

3rd International Conference on Information Warfare and Security 2008

(ICIW 2008)

**Omaha, Nebraska, USA
24 – 25 April 2008**

Editors:

Leigh Armistead

ISBN: 978-1-62993-928-5

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, (2008). 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. (2014)

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

ICIW 2008

Contents

Paper Title	Author(s)	Page No.
Preface		v
Biographies of Conference Chairs, Programme Chair, Keynote Speaker and Mini-track Chairs		vii
Biographies of contributing authors		viii
Understanding IRC Bot Behaviors in a Network-centric Attack Detection and Prevention Framework	<i>Gail-Joon Ahn, Napoleon Paxton, and Kevin Pearson University of North Carolina at Charlotte, NC, USA</i>	1-10
Adapting Information Operations to a Changing World: Future Options for the United States	<i>Edwin Armistead Edith Cowan University, Perth, Australia</i>	11-16
A Framework for Improving Consistency of the Protection of Critical Technologies	<i>Eric Ashe¹, Michael Grimaila¹, and Brian Carter² ¹Air Force Institute of Technology, Wright-Patterson AFB, OH USA ²Air Force Research Laboratory, Wright-Patterson Air Force Base, OH, USA</i>	17-26
Interactive Visualization of Fused Intrusion Detection Data	<i>Serafin Avitia, Stuart Kurkowski, and Luke van der Hoeven Air Force Institute of Technology, Wright-Patterson AFB, OH, USA</i>	27-36
Jam Resistance Communications without Shared Secrets	<i>William Bahn, Leemon Baird III and Michael Collins United States Air Force Academy, Colorado Springs, CO, USA</i>	37-44
Developing Cyber Warriors	<i>Jeff Boleng, Dino Schweitzer, and David Gibson United States Air Force Academy, Colorado Springs, CO, USA</i>	45-50
Sensor Collection and Analysis of Radio Frequencies (SCARF)	<i>Jeff Boleng¹, Thorsten Wirges¹, Dino Schweitzer¹, Seana Hagerman² