

17th International Conference on Cyber Warfare and Security (ICCWS 2022)

Albany, New York, USA
17 – 18 March 2022

Editors:

**Dean Robert P. Griffin
Unal Tatar
Benjamin Yankson**

ISBN: 978-1-7138-4538-6

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 The Authors, (2022). All Rights Reserved. No reproduction, copy or transmission may be made without written permission from the individual authors.

Printed with permission by Curran Associates, Inc. (2022)

Review Process

Papers submitted to this conference have been double-blind peer reviewed before final acceptance to the conference. Initially, abstracts were reviewed for relevance and accessibility and successful authors were invited to submit full papers. Many thanks to the reviewers who helped ensure the quality of all the submissions.

Ethics and Publication Malpractice Policy

ACPIL adheres to a strict ethics and publication malpractice policy for all publications – details of which can be found here:

<http://www.academic-conferences.org/policies/ethics-policy-for-publishing-in-the-conference-proceedings-of-academicconferences-and-publishing-international-limited/>

Conference Proceedings

The Conference Proceedings is a book published with an ISBN and ISSN. The proceedings have been submitted to a number of accreditation, citation and indexing bodies including Thomson ISI Web of Science and Elsevier Scopus.

Author affiliation details in these proceedings have been reproduced as supplied by the authors themselves.

Published by Academic Conferences and Publishing International Ltd.
33 Wood Lane
Sonning Common RG4 9SJ UK

Phone: 441 189 724 148
Fax: 441 189 724 691
info@academic-conferences.org

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

Contents

Paper Title	Author(s)	Page No
Preface		vii
Committee		ix
Biographies		xi
Research papers		
Cyberbullying Indicator as a Precursor to a Cyber Construct Development	Salam Khalifa Al-Romaihi and Richard Adeyemi Ikuesan	1
Education and Training Against Threat of Phishing Emails	Ladislav Burita, Ivo Klavan and Tomas Racil	7
Don't Drink the Cyber: Extrapolating the Possibilities of Oldsmar's Water Treatment Cyberattack	James Cervini, Aviel Rubin and Lanier Watkins	19
An Ontology for Effective Security Incident Management	Sabarathinam Chockalingam and Clara Maathuis	26
Bureau of Justice Student Computer and Digital Forensics Educational Opportunities Program: The Assessment of Online Graduate Students	Kyung-Shick Choi, Chitkushev Lou, Kyung-Seok Choo and Claire Seungeun Lee	36
Protecting Networks with Intelligent Diodes	Jason Dahlstrom and Stephen Taylor	45
Can Attrition Theory Provide Insight for Cyber Warfare?	Stephen Defibaugh and Donna Schaeffer	55
A Novel DevSecOps Model for Robust Security in an MQTT Internet of Things	Manasa Ekoramaradhya and Christina Thorpe	63
Exploring Ontologies for Mitigation Selection of Industrial Control System Vulnerabilities	Thomas Heverin, Michael Cordano, Andy Zeyher, Matthew Lashner and Sanjana Suresh	72
Future Needs of the Cybersecurity Workforce	Connie Justice, Char Sample, Sin Ming Loo, Alex Ball and Clay Hampton	81
Zero Trust and Advanced Persistent Threats: Who Will Win the War?	Bilge Karabacak and Todd Whittaker	92
Advancing Cybersecurity Capabilities for South African Organisations Through R&D	Zubeida Casmod Khan and Nenekazi Nokuthala Penelope Mkuzangwe	102
Zero Trust Container Architecture (ZTCA): A Framework for Applying Zero Trust Principals to Docker Containers	Darragh Leahy and Christina Thorpe	111
APT Cyber-Attack Modelling: Building a General Model	Martti Lehto	121
Design and Evaluation of a Cyber Protection Team Planner Work Aid	Kristen Liggett, Arielle Stephenson, Meghan Strang and Geoffrey Dobson	130
I Know You by Heart: Biometric Authentication based on Electrocardiogram (ECG) signals	Christoph Lipps, Lea Bergkemper, Jan Herbst and Hans Dieter Schotten	135
Shallow Deep Learning using Space-filling Curves for Malware Classification	David Long and Stephen O'Shaughnessy	145

