

**2015 4th International Workshop
on Building Analysis Datasets
and Gathering Experience
Returns for Security
(BADGERS 2015)**

**Kyoto, Japan
5 November 2015**



**IEEE Catalog Number: CFP15B98-POD
ISBN: 978-1-4673-8945-7**

**Copyright © 2015 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 publication is a representation of what appears in the IEEE Digital Libraries. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP15B98-POD
ISBN (Print-On-Demand):	978-1-4673-8945-7
ISBN (Online):	978-1-4673-8944-0

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

2015 4th International Workshop on Building Analysis Datasets and Gathering Experience Returns for Security

BADGERS 2015

Table of Contents

Preface.....	vii
Conference Organization.....	viii
Program Committee.....	ix
Sponsors.....	x

Network Monitoring

Tracking Network Events with Write Optimized Data Structures	1
<i>Nolan P. Donoghue, Bridger Hahn, Helen Xu, Thomas M. Kroeger, David Zage, and Rob Johnson</i>	
MAD: A Middleware Framework for Multi-step Attack Detection	8
<i>Panagiotis Papadopoulos, Thanasis Petsas, Giorgos Christou, and Giorgos Vasiliadis</i>	
INTERCEPT+: SDN Support for Live Migration-Based Honeypots	16
<i>Ayumu Hirata, Daisuke Miyamoto, Masaya Nakayama, and Hiroshi Esaki</i>	

Network Analytics

The Significant Features of the UNSW-NB15 and the KDD99 Data Sets for Network Intrusion Detection Systems	25
<i>Nour Moustafa and Jill Slay</i>	
Using Bayesian Decision Making to Detect Slow Scans	32
<i>Ichiro Shimada, Yu Tsuda, Masashi Eto, and Daisuke Inoue</i>	
DGA Bot Detection with Time Series Decision Trees	42
<i>Anaël Bonneton, Daniel Migault, Stephane Senecal, and Nizar Kheir</i>	

User Analytics

Social Forensics: Searching for Needles in Digital Haystacks	54
<i>Iasonas Polakis, Panagiotis Ilia, Zacharias Tzermias, Sotiris Ioannidis, and Paraskevi Fragopoulou</i>	
Text-Mining Approach for Estimating Vulnerability Score	67
<i>Yasuhiro Yamamoto, Daisuke Miyamoto, and Masaya Nakayama</i>	
AJNA: Anti-phishing JS-based Visual Analysis, to Mitigate Users' Excessive Trust in SSL/TLS	74
<i>Pernelle Mensah, Gregory Blanc, Kazuya Okada, Daisuke Miyamoto, and Youki Kadobayashi</i>	
Author Index	85