

# **Network and Distributed System Security Symposium 2016 (NDSS'16)**

San Diego, California, USA  
21 – 24 February 2016

Volume 1 of 2

ISBN: 978-1-7138-2201-1

**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© (2016) 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](http://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](mailto:curran@proceedings.com)  
Web: [www.proceedings.com](http://www.proceedings.com)

# TABLE OF CONTENTS

## VOLUME 1

### **SESSION 1: TRANSPORT LAYER SECURITY**

TRANSCRIPT COLLISION ATTACKS: BREAKING AUTHENTICATION IN TLS, IKE AND SSH.....	1
<i>Karthikeyan Bhargavan, Gaetan Leurent</i>	
TLS IN THE WILD: AN INTERNET-WIDE ANALYSIS OF TLS-BASED PROTOCOLS FOR ELECTRONIC COMMUNICATION .....	18
<i>Ralph Holz , Johanna Amann , Olivier Mehani, Mohamed Ali Kaafar, Matthias Wachs</i>	
KILLED BY PROXY: ANALYZING CLIENT-END TLS INTERCEPTION SOFTWARE.....	33
<i>Xavier De Carné De Carnavalet, Mohammad Mannan</i>	

### **SESSION 2: NETWORK SECURITY – PART I**

SIBRA: SCALABLE INTERNET BANDWIDTH RESERVATION ARCHITECTURE.....	50
<i>Cristina Basescu, Raphael M. Reischuk, Pawel Szalachowski, Adrian Perrig , Yao Zhang , Hsu-Chun Hsiao , Ayumu Kubota, Jumpei Urakawa</i>	
DON'T FORGET TO LOCK THE BACK DOOR! A CHARACTERIZATION OF IPV6 NETWORK SECURITY POLICY .....	66
<i>Jakub Czyz , Matthew Luckie , Mark Allman , Michael Bailey</i>	
ATTACKING THE NETWORK TIME PROTOCOL .....	81
<i>Aanchal Malhotra, Isaac E. Cohen, Erik Brakke, Sharon Goldberg</i>	
SPIFFY: INDUCING COST-DETECTABILITY TRADEOFFS FOR PERSISTENT LINK-FLOODING ATTACKS .....	96
<i>Min Suk Kang, Virgil D. Gligor, Vyas Sekar</i>	

### **SESSION 3: WEB SECURITY**

CROSSFIRE: AN ANALYSIS OF FIREFOX EXTENSION-REUSE VULNERABILITIES .....	111
<i>Ahmet Buyukkayhan, Kaan Onarlioglu, William Robertson, Engin Kirda</i>	
IT'S FREE FOR A REASON: EXPLORING THE ECOSYSTEM OF FREE LIVE STREAMING SERVICES .....	123
<i>M. Zubair Rafique, Tom Van Goethem, Wouter Joosen, Christophe Huygens , Nick Nikiforakis</i>	
ATTACK PATTERNS FOR BLACK-BOX SECURITY TESTING OF MULTI-PARTY WEB APPLICATIONS.....	138
<i>Avinash Sudhodanan , Alessandro Armando , Roberto Carbone , Luca Compagna</i>	
ARE THESE ADS SAFE: DETECTING HIDDEN ATTACKS THROUGH THE MOBILE APP-WEB INTERFACES .....	153
<i>Vaibhav Rastogi , Rui Shao , Yan Chen, Xiang Pan , Shihong Zou , Ryan Riley</i>	

## **SESSION 4: NETWORK SECURITY PART II**

ENABLING PRACTICAL SOFTWARE-DEFINED NETWORKING SECURITY APPLICATIONS WITH OFX .....	168
<i>John Sonchack, Jonathan M. Smith , Adam J. Aviv , Eric Keller</i>	
FORWARDING-LOOP ATTACKS IN CONTENT DELIVERY NETWORKS .....	183
<i>Jianjun Chen, Xiaofeng Zheng, Haixin Duan, Jinjin Liang, Jian Jiang, Kang Li, Tao Wan, Vern Paxson</i>	
CDN-ON-DEMAND: AN AFFORDABLE DDOS DEFENSE VIA UNTRUSTED CLOUDS .....	196
<i>Yossi Gilad , Amir Herzberg, Michael Sudkovitch, Michael Goberman</i>	
TOWARDS SDN-DEFINED PROGRAMMABLE BYOD (BRING YOUR OWN DEVICE) SECURITY .....	211
<i>Sungmin Hong, Robert Baykov, Lei Xu, Srinath Nadimpalli, Guofei Gu</i>	

