

# **Network and Distributed System Security Symposium 2015 (NDSS'15)**

San Diego, California, USA  
8 – 11 February 2015

ISBN: 978-1-7138-2072-7

**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© (2015) 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

## **SESSION 1: WEB SECURITY**

IDENTIFYING CROSS-ORIGIN RESOURCE STATUS USING APPLICATION CACHE .....	1
<i>Sangho Lee, Hyungsub Kim, Jong Kim</i>	
PARKING SENSORS: ANALYZING AND DETECTING PARKED DOMAINS .....	13
<i>Thomas Vissers, Wouter Joosen , Nick Nikiforakis</i>	
SEVEN MONTHS' WORTH OF MISTAKES: A LONGITUDINAL STUDY OF TYPOSQUATTING ABUSE.....	27
<i>Pieter Agten, Wouter Joosen, Frank Piessens , Nick Nikiforakis</i>	
UPGRADING HTTPS IN MID-AIR: AN EMPIRICAL STUDY OF STRICT TRANSPORT SECURITY AND KEY PINNING .....	40
<i>Joseph Bonneau, Michael Kranch</i>	
I DO NOT KNOW WHAT YOU VISITED LAST SUMMER: PROTECTING USERS FROM STATEFUL THIRD-PARTY WEB TRACKING WITH TRACKINGFREE BROWSER.....	55
<i>Xiang Pan , Yinzhi Cao , Yan Chen</i>	

## **SESSION 2: MOBILE SECURITY**

INFORMATION FLOW ANALYSIS OF ANDROID APPLICATIONS IN DROIDS SAFE .....	70
<i>Michael I. Gordon, Deokhwan Kim, Jeff Perkins , Limei Gilham , Nguyen Nguyen , Martin Rinard</i>	
WHAT'S IN YOUR DONGLE AND BANK ACCOUNT? MANDATORY AND DISCRETIONARY PROTECTION OF ANDROID EXTERNAL RESOURCES .....	86
<i>Soteris Demetriou , Xiaoyong Zhou , Muhammad Naveed , Yeonjoon Lee, Kan Yuan, Xiaofeng Wang , Carl A. Gunter</i>	
EDGEMINER: AUTOMATICALLY DETECTING IMPLICIT CONTROL FLOW TRANSITIONS THROUGH THE ANDROID FRAMEWORK.....	101
<i>Yinzhi Cao , Yanick Fratantonio, Antonio Bianchi , Manuel Egele , Christopher Kruegel, Giovanni Vigna , Yan Chen</i>	
COPPERDROID: AUTOMATIC RECONSTRUCTION OF ANDROID MALWARE BEHAVIORS .....	116
<i>Kimberly Tam , Aristide Fattori , Salahuddin J. Khan, Lorenzo Cavallaro</i>	
DEEPDROID: DYNAMICALLY ENFORCING ENTERPRISE POLICY ON ANDROID DEVICES .....	131
<i>xueqiang wang , kun sun , yuewu wang, jiwu jing</i>	

## **SESSION 3: DETECTION, ANALYSIS, PREVENTION & RESPONSE – PART I**

VTINT: PROTECTING VIRTUAL FUNCTION TABLES' INTEGRITY .....	146
<i>Chao Zhang , Chengyu Song , Kevin Zhijie Chen , Zhaofeng Chen , Dawn Song</i>	

PHONEYPOT: DATA-DRIVEN UNDERSTANDING OF TELEPHONY THREATS.....	161
<i>Payas Gupta , Bharat Srinivasan , Vijay Balasubramaniyan ,Mustaque Ahamad</i>	
SECRET: SECURE CHANNEL BETWEEN RICH EXECUTION ENVIRONMENT AND TRUSTED EXECUTION ENVIRONMENT .....	175
<i>Jinsoo Jang, Sunjune Kong, Minsu Kim, Daegyeong Kim,Brent Byunghoon Kang</i>	
FREESENTRY: PROTECTING AGAINST USE-AFTER-FREE VULNERABILITIES DUE TO DANGLING POINTERS .....	190
<i>Yves Younan</i>	
EKHUNTER: A COUNTER-OFFENSIVE TOOLKIT FOR EXPLOIT KIT INFILTRATION .....	205
<i>Birhanu Eshete, Abeer Alhuzali,Maliheh Monshizadeh , Phillip Porras , V.N. Venkatakrishnan , Vinod Yegneswaran</i>	

