

# **4th European Conference on Information Warfare and Security 2005**

**(ECIW 2005)**

**Glamorgan, United Kingdom  
11-12 July 2005**

**Editors:**

**Bill Hutchinson**

**ISBN: 978-1-62276-530-0**

**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, (2005). 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](mailto: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](mailto:curran@proceedings.com)  
Web: [www.proceedings.com](http://www.proceedings.com)

# ECIW 2005

## Contents

<b>Paper Title</b>	<b>Author(s)</b>	<b>Proceedings Page</b>
Preface		vi
Biographies of Conference Chairs, Programme Chair and Keynote Speaker		viii
Biographies of contributing authors		ix
Governance Principles for Sharing Information in the Network Enabled Capability (NEC) Environment	<i>Debi Ashenden RMCS, Cranfield University, Shrivenham, UK</i>	1
Data Unification and Data Fusion of Intrusion Detection Logs in a Network Centric Environment	<i>Nikolaos Avourdiadis and Andrew Blyth University of Glamorgan, Pontypridd, Wales-UK</i>	9
Incorporating Security Requirements Into the Software Development Process	<i>T. Balopoulos<sup>1</sup>, S.Dritsas<sup>2</sup>, L.Gymnopoulos<sup>1</sup>, M.Karyda<sup>2</sup>, S.Kokolakis<sup>1</sup>, S.Gritzalis<sup>1</sup> <sup>1</sup>University of the Aegean, Samos, Greece <sup>2</sup>Athens University of Economics and Business, Greece</i>	21
Securing Against the Possibility of an Improbable Event: Concepts for Managing Predictable Threats and Normal Compromises	<i>Richard Baskerville and Robert Sainsbury Georgia State University Atlanta, USA</i>	29
Development of a “Zero-Skills” Forensic Laptop Registration and Identification Tool	<i>Barry Blundell, Huang Xiao Dong, Jill Slay, B. Turnbull, Tom Wilsdon University of South Australia</i>	39
Agent-based Forensic Investigations with an Integrated Framework	<i>William Buchanan, J Graves, Lionel Saliou, H Al Sebea and Nikos Migas School of Computing, Napier University, Edinburgh</i>	47
An Approach for Critical Information Infrastructure Protection	<i>T. B. Busuttil, and M. J. Warren School of Information Technology, Deakin University, Australia</i>	53
Securing the Infrastructure in Information Operations	<i>Catharina Candolin Helsinki University of Technology, Finland</i>	63
Content Analysis as a Tool of Information Warfare	<i>Geoffrey Darnton Bournemouth University, Poole, UK</i>	73

<b>Paper Title</b>	<b>Author(s)</b>	<b>Proceedings Page</b>
Is NATO in Need of a Renewed Security Concept?	<i>Marios Panagiotis Efthymiopoulos Department of Politics, University of Crete, Rethimnon, Greece.</i>	83
Architecture for Near Real-Time Threat Assessment Using IDS Data	<i>Grigorios Fragkos and Andrew Blyth School of Computing, University of Glamorgan, Pontypridd, U.K</i>	91
The use of Computers Idle-Time and Parallel Processing Over a Network to Perform Password Threat Assessment	<i>Grigorios Fragkos, Konstantinos Xynos and Andrew Blyth School of Computing, University of Glamorgan, UK</i>	99
Introducing Ontology-based Security Policy Management in the Grid	<i>Lazaros Gymnopoulos and Stefanos Gritzalis University of the Aegean, Samos, Greece</i>	107
Electromagnetic (EM) Susceptibility of information Systems– The Need for Em Detection	<i>Richard Hoad<sup>1</sup> and Andrew Blyth<sup>2</sup> <sup>1</sup>QinetiQ Ltd., Cody Technology Park, Farnborough, UK <sup>2</sup>University of Glamorgan, School of Computing, Pontypridd, UK</i>	117
Analysis of Information Security Risks: Policy for Protection Through to Implementation	<i>Kay Hughes and Simon Wiseman QinetiQ, Malvern, Worcs, UK</i>	129
Pre-emptive Military Action: The Fight for Recipients - War as a Part of Story Society Created by the Media	<i>Aki-Mauri Huhtinen National Defence College, Helsinki, Finland</i>	141
The 'Will' and Information Operations	<i>William E.Hutchinson Edith Cowan University, Perth, Australia</i>	151
Finite Field Parallel Multiplier for FPGA	<i>Lory Kimsoeun, Takakazu Kurokawa, and Keisuke Iwai Department of Computer Science, National Defence Academy, Japan</i>	157
Risk Consequence Analysis as a Part of Anticipatory Decision-Making Using a Bayesian Network	<i>Pertti Kuokkanen Department of Computer Science, University of Helsinki, Finland</i>	165
Common Operational Picture, Situation Awareness and Information Operations	<i>Rauno Kuusisto<sup>1</sup>, Tuija Kuusisto<sup>1</sup> and Leigh Armistead<sup>2</sup> <sup>1</sup>National Defence College, Helsinki, Finland <sup>2</sup>Edith Cowan University, Perth, Australia</i>	175