## **SESSION 5: MISC: CRYPTOCURRENCIES, CAPTCHAS, AND GAMEBOTS**

CENTRALLY BANKED CRYPTOCURRENCIES .....	226
<i>Yossi Gilad , Amir Herzberg, Michael Sudkovitch, Michael Goberman</i>	
EQUIHASH: ASYMMETRIC PROOF-OF-WORK BASED ON THE GENERALIZED BIRTHDAY PROBLEM.....	240
<i>Alex Biryukov, Dmitry Khovratovich</i>	
A SIMPLE GENERIC ATTACK ON TEXT CAPTCHAS .....	253
<i>Haichang Gao , Jeff Yan , Fang Cao, Zhengya Zhang, Lei Lei, Mengyun Tang, Ping Zhang, Xin Zhou, Xuqin Wang, Jiawei Li</i>	
YOU ARE A GAME BOT!: UNCOVERING GAME BOTS IN MMORPGS VIA SELF-SIMILARITY IN THE WILD.....	267
<i>Junjo Lee , Jiyoung Woo , Hyounghick Kim , Aziz Mohaisen , Huy Kang Kim</i>	

## **SESSION 6: PRIVACY IN MOBILE**

TRACKING MOBILE WEB USERS THROUGH MOTION SENSORS: ATTACKS AND DEFENSES .....	282
<i>Anupam Das, Nikita Borisov, Matthew Caesar</i>	
THE PRICE OF FREE: PRIVACY LEAKAGE IN PERSONALIZED MOBILE IN-APPS ADS .....	297
<i>Wei Meng, Ren Ding, Simon P. Chung, Steven Han, Wenke Lee</i>	
WHAT MOBILE ADS KNOW ABOUT MOBILE USERS .....	312
<i>Sooel Son , Daehyeok Kim , Vitaly Shmatikov</i>	
FREE FOR ALL! ASSESSING USER DATA EXPOSURE TO ADVERTISING LIBRARIES ON ANDROID.....	326
<i>Soteris Demetriou, Whitney Merrill, Wei Yang, Aston Zhang, Carl A. Gunter</i>	
PRACTICAL ATTACKS AGAINST PRIVACY AND AVAILABILITY IN 4G/LTE MOBILE COMMUNICATION SYSTEMS .....	341
<i>Altaf Shaik, Jean-Pierre Seifert , Ravishankar Borgaonkar , N. Asokan , Valtteri Niemi</i>	

## **SESSION 7: SOFTWARE SECURITY**

TOWARDS AUTOMATED DYNAMIC ANALYSIS FOR LINUX-BASED EMBEDDED FIRMWARE .....	356
<i>Daming D. Chen, Maverick Woo, David Brumley , Manuel Egele</i>	
DISCOVERE: EFFICIENT CROSS-ARCHITECTURE IDENTIFICATION OF BUGS IN BINARY CODE.....	372
<i>Sebastian Eschweiler, Khaled Yakdan , Elmar Gerhards-Padilla</i>	
DRILLER: AUGMENTING FUZZING THROUGH SELECTIVE SYMBOLIC EXECUTION .....	387
<i>Nick Stephens, John Grosen, Christopher Salls, Andrew Dutcher, Ruoyu Wang, Jacopo Corbetta, Yan Shoshitaishvili, Christopher Kruegel, Giovanni Vigna</i>	
VTRUST: REGAINING TRUST ON VIRTUAL CALLS .....	403
<i>Chao Zhang, Dawn Song , Scott A. Carr, Mathias Payer , Tongxin Li, Yu Ding , Chengyu Song</i>	
PROTECTING C++ DYNAMIC DISPATCH THROUGH VTABLE INTERLEAVING .....	418
<i>Dimitar Bounov, Rami Gökhan Kici, Sorin Lerner</i>	

## **SESSION 8: SYSTEM SECURITY – PART I**

PROTRACER: TOWARDS PRACTICAL PROVENANCE TRACING BY ALTERNATING BETWEEN LOGGING AND TAINTING .....	433
<i>Shiqing Ma, Xiangyu Zhang, Dongyan Xu</i>	

