

PROCEEDINGS OF SPIE

Cyber Sensing 2013

Igor V. Ternovskiy
Peter Chin
Editors

30 April –1 May 2013
Baltimore, Maryland, United States

Sponsored and Published by
SPIE

Volume 8757

Proceedings of SPIE 0277-786X, V. 8757

SPIE is an international society advancing an interdisciplinary approach to the science and application of light.

Cyber Sensing 2013, edited by Igor V. Ternovskiy, Peter Chin, Proc. of SPIE Vol. 8757, 875701
© 2013 SPIE · CCC code: 0277-786X/13/\$18 · doi: 10.1117/12.2032137

Proc. of SPIE Vol. 8757 875701-1

The papers included in this volume were part of the technical conference cited on the cover and title page. Papers were selected and subject to review by the editors and conference program committee. Some conference presentations may not be available for publication. The papers published in these proceedings reflect the work and thoughts of the authors and are published herein as submitted. The publisher is not responsible for the validity of the information or for any outcomes resulting from reliance thereon.

Please use the following format to cite material from this book:

Author(s), "Title of Paper," in *Cyber Sensing 2013*, edited by Igor V. Ternovskiy, Peter Chin, Proceedings of SPIE Vol. 8757 (SPIE, Bellingham, WA, 2013) Article CID Number.

ISSN: 0277-786X

ISBN: 9780819495488

Published by

SPIE

P.O. Box 10, Bellingham, Washington 98227-0010 USA

Telephone +1 360 676 3290 (Pacific Time) · Fax +1 360 647 1445

SPIE.org

Copyright © 2013, Society of Photo-Optical Instrumentation Engineers.

Copying of material in this book for internal or personal use, or for the internal or personal use of specific clients, beyond the fair use provisions granted by the U.S. Copyright Law is authorized by SPIE subject to payment of copying fees. The Transactional Reporting Service base fee for this volume is \$18.00 per article (or portion thereof), which should be paid directly to the Copyright Clearance Center (CCC), 222 Rosewood Drive, Danvers, MA 01923. Payment may also be made electronically through CCC Online at copyright.com. Other copying for republication, resale, advertising or promotion, or any form of systematic or multiple reproduction of any material in this book is prohibited except with permission in writing from the publisher. The CCC fee code is 0277-786X/13/\$18.00.

Printed in the United States of America.

Publication of record for individual papers is online in the SPIE Digital Library.



SPIDigitalLibrary.org

Paper Numbering: Proceedings of SPIE follow an e-First publication model, with papers published first online and then in print and on CD-ROM. Papers are published as they are submitted and meet publication criteria. A unique, consistent, permanent citation identifier (CID) number is assigned to each article at the time of the first publication. Utilization of CIDs allows articles to be fully citable as soon as they are published online, and connects the same identifier to all online, print, and electronic versions of the publication. SPIE uses a six-digit CID article numbering system in which:

- The first four digits correspond to the SPIE volume number.
- The last two digits indicate publication order within the volume using a Base 36 numbering system employing both numerals and letters. These two-number sets start with 00, 01, 02, 03, 04, 05, 06, 07, 08, 09, 0A, 0B ... 0Z, followed by 10-1Z, 20-2Z, etc.

The CID Number appears on each page of the manuscript. The complete citation is used on the first page, and an abbreviated version on subsequent pages. Numbers in the index correspond to the last two digits of the six-digit CID Number.

Contents

v *Conference Committee*

ANALYSIS OF CYBER ATTACKS

- 8757 03 **On localization attacks against cloud infrastructure** [8757-2]
L. Ge, W. Yu, M. A. Sistani, Towson Univ. (United States)
- 8757 04 **Quantitative analysis of intrusion detection systems: Snort and Suricata** [8757-20]
J. S. White, T. Fitzsimmons, J. N. Matthews, Clarkson Univ. (United States)
- 8757 05 **ICS logging solution for network-based attacks using Gumistix technology** [8757-3]
J. R. Otis, D. Berman, J. Butts, J. Lopez Jr., Air Force Institute of Technology (United States)

SECURITY OF INTERNET AND CLOUDS

- 8757 08 **A framework for network-wide semantic event correlation** [8757-8]
R. T. Hall, J. Taylor, Assured Information Security, Inc. (United States)
- 8757 09 **Efficient identity management and access control in cloud environment** [8757-9]
J. Gloster, Van Dyke Technology Group, Inc. (United States)
- 8757 0A **Software analysis in the semantic web** [8757-10]
J. Taylor, R. T. Hall, Assured Information Security, Inc. (United States)

NOVEL CYBER SENSORS

- 8757 0B **Remote suspect identification and the impact of demographic features on keystroke dynamics** [8757-12]
R. A. Dora, P. D. Schalk, J. E. McCarthy, S. A. Young, Assured Information Security, Inc. (United States)
- 8757 0D **Dynamic malware analysis using IntroVirt: a modified hypervisor-based system** [8757-14]
J. S. White, S. R. Pape, A. T. Meily, R. M. Gloo, Assured Information Security, Inc. (United States)

NOVEL ALGORITHMS FOR CYBER SENSING

- 8757 0F **Performance comparison of the Prophecy (forecasting) Algorithm in FFT form for unseen feature and time-series prediction** [8757-16]
H. Jaenisch, Licht Strahl Engineering, Inc. (United States) and Johns Hopkins Univ. (United States); J. Handley, Licht Strahl Engineering, Inc. (United States)

- 8757 0G **A multi-resolution fractal additive scheme for blind watermarking of 3D point data** [8757-17]
M. Rahmes, K. Wilder, K. Fox, Harris Corp. (United States)

ALGORITHMS FOR ATTACK DETECTION

- 8757 0H **A study of malware detection on smart mobile devices** [8757-21]
W. Yu, H. Zhang, G. Xu, Towson Univ. (United States)

LESSONS LEARNED AND FUTURE IDEAS

- 8757 0L **Secure it now or secure it later: the benefits of addressing cyber-security from the outset** [8757-25]
M. M. Olama, J. Nutaro, Oak Ridge National Lab. (United States)
- 8757 0N **Digital microarray analysis for digital artifact genomics** [8757-31]
H. Jaenisch, Johns Hopkins Univ. (United States), Licht Strahl Engineering, Inc. (United States), and Sentar, Inc. (United States); J. Handley, Licht Strahl Engineering, Inc. (United States) and Sentar, Inc. (United States); D. Williams, Sentar, Inc. (United States)

Author Index

Conference Committee

Symposium Chair

Kenneth R. Israel, Major General (USAF Retired) (United States)

Symposium Cochair

David A. Whelan, Boeing Defense, Space, and Security
(United States)

Conference Chairs

Igor V. Ternovskiy, Air Force Research Laboratory (United States)

Peter Chin, Johns Hopkins University Applied Physics Laboratory
(United States)

Session Chairs

- 1 Analysis of Cyber Attacks
Peter Chin, Johns Hopkins University Applied Physics Laboratory
(United States)
- 2 Cyber Security of Infrastructures
Peter Chin, Johns Hopkins University Applied Physics Laboratory
(United States)
- 3 Security of Internet and Clouds
Peter Chin, Johns Hopkins University Applied Physics Laboratory
(United States)
- 4 Novel Cyber Sensors
Peter Chin, Johns Hopkins University Applied Physics Laboratory
(United States)
- 5 Novel Algorithms for Cyber Sensing
Peter Chin, Johns Hopkins University Applied Physics Laboratory
(United States)
- 6 Algorithms for Attack Detection
Peter Chin, Johns Hopkins University Applied Physics Laboratory
(United States)

- 7 Lessons Learned and Future Ideas
Peter Chin, Johns Hopkins University Applied Physics Laboratory
(United States)