

# **Network and Distributed System Security Symposium 2013 (NDSS'13)**

San Diego, California, USA  
25 – 27 February 2013

Volume 1 of 2

ISBN: 978-1-7138-2067-3

**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© (2013) 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

### **MONDAY KEYNOTE**

KEYNOTE PRESENTATION.....	1
<i>Richard Kemmerer</i>	

### **SESSION 1: AUTHENTICATION**

I CAN BE YOU: QUESTIONING THE USE OF KEYSTROKE DYNAMICS AS BIOMETRICS .....	38
<i>Tey Chee Meng, Payas Gupta, Debin Gao</i>	
A PRACTICAL, TARGETED, AND STEALTHY ATTACK AGAINST WPA ENTERPRISE AUTHENTICATION.....	54
<i>Aldo Cassola, William Robertson, Engin Kirda, Guevara Noubir</i>	

### **SESSION 2: MOBILE SECURITY**

UNOBSERVABLE RE-AUTHENTICATION FOR SMARTPHONES .....	69
<i>Lingjun Li, Xinxin Zhao, Guoliang Xue</i>	
PLACERAIDER: VIRTUAL THEFT IN PHYSICAL SPACES WITH SMARTPHONES .....	85
<i>Robert Templeman, Zahid Rahman, David Crandall, Apu Kapadia</i>	
DETECTING PASSIVE CONTENT LEAKS AND POLLUTION IN ANDROID APPLICATIONS.....	100
<i>Yajin Zhou, Xuxian Jiang</i>	
SECURITY ENHANCED (SE) ANDROID: BRINGING FLEXIBLE MAC TO ANDROID .....	116
<i>Stephen Smalley, Robert Craig</i>	
THE CORE OF THE MATTER: ANALYZING MALICIOUS TRAFFIC IN CELLULAR CARRIERS .....	134
<i>Charles Lever, Manos Antonakakis, Brad Reaves, Patrick Traynor, Wenke Lee</i>	

### **SESSION 3: SYSTEMS AND SOFTWARE SECURITY**

HIGH ACCURACY ATTACK PROVENANCE VIA BINARY-BASED EXECUTION PARTITION.....	150
<i>Kyu Hyung Lee, Xiangyu Zhang, Dongyan Xu</i>	
ATTACK SURFACE METRICS AND AUTOMATED COMPILE-TIME OS KERNEL TAILORING .....	166
<i>A. Kurmus, R. Tartler, D. Dorneau, B. Heinloth, V. Rothberg, A. Ruprecht, W. Schöder-Preikschat, D. Lohmann, R. Kapitza</i>	
TAMING HOSTED HYPERVISORS WITH (MOSTLY) DEPRIVILEGED EXECUTION.....	184
<i>Chiachih Wu, Zhi Wang, Xuxian Jiang</i>	

WHEN FIRMWARE MODIFICATIONS ATTACK: A CASE STUDY OF EMBEDDED EXPLOITATION.....	199
<i>Ang Cui, Michael Costello, Salvatore J. Stolfo</i>	

CAMP: CONTENT-AGNOSTIC MALWARE PROTECTION .....	212
<i>Niels Provos, Moheeb Abu Rajab, Lucas Ballard, Noe Lutz, Panayiotis Mavrommatis</i>	

#### **SESSION 4: WEB SECURITY**

INTEGUARD: TOWARD AUTOMATIC PROTECTION OF THIRD-PARTY WEB SERVICE INTEGRATIONS.....	227
<i>Luyi Xing, Yangyi Chen, Xiaofeng Wang, Shuo Chen</i>	

PREVENTING SIDE-CHANNEL LEAKS IN WEB TRAFFIC: A FORMAL APPROACH .....	244
<i>Michael Backes, Goran Doychev, Boris Köpf</i>	

NEIGHBORWATCHER: A CONTENT-AGNOSTIC COMMENT SPAM INFERENCE SYSTEM .....	261
<i>Jialong Zhang, Guofei Gu</i>	

AUTHSCAN: AUTOMATIC EXTRACTION OF WEB AUTHENTICATION PROTOCOLS FROM IMPLEMENTATIONS.....	277
<i>Guangdong Bai, Guozhu Meng, Jike Lei, Sai Sathyanarayan Venkatraman, Prateek Saxena, Jun Sun, Yang Liu, Jinsong Dong</i>	

THE POSTMAN ALWAYS RINGS TWICE: ATTACKING AND DEFENDING POSTMESSAGE IN HTML5 WEBSITES.....	297
<i>Sooel Son, Vitaly Shmatikov</i>	

#### **TUESDAY KEYNOTE**

LAYING A SECURE FOUNDATION FOR MOBILE DEVICES.....	311
<i>Stephen Smalley</i>	

#### **SESSION 5: SOCIAL NETWORKS AND APPLICATION SECURITY**

PISCES: ANONYMOUS COMMUNICATION USING SOCIAL NETWORKS.....	330
<i>Prateek Mittal, Matthew Wright, Nikita Borisov</i>	

PRESERVING LINK PRIVACY IN SOCIAL NETWORK BASED SYSTEMS .....	348
<i>Prateek Mittal, Charalampos Papamanthou, Dawn Song</i>	

