PROCEEDINGS OF SPIE

Cyber Sensing 2018

Igor V. Ternovskiy
Peter Chin
Editors

17–18 April 2018
Orlando, Florida, United States

Sponsored and Published by
SPIE

Volume 10630

Proceedings of SPIE 0277-786X, V. 10630

The papers 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. Additional papers and presentation recordings may be available online in the SPIE Digital Library at SPIEDigitalLibrary.org.

The papers 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 these proceedings:
Author(s), "Title of Paper," in *Cyber Sensing 2018*, edited by Igor V. Ternovskiy, Peter Chin, Proceedings of SPIE Vol. 10630 (SPIE, Bellingham, WA, 2018) Seven-digit Article CID Number.

ISSN: 0277-786X
ISSN: 1996-756X (electronic)

ISBN: 9781510617711
ISBN: 9781510617728 (electronic)

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

Printed in the United States of America by Curran Associates, Inc., under license from SPIE.

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

SPIE. DIGITAL LIBRARY
SPIEDigitalLibrary.org

Paper Numbering: *Proceedings of SPIE* follow an e-First publication model. A unique citation identifier (CID) number is assigned to each article at the time of 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 and print versions of the publication. SPIE uses a seven-digit CID article numbering system structured as follows:

- The first five 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.

Contents

v *Authors*

vii *Conference Committee*

SESSION 1 CYBER SECURITY FRAMEWORK

10630 03 **The growing threat of cybersecurity attacks in sports** [10630-2]

10630 04 **Security tag computation and propagation in OSFA** [10630-4]

SESSION 2 ANALOG DOMAIN AND CYBER SECURITY I

10630 05 **Detailed tracking of program control flow using analog side-channel signals: a promise for IoT malware detection and a threat for many cryptographic implementations** [10630-5]

10630 06 **Deep learning-based classification and anomaly detection of side-channel signals** [10630-6]

10630 07 **Overhead analysis of the utilization of hardware assisted virtualization for protecting guest operating system applications** [10630-7]

SESSION 3 ANALOG DOMAIN AND CYBER SECURITY II

10630 08 **Block-level algorithm classification based on RF side-channel** [10630-8]

10630 09 **Register Hamming distance from side channels** [10630-9]

10630 0A **Exploiting side-channel emissions to detect changes in FPGA firmware** [10630-10]

10630 0B **Classification of low-SNR side channels** [10630-11]

10630 0C **Generalization of algorithm recognition in RF side channels between devices** [10630-12]

SESSION 4 ANALOG DOMAIN AND CYBER SECURITY III

10630 0D **Utilizing electromagnetic emanations for out-of-band detection of unknown attack code in a programmable logic controller** [10630-13]

10630 0E **Preliminary classification results of RF emission based feature extraction in Internet of Things devices** [10630-14]

10630 0G **A graph-theoretic understanding of network-wide implications of local cyber protections for mission assurance** [10630-16]

10630 0H **Lightweight hardware monitoring of IoT devices** [10630-17]

10630 0I **Control flow graph modifications for improved RF-based processor tracking performance** [10630-18]

SESSION 5 CYBER SENSING PHENOMENOLOGY

10630 0J **A mixed numeric and analytic method for investigating OAM beam scattering in turbid water** [10630-19]

10630 0M **Comparison of error in two passive phase localization algorithms** [10630-22]

SESSION 6 MACHINE LEARNING AND CYBER SENSING

10630 0N **Track generation in semi-supervised learning of self-structured algorithm using noisy and sparse visual and infrared data** [10630-23]

10630 0O **Similarity measures for target tracking with aerial images** [10630-24]

10630 0Q **Understanding adversarial attack and defense towards deep compressed neural networks** [10630-26]

SESSION 7 NETWORKS AND CYBER SENSING

10630 0S **Development and implementation of VoIP honeypots with wide range of analysis** [10630-28]

10630 0U **Identifying and detecting applications within TLS traffic** [10630-31]

10630 0V **CASPER: an efficient approach to detect anomalous code execution from unintended electronic device emissions** [10630-32]