

Network and Distributed System Security Symposium 2012 (NDSS'12)

San Diego, California, USA
5 – 8 February 2012

ISBN: 978-1-7138-2066-6

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© (2012) 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: NETWORKING 1

PLAIN-TEXT RECOVERY ATTACKS AGAINST DATAGRAM TLS.....	1
<i>Kenneth Paterson, Nadhem Alfordan</i>	
ANDANA: ANONYMOUS NAMED DATA NETWORKING APPLICATION	19
<i>Steven Dibenedetto, Paolo Gasti, Gene Tsudik, Ersin Uzun</i>	
PERSISTENT OSPF ATTACKS	37
<i>Gabi Nakibly, Alex Kirshon, Dima Gonikman, Dan Boneh</i>	

SESSION 2: SOCIAL NETWORKS AND USER BEHAVIOR I

YOU ARE WHAT YOU LIKE! INFORMATION LEAKAGE THROUGH USERS' INTERESTS	48
<i>Abdelberi Chaabane, Gergely Acs, Mohamed Ali Kaafar</i>	
X-VINE: SECURE AND PSEUDONYMOUS ROUTING IN DHTS USING SOCIAL NETWORKS.....	70
<i>Prateek Mittal, Matthew Caesar, Nikita Borisov</i>	
TOWARDS ONLINE SPAM FILTERING IN SOCIAL NETWORKS.....	87
<i>Hongyu Gao, Yan Chen, Kathy Lee, Diana Palsetia, Alok Choudhary</i>	

SESSION 3: MOBILE NETWORKS

LOCATION LEAKS OVER THE GSM AIR INTERFACE	103
<i>Denis Foo Kune, John Koelndorfer, Nicholas Hopper, Yongdae Kim</i>	
TRACK ME IF YOU CAN: ON THE EFFECTIVENESS OF CONTEXT-BASED IDENTIFIER CHANGES IN DEPLOYED MOBILE NETWORKS.....	113
<i>Laurent Bindschaedler, Murtuza Jadliwala, Igor Bilogrevic, Imad Aad, Philip Ginzboorg, Valteri Niemi, Jean-Pierre Hubaux</i>	
YOU CAN RUN, BUT YOU CAN'T HIDE: EXPOSING NETWORK LOCATION FOR TARGETED DOS ATTACKS IN CELLULAR NETWORKS.....	130
<i>Zhiyun Qian, Zhaoguang Wang, Qiang Xu, Z. Morley Mao, Ming Zhang, Yi-Min Wang</i>	
WEAPONIZING FEMTOCELLS: THE EFFECT OF ROGUE DEVICES ON MOBILE TELECOMMUNICATIONS	146
<i>Nico Golde, Kévin Redon, Ravishankar Borgaonkar</i>	

SESSION 4: CLOUDS/CRYPTO

PRIVACY-PRESERVING LOGARITHMIC-TIME SEARCH ON ENCRYPTED DATA IN CLOUD	154
<i>Yanbin Lu</i>	

LARGE-SCALE PRIVACY-PRESERVING MAPPING OF HUMAN GENOMIC SEQUENCES ON HYBRID CLOUDS	162
<i>Yangyi Chen, Bo Peng, Xiaofeng Wang, Haixu Tang</i>	
MAKING ARGUMENT SYSTEMS FOR OUTSOURCED COMPUTATION PRACTICAL (SOMETIMES)	180
<i>Srinath Setty, Richard Mcpherson, Andrew Blumberg, Michael Walfish</i>	
TOWARDS PRACTICAL OBLIVIOUS RAM.....	200
<i>Emil Stefanov, Elaine Shi, Dawn Song</i>	

SESSION 5: SOCIAL NETWORKS AND APPLICATION SECURITY

HUBBLE: TRANSPARENT AND EXTENSIBLE MALWARE ANALYSIS BY COMBINING HARDWARE VIRTUALIZATION AND SOFTWARE EMULATION.....	219
<i>Lok Yan, Manjukumar Jayachandra, Mu Zhang, Heng Yin</i>	
FREEMARKET: SHOPPING FOR FREE IN ANDROID APPLICATIONS.....	220
<i>Daniel Reynaud, Dawn Song, Tom Magrino, Edward Wu, Richard Shin</i>	
DISTANCE HIJACKING ATTACKS ON DISTANCE BOUNDING PROTOCOLS	221
<i>Cas Cremers, Kasper Bonne Rasmussen, Srdjan Capkun</i>	
THROTTLING TOR BANDWIDTH PARASITES	222
<i>Rob Jansen, Nicholas Hopper, Paul Syverson</i>	
TAKING ROUTERS OFF THEIR MEDS: WHY ASSUMPTIONS OF ROUTER STABILITY ARE DANGEROUS	223
<i>Maxfield Schuchard, Christopher Thompson, Nicholas Hopper, Yongdae Kim</i>	
NEWTON MEETS VIVALDI: USING PHYSICAL LAWS TO SECURE VIRTUAL COORDINATE SYSTEMS	224
<i>Jeff Seibert, Sheila Becker, Cristina Nita-Rotaru, Radu State</i>	
CHARM: A FRAMEWORK FOR RAPIDLY PROTOTYPING CRYPTOSYSTEMS.....	225
<i>Joseph A. Akinyele, Matthew D. Green, Aviel D. Rubin</i>	
ABUSE DETECTION AND PREVENTION SYSTEMS AT A LARGE SCALE VIDEO SHARING WEBSITE.....	226
<i>Yu-To Chen, Pierre Grinspan, Blake Livingston, Palash Nandy, Brian Palmer</i>	