COMPA: DETECTING COMPROMISED ACCOUNTS ON SOCIAL NETWORKS.....	367
<i>Manuel Egele, Gianluca Stringhini, Christopher Kruegel, Giovanni Vigna</i>	

#### **SESSION 6: MOBILE AND WIRELESS SECURITY AND PRIVACY**

SOCIAL TURING TESTS: CROWDSOURCING SYBIL DETECTION.....	384
<i>Gang Wang, Manish Mohanlal, Christo Wilson, Xiao Wang, Miriam Metzger, Haitao Zheng, Ben Y. Zhao</i>	

COMPARING MOBILE PRIVACY PROTECTION THROUGH CROSS-PLATFORM APPLICATIONS.....	400
<i>Jin Han, Qiang Yan, Debin Gao, Jianying Zhou, Robert Deng</i>	

ON IMPLEMENTING DENIABLE STORAGE ENCRYPTION FOR MOBILE DEVICES ..... 415  
*Adam Skillen, Mohammad Mannan*

CONTEXTUAL POLICY ENFORCEMENT IN ANDROID APPLICATIONS WITH  
PERMISSION EVENT GRAPHS..... 432  
*Kevin Chen, Noah Johnson, Vijay D'Silva, Shuaifu Dai, Kyle Macnamara, Tom Magrino,  
Edward Wu, Martin Rinard, Dawn Song*

## VOLUME 2

LOW-COST STANDARD SIGNATURES IN WIRELESS SENSOR NETWORKS: A CASE FOR  
REVIVING PRE-COMPUTATION TECHNIQUES? ..... 451  
*Giuseppe Ateniese, Giuseppe Bianchi, Angelo Caposese, Chiara Petrioli*

### **SESSION 7: NETWORK SECURITY I**

CLICKONOMICS: DETERMINING THE EFFECT OF ANTI-PIRACY MEASURES FOR ONE-  
CLICK HOSTING ..... 463  
*Tobias Lauinger, Martin Szydlowski, Kaan Onarlioglu, Gilbert Wondracek, Engin Kirda,  
Christopher Kruegel*

FRESCO: MODULAR COMPOSABLE SECURITY SERVICES FOR SOFTWARE-DEFINED  
NETWORKS..... 477  
*Seungwon Shin, Phil Porras, Vinod Yegneswaran, Martin Fong, Guofei Gu, Mabry Tyson*

INTENTION AND ORIGINATION: AN INSIDE LOOK AT LARGE-SCALE BOT QUERIES ..... 493  
*Junjie Zhang, Yinglian Xie, Fang Yu, David Soukal, Wenke Lee*

JUICE: A LONGITUDINAL STUDY OF AN SEO CAMPAIGN ..... 509  
*David Y. Wang, Stefan Savage, Geoffrey M. Voelker*

I WANT MY VOICE TO BE HEARD: IP OVER VOICE-OVER-IP FOR UNOBSERVABLE  
CENSORSHIP CIRCUMVENTION ..... 526  
*Amir Houmansadr, Thomas Riedl, Nikita Borisov, Andrew Singer*

### **SESSION 8: SHORT TALKS**

OIRS: OUTSOURCED IMAGE RECOVERY SERVICE FROM COMPRESSIVE SENSING  
WITH PRIVACY ASSURANCE ..... 543  
*Cong Wang, Zhen Xu, Kui Ren, Janet Wang*

HOW PRIVACY LEAKS FROM BLUETOOTH MOUSE? ..... 546  
*Xian Pan, Zhen Ling, Aniket Pingley, Wei Yu, Kui Ren, Nan Zhang, Xinwen Fu*

PRACTICAL TIMING SIDE CHANNEL ATTACKS AGAINST KERNEL SPACE ASLR..... 549  
*Ralf Hund, Carsten Willems, Thorsten Holz*

UPDATES FROM THE INTERNET BACKBONE: AN RPKI/RTR ROUTER  
IMPLEMENTATION, MEASUREMENTS, AND ANALYSIS..... 552  
*Matthias Wählisch, Fabian Holler, Thomas C. Schmidt, Jochen Schiller*

A FORMAL FRAMEWORK FOR NETWORK SECURITY DESIGN SYNTHESIS..... 555  
*Mohammad Rahman, Ehab Al-Shaer*

AUTOMATIC PROTOCOL SELECTION IN SECURE TWO-PARTY COMPUTATIONS.....	558
<i>Florian Kerschbaum, Thomas Schneider, Axel Schroepfer</i>	
ASSESSING SOFTWARE INTEGRITY OF VIRTUAL APPLIANCES THROUGH SOFTWARE WHITELISTS: IS IT ANY GOOD? .....	561
<i>Jun Ho Huh, Mirko Montanari, Derek Dagit, Rakesh Bobba, Dong Wook Kim, Yoonjoo Choi, Roy Campbell</i>	
PRIVACY-ENHANCING TECHNOLOGIES FOR MEDICAL TESTS USING GENOMIC DATA.....	564
<i>Erman Ayday, Jean Louis Raisaro, Jean-Pierre Hubaux</i>	
OBLIVISTORE: HIGH PERFORMANCE OBLIVIOUS DISTRIBUTED CLOUD DATA STORE.....	567
<i>Emil Stefanov, Elaine Shi</i>	
A NON-INTERACTIVE DUAL CHANNEL AUTHENTICATION PROTOCOL FOR ASSURING PSUEDO-CONFIDENTIALITY .....	570
<i>David Irakiza, Md Karim, Vir Phoha</i>	
MACROECONOMIC ANALYSIS OF MALWARE.....	573
<i>Vaibhav Garg, L. Jean Camp</i>	
TRANSFORMING AND TAMING PRIVACY-BREACHING ANDROID APPLICATIONS.....	576
<i>Mu Zhang, Heng Yin</i>	

### **WEDNESDAY KEYNOTE**

YOU CAN'T DO TODAY'S SECURITY WITH YESTERDAY'S METHODS .....	578
<i>Joe Sullivan</i>	

### **SESSION 9: PRIVACY AND ANONYMITY**

ONE (BLOCK) SIZE FITS ALL: PIR AND SPIR OVER ARBITRARY-LENGTH RECORDS VIA MULTI-BLOCK PIR QUERIES .....	596
<i>Ryan Henry, Yizhou Huang, Ian Goldberg</i>	
RBRIDGE: USER REPUTATION BASED TOR BRIDGE DISTRIBUTION WITH PRIVACY PRESERVATION .....	614
<i>Qiyang Wang, Zi Lin, Nikita Borisov, Nicholas J. Hopper</i>	
AN EMPIRICAL EVALUATION OF RELAY SELECTION IN TOR.....	633
<i>Christopher Wacek, Henry Tan, Kevin Bauer, Micah Sherr</i>	

### **SESSION 10: ANONYMITY, AUTHENTICATION AND ATTACKS**

LIRA: LIGHTWEIGHT INCENTIVIZED ROUTING FOR ANONYMITY .....	650
<i>Rob Jansen, Aaron Johnson, Paul Syverson</i>	
KINWRITE: HANDWRITING-BASED AUTHENTICATION USING KINECT .....	667
<i>Jing Tian, Chengzhang Qu, Wenyuan Xu, Song Wang</i>	
TAILING RFID TAGS FOR CLONE DETECTION .....	685
<i>Davide Zanetti, Srdjan Capkun, Ari Juels</i>	

ONE BAD APPLE: BACKWARDS COMPATIBILITY ATTACKS ON STATE-OF-THE-ART CRYPTOGRAPHY .....	702
<i>Tibor Jager, Kenneth G. Paterson, Juraj Somorovsky</i>	

DOES COUNTING STILL COUNT? REVISITING THE SECURITY OF COUNTING BASED USER AUTHENTICATION PROTOCOLS AGAINST STATISTICAL ATTACKS.....	721
<i>Hassan Jameel Asghar, Shujun Li, Ron Steinfeld, Josef Pieprzyk</i>	

## **SESSION 11: DISTRIBUTED SYSTEMS SECURITY**

TOWARD ONLINE VERIFICATION OF CLIENT BEHAVIOR IN DISTRIBUTED APPLICATIONS.....	739
<i>Robert A. Cochran, Michael K. Reiter</i>	

CLEAR AND PRESENT DATA: OPAQUE TRAFFIC AND ITS SECURITY IMPLICATIONS FOR THE FUTURE.....	755
<i>A. M. White, S. Krishnan, M. Bailey, F. Monrose, P. Porras</i>	

VERITO: A PRACTICAL SYSTEM FOR TRANSPARENCY AND ACCOUNTABILITY IN VIRTUAL ECONOMIES .....	771
<i>Raghav Bhaskar, Saikat Guha, Srivatsan Laxman, Prasad Naldurg</i>	

SECURE COMPUTATION ON FLOATING POINT NUMBERS .....	785
<i>Mehrdad Aliasgari, Marina Blanton, Yihua Zhang, Aaron Steele</i>	

ANALYZING UNIQUE-BID AUCTION SITES FOR FUN AND PROFIT .....	803
<i>Ory Samorodnitzky, Eran Tromer, Avishai Wool</i>	

## **SESSION 12: NETWORK SECURITY II**

FIX ME UP: REPAIRING ACCESS-CONTROL BUGS IN WEB APPLICATIONS .....	821
<i>Sooel Son, Kathryn S. McKinley, Vitaly Shmatikov</i>	

AUTOMATICALLY INFERRING THE EVOLUTION OF MALICIOUS ACTIVITY ON THE INTERNET .....	837
<i>Shobha Venkataraman, David Brumley, Subhabrata Sen, Oliver Spatscheck</i>	

DETECTION OF MALICIOUS PDF FILES BASED ON HIERARCHICAL DOCUMENT STRUCTURE.....	854
<i>Nedim Šrndić, Pavel Laskov</i>	

BEHIND THE SCENES OF ONLINE ATTACKS: AN ANALYSIS OF EXPLOITATION BEHAVIORS ON THE WEB .....	870
<i>Davide Canali, Davide Balzarotti</i>	

## **Author Index**