6th European Conference on Information Warfare and Security 2007

(ECIW 2007)

Shrivenham, United Kingdom
2-3 July 2007

Editors:

Dan Remenyi

ISBN: 978-1-62276-532-4

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, (2007). 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. (2012)

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

ECIW 2007

Contents

Paper Title	Author(s)	**Proceedings Page**
Preface		v
Biographies of Conference Chairs, Programme Chair, Keynote Speaker and Mini-track Chairs		vii
Biographies of contributing authors		viii
Minimizing Network Risk with Application to Critical Infrastructure Protection	*Waleed Almannai and Ted Lewis* *Naval Postgraduate School, Monterey, CA, USA*	1-16
A Proposed Cyber-terrorism SCADA Risk Framework Concept for Australia	*Christopher Beggs[1] and Matt Warren[2]* *[1]Monash University, Berwick, Victoria, Australia* *[2]Deakin University, Burwood, Victoria Australia*	17-26
The Layered Security Model: Analysis of Systems from the Conceptual, Logical and Physical Viewpoints	*Clive Blackwell* *Information Security Group University of London, Egham, UK*	27-36
A Roadmap Towards Content Based Information Security	*Catharina Candolin[1] and Mikko Kiviharju[2]* *[1]The Finnish Defence Forces, Helsinki, Finland* *[2]The Finnish Defence Forces, Riihimäki, Finland*	37-46
The Design of Information Security Management Systems for Small-to-Medium Size Enterprises	*Elizabeth Coles-Kemp and Richard Overill* *King's College London, Strand, London, UK*	47-54
Developing Information Security Culture in Small and Medium Size Enterprises: Australian Case Studies	*Sneza Dojkovski, Sharman Lichtenstein and Matthew Warren* *School of Information Systems, Deakin University, Australia*	55-66
Fighting Shadows and Ignoring the Elephant: Lessons for PsyOps Strategy from Organisational Responses to Risk and Crisis	*Mils Hills* *Analytic Red LLP, Milton Keynes, UK*	67-76
The Forensic Utility of Detecting Disruptive Electromagnetic Interference	*Richard Hoad[1] and Iain Sutherland[2]* *[1]QinetiQ Ltd, Cody Technology Park, Farnborough, UK* *[2]University of Glamorgan, Pontypridd, Wales*	77-88
Strategically Leading for Identity in War on Terror– The Transformation and Meaning (Lessness) of Motivation in Western Male Militarized Culture	*Aki-Maur Huhtinen* *National Defence University, Helsinki, Finland*	89-98

Paper Title	Author(s)	**Proceedings Page**
Lethal Mutation Versus Messianic Singularity: "A New Multidimensional Perspective on the Reciprocal Function of Digital Information Technologies as Offensive and Defensive Weapon Systems."	*Berg Hyacinthe[1], Mourad Debbabi[2], Abdeslem Boukhtouta[3], Zia Hayat[4] and Yves Anglade[5]* *[1]Florida State University, Tallahassee, Florida, USA* *[2]Concordia University, Montreal, Quebec, Canada* *[3]Defence Research and Development Canada, Quebec, Canada* *[4]BAE systems, UK* *[5]Florida A&M University, Tallahassee, Florida USA*	99-108
Security Policies: Making it Work	*Anushia Inthiran and Andrew Seddon* *University College of Technology and Innovation, Kuala Lumpur, Malaysia*	109-114
Digital Anti Forensics: Tools and Approaches	*Hamid Jahankhani[1], Bouras Anastasios[1] and Kenneth Revett[2]* *[1]University of East London, UK* *[2]University of Westminster, UK*	115-120
The Role of Dynamic Security Policy in Military Scenarios	*Helge Janicke[1] and Linda Finch[2]* *[1]De Montfort University, Leicester, UK* *[2]General Dynamics United Kingdom Limited, Newbridge, UK*	121-130
Critical Infrastructure Protection – Developments Since the Inception of the Concept	*Andrew Jones* *BT Security Research Centre, UK* *Edith Cowan University, Austraila*	131-138
A Novel Approach to Offline Signature Verification using Gaussian Empirical Rule	*Dakshina Ranjan Kisku, Ajita Rattani and Phalguni Gupta* *Indian Institute of Technology Kanpur, India*	139-150
Simplifying Security Management of Cross-Organisation Collaborative Decision Making	*Ulrich Lang and Rudolf Schreiner* *Object Security Ltd., St John's Innovation Centre, Cambridge, UK*	151-162
Development of Command and Control in Air Force – Transformation or Gradual Evolution	*Martti Lehto[1] and Pertti Kuokkanen[2]* *[1]Finnish Air Force Headquarters,Tikkakoski, Finland* *[2]Defence Command Finland Helsinki, Finland*	163-170
A Subliminal Channel Scheme Based on Random Numbers Approximation Sequence	*Gang Luo[1], Xing-ming Sun[1,2], and Jun-wei Huang[1]* *[1]Hunan University, Changsha, China* *[2]University College London, London, UK*	171-180
The Role of Knowledge Centres in Information Warfare	*Károly Nagy* *The Hungarian Prime minister's Office, Budapest*	181-186

Paper Title	Author(s)	**Proceedings Page**
Body Movement Identification (BMI)	*Dan Ophir, Itzhak Schlissel and Benyamin Tamir* *Faculty of Scientific Studies, the College of Judea and Samaria, Ariel, Israel*	187-196
A Flexible Threat Model for Computer Based Systems	*Venkat Pothamsetty* *Critical Infrastructure Assurance Group, Cisco Systems ,Austin, Texas, USA*	197-206
Benchmarks for Critical Infrastructure Systems Modelling	*Graeme Pye and Matthew Warren* *School of Information Systems, Deakin University, Geelong, Australia*	207-216
An Investigation into the Suitability of Unidirectional Networks for use in e-Commerce Security	*Vanja Radjenovich and Jill Slay* *University of South Australia, Mawson Lakes, South Australia*	217-226
Scenario Analysis using Out-of-Line Firewall Evaluation Framework	*Lionel Saliou, William Buchanan, Jamie Graves, and Jose Munoz* *Napier University,Edinburgh, UK*	227-236
Hybrid Intelligent Intrusion Detection/Prevention System using Fuzzylogic and Data Mining	*Bharanidharan Shanmugam and Norbik Bashah Idris* *University Teknology, Kuala Lumpur, Malaysia*	237-244
An Intrusion Detection Countermeasure for 4th-Generation TLB-Assisted Rootkits and Self-Hashing Attacks	*Dave Sharp and Carlisle Adams* *University of Ottawa, Ottawa, Ontario, Canada*	245-252
Greater is our Terror of the Unknown the Diasporic Internet Networks and their Inference with Global Security	*Marina Shorer-Zeltser and Galit . Ben-Israel* *Institute for Identity research in Media and Politics, Israel*	253-262
SQL Infections Through RFID	*Anthonius Sulaiman, Vignesh Venkataramana, Srinivas Mukkamala and Andrew Sung* *Institute for Complex Additive Systems Analysis, NM, USA*	263-272
Information Technologies for the Information Agent	*Sérgio Tenreiro de Magalhães[1], Henrique Santos[1], Leonel Duarte Santos[1], Kenneth Revett[2] and Paulo Viegas Nunes[3]* *[1]University of Minho, Guimarães, Portugal* *[2]University of Westminster, London, UK* *[3]Military Academy Research Center (CINAMIL), Lisboa, Portugal*	273-280
Malicious Software and System Damages: Is There a Case for Liability of Software Vendors?	*Theodore Tryfonas, Paul Owen and Paula Thomas* *Faculty of Advanced Technology, University of Glamorgan, U K*	281-290

Paper Title	Author(s)	**Proceedings Page**
Network Forensics of SSL/TLS Encrypted Channels	*Meng-Da Wu and Stephen Wolthusen* *Information Security Group, Royal Holloway, University of London, UK*	303-312
Lexical Natural Language Steganography Systems with Human Interaction	*Brecht Wyseur, Karel Wouters and Bart Preneel* *K.U. Leuven, Heverlee, Belgium*	313-320
Experential Operations: An Information-Based Operational Management Approach for Managing National Security Operations	*Ken Webb* *Edith Cowan University, Perth, Western Australia*	291-302
Public Key Usage Model in Converge Network	*Lee Fueng Yap[1] and Andy Jones[23]* *[1]British Telecommunications plc., Asian Research Centre, Kuala Lumpur, Malaysia* *[2]British Telecommunications plc., Security Research Centre, Ipswich, UK* *[3]Adjunct, Edith Cowan University, Perth, Australia*	321-326
Investigating the Evasion-Resilience of Network Intrusion Detection Systems	*JarleYtreberg and Maria Papadaki* *University of Plymouth, Plymouth, UK*	327-334
Identifying Computers Hidden Behind a NAT using Machine Learning Techniques	*Ori Zakin, Metal Levi, Yuval Elovici, Lior Rockach, Nir Shafrir, Guy Sinter and Ofer Pen* *Ben-Gurion University of the Negev, Beer-Sheva, Israel*	335-340
NATO's war on Terror and the Electronic Medium: A Retrospective Analysis on Combating Terrorist Iinsurgence	*Marios-Panagiotis Efthymiopoulos[1] and Josef Demergis[2]* *[1]University of Crete, Greece* *[2]University of Macedonia, Greece,*	341-348