## **VOLUME 2**

WHO'S IN CONTROL OF YOUR CONTROL SYSTEM? DEVICE FINGERPRINTING FOR CYBER-PHYSICAL SYSTEMS .....	448
<i>David Formby, Preethi Srinivasan, Andrew Leonard, Jonathan Rogers, Raheem Beyah</i>	
SKEE: A LIGHTWEIGHT SECURE KERNEL-LEVEL EXECUTION ENVIRONMENT FOR ARM.....	463
<i>Ahmed Azab, Kirk Swidowski, Rohan Bhutkar, Jia Ma, Wenbo Shen, Ruowen Wang, Peng Ning</i>	
OPENSX: AN OPEN PLATFORM FOR SGX RESEARCH.....	478
<i>Prerit Jain, Soham Desai, Ming-Wei Shih, Taesoo Kim , Seongmin Kim, Jaehyuk Lee, Changho Choi, Youjung Shin, Brent Byunghoon Kang, Dongsu Han</i>	

## **SESSION 9: PRIVACY – PART I**

EFFICIENT PRIVATE STATISTICS WITH SUCCINCT SKETCHES .....	494
<i>Luca Melis, George Danezis, Emiliano De Cristofaro</i>	
DEPENDENCE MAKES YOU VULNERABLE: DIFFERENTIAL PRIVACY UNDER DEPENDENT TUPLES .....	509
<i>Changchang Liu, Prateek Mittal , Supriyo Chakraborty</i>	
PRIVACY-PRESERVING SHORTEST PATH COMPUTATION .....	524
<i>David J. Wu, Joe Zimmerman, Jérémy Planul, John C. Mitchell</i>	

LINKMIRAGE: ENABLING PRIVACY-PRESERVING ANALYTICS ON SOCIAL RELATIONSHIPS .....	539
<i>Changchang Liu, Prateek Mittal</i>	

## **SESSION 10: PRIVACY – PART II**

DO YOU SEE WHAT I SEE? DIFFERENTIAL TREATMENT OF ANONYMOUS USERS .....	554
<i>Sheharbano Khattak , David Fifield, Sadia Afroz, Mobin Javed , Srikanth Sundaresan, Damon McCoy , Vern Paxson , Steven J. Murdoch</i>	
MEASURING AND MITIGATING AS-LEVEL ADVERSARIES AGAINST TOR .....	569
<i>Rishab Nithyanand, Oleksii Starov, Phillipa Gill , Adva Zair, Michael Schapira</i>	
WEBSITE FINGERPRINTING AT INTERNET SCALE.....	584
<i>Andriy Panchenko, Fabian Lanze, Jan Pennekamp, Thomas Engel , Andreas Zinnen , Martin Henze, Klaus Wehrle</i>	

## **SESSION 11: MALWARE**

EXTRACT ME IF YOU CAN: ABUSING PDF PARSERS IN MALWARE DETECTORS .....	599
<i>Curtis Carmony, Xunchao Hu, Heng Yin, Abhishek Vasisht , Mu Zhang</i>	
AUTOMATICALLY EVADING CLASSIFIERS: A CASE STUDY ON PDF MALWARE CLASSIFIERS .....	614
<i>Weilin Xu, Yanjun Qi, David Evans</i>	
CACHE, TRIGGER, IMPERSONATE: ENABLING CONTEXT-SENSITIVE HONEYCLIENT ANALYSIS ON-THE-WIRE .....	629
<i>Teryl Taylor, Kevin Z. Snow, Nathan Otterness, Fabian Monroe</i>	
LO-PHI: LOW-OBSERVABLE PHYSICAL HOST INSTRUMENTATION FOR MALWARE ANALYSIS .....	644
<i>Chad Spensky , Hongyi Hu , Kevin Leach</i>	
WHEN A TREE FALLS: USING DIVERSITY IN ENSEMBLE CLASSIFIERS TO IDENTIFY EVASION IN MALWARE DETECTORS.....	659
<i>Charles Smutz, Angelos Stavrou</i>	

