

6th International Conference on Information Warfare and Security 2011

(ICIW 2011)

**Washington, DC, USA
17-18 March 2011**

Editors:

Leigh Armistead

ISBN: 978-1-62276-675-8

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, (2011). 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
Biographies of Conference Chairs, Programme Chair, Keynote Speaker and Mini-track Chairs		iv
Biographies of contributing authors		v
Using the Longest Common Substring on Dynamic Traces of Malware to Automatically Identify Common Behaviors	<i>Jaime Acosta</i>	1
Modeling and Justification of the Store and Forward Protocol: Covert Channel Analysis	<i>Hind Al Falasi and Liren Zhang</i>	8
The Evolution of Information Assurance (IA) and Information Operations (IO) Contracts across the DoD: Growth Opportunities for Academic Research – an Update	<i>Edwin Leigh Armistead and Thomas Murphy</i>	14
The Uses and Limits of Game Theory in Conceptualizing Cyberwarfare	<i>Merritt Baer</i>	23
Who Needs a Botnet if you Have Google?	<i>Ivan Burke and Renier van Heerden</i>	32
Mission Resilience in Cloud Computing: A Biologically Inspired Approach	<i>Marco Carvalho, Dipankar Dasgupta, Michael Grimaila and Carlos Perez</i>	42
Link Analysis and Link Visualization of Malicious Websites	<i>Manoj Cherukuri and Srinivas Mukkamala</i>	52
The Strategies for Critical Cyber Infrastructure (CCI) Protection by Enhancing Software Assurance	<i>Mecealus Cronkrite, John Szydluk and Joon Park</i>	68
Building an Improved Taxonomy for IA Education Resources in PRISM	<i>Vincent Garramone, Daniel Likarish</i>	76
Using Dynamic Addressing for a Moving Target Defense	<i>Stephen Groat, Matthew Dunlop, Randy Marchany and Joseph Tront</i>	84
Changing the Face of Cyber Warfare with International Cyber Defense Collaboration	<i>Marthie Grobler, Joey Jansen van Vuuren and Jannie Zaaiman,</i>	92
Cyber Strategy and the Law of Armed Conflict	<i>Ulf Haeussler</i>	99
eGovernance and Strategic Information Warfare – non Military Approach	<i>Karim Hamza and Van Dalen</i>	106
Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains	<i>Eric Hutchins, Michael Cloppert and Rohan Amin</i>	113
The Hidden Grand Narrative of Western Military Policy: A Linguistic Analysis of American Strategic Communication	<i>Saara Jantunen and Aki-Mauri Huhtinen</i>	126
Host-Based Data Exfiltration Detection via System Call Sequences	<i>Brian Jewell and Justin Beaver</i>	134
Detection of YASS Using Calibration by Motion Estimation	<i>Kesav Kancherla and Srinivas Mukkamala</i>	143

Paper Title	Author(s)	Page No.
Developing a Knowledge System for Information Operations	<i>Louise Leenen, Ronell Alberts, Katarina Britz, Aurna Gerber and Thomas Meyer</i>	151
CAESMA – An On-Going Proposal of a Network Forensic Model for VoIP traffic	<i>Jose Mas y Rubi, Christian Del Carpio, Javier Espinoza, and Oscar Nuñez Mori</i>	160
Secure Proactive Recovery – a Hardware Based Mission Assurance Scheme	<i>Ruchika Mehresh, Shambhu Upadhyaya and Kevin Kwiat</i>	171
Identifying Cyber Espionage: Towards a Synthesis Approach	<i>David Merritt and Barry Mullins</i>	180
Security Analysis of Webservers of Prominent Organizations in Pakistan	<i>Muhammad Naveed</i>	188
International Legal Issues and Approaches Regarding Information Warfare	<i>Alexandru Nitu</i>	200
Cyberwarfare and Anonymity	<i>Christopher Perr</i>	207
Catch Me If You Can: Cyber Anonymity	<i>David Rohret and Michael Kraft</i>	213
Neutrality in the Context of Cyberwar	<i>Julie Ryan and Daniel Ryan</i>	221
Labelling: Security in Information Management and Sharing	<i>Harm Schotanus, Tim Hartog, Hidde Hut and Daniel Boonstra</i>	228
Information Management Security for Inter-Organisational Business Processes, Services and Collaboration	<i>Maria Th. Semmelrock-Picej, Alfred Possegger and Andreas Stopper</i>	238
Anatomy of Banking Trojans – Zeus Crimeware (how Similar are its Variants)	<i>Madhu Shankarapani and Srinivas Mukkamala</i>	252
Terrorist use of the Internet: Exploitation and Support Through ICT Infrastructure	<i>Namosha Veerasamy and Marthie Grobler</i>	260
Evolving an Information Security Curriculum: New Content, Innovative Pedagogy and Flexible Delivery Formats	<i>Tanya Zlateva, Virginia Greiman, Lou Chitkushev and Kip Becker</i>	268
Research in Progress Papers		277
Towards Persistent Control over Shared Information in a Collaborative Environment	<i>Shada Alsalamah, Alex Gray and Jeremy Hilton</i>	279
3D Execution Monitor (3D-EM): Using 3D Circuits to Detect Hardware Malicious Inclusions in General Purpose Processors	<i>Michael Bilzor</i>	289
Towards An Intelligent Software Agent System As Defense Against Botnets	<i>Evan Dembskey and Elmarie Biermann</i>	299
Theoretical Offensive Cyber Militia Models	<i>Rain Ottis</i>	308
Work in Progress		315
Large-scale analysis of continuous data in cyber-warfare threat detection	<i>William Acosta</i>	317
A System and Method for Designing Secure Client-Server Communication Protocols Based on Certificateless PKI	<i>Natarajan Vijayarangan</i>	320