

PROCEEDINGS OF SPIE

Cyber Sensing 2012

Igor V. Ternovskiy
Peter Chin
Editors

24–25 April 2012
Baltimore, Maryland, United States

Sponsored and Published by
SPIE

Volume 8408

Proceedings of SPIE, 0277-786X, v. 8408

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

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 2012*, edited by Igor V. Ternovskiy, Peter Chin, Proceedings of SPIE Vol. 8408 (SPIE, Bellingham, WA, 2012) Article CID Number.

ISSN 0277-786X
ISBN 9780819490865

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 © 2012, 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/12/\$18.00.

Printed in the United States of America.

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

The logo for SPIE Digital Library features the word "SPIE" in a bold, sans-serif font above the words "Digital Library" in a similar font. To the right of the text is a stylized graphic consisting of three vertical bars of varying heights, with a red arc above them.

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

vii *Conference Committee*

SESSION 1

- 8408 02 **Insider threat detection enabled by converting user applications into fractal fingerprints and autonomously detecting anomalies** [8408-01]
H. Jaenisch, Johns Hopkins Univ. (United States) and Licht Strahl Engineering, INC (United States); J. Handley, Licht Strahl Engineering, INC (United States)
- 8408 03 **Cyber situational awareness and differential hardening** [8408-02]
A. Dwivedi, D. Tebben, The Johns Hopkins Univ. Applied Physics Lab. (United States)
- 8408 06 **From measurements to metrics: PCA-based indicators of cyber anomaly** [8408-04]
F. Ahmed, T. Johnson, S. Tsui, The Johns Hopkins Univ. Applied Physics Lab. (United States)
- 8408 07 **Anomaly detection for internet surveillance** [8408-05]
H. Bouma, S. Raaijmakers, A. Halma, H. Wedemeijer, TNO (Netherlands)

SESSION 2

- 8408 08 **PeerShield: determining control and resilience criticality of collaborative cyber assets in networks** [8408-06]
H. Cam, U.S. Army Research Lab. (United States)
- 8408 09 **RISE: Relational-Integrity-Sensitive-Encoding and data aggregation for intrusion detection** [8408-07]
H. Cam, U.S. Army Research Lab. (United States)
- 8408 0A **Coalmine: an experience in building a system for social media analytics** [8408-08]
J. S. White, J. N. Matthews, J. L. Stacy, Clarkson Univ. (United States)
- 8408 0B **A method for the automated detection phishing websites through both site characteristics and image analysis** [8408-09]
J. S. White, J. N. Matthews, J. L. Stacy, Clarkson Univ. (United States)

SESSION 3

- 8408 0D **A solution for parallel network architectures applied to network defense appliances and sensors (Invited Paper)** [8408-11]
E. C. Naber, P. G. Velez, A. S. Johal, The Johns Hopkins Univ. Applied Physics Lab. (United States)
- 8408 0E **Data fusion in cyber security: first order entity extraction from common cyber data** [8408-12]
N. A. Giacobe, The Pennsylvania State Univ. (United States)

- 8408 OF **Cyber situation awareness as distributed socio-cognitive work** [8408-13]
M. Tyworth, N. A. Giacobe, V. Mancuso, The Pennsylvania State Univ. (United States)
- 8408 OG **Operational advantages of using Cyber Electronic Warfare (CEW) in the battlefield** [8408-14]
N. Yasar, F. M. Yasar, Y. Topcu, Turkish Air War College (Turkey)

SESSION 4

- 8408 OH **Analysis of web-related threats in ten years of logs from a scientific portal** [8408-16]
R. D. C. Santos, National Institute for Space Research (Brazil) and The Johns Hopkins Univ. (United States); A. R. A. Grégio, Renato Archer Information Technology Research Ctr. (Brazil); J. Raddick, V. Vattki, A. Szalay, The Johns Hopkins Univ. (United States)
- 8408 OI **Scalable wavelet-based active network detection of stepping stones** [8408-17]
J. I. Gilbert, D. J. Robinson, J. W. Butts, T. H. Lacey, Air Force Institute of Technology (United States)
- 8408 OJ **Distributed pattern detection in cyber networks** [8408-18]
R. C. Paffenroth, P. C. Du Toit, Numerica Corp. (United States); L. L. Scharf, A. P. Jayasumana, V. Banadara, Colorado State Univ. (United States); R. Nong, Numerica Corp. (United States)

SESSION 5

- 8408 OL **Improved near-earth object detection using dynamic logic** [8408-20]
T. G. Allen, A. C. O'Connor, I. Ternovskiy, Air Force Research Lab. (United States)
- 8408 OM **Automatic decision support in heterogeneous sensor networks** [8408-21]
R. Kozma, T. Tanigawa, O. Furxhi, S. Consul, The Univ. of Memphis (United States)
- 8408 ON **Multi-agent system for target-adaptive radar tracking** [8408-22]
A. C. O'Connor, Air Force Research Lab. (United States)
- 8408 OO **Application of dynamic logic algorithm to analyze AFRL gotcha data** [8408-23]
F. C. Lin, L. I. Perlovsky, Air Force Research Lab. (United States)

SESSION 6

- 8408 OQ **Human-computer symbiosis in cyberspace environments** [8408-25]
J. Carter, E. Levin, A. Sergeyev, Michigan Technological Univ. (United States)
- 8408 OR **Wavefront sensor alignment and calibration techniques for laser communication systems** [8408-26]
A. V. Sergeyev, E. Levin, M. C. Roggemann, Michigan Technological Univ. (United States)

SESSION 7

- 8408 0V **Towards a trustworthy distributed architecture for complex sensing networks** [8408-31]
H. Schubert, Real-Time Innovations (United States); J. A. Luke, Air Force Research Lab.
(United States)
- 8408 0W **Blind extraction and security analysis of spread spectrum hidden watermarks** [8408-32]
J. A. Marsh, SUNY Institute of Technology (United States) and Assured Information Security,
Inc. (United States); G. F. Wohlrab, Air Force Research Lab. (United States)
- 8408 0X **Fractals, malware, and data models** [8408-33]
H. M. Jaenisch, Sentar, Inc. (United States) and Licht Strahl Engineering INC (United States)
and Johns Hopkins Univ. (United States); A. N. Potter, D. Williams, Sentar, Inc. (United States);
J. W. Handley, Licht Strahl Engineering INC (United States)

Author Index

Conference Committee

Symposium Chair

Kevin P. Meiners, Office of the Secretary of Defense (United States)

Symposium Cochair

Kenneth R. Israel, Lockheed Martin Corporation (United States)

Conference Chairs

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

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

Program Committee

Mohiuddin Ahmed, HRL Laboratory, LLC (United States)

Thomas G. Allen, Air Force Research Laboratory (United States)

H. John Caulfield, Alabama A&M University (United States)

Tuan A. Duong, Jet Propulsion Laboratory (United States)

Tony C. Kim, Air Force Research Laboratory (United States)

Eugene Levin, Michigan Technological University (United States)

Leonid I. Perlovsky, Air Force Research Laboratory (United States)

Aleksandr V. Sergeev, Michigan Technological University (United
States)

Session Chairs

Session 1

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

Session 2

Mohiuddin Ahmed, HRL Laboratory, LLC (United States)

Session 3

Freeman C. Lin, Air Force Research Laboratory (United States)

Alan C. O'Connor, Air Force Research Laboratory (United States)

Session 4

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

Thomas G. Allen, Air Force Research Laboratory (United States)

Session 5

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

Session 6

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

Aleksandr V. Sergeyev, Michigan Technological University (United States)

Session 7

Thomas G. Allen, Air Force Research Laboratory (United States)

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