Paper Title	Author(s)	Page No
Integrating Democratic Cybersecurity: Empowerment of Traditional Law Enforcement and Democratic Public Safety	Michael Losavio, Jeffrey C. Sun, Sharon Kerrick, Adel Elmaghraby, Cheryl Purdy and Clay Johnson	155
On Explainable AI Solutions for Targeting in Cyber Military Operations	Clara Maathuis	166
Analyzing the Performance of Block-Splitting in LLVM Fingerprinting	William Mahoney, Philip Sigillito, Jeff Smolinski, J. Todd McDonald and George Grispos	176
Taxonomy of Social Engineering Attacks: A Survey of Trends and Future Directions	Arianit Maraj and William Butler	185
Blockchain Technology for Addressing Privacy and Security Issues in Cloud Computing	Pardis Moslemzadeh Tehrani, Gabriele Kotsis and Andasmara Rizky Pranata	194
Context-Aware Cyber Threat Intelligence Exchange Platform	Michael Motlhabi, Phumeza Pantsi, Bokang Mangoale, Rofhiwa Netshiya and Samson Chishiri	201
The Development of Cybersecurity Awareness Measurement Model in the Water Sector	Bryan S. Mufor, Annlizé Marnewick and Suné von Solms	211
Circuit-Variant Moving Target Defense for Side-Channel Attacks	Tristen Mullins, Brandon Baggett, Todd R. Anandel and J. Todd McDonald	219
A Modern ICT Network Simulator for Co-Simulations in Smart Grid Applications	Fabian Niehaus, Bastian Fraune, Giacomo Gritzan and Richard Sethmann	227
Towards Detection of Selfish Mining Using Machine Learning	Matthew Peterson, Todd Anandel and Ryan Benton	237
Specialised Media Monitoring Tool to Observe Situational Awareness	Heloise Pieterse, Carien Van 't Wout, Zubeida Khan and Chris Serfontein	244
A New Dawn for Space Security	Jordan J. Plotnek and Jill Slay	253
Assessment of Cybersecurity Risks: Maritime Automated Piloting Process	Jouni Pöyhönen and Martti Lehto	262
Utilizing Switch Port Link State to Detect Rogue Switches	Travis Quitiquit and Vijay Bhuse	272
Aligning South African Data and Cloud Policy with the PoPI Act	Emma Raaff, Nicole Rothwell and Aidan Wynne	279
Transient Execution and Side Channel Analysis: A Vulnerability or a Science Experiment?	Michael Shepherd, Scott Brookes and Robert Denz	288
Bug Bounties: Between New Regulations and Geopolitical Dynamics	Jantje Silomon, Mischa Hansel and Fabiola Schwarz	298
Emerging Cyber risk Challenges in Maritime Transportation	Jussi Simola and Jouni Pöyhönen	306
Improving Protection Against Cybersecurity Attacks of Emergency Dispatch Centers	James Sweeney and Vu Tran	315
Increasing Industry Profitability and Cyber Hygiene Utilizing Awareness Progression Methods	John Thebarger, Mark Reith and Wayne Henry	325
Identifying Adversaries' Signatures Using Knowledge Representations of Cyberattack Techniques on Cloud Infrastructure	Gilliam van der Merwe, Christian Muller, Wilhelm van der Merwe and Dewald Blaauw	333

