AAAI Workshops 2018

Technical Report WS-05

New Orleans, Louisiana, USA
2 – 3 February 2018

ISBN: 978-1-7138-2747-4

Printed from e-media with permission by:

Curran Associates, Inc.
57 Morehouse Lane
Red Hook, NY 12571

Some format issues inherent in the e-media version may also appear in this print version.

Copyright© (2018) by Association for the Advancement of Artificial Intelligence
All rights reserved.

Printed with permission by Curran Associates, Inc. (2021)

For permission requests, please contact Association for the Advancement of Artificial Intelligence
at the address below.

Association for the Advancement of Artificial Intelligence
2275 East Bayshore Road
Suite 160
Palo Alto, California 94303
USA

Phone: 1-650-328-3123
Fax: 1-650-321-4457

https://aaai.org/Press/press.php

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
Email: curran@proceedings.com
Web: www.proceedings.com

TABLE OF CONTENTS

END-TO-END ACTIVE LEARNING FOR COMPUTER SECURITY EXPERTS 217
Anaël Beaugnon, Pierre Chifflier, Francis Bach

RADMAX: RISK AND DEADLINE AWARE PLANNING FOR MAXIMUM UTILITY 225
Jingkai Chen, Cheng Fang, Christian Muise, Howard Shrobe, Brian C. Williams, Peng Yu

"ATTENTION" FOR DETECTING UNRELIABLE NEWS IN THE INFORMATION AGE 231
Venkatesh Duppada

ADEQUACY OF THE GRADIENT-DESCENT METHOD FOR CLASSIFIER EVASION ATTACKS 237
Yi Han, Benjamin Rubinstein

BLACK-BOX ATTACKS AGAINST RNN BASED MALWARE DETECTION ALGORITHMS 245
Weiwei Hu, Ying Tan

STEGANOGRAPHIC INTERNET OF THINGS: GRAPH TOPOLOGY TIMING CHANNELS 252
Ira S. Moskowitz, Stephen Russell, Brian Jalaian

DECEITFUL ATTACKS IN SECURITY GAMES 260
Thanh Hong Nguyen, Michael Wellman, Arunesh Sinha

MALWARE DETECTION BY EATING A WHOLE EXE 268
Edward Raff, Jon Barker, Jared Sylvester, Robert Brandon, Bryan Catanzaro, Charles K. Nicholas

DETECTING CYBERATTACK ENTITIES FROM AUDIT DATA VIA MULTI-VIEW ANOMALY DETECTION WITH FEEDBACK 277
Md Amran Siddiqui, Alan Fern, Ryan Wright, Alec Theriault, David Archer, William Maxwell

RECURRENT NEURAL NETWORK LANGUAGE MODELS FOR OPEN VOCABULARY EVENT-LEVEL CYBER ANOMALY DETECTION 285
Aaron Randall Tuor, Ryan Baerwolf, Nicolas Knowles, Brian Hutchinson, Nicole Nichols, Rob Jasper

Author Index