## **SESSION 12: SYSTEM SECURITY – PART II**

KRATOS: DISCOVERING INCONSISTENT SECURITY POLICY ENFORCEMENT IN THE ANDROID FRAMEWORK.....	674
<i>Yuru Shao, Qi Alfred Chen, Z. Morley Mao , Jason Ott, Zhiyun Qian</i>	
HOW TO MAKE ASLR WIN THE CLONE WARS: RUNTIME RE-RANDOMIZATION.....	689
<i>Kangjie Lu, Wenke Lee , Stefan Nürnbergger, Michael Backes</i>	
LEAKAGE-RESILIENT LAYOUT RANDOMIZATION FOR MOBILE DEVICES .....	704
<i>Kjell Braden, Lucas Davi, Christopher Liebchen, Ahmad-Reza Sadeghi , Stephen Crane , Michael Franz, Per Larsen</i>	
ENABLING CLIENT-SIDE CRASH-RESISTANCE TO OVERCOME DIVERSIFICATION AND INFORMATION HIDING .....	719
<i>Robert Gawlik, Benjamin Kollenda, Philipp Koppe, Behrad Garmany, Thorsten Holz</i>	

ENFORCING KERNEL SECURITY INVARIANTS WITH DATA FLOW INTEGRITY .....	734
<i>Chengyu Song, Byoungyoung Lee, Kangjie Lu, William Harris, Taesoo Kim, Wenke Lee</i>	

### **SESSION 13: ANDROID SECURITY**

GOING NATIVE: USING A LARGE-SCALE ANALYSIS OF ANDROID APPS TO CREATE A PRACTICAL NATIVE-CODE SANDBOXING POLICY .....	749
<i>Vitor Afonso, Paulo De Geus, Antonio Bianchi, Yanick Fratantonio, Christopher Kruegel, Giovanni Vigna , Adam Doupe , Mario Polino</i>	

LIFE AFTER APP UNINSTALLATION: ARE THE DATA STILL ALIVE? DATA RESIDUE ATTACKS ON ANDROID .....	764
<i>Xiao Zhang, Kailiang Ying, Yousra Aafer, Zhenshen Qiu, Wenliang Du</i>	

FLEXDROID: ENFORCING IN-APP PRIVILEGE SEPARATION IN ANDROID .....	779
<i>Jaebaek Seo, Daehyeok Kim, Donghyun Cho, Insik Shin , Taesoo Kim</i>	

INTELLIDROID: A TARGETED INPUT GENERATOR FOR THE DYNAMIC ANALYSIS OF ANDROID MALWARE .....	794
<i>Michelle Y. Wong, David Lie</i>	

HARVESTING RUNTIME VALUES IN ANDROID APPLICATIONS THAT FEATURE ANTI-ANALYSIS TECHNIQUES .....	809
<i>Siegfried Rasthofer, Steven Arzt, Marc Miltenberger , Eric Bodden</i>	

### **SESSION 14: USER AUTHENTICATION**

AUTOMATIC FORGERY OF CRYPTOGRAPHICALLY CONSISTENT MESSAGES TO IDENTIFY SECURITY VULNERABILITIES IN MOBILE SERVICES .....	824
<i>Chaoshun Zuo, Wubing Wang, Zhiqiang Lin , Rui Wang</i>	

DIFFERENTIALLY PRIVATE PASSWORD FREQUENCY LISTS .....	841
<i>Jeremiah Blocki , Anupam Datta , Joseph Bonneau</i>	

WHO ARE YOU? A STATISTICAL APPROACH TO MEASURING USER AUTHENTICITY.....	856
<i>David Freeman, Sakshi Jain, Markus Duermuth, Battista Biggio, Giorgio Giacinto</i>	

PITFALLS IN DESIGNING ZERO-EFFORT DEAUTHENTICATION: OPPORTUNISTIC HUMAN OBSERVATION ATTACKS.....	871
<i>Otto Huhta, Swapnil Udar, Mika Juuti, Prakash Shrestha, Nitesh Saxena, N. Asokan</i>	

VISIBLE: VIDEO-ASSISTED KEYSTROKE INFERENCE FROM TABLET BACKSIDE MOTION.....	885
<i>Jingchao Sun, Xiaocong, Yimin Chen, Jinxue Zhang, Yanchao Zhang , Rui Zhang</i>	

### **Author Index**