

2016 11th International Conference on Malicious and Unwanted Software (MALWARE 2016)

**Fajardo, Puerto Rico, USA
18-21 October 2016**



**IEEE Catalog Number: CFP1659F-POD
ISBN: 978-1-5090-4543-3**

**Copyright © 2016 by the Institute of Electrical and Electronics Engineers, Inc
All Rights Reserved**

Copyright and Reprint Permissions: Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

****** This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP1659F-POD
ISBN (Print-On-Demand):	978-1-5090-4543-3
ISBN (Online):	978-1-5090-4542-6

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
E-mail: curran@proceedings.com
Web: www.proceedings.com

CURRAN ASSOCIATES INC.
proceedings
.com

TABLE OF CONTENTS

Session 1 – Emerging Threats and Malware Classification

Reverse Engineering with Bioinformatics Algorithms over a Sound Android Covert Channel	3
<i>Sergio Ivan Vargas Razo, Eleazar Aguirre Anaya and Ponciano Jorge Escamilla Ambrosio</i>	
Dissecting Developer Policy Violating Apps: Characterization and Detection	10
<i>Su Mon Kywe, Yingjiu Li, Jason Hong and Cheng Yao</i>	
Impact of Base Transceiver Station Selection Mechanisms on a Mobile Botnet over a LTE Network	20
<i>Asem Kitana, Issa Traore and Isaac Woungang</i>	

Session 2 – Broad Spectrum Malware, Defense Strategies and Mechanisms

RePEconstruct: Reconstructing Binaries with Self-Modifying Code and Import Address Table Destruction	31
<i>David Korczynski</i>	
CARDINAL: Similarity Analysis to Defeat Malware Compiler Variations	39
<i>Luke Jones, Andrew Sellers and Martin Carlisle</i>	
Automatic Extraction of Malicious Behaviors	47
<i>Khanh-Huu-The Dam and Tayssir Touili</i>	

Session 3 – Mobile Malware, Detection and Thwarting

SigPID: Significant Permission Identification for Android Malware Detection	59
<i>Lichao Sun, Zhiqiang Li, Qiben Yan, Witawas Srisa-an and Yu Pan</i>	
Native Malware Detection in Smartphones with Android OS using Static Analysis, Feature Selection and Ensemble Classifiers	67
<i>S. Morales-Ortega, P.J. Escamilla-Ambrosio, A. Rodríguez-Mota and L.D. Coronado-De-Alba</i>	
On the Effectiveness of Application Characteristics in the Automatic Classification of Malware on Smartphones	75
<i>Matthew Ping, Bander Alsulami and Spiros Mancoridis</i>	

Session 4 – Offense, Defense, and Malware Provenance

On Periodic Behavior of Malware: Experiments, Opportunities and Challenges	85
<i>Ngoc Anh Huynh, Wee-Keong Ng and Hoang Giang Do</i>	
A Covert Data Transport Protocol	93
<i>Yu Fu, Zhe Jia, Lu Yu and Richard Brooks</i>	
Malware Provenance: Code Reuse Detection in Malicious Software at Scale	101
<i>Jason Upchurch and Xiaobo Zhou</i>	

Session 5 – Malware: The Emergence of New Threats and the Analysis of Old Friends

ZoneDroid: Control your Droid through Application Zoning	113
<i>Md Shahrear Iqbal and Mohammad Zulkernine</i>	
Advanced Transcriptase for JavaScript Malware	121
<i>Fabio Di Troia, Corrado Aaron Visaggio, Thomas H. Austin and Mark Stamp</i>	
Anti-Analysis Trends in Banking Malware	129
<i>Paul Black and Joseph Opacki</i>	

Session 6 – Mechanisms and Strategies to Detect Mobile Malware

DySign: Dynamic Fingerprinting for the Automatic Detection of Android Malware	139
<i>ElMouatez Billah Karbab, Mourad Debbabi, Saed Alrabaee and Djedjiga Mouheb</i>	
Signature Limits: An Entire Map of Clone Features and their Discovery in Nearly Linear Time	147
<i>William Casey and Aaron Shelmire</i>	
Function Identification and Recovery Signature Tool	157
<i>Angel M. Villegas</i>	