CUSTOM PERMISSIONS.....	945
<i>Guliz Seray Tuncay , Soteris Demetriou , Karan Ganju, Carl A Gunter</i>	

SESSION 9: BLOCKCHAIN AND SMART CONTRACTS

ZEUS: ANALYZING SAFETY OF SMART CONTRACTS.....	960
<i>Sukrit Kalra , Seep Goel , Mohan Dhawan, Subodh Sharma</i>	

CHAINSPACE: A SHARDED SMART CONTRACTS PLATFORM.....	975
<i>Mustafa Al-Bassam , Alberto Sonnino , Shehar Bano , Dave Hryczyn, George Danezis</i>	

SETTLING PAYMENTS FAST AND PRIVATE: EFFICIENT DECENTRALIZED ROUTING FOR PATH-BASED TRANSACTIONS.....	990
<i>Stefanie Roos , Pedro Moreno-Sanchez , Aniket Kate, Ian Goldberg</i>	

TLS-N: NON-REPUDIATION OVER TLS ENABLIGN UBIQUITOUS CONTENT SIGNING.....	1005
<i>Hubert Ritzdorf , Karl Wust , Arthur Gervais , Guillaume Felley, Srdjan Capkun</i>	

SESSION 10: SOCIAL NETWORKS AND ANONYMITY

INVESTIGATING AD TRANSPARENCY MECHANISMS IN SOCIAL MEDIA: A CASE STUDY OF FACEBOOKS EXPLANATIONS.....	1020
<i>Athanasios Andreou , Giridhari Venkatadri , Oana Goga , Krishna P Gummadi , Patrick Loiseau, Alan Mislove</i>	

INSIDE JOB: APPLYING TRAFFIC ANALYSIS TO MEASURE TOR FROM WITHIN.....	1035
<i>Rob Jansen , Marc Juarez , Rafa Galvez , Tariq Elahi, Claudia Diaz</i>	

SMOKE SCREENER OR STRAIGHT SHOOTER: DETECTING ELITE SYBIL ATTACKS IN USER-REVIEW SOCIAL NETWORKS.....	1050
<i>Haizhong Zheng , Minhui Xue , Hao Lu , Shuang Hao , Haojin Zhu , Xiaohui Liang, Keith Ross</i>	

Author Index