#### **SESSION 4: PRIVACY – PART I**

MACHINE LEARNING CLASSIFICATION OVER ENCRYPTED DATA.....	220
<i>Raphael Bost, Raluca Ada Popa, Stephen Tu,Shafi Goldwasser</i>	
GRACEWIPE: SECURE AND VERIFIABLE DELETION UNDER COERCION .....	234
<i>Lianying Zhao, Mohammad Mannan</i>	
PRIVACY PRESERVING PAYMENTS IN CREDIT NETWORKS: ENABLING TRUST WITH PRIVACY IN ONLINE MARKETPLACES .....	250
<i>Pedro Moreno-Sanchez, Aniket Kate , Matteo Maffei, Kim Pecina</i>	
CHECKING MORE AND ALERTING LESS: DETECTING PRIVACY LEAKAGES VIA ENHANCED DATA-FLOW ANALYSIS AND PEER VOTING .....	265
<i>Kangjie Lu , Zhichun Li , Vasileios P. Kemerlis , Zhenyu Wu , Long Lu , Cong Zheng , Zhiyun Qian , Wenke Lee ,Guofei Jiang</i>	
DEFY: A DENIABLE, ENCRYPTED FILE SYSTEM FOR LOG-STRUCTURED STORAGE.....	280
<i>Timothy M. Peters , Mark A. Gondree ,Zachary N. J. Peterson</i>	

#### **SESSION 5: DETECTION, ANALYSIS, PREVENTION & RESPONSE – PART II**

PREVENTING USE-AFTER-FREE WITH DANGLING POINTERS NULLIFICATION.....	293
<i>Byoungyoung Lee, Chengyu Song, Yeongjin Jang, Tielei Wang,Taesoo Kim , Long Lu ,Wenke Lee</i>	
STACKARMOR: COMPREHENSIVE PROTECTION FROM STACK-BASED MEMORY ERROR VULNERABILITIES.....	308
<i>Xi Chen, Cristiano Giuffrida, Asia Slowinska, Dennis Andriess,Herbert Bos</i>	
ISOMERON: CODE RANDOMIZATION RESILIENT TO (JUST-IN-TIME) RETURN-ORIENTED PROGRAMMING.....	323
<i>Lucas Davi, Christopher Liebchen,Ahmad-Reza Sadeghi , Kevin Z. Snow, Fabian Monroe</i>	
THWARTING CACHE SIDE-CHANNEL ATTACKS THROUGH DYNAMIC SOFTWARE DIVERSITY .....	338
<i>Stephen Crane, Andrei Homescu, Stefan Brunthaler, Per Larsen,Michael Franz</i>	

## **SESSION 6A: DETECTION, ANALYSIS, PREVENTION & RESPONSE – PART II**

PRINCIPLED SAMPLING FOR ANOMALY DETECTION .....	352
<i>Brendan Juba , Fan Long, Christopher Musco, Stelios Sidiroglou-Douskos,Martin Rinard</i>	
INTEGRATED CIRCUIT (IC) DECAMOUFLAGING: REVERSE ENGINEERING CAMOUFLAGED ICS WITHIN MINUTES .....	366
<i>Mohamed El Massad, Siddharth Garg,Mahesh Tripunitara</i>	
OPAQUE CONTROL-FLOW INTEGRITY .....	380
<i>Vishwath Mohan , Per Larsen,Stefan Brunthaler , Kevin W. Hamlen , Michael Franz</i>	

## **SESSION 6B: PRIVACY – PART II**

BLOOM COOKIES: WEB SEARCH PERSONALIZATION WITHOUT USER TRACKING .....	395
<i>Nitesh Mor , Oriana Riva, Suman Nath ,John Kubiatoiwicz</i>	
NSEC5: PROVABLY PREVENTING DNSSEC ZONE ENUMERATION .....	410
<i>Sharon Goldberg , Moni Naor , Dimitrios Papadopoulos, Leonid Reyzin,Sachin Vasant ,Asaf Ziv</i>	

## **SESSION 7: SOCIAL NETWORKS AND CLOUD SERVICES**

PREDICTING USERS' MOTIVATIONS BEHIND LOCATION CHECK-INS AND UTILITY IMPLICATIONS OF PRIVACY PROTECTION MECHANISMS .....	425
<i>Igor Bilogrevic , Kevin Huguenin, Stefan Mihaila , Reza Shokri ,Jean-Pierre Hubaux</i>	
ON YOUR SOCIAL NETWORK DE-ANONYMIZABILITY: QUANTIFICATION AND LARGE SCALE EVALUATION WITH SEED KNOWLEDGE .....	437
<i>Shouling Ji, Weiqing Li , Neil Z. Gong , Prateek Mittal ,Raheem Beyah</i>	
EFFICIENT RAM AND CONTROL FLOW IN VERIFIABLE OUTSOURCED COMPUTATION.....	452
<i>Riad Wahby , Srinath Setty, Zuocheng Ren,Andrew Blumberg ,Michael Walfish</i>	
INTEGRO: LEVERAGING VICTIM PREDICTION FOR ROBUST FAKE ACCOUNT DETECTION IN OSNS .....	467
<i>Yazan Boshmaf , Dionysios Logothetis, Georgos Siganos , Jorge Rodriguez Leria, Jose Lorenzo ,Matei Ripeanu, Konstantin Beznosov</i>	

## **SESSION 8: AUTHENTICATION**

SPACED REPETITION AND MNEMONICS ENABLE RECALL OF MULTIPLE STRONG PASSWORDS .....	482
<i>Jeremiah Blocki, Saranga Komanduri, Lorrie Cranor,Anupam Datta</i>	
ABY – A FRAMEWORK FOR EFFICIENT MIXED-PROTOCOL SECURE TWO-PARTY COMPUTATION .....	497
<i>Daniel Demmler, Thomas Schneider,Michael Zohner</i>	
PREVENTING LUNCHTIME ATTACKS: FIGHTING INSIDER THREATS WITH EYE MOVEMENT BIOMETRICS .....	512
<i>Simon Eberz, Kasper B. Rasmussen , Vincent Lenders ,Ivan Martinovic</i>	

KNOCK YOURSELF OUT: SECURE AUTHENTICATION WITH SHORT RE-USABLE PASSWORDS.....	525
<i>Benjamin Guldenring, Volker Roth,Lars Ries</i>	

VERIFIED CONTRIBUTIVE CHANNEL BINDINGS FOR COMPOUND AUTHENTICATION .....	539
<i>Karthikeyan Bhargavan, Antoine Delignat-Lavaud,Alfredo Pironti</i>	

### **SESSION 9: WEB SECURITY**

THE DEVIL IS IN THE CONSTANTS: BYPASSING DEFENSES IN BROWSER JIT ENGINES .....	554
<i>Michalis Athanasakis, Elias Athanasopoulos , Michalis Polychronakis , Georgios Portokalidis ,Sotiris Ioannidis</i>	

EXPLOITING AND PROTECTING DYNAMIC CODE GENERATION.....	567
<i>Chengyu Song , Chao Zhang , Tielei Wang, Wenke Lee ,David Melski</i>	

TOO LEJIT TO QUIT: EXTENDING JIT SPRAYING TO ARM .....	582
<i>Wilson Lian, Hovav Shacham,Stefan Savage</i>	

RUN-TIME MONITORING AND FORMAL ANALYSIS OF INFORMATION FLOWS IN CHROMIUM.....	597
<i>Lujo Bauer , Shaoying Cai ,Limin Jia, Timothy Passaro, Michael Stroucken,Yuan Tian</i>	

### **SESSION 10: NETWORK SECURITY**

MIND YOUR BLOCKS: ON THE STEALTHINESS OF MALICIOUS BGP HIJACKS .....	612
<i>Pierre-Antoine Vervier , Olivier Thonnard ,Marc Dacier</i>	

SPHINX: DETECTING SECURITY ATTACKS IN SOFTWARE-DEFINED NETWORKS.....	627
<i>Mohan Dhawan, Rishabh Poddar, Kshiteej Mahajan,Vijay Mann</i>	

SECURING THE SOFTWARE DEFINED NETWORK CONTROL LAYER .....	642
<i>Phillip Porras, Martin Fong, Vinod Yegneswaran, Steven Cheung,Keith Skinner</i>	

POISONING NETWORK VISIBILITY IN SOFTWARE-DEFINED NETWORKS: NEW ATTACKS AND COUNTERMEASURES .....	657
<i>Sungmin Hong, Lei Xu, Haopei Wang,Guofei Gu</i>	

### **SESSION 11: DETECTION, ANALYSIS, PREVENTION & RESPONSE – PART IV**

FIRMALICE – AUTOMATIC DETECTION OF AUTHENTICATION BYPASS VULNERABILITIES IN BINARY FIRMWARE.....	672
<i>Yan Shoshitaishvili, Fish Wang, Christophe Hauser, Christopher Kruegel,Giovanni Vigna</i>	

VFGUARD: STRICT PROTECTION FOR VIRTUAL FUNCTION CALLS IN COTS C++ BINARIES .....	687
<i>Aravind Prakash, Xunchao Hu,Heng Yin</i>	

P2C: UNDERSTANDING OUTPUT DATA FILES VIA ON-THE-FLY TRANSFORMATION FROM PRODUCER TO CONSUMER EXECUTIONS .....	702
<i>Yonghwi Kwon, Fei Peng, Dohyeong Kim, Kyungtae Kim, Xiangyu Zhang,Dongyan Xu , Vinod Yegneswaran ,John Qian</i>	

NO MORE GOTOS: DECOMPILATION USING PATTERN-INDEPENDENT CONTROL-  
FLOW STRUCTURING AND SEMANTIC-PRESERVING TRANSFORMATIONS ..... 716  
*Khaled Yakdan , Sebastian Eschweiler, Elmar Gerhards-Padilla ,Matthew Smith*

**Author Index**