SESSION 6: APPLIED CRYPTO

ACCESS PATTERN DISCLOSURE ON SEARCHABLE ENCRYPTION: RAMIFICATION, ATTACK AND MITIGATION	227
<i>Mohammad Islam, Mehmet Kuzu, Murat Kantarcioglu</i>	
ON LIMITATIONS OF DESIGNING LEAKAGE-RESILIENT PASSWORD SYSTEMS: ATTACKS, PRINCIPALS AND USABILITY	242
<i>Qiang Yan, Jin Han, Yingjiu Li, Robert H. Deng</i>	
ADAPTIVE PASSWORD-STRENGTH METERS FROM MARKOV MODELS.....	258
<i>Claude Castelluccia, Markus Duermuth, Daniele Perito</i>	

PRIVATE SET INTERSECTION: ARE GARBLED CIRCUITS BETTER THAN CUSTOM PROTOCOLS?	272
<i>Yan Huang, David Evans, Jonathan Katz</i>	

SESSION 7: SMARTPHONES

GUESS WHO'S TEXTING YOU? EVALUATING THE SECURITY OF SMARTPHONE MESSAGING APPLICATIONS	284
<i>Sebastian Schrittwieser, Peter Frühwirt, Peter Kieseberg, Manuel Leithner, Martin Mulazzani, Markus Huber, Edgar Weippl</i>	

MOCFI: A FRAMEWORK TO MITIGATE CONTROL-FLOW ATTACKS ON SMARTPHONES.....	293
<i>Lucas Davi, Alexandra Dmitrienko, Manuel Egele, Thomas Fischer, Thorsten Holz, Ralf Hund, Stefan Nürnberg, Ahmad-Reza Sadeghi</i>	

TOWARDS TAMING PRIVILEGE-ESCALATION ATTACKS ON ANDROID	310
<i>Sven Bugiel, Lucas Davi, Alexandra Dmitrienko, Thomas Fischer, Ahmad-Reza Sadeghi, Bhargava Shastry</i>	

SYSTEMATIC DETECTION OF CAPABILITY LEAKS IN STOCK ANDROID SMARTPHONES.....	330
<i>Michael Grace, Yajin Zhou, Zhi Wang, Xuxian Jiang</i>	

HEY, YOU, GET OFF OF MY MARKET: DETECTING MALICIOUS APPS IN OFFICIAL AND ALTERNATIVE ANDROID MARKETS	343
<i>Yajin Zhou, Zhi Wang, Wu Zhou, Xuxian Jiang</i>	

SESSION 8: SOCIAL NETWORKS AND USER BEHAVIOR II

INSIGHTS INTO USER BEHAVIOR IN DEALING WITH INTERNET ATTACKS.....	355
<i>Kaan Onarlioglu, Utku Ozan Yilmaz, Engin Kirda, Davide Balzarotti</i>	

PATHCUTTER: SEVERING THE SELF-PROPAGATION PATH OF XSS JAVASCRIPT WORMS IN SOCIAL WEB NETWORKS	368
<i>Yinzhi Cao, Vinod Yegneswaran, Phillip Porras, Yan Chen</i>	

THE LATENT COMMUNITY MODEL FOR DETECTING SYBILS IN SOCIAL NETWORKS.....	383
<i>Zhuhua Cai, Christopher Jermaine</i>	

SESSION 9: PRIVACY AND ANONYMITY

BLACR: TTP-FREE BLACKLISTABLE ANONYMOUS CREDENTIALS WITH REPUTATION.....	399
<i>Man Ho Au, Apu Kapadia, Willy Susilo</i>	

ACCOUNTABLE WIRETAPPING -OR- I KNOW THEY CAN HEAR YOU NOW.....	408
<i>Adam Bates, Kevin Butler, Micah Sherr, Clay Shields, Patrick Traynor, Dan Wallach</i>	

