

Network and Distributed System Security Symposium 2014 (NDSS'14)

San Diego, California, USA
23 – 26 February 2014

ISBN: 978-1-7138-2071-0

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© (2014) 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

SESSION 1: NETWORK SECURITY

ON THE MISMANAGEMENT AND MALICIOUSNESS OF NETWORKS	1
<i>Jing Zhang, Zakir Durumeric, Michael Bailey, Manish Karir, Mingyan Liu</i>	
NO DIRECTION HOME: THE TRUE COST OF ROUTING AROUND DECOYS	13
<i>Amir Houmansadr, Edmund Wong, Vitaly Shmatikov</i>	
GAINING CONTROL OF CELLULAR TRAFFIC ACCOUNTING BY SPURIOUS TCP RETRANSMISSION	27
<i>Younghwan Go, Jongil Won, Denis Foo Kune, Eunyong Jeong, Yongdae Kim, Kyoungsoo Park</i>	
CYBERPROBE: TOWARDS INTERNET-SCALE ACTIVE DETECTION OF MALICIOUS SERVERS	42
<i>Antonio Nappa, Zhaoyan Xu, M. Zubair Rafique, Juan Caballero, Guofei Gu</i>	
AMPLIFICATION HELL: REVISITING NETWORK PROTOCOLS FOR DDOS ABUSE	57
<i>Christian Rossow</i>	

SESSION 2: SOFTWARE AND SYSTEM SECURITY

ROPECKER: A GENERIC AND PRACTICAL APPROACH FOR DEFENDING AGAINST ROP ATTACKS	72
<i>Yueqiang Cheng, Zongwei Zhou, Miao Yu, Xuhua Ding, Robert H. Deng</i>	
A TRUSTED SAFETY VERIFIER FOR PROCESS CONTROLLER CODE	86
<i>Stephen McLaughlin, Saman Zonouz, Devin Pohly, Patrick Drew McDaniel</i>	
AVATAR: A FRAMEWORK TO SUPPORT DYNAMIC SECURITY ANALYSIS OF EMBEDDED SYSTEMS' FIRMWARES	101
<i>Jonas Zaddach, Luca Bruno, Aurélien Francillon, Davide Balzarotti</i>	
SAFEDISPATCH: SECURING C++ VIRTUAL CALLS FROM MEMORY CORRUPTION ATTACKS	117
<i>Dongseok Jang, Zachary Tatlock, Sorin Lerner</i>	
HYBRID-BRIDGE: EFFICIENTLY BRIDGING THE SEMANTIC-GAP IN VMI VIA DECOUPLED EXECUTION AND TRAINING MEMOIZATION	132
<i>Alireza Saberi, Yangchun Fu, Zhiqiang Lin</i>	

SESSION 3: SECURITY OF MOBILE DEVICES I

SCREENMILKER: HOW TO MILK YOUR ANDROID SCREEN FOR SECRETS	147
<i>Chia-Chi Lin, Hongyang Li, Xiaoyong Zhou, Xiaofeng Wang</i>	
ACCELPRINT: IMPERFECTIONS OF ACCELEROMETERS MAKE SMARTPHONES TRACKABLE	161
<i>Sanorita Dey, Nirupam Roy, Wenyan Xu, Romit Roy Choudhury, Srihari Nelakuditi</i>	

SMARTPHONES AS PRACTICAL AND SECURE LOCATION VERIFICATION TOKENS FOR PAYMENTS.....	177
<i>Claudio Marforio, Nikolaos Karapanos, Claudio Soriente, Kari Kostianen, Srdjan Capkun</i>	

BREAKING AND FIXING ORIGIN-BASED ACCESS CONTROL IN HYBRID WEB/MOBILE APPLICATION FRAMEWORKS.....	192
<i>Martin Georgiev, Suman Jana, Vitaly Shmatikov</i>	

INSIDE JOB: UNDERSTANDING AND MITIGATING THE THREAT OF EXTERNAL DEVICE MIS-BINDING ON ANDROID	207
<i>Muhammad Naveed, Xiaoyong Zhou, Soteris Demetriou, Xiaofeng Wang, Carl Gunter</i>	

SESSION 4: WEB SECURITY

DSPIN: DETECTING AUTOMATICALLY SPUN CONTENT ON THE WEB.....	221
<i>Qing Zhang, David Y. Wang, Geoffrey M. Voelker</i>	

TOWARD BLACK-BOX DETECTION OF LOGIC FLAWS IN WEB APPLICATIONS	237
<i>Giancarlo Pellegrino, Davide Balzarotti</i>	

MACAROONS: COOKIES WITH CONTEXTUAL CAVEATS FOR DECENTRALIZED AUTHORIZATION IN THE CLOUD.....	252
<i>Arnar Birgisson, Joe Politz, Ulfar Erlingsson, Ankur Taly, Michael Vrable, Mark Lentczner</i>	

DETECTING LOGIC VULNERABILITIES IN E-COMMERCE APPLICATIONS.....	268
<i>Fangqi Sun, Liang Xu, Zhendong Su</i>	

SIMULATION OF BUILT-IN PHP FEATURES FOR PRECISE STATIC CODE ANALYSIS.....	284
<i>Johannes Dahse, Thorsten Holz</i>	

SESSION 5: PRIVACY

ENHANCED CERTIFICATE TRANSPARENCY AND END-TO-END ENCRYPTED MAIL.....	299
<i>Mark D. Ryan</i>	

PRIVACY THROUGH PSEUDONYMITY IN MOBILE TELEPHONY SYSTEMS	313
<i>Loretta Ilaria Mancini, Myrto Arapinis, Mark Ryan, Eike Ritter</i>	

PRIVACY-PRESERVING DISTRIBUTED STREAM MONITORING	327
<i>Arik Friedman, Izchak Sharfman, Daniel Keren, Assaf Schuster</i>	

THE SNIPER ATTACK: ANONYMOUSLY DEANONYMIZING AND DISABLING THE TOR NETWORK	341
<i>Rob Jansen, Florian Tschorsch, Aaron Johnson, Björn Scheuermann</i>	

SELLING OFF USER PRIVACY AT AUCTION	356
<i>Claude Castelluccia, Lukasz Olejnik, Minh-Dung Tran</i>	

SESSION 6: AUTHENTICATION AND IDENTITY I

THE TANGLED WEB OF PASSWORD REUSE	371
<i>Anupam Das, Joseph Bonneau, Matthew Caesar, Nikita Borosiv, Xiaofeng Wang</i>	

ON SEMANTIC PATTERNS OF PASSWORDS AND THEIR SECURITY IMPACT 386
Rafael Veras, Christopher Collins, Julie Thorpe

FROM VERY WEAK TO VERY STRONG: ANALYZING PASSWORD-STRENGTH METERS 402
Xavier De Carné De Carnavalet, Mohammad Mannan

SESSION 7: CRYPTO I

COPKER: COMPUTING WITH PRIVATE KEYS WITHOUT RAM 418
Le Guan, Jingqiang Lin, Bo Luo, Jiwu Jing

PRACTICAL DYNAMIC SEARCHABLE ENCRYPTION WITH SMALL LEAKAGE 433
Emil Stefanov, Charalampos Papamanthou, Elaine Shi

DECENTRALIZED ANONYMOUS CREDENTIALS 448
Christina Garman, Matthew Green, Ian Miers

DYNAMIC SEARCHABLE ENCRYPTION IN VERY-LARGE DATABASES: DATA
STRUCTURES AND IMPLEMENTATION 463
*David Cash, Joseph Jaeger, Stanislaw Jarecki, Charanjit Jutla, Hugo Krawczyk, Marcel
Rosu, Michael Steiner*

SESSION 8: AUTHENTICATION AND IDENTITY II

AUTHENTICATION USING PULSE-RESPONSE BIOMETRICS 479
Kasper B. Rasmussen, Marc Roeschlin, Ivan Martinovic, Gene Tsudik

HARDENING PERSONA – IMPROVING FEDERATED WEB LOGIN 493
Michael Dietz, Dan S. Wallach

TWO-FACTOR AUTHENTICATION RESILIENT TO SERVER COMPROMISE USING MIX-
BANDWIDTH DEVICES..... 508
Maliheh Shirvanian, Stanislaw Jarecki, Nitesh Saxena, Naveen Nathan

LEVERAGING USB TO ESTABLISH HOST IDENTITY USING COMMODITY DEVICES 524
Adam Bates, Ryan Leonard, Hannah Pruse, Kevin Butler, Daniel Lowd

SESSION 9: NEW APPLICATIONS, ATTACKS, AND SECURITY ECONOMICS

PLACEVOIDER: STEERING FIRST-PERSON CAMERAS AWAY FROM SENSITIVE
SPACES 538
Robert Templeman, Mohammed Korayem, David Crandall, Apu Kapadia

AUDITABLE VERSION CONTROL SYSTEMS 553
Bo Chen, Reza Curtmola

POWER ATTACK: AN INCREASING THREAT TO DATA CENTERS 569
Zhang Xu, Haining Wang, Zichen Xu, Xiaorui Wang

SCAMBAITER: UNDERSTANDING TARGETED NIGERIAN SCAMS ON CRAIGSLIST 584
Youngsam Park, Jackie Jones, Damon McCoy, Elaine Shi, Markus Jakobsson

BOTCOIN: MONETIZING STOLEN CYCLES	599
<i>Danny Yuxing Huang, Hitesh Dharmdasani, Sarah Meiklejohn, Vacha Dave, Chris Grier, Damon McCoy, Stefan Savage, Alex C. Snoeren, Nicholas Weaver, Kirill Levchenko</i>	

SESSION 10: SECURITY OF MOBILE DEVICES II

A MACHINE-LEARNING APPROACH FOR CLASSIFYING AND CATEGORIZING ANDROID SOURCES AND SINKS.....	615
<i>Steven Arzt, Siegfried Rasthofer, Eric Bodden</i>	

AIRBAG: BOOSTING SMARTPHONE RESISTANCE TO MALWARE INFECTION.....	630
<i>Chiachih Wu, Yajin Zhou, Kunal Patel, Zhenkai Liang, Xuxian Jiang</i>	

SMV-HUNTER: LARGE SCALE, AUTOMATED DETECTION OF SSL/TLS MAN-IN-THE-MIDDLE VULNERABILITIES IN ANDROID APPS	643
<i>David Sounthiraraj, Justin Sahs, Zhiqiang Lin, Latifur Khan, Garrett Greenwood</i>	

APPSEALER: AUTOMATIC GENERATION OF VULNERABILITY-SPECIFIC PATCHES FOR PREVENTING COMPONENT HIJACKING ATTACKS IN ANDROID APPLICATIONS	657
<i>Mu Zhang, Heng Yin</i>	

EXECUTE THIS! ANALYZING UNSAFE AND MALICIOUS DYNAMIC CODE LOADING IN ANDROID APPLICATIONS	672
<i>Sebastian Poelplau, Yanick Fratantonio, Antonio Bianchi, Christopher Kruegel, Giovanni Vigna</i>	

SESSION 11: MALWARE

NAZCA: DETECTING MALWARE DISTRIBUTION IN LARGE-SCALE NETWORKS	688
<i>Luca Invernizzi, Stanislav Miskovic, Ruben Torres, Sabyasachi Saha, Sij Lee, Marco Mellia, Christopher Kruegel, Giovanni Vigna</i>	

PERSISTENT DATA-ONLY MALWARE: FUNCTION HOOKS WITHOUT CODE.....	704
<i>Sebastian Vogl, Jonas Pföh, Thomas Kittel, Claudia Eckert</i>	

DREBIN: EFFECTIVE AND EXPLAINABLE DETECTION OF ANDROID MALWARE IN YOUR POCKET	720
<i>Daniel Arp, Michael Spreitzenbarth, Malte Hübner, Hugo Gascon, Konrad Rieck</i>	

GYRUS: A FRAMEWORK FOR USER-INTENT MONITORING OF TEXT-BASED NETWORKED APPLICATIONS	732
<i>Yeongjin Jang, Simon P. Chung, Bryan D. Payne, Wenke Lee</i>	

NEURAL SIGNATURES OF USER-CENTERED SECURITY: AN FMRI STUDY OF PHISHING, AND MALWARE WARNINGS.....	748
<i>Ajaya Neupane, Nitesh Saxena, Keya Kuruvilla, Michael Georgescu, Rajesh Kana</i>	

SESSION 12: CRYPTO II

WEB PKI: CLOSING THE GAP BETWEEN GUIDELINES AND PRACTICES	764
<i>Antoine Delignat-Lavaud, Martín Abadi, Andrew Birrell, Ilya Mironov, Ted Wobber, Yinglian Xie</i>	

EFFICIENT PRIVATE FILE RETRIEVAL BY COMBINING ORAM AND PIR.....	779
<i>Travis Mayberry, Erik-Oliver Blass, Agnes Hui Chan</i>	
PRACTICAL KNOWN-PLAINTEXT ATTACKS AGAINST PHYSICAL LAYER SECURITY IN WIRELESS MIMO SYSTEMS	790
<i>Matthias Schulz, Adrian Loch, Matthias Hollick</i>	
PRACTICAL ISSUES WITH TLS CLIENT CERTIFICATE AUTHENTICATION.....	803
<i>Arnis Parsovs</i>	

Author Index