

8th International Conference on Information Warfare and Security 2013

(ICIW 2013)

**Denver, Colorado, USA
25-26 March 2013**

Editors:

Doug Hart

**ISBN: 978-1-62748-017-8
ISSN: 2048-9870**

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, (2013). 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. (2013)

Published by Academic Conferences Ltd.
Curtis Farm Kidmore End
Reading RG4 9AY 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: 845-758-2634
Email: curran@proceedings.com
Web: www.proceedings.com

Contents

Paper Title	Author(s)	Page No.
Preface		iii
Committee		iv
Biographies		vi
Strategies for Combating Sophisticated Attacks	Chad Arnold, Jonathan Butts, and Krishnaprasad Thirunarayan	1
Analysis of Programmable Logic Controller Firmware for Threat Assessment and Forensic Investigation	Zachry Basnight, Jonathan Butts, Juan Lopez and Thomas Dube	9
Top-Level Goals in Reverse Engineering Executable Software	Adam Bryant, Robert Mills, Michael Grimala and Gilbert Peterson	16
An Investigation of the Current State of Mobile Device Management Within South Africa	Ivan Burke and F. Mouton	24
A Taxonomy of Web Service Attacks	Ka Fai Peter Chan, Martin Olivier and Renier Pelser van Heerden	34
DUQU'S DILEMMA: The Ambiguity Assertion and the Futility of Sanitized Cyber War	Matthew Crosston	43
Hacking for the Homeland: Patriotic Hackers Versus Hacktivists	Michael Dahan	51
Consequences of Diminishing Trust in Cyberspace	Dipankar Dasgupta and Denise Ferebee	58
Towards a Theory of Just Cyberwar	Klaus-Gerd Giesen	65
Defamation in Cyber Space: Who do you sue?	Samiksha Godara	72
Identifying Tools and Technologies for Professional Offensive Cyber Operations	Tim Grant and Ronald Prins	80
The Emergence of Cyber Activity as a Gateway to Human Trafficking	Virginia Greiman and Christina Bain	90
Deep Routing Simulation	Barry Irwin and Alan Herbert	97
Development of a South African Cybersecurity Policy Implementation Framework	Joey Jansen van Vuuren, Louise Leenen, Jackie Phahlamohlaka and Jannie Zaaiman	106
Replication and Diversity for Survivability in Cyberspace: A Game Theoretic Approach	Charles Kamhoua, Kevin Kwiat, Mainak Chatterjee, Joon Park and Patrick Hurley	116
Situation Management in Aviation Security – A Graph-Theoretic Approach	Rainer Koelle and Denis Kolev	125
Exercising State Sovereignty in Cyberspace: An International Cyber-Order Under Construction?	Andrew Liaropoulos	136
SCADA Threats in the Modern Airport	John McCarthy and William Mahoney	141
Improving Public-Private Sector Cooperation on Cyber Event Reporting	Julie McNally	147
Copyright Protection Based on Contextual Web Watermarking	Nighat Mir	154

Paper Title	Author(s)	Page No.
Towards a South African Crowd Control Model	Mapule Modise, Zama Dlamini, Sifiso Simelane, Linda Malinga, Thami Mnisi and Siphon Ngobeni	159
A Vulnerability Model for a Bit-Induced Reality	Erik Moore	169
Results From a SCADA-Based Cyber Security Competition	Heath Novak and Dan Likarish	177
Design of a Hybrid Command and Control Mobile Botnet	Heloise Pieterse and Martin Olivier	183
Functional Resilience, Functional Resonance and Threat Anticipation for Rapidly Developed Systems	David Rohret, Michael Kraft and Michael Vella	193
What Lawyers Want: Legally Significant Questions That Only IT Specialists can Answer	Yaroslav Shiryayev	203
The Weakest Link – The ICT Supply Chain and Information Warfare	Dan Shoemaker and Charles Wilson	208
Thirst for Information: The Growing Pace of Information Warfare and Strengthening Positions of Russia, the USA and China	Inna Vasilyeva and Yana Vasilyeva	215
Investigating Hypothesis Generation in Cyber Defense Analysis Through an Analogue Task	Rachel Vickhouse, Adam Bryant and Spencer Bryant	221
PHD Papers		229
The Potential Threat of Cyber-Terrorism on National Security of Saudi Arabia	Abdulrahman Alqahtani	231
Improving Cyber Warfare Decision-Making by Incorporating Leadership Styles and Situational Context into Poliheuristic Decision Theory	Daryl Caudle	240
Work in Progress		249
Attack-Aware Supervisory Control and Data Acquisition (SCADA)	Otis Alexander, Sam Chung and Barbara Endicott-Popovsky	251
Cyber Disarmament Treaties and the Failure to Consider Adequately Zero-Day Threats	Merritt Baer	255
Evaluation of a Cryptographic Security Scheme for Air Traffic Control's Next Generation Upgrade	Cindy Finke, Jonathan Butts, Robert Mills and Michael Grimaila	259
Attack Mitigation Through Memory Encryption of Security-Enhanced Commodity Processors	Michael Henson and Stephen Taylor	265
Action and Reaction: Strategies and Tactics of the Current Political Cyberwarfare in Russia	Volodymyr Lysenko and Barbara Endicott-Popovsky	269
Non Academic Papers		27
The Adam and Eve Paradox	Michael Kraft, David Rohret, Michael Vella and Jonathan Holston	275
Offensive Cyber Initiative Framework (OCIF) Raid and Re-Spawn Project	David Rohret, Michael Vella, and Michael Kraft	284