

2017 12th International Conference on Malicious and Unwanted Software (MALWARE 2017)

**Fajardo, Puerto Rico, USA
11-14 October 2017**



**IEEE Catalog Number: CFP1759F-POD
ISBN: 978-1-5386-2592-7**

**Copyright © 2017 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:	CFP1759F-POD
ISBN (Print-On-Demand):	978-1-5386-2592-7
ISBN (Online):	978-1-5386-1436-5

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

KALI: Scalable Encryption Fingerprinting in Dynamic Malware Traces	3
<i>Lorenzo De Carli, Ruben Torres, Gaspar Modelo-Howard, Alok Tongaonkar and Somesh Jha</i>	
Mining Malware Secrets	11
<i>Arun Lakhotia and Paul Black</i>	
Rootkit Detection through Phase-Space Analysis of Power Voltage Measurements	19
<i>Joel A. Dawson, J. Todd McDonald, Jordan Shropshire, Todd R. Andel, Patrick Luckett and Lee Hively</i>	

Session 2 – Malware in the Times of Mobile Devices

Android Malware Family Classification based on Resource Consumption over Time	31
<i>Luca Massarelli, Leonardo Aniello, Claudio Ciccotelli, Leonardo Querzoni, Daniele Ucci and Roberto Baldoni</i>	
GPFinder – Tracking the Invisible in Android Malware	39
<i>Mourad Leslous, Valérie Viet Triem Tong, Jean-François Lalande and Thomas Genet</i>	
Behavioral Anomaly Detection of Malware on Home Routers	47
<i>Ni An, Alexander Duff, Gaurav Naik, Michalis Faloutsos, Steven Weber and Spiros Mancoridis</i>	

Session 3 – Evolution of Our Defense Strategies – How Can We Win?

Phantom I/O Projector: Entrapping Malware on Machines in Production	57
<i>Julian L. Rrushi</i>	
Preliminary Study of Fission Defenses Against Low-Volume DoS Attacks on Proxied Multiserver Systems	67
<i>Yuquan Shan, George Kesidis, Daniel Fleck and Angelos Stavrou</i>	
Lightweight Behavioral Malware Detection for Windows Platforms	75
<i>Bander Alsulami, Avinash Srinivasan, Hunter Dong and Spiros Mancoridis</i>	

Session 4 – Malware, Industrial Control Systems and Defenses in the Age of "Internet of Things"

A Virtual Testbed for Security Management of Industrial Control Systems	85
<i>Venkata S. Koganti, Mohammad Ashrafuzzaman, Ananth A. Jillepalli and Frederick T. Sheldon</i>	

TARN: A SDN-Based Traffic Analysis Resistant Network Architecture	91
<i>Lu Yu, Qing Wang, Geddings Barrineau, Jon Oakley, Richard R. Brooks and Kuang-Ching Wang</i>	
A Construction of a Self-Modifying Language with a Formal Correction Proof	99
<i>Guillaume Bonfante, Hubert Godfroy and Jean-Yves Marion</i>	

Session 6 – Theoretical Approaches for Malware Detection

What can N-Grams Learn for Malware Detection?	109
<i>Richard Zak, Edward Raff and Charles Nicholas</i>	
Efficient Fuzzy Extractor Implementations for PUF based Authentication	119
<i>Yuejiang Wen and Yingjie Lao</i>	
Predicting Signatures of Future Malware Variants	126
<i>Michael Howard, Avi Pfeffer, Mukesh Dalal and Michael Reposa</i>	