Paper Title	Author(s)	Page No
Rising Above Misinformation and Deepfakes	Namosha Veerasamy and Heloise Pieterse	340
Multi-Purpose Cyber Environment for Maritime Sector	Gabor Visky, Arturs Lavrenovs, Erwin Orye, Dan Heering, Kimberly Tam and Olaf M. Maennel	349
Ethical and Legal Aspects Pertaining to law Enforcement use of Drones	MM Watney	358
Social Media Privacy Using EDEE Security Model	Benjamin Yankson, Eric Cajigal Delgado, Amjad Al-Jabri, Natalie Gitin and Sydney Davidson	366
PHD Papers		
The Impact of CISO Appointment Announcements on the Market Value of Firms	Adrian Ford, Ameer Al-Nemrat, Seyed Ali Ghorashi and Julia Davidson	375
What is a Substantial Contribution to a Research Project in Offensive Cyberspace Operations that Merits Co-Authorship?	Gazmend Huskaj	385
Human Errors: A Cybersecurity Concern and the Weakest Link to Small Businesses	Tabisa Ncubekezi	395
Need for a Cyber Resilience Framework for Critical Space Infrastructure	Syed Shahzad, Li Qiao and Keith Joiner	404
Ransomware Detection using Process Memory	Avinash Singh, Richard Adeyemi Ikuesan and Hein Venter	413
Evaluating the Reliability of Android Userland Memory Forensics	Sneha Sudhakaran, Aisha Ali-Gombe, Andrew Case and Golden G Richard III	423
The Cumulative Cyber Deterrence	Maija Turunen and Martti J. Kari	433
Masters Research Papers		
Performance Implications for Multi-Core RISC-V Systems with Dedicated Security Hardware	Samuel Chadwick, Scott Graham and James Dean	440
Analysis of Image Thresholding Algorithms for Automated Machine Learning Training Data Generation	Tristan Creek and Barry E. Mullins	449
Securing InfiniBand Networks with the Bluefield-2 Data Processing Unit	Noah Diamond, Scott Graham and Gilbert Clark	459
Malware Binary Image Classification Using Convolutional Neural Networks	John Kiger, Shen-Shyang Ho and Vahid Heydari	469
Defending Small Satellites from Malicious Cybersecurity Threats	Banks Lin, Wayne Henry and Richard Dill	479
Improving Hardware Security on Talos II Architecture Through Boot Image Encryption	Calvin Muramoto, Stephen Dunlap and Scott Graham	489
Technical Analysis of Thanos Ransomware	Ikuromor Ogiriki, Christoper Beck and Vahid Heydari	497
Analysis of Sexual Abuse of Children Online and CAM Investigations in Finland	Johanna Parviainen and Jyri Rajamäki	505
Digital Risk Management: Investigating Human-Factor Security with a Behaviorist Approach	Ruan Pretorius and Dewald Blaauw	513

Paper Title	Author(s)	Page No
Ensuring the Security of Space Systems from Eavesdropping Attacks	Caleb Richardson, Mark Reith and Wayne Henry	522
Work In Progress Papers		
Mitigating Global Cyber Risk Through Bridging the National Incident Response Capacity Gap	Elisabeth Dubois and Unal Tatar	527
An Exploration on APTs in Biocybersecurity and Cyberbiosecurity	Xavier-Lewis Palmer, Lucas Potter and Saltuk Karahan	532
Late Submissions		
Cyberwarfare and its Effects on Critical Infrastructure	Humairaa Yacoob Bhaiyat and Siphesihle Philezwini Sithungu	536
Addressing the Skills Shortage in Cybersecurity	Gareth Davies, Angela Mison and Peter Eden	544
Critical Systems Protection (CSP): The US Secret Service's Tactical Cyber Capability for Securing Protectees	Austin Hyman, Brian Nussbaum, Mario Bencivenga and Zachary Rizzo	552
WFH, not WTH? The Security Challenges of Working-From-Home	Neal Kushwaha, Piret Pernik and Bruce W. Watson	559
The Failure of Trust in Trusted Systems	Angela Mison, Gareth Davies and Peter Eden	568
New Wave Cyber Attacks	Angela Mison, Gareth Davies and Peter Eden	576
The Role of Big Tech in Future Cyber Defence	Angela Mison, Gareth Davies and Peter Eden	583
Data Mining for the Security of Cyber Physical Systems Using Deep-Learning Methods	Bhagawan Nath, Timo Hamalainen and Soundararajan Ezekiel	591
'Out Beyond Jointery': Developing a Model for Gaming Multi-Domain Warfare	Keith Scott	599
Research Gaps and Opportunities for Secure Access Service Edge	Stephanus Petrus van der Walt and Hein Venter	609