<b>Paper Title</b>	<b>Author(s)</b>	<b>Proceedings Page</b>
Information Needs of Strategic Level Decision-Makers in Crisis Situations	<i>Tuija Kuusisto<sup>1</sup>, Rauno Kuusisto<sup>1</sup> and Terhi Yliniemi<sup>2</sup></i> <i><sup>1</sup>The National Defence College, Helsinki, Finland</i> <i><sup>2</sup>Tampere University of Technology, Finland</i>	187
The Evolution of US Military Conceptions of Information Warfare and Information Operations, 1979-2004: An Initial Report	<i>Tara Leweling and Ron Walters</i> <i>Naval Postgraduate School, Monterey, California, USA</i>	195
An Evaluation Framework for the Analysis of Covert Channels in the TCP/IP Protocol Suite	<i>David Llamas, Alan Miller and Colin Allison</i> <i>School of Computer Science, University of St Andrews, Scotland, UK</i>	205
The Threat Response Spy Files: A Case Study About an Arms Manufacturer, a Private Intelligence Company and Many Infiltrators	<i>Eveline Lubbers</i> <i>Department of Geography and Sociology, Strathclyde University</i>	215
Windows Event Logs and Their Forensic Usefulness	<i>Vivienne Mee and Iain Sutherland</i> <i>School of Computing, University of Glamorgan, Pontypridd, UK</i>	225
Phish or Treat? Understanding the Tactics and Responses to Electronic Identity Theft on the Internet.	<i>Evangelos Moustakas<sup>1</sup>, Penny Duquenoy<sup>1</sup> and C Ranganathan<sup>2</sup></i> <i><sup>1</sup>Middlesex University, London, UK <sup>2</sup>University of Illinois at Chicago, USA</i>	239
Australian Commercial - Critical Infrastructure Management Protection	<i>Graeme Pye and Matthew Warren</i> <i>School of Information Systems, Deakin University, Geelong, Australia</i>	249
Targeting a Warlord - The Challenges of Information Operations in Afghanistan	<i>Jari Rantapelkonen</i> <i>National Defence College, Helsinki, Finland</i>	261
A Two-Tier Intrusion Detection System for Mobile Ad Hoc Networks	<i>Shukor A. Razak, Steven. M. Furnell and Phil. J. Brooke</i> <i>Network Research Group, University of Plymouth, Plymouth, Devon, UK</i>	271
Visualisation Techniques: Their Application Within Unified Intrusion Detection Systems Data	<i>Huw Read and Andrew Blyth</i> <i>School of Computing, University of Glamorgan, Pontypridd, UK</i>	281
Inside and out? The Information Security Threat From Insiders	<i>Robert Rowlingson</i> <i>QinetiQ, Malvern, UK</i>	293
Novel Framework for Automated Security Abstraction, Modelling, Implementation and Verification	<i>Lionel Saliou, William J Buchanan, Jamie Graves and Jose Munoz</i> <i>School of Computing, Napier University, Edinburgh, UK</i>	303

<b>Paper Title</b>	<b>Author(s)</b>	<b>Proceedings Page</b>
Security in Symbian Smartphones: Threats, Needed Functionalities and Existing Implementations	<i>Ville Salmensuu, Joakim Koskela and Teemupekka Virtanen Helsinki University of Technology, Espoo, Finland</i>	313
Information Operations Education: Lessons Learned from Information Assurance	<i>Corey Schou<sup>1</sup>, Dan Kuehl<sup>2</sup> and Leigh Armistead<sup>3</sup> <sup>1</sup>Idaho State University, Pocatello, USA <sup>2</sup>National Defence University, Washington, DC <sup>3</sup>Edith Cowan University, Perth, Australia</i>	325
Technical Comparison of Domain Keys and Sender ID	<i>Pekka Sillanpää, Mikko Voipio and Teemupekka Virtanen Helsinki University of Technology, Espoo, Finland</i>	335
The use of Balanced Scorecards for Information Security	<i>Michael Stubbings Malvern Technology Centre, Worcestershire, UK</i>	345
Distribution of Offensive Material Over Computer Networks: A Research Agenda	<i>Theodore Tryfonas, Vivienne Mee, Iain Sutherland and Paula Thomas School of Computing, University of Glamorgan, UK</i>	355
Issues Relating to the Forensics Analysis of PDA and Telephony (PDAT) Enabled Devices	<i>Craig Valli Edith Cowan University, Perth, Western Australia</i>	363
Analyzing Threat Agents and Their Attributes	<i>Stilianos Vidalis<sup>1</sup> and Andrew Jones<sup>2</sup> <sup>1</sup>University of Glamorgan, UK <sup>2</sup>BT Group, Security Research Centre, UK</i>	369
Mail Stream Analysis Using Self-Organizing Map	<i>Mikko Voipio Helsinki University of Technology, Espoo, Finland</i>	381
Is There a Need for Enhancing National Security Against Terrorists Conducting Information Warfare? A Confident Performance for Australia Context	<i>Ken Webb Edith Cowan University, Perth, Western Australia</i>	391
Where are the Policies for PDA Usage in the Australian Healthcare Environment?	<i>Patricia A. H. Williams Edith Cowan University, Perth, Western Australia</i>	401
Towards A Validation Framework for Forensic Computing Tools in Australia	<i>Tom Wilsdon and Jill Slay University of South Australia, Adelaide, Australia</i>	409

<b>Paper Title</b>	<b>Author(s)</b>	<b>Proceedings Page</b>
Information Security Culture and Leadership	<i>Omar Zakaria Information Security Group, Royal Holloway, University of London, UK</i>	415