

12th International Conference on Cyber Warfare and Security (ICCWS 2017)

Dayton, Ohio, USA
2 – 3 March 2017

Editors:

Adam R. Bryant
Robert F. Mills
Juan Lopez Jr.

ISBN: 978-1-5108-3790-4

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© The Authors, (2017). All Rights Reserved.

No reproduction, copy or transmission may be made without written permission from the individual authors.

Papers have been double-blind peer reviewed before final submission to the conference. Initially, paper abstracts were read and selected by the conference panel for submission as possible papers for the conference.

Many thanks to the reviewers who helped ensure the quality of the full papers.

Printed by Curran Associates, Inc. (2017)

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		v
Committee		vi
Biographies		viii
Information Classification Scheme for Next Generation Access Control Models in Mobile Patient-Centered Care Systems	Shada Alsalamah	1
CyberMix: A Roadmap of SDN-Based Intelligent Cybersecurity Immune System	Abdullahi Arabo	10
The Utilisation of the Deep Web for Military Counter Terrorist Operations	Michael Aschmann, Louise Leenen and Joey Jansen van Vuuren	15
Offensive Deception in Computing	Jeffrey Avery, Mohammed Almeshekah and Eugene Spafford	23
Mobile Cloud Security in the Literature: A Bibliometric Analysis	Zakariya Belkhamza	32
Support for Secure Code Execution in Unix-Like Operating Systems	Vijay Bhuse and Jagadeesh Nandigam	40
Automated Intelligence Gathering Through Comparison of JPEG Images and their Thumbnails	Nicolas Bodin, Clément Coddet, Olivier Fatou and Eric Filiol	48
A High-Level Comparison Between the South African Protection of Personal Information Act and International Data Protection Laws	Johnny Botha, M.M. Grobler, Jade Hahn, Mariki Eloff	57
I Think I CAN	Adam Brown, Todd Andel, Jeffrey McDonald and Mark Yampolskiy	67
Transforming Network Simulation Data to Semantic Data for Network Attack Planning	Ka Fai Peter Chan and Pedro de Souza	74
Deterrence and its Implementation in Cyber Warfare	Jim Chen	83
A Framework of Cybersecurity Approaches in Precision Agriculture	Hongmei Chi, Stephen Welch, Eugene Vasserman and and Ezhil Kalaimannan	90
Cyber Wargaming on SCADA Systems	Edward Colbert, Daniel Sullivan and Alexander Kott	96
Cyber Resilience: Rethinking Cybersecurity Strategy to Build a Cyber Resilient Architecture	William Arthur Conklin, Dan Shoemaker and Anne Kohnke	105
Building Cybersecurity Resilience in Africa	Wayne Dalton, Joey Jansen van Vuuren and Justin Westcott	112
Anomaly Detection for Data Streams in Large-Scale Distributed Heterogeneous Computing Environments	Yue Dang, Bin Wang, Ryan Brant, Zhiping Zhang, Maha Alqallaf and Zhiqiang Wu	121
Cyber-War and Contemporary Marxism	Nick Dyer-Witford and Svitlana Matviyenko	131

Paper Title	Author(s)	Page No
Anticipating Cyber Battlefields	Michael Fowler	138
Audit Analysis Models, Security Frameworks and Their Relevance for VoIP	Oscar Gavilanez, Glen Rodriguez and Franklin Gavilanez	143
Speeding up Parliamentary Decision Making for Cyber Counter-Attack	Tim Grant	152
Crime and Punishment in Cyberspace: National and International Perspectives	Virginia Greiman	160
Securing Bluetooth Low Energy Enabled Industrial Monitors	Jose Gutierrez del Arroyo, Jason Bindewald and Benjamin Ramsey	167
Wireless Security Within new Model Vehicles	Jennifer Halahan and Weifeng Chen	177
Information Sensitive Cyber Sensor	Steve Hutchinson, Jason Ellis and Char Sample	186
Cyber Deception via System Manipulation	James Jones	194
On the Future of Cybersecurity	Robert Koch	202
Cyberterrorists Bringing Down Airplanes: Will it Happen Soon?	Anthony Lam, José Fernandez and Richard Frank	210
Affecting Freedom of Action in Cyber Space: Subtle Effects and Skilled Operators	Antoine Lemay, Sylvain Leblanc, Scott Knight and José Fernandez	220
Security for Mobile Device Assets: A Survey	António Lima, Bruno Sousa, Tiago Cruz and Paulo Simões	227
Stockpiling Zero-Day Exploits: The Next International Weapons Taboo	Paul Maxwell	237
An Open Source Tool to Support the Quantitative Assessment of Cybersecurity	Vidhyashree Nagaraju, Lance Fiondella and Thierry Wandji	244
Proving Cybercriminals' Possession of Stolen Credit Card Details on Compromised POS Devices	Wynand Nel and Andries Burger	254
Comparison of Various Discrimination Techniques on Counterfeit Mixed-Signal Integrated Circuits	Sean O'Neill, Addison Betances, Samuel Stone and Rusty Baldwin	261
WhatsApp Security and Role of Metadata in Preserving Privacy	Nidhi Rastogi and James Hendler	269
Security by Design in System on a Chip Applications	Patrick Reber and Scott Graham	275
Measuring Cyber Intrusion Chains, Adaptive Adversarial Behavior, and Group Dynamics	Aunshul Rege, Brian Singer, Nicholas Masceri and Quinn Heath	285
Operationalizing Cyber: Recommendations for Future Research	Mark Reith, Seeley Pentecost, Daniel Celebucki and Robert Kaufman	295
BlueFinder: A Range-Finding Tool for Bluetooth Classic and Low Energy	Anthony Rose, Jose Guitierrez Del Arroyo, Jason Bindewald and Benjamin Ramsey	303

Paper Title	Author(s)	Page No
Home Automation Simulcasted Power Line Communication Network (SPN) Discrimination Using Wired Signal Distinct Native Attribute (WS-DNA)	Brady Ross, Timothy Carbino and Michael Temple	313
Cyber Threats Mega Trends in Cyber Space	Tarja Rusi and Martti Lehto	323
What's in a Name? Cultural Observations on Nationally Named Hacking Groups	Char Sample, Jonathan Bakdash, Jose Abdelnour-Nocera and Carsten Maple	332
A Semantics-Based Approach to Concept Assignment in Assembly Code	Zachary Sisco and Adam Bryant	341
The use of Entropy in Lossy Network Traffic Compression for Network Intrusion Detection Applications	Sidney Smith, Stephen Neyens and Robert Hammell II	352
Indistinguishability of Actions in Manipulated Information Systems	Mikhail Styugin	361
Who Will Defend the Nation in the Digital Domain?	Natalie Vanatta	367
The Double Life of Your Browser: Implications on Privacy and Forensics	Natalija Vlajic, Xue Ying Shi and Hamzeh Roumani	374
Security Analysis of a Software-Defined Radar	Blake Yerkes, Benjamin Ramsey, Mason Rice, John Pecarina and Stephen Dunlap	386
PHD Research Papers		397
An Intrusion Detection System for Heavy-Duty Truck Networks	Matthew Butler	399
Capability Detection and Evaluation Metrics for Cyber Security lab Exercises	Emin Caliskan, Unal Tatar, Hayretdin Bahsi, Rain Ottis and Risto Vaarandi	407
Timing and Resilience in Cyber Conflict: A Theoretical Framework	Brian Connett	415
Establishing a Cognitive Understanding of Cyber Reverse Engineering Tasks	Patrick Dudenhofer and Adam Bryant	419
System Complexity Meets Decision Makers: A Framework for Level-Appropriate Information Processing	Volker Eiseler, Robert Koch and Gabi Dreo Rodosek	427
Towards a Cyber Counterintelligence Maturity Model	Victor Jaquire and Sebastiaan von Solms	432
Framework Design for Implementation of Secured TPM on E-commerce	Chinyere Grace Kennedy, DongSub Cho, Funminiyi Olajide and Samuel John	441
Masters Papers		451
Proactive Host Mutation in Software-Defined Networking	Matthew Aust and Barry Mullins	453
A Method of Securing a Vehicle's Controller Area Network	Eddie Caberto and Scott Graham	461
Active Network Response Using Host-Based IDS and Software Defined Networking	Jonathan Goodgion and Barry Mullins	469

Paper Title	Author(s)	Page No
Analysis of Denial-of-Service Attack Vectors in Software Defined Networks	Anthony Portante and Barry Mullins	479
Dynamic Attestation of Real-Time Systems	Travis Potthoff and Scott Graham	489
Securing Insteon Home Automation Systems Using Radio Frequency Distinct Native Attribute (RF-DNA) Fingerprints	Christopher Talbot, Michael Temple and Timothy Carbino	497
Non Academic Papers		507
Data-Driven Approach to Protecting Critical Infrastructure	John Hurley	509
Work In Progress Papers		515
The Development of a Stochastic Model for Software Diversity	Andrew Gearhart and Douglas Kelly	517
The Economics of Cybersecurity	Douglas Kelly	522
Evaluation of Security Flaws in the Current Probe Request Design and Proposed Solutions	Eric McKinion and Alan Lin	529
A Mixed-Initiative Approach to Knowledge Discovery	Uday Sagar Panjala, Vahid Eyorokon and Michael Cox	533
Detecting and Mitigating Rootkits in Embedded Systems	Jeremy Porter and Adam Bryant	537
Ontologies for Network Security and Future Challenges	Danny Velasco Silva and Glen Rodríguez Rafael	541