SHADOW: RUNNING TOR IN A BOX FOR ACCURATE AND EFFICIENT EXPERIMENTATION	418
<i>Rob Jansen, Nicholas Hopper</i>	

SESSION 10: HOST SECURITY

DISCOVERING SEMANTIC DATA OF INTEREST FROM UN-MAPPABLE MEMORY WITH CONFIDENCE.....	436
<i>Zhiqiang Lin, Junghwan Rhee, Chao Wu, Xiangyu Zhang, Dongyan Xu</i>	
SECURESWITCH: BIOS-ASSISTED ISOLATION AND SWITCH BETWEEN TRUSTED AND UNTRUSTED COMMODITY OSES.....	447
<i>Kun Sun, Jiang Wang, Fengwei Zhang, Angelos Stavrou</i>	
SMART: SECURE AND MINIMAL ARCHITECTURE FOR (ESTABLISHING DYNAMIC) ROOT OF TRUST	462
<i>Karim Eldefrawy, Gene Tsudik, Aurélien Francillon, Daniele Perito</i>	
KRUISER: SEMI-SYNCHRONIZED NON-BLOCKING CONCURRENT KERNEL HEAP BUFFER OVERFLOW MONITORING	473
<i>Donghai Tian, Qiang Zeng, Dinghao Wu, Peng Liu, Changzhen Hu</i>	

SESSION 11: WEB

WARNINGBIRD: DETECTING SUSPICIOUS URLS IN TWITTER STREAM	486
<i>Sangho Lee, Jong Kim</i>	
USING REPLICATED EXECUTION FOR A MORE SECURE AND RELIABLE WEB BROWSER.....	499
<i>Hui Xue, Nathan Dautenhahn, Samuel King</i>	
HOST FINGERPRINTING AND TRACKING ON THE WEB: PRIVACY AND SECURITY IMPLICATIONS.....	513
<i>Ting-Fang Yen, Yinglian Xie, Fang Yu, Roger Peng Yu, Martin Abadi</i>	
CHROME EXTENSIONS: THREAT ANALYSIS AND COUNTERMEASURES.....	529
<i>Lei Liu, Xinwen Zhang, Guanhua Yan, Songqing Chen</i>	

SESSION 12: NETWORKING II

GHOST DOMAIN NAMES: REVOKED YET STILL RESOLVABLE	543
<i>Jian Jiang, Jinjin Liang, Kang Li, Jun Li, Haixin Duan, Jianping Wu</i>	
SHORTMAC: EFFICIENT DATA-PLANE FAULT LOCALIZATION.....	556
<i>Xin Zhang, Zongwei Zhou, Hsu-Chun Hsiao, Tiffany Hyun-Jin Kim, Adrian Perrig, Patrick Tague</i>	
BYPASSING SPACE EXPLOSION IN REGULAR EXPRESSION MATCHING FOR NETWORK INTRUSION DETECTION AND PREVENTION SYSTEMS	564
<i>Jignesh Patel, Alex Liu, Eric Torng</i>	
THE CASE FOR PREFETCHING AND PREVALIDATING TLS SERVER CERTIFICATES	572
<i>Emily Stark, Lin-Shung Huang, Dinesh Israni, Collin Jackson, Dan Boneh</i>	

SESSION 13: DISTRIBUTED SYSTEMS

GATLING: AUTOMATIC ATTACK DISCOVERY IN LARGE-SCALE DISTRIBUTED SYSTEMS..... 594

Hyojeong Lee, Jeff Seibert, Charles Killian, Cristina Nita-Rotaru

AUTOMATED SYNTHESIS OF SECURE DISTRIBUTED APPLICATIONS..... 611

Michael Backes, Matteo Maffei, Kim Pecina

SESSION 14: SOFTWARE

A GENERAL APPROACH FOR EFFICIENTLY ACCELERATING SOFTWARE-BASED DYNAMIC DATA FLOW TRACKING ON COMMODITY HARDWARE..... 627

Kangkook Jee, Georgios Portokalidis, Vasileios P. Kemerlis, Soumyadeep Ghosh, David I.

August, Angelos D. Keromytis

STATIC DETECTION OF C++ VTABLE ESCAPE VULNERABILITIES IN BINARY CODE..... 649

David Dewey, Jon Giffin

IDENTIFYING AND ANALYZING POINTER MISUSES FOR SOPHISTICATED MEMORY-CORRUPTION EXPLOIT DIAGNOSIS..... 660

Mingwei Zhang, Aravind Prakash, Xiaolei Li, Zhenkai Liang, Heng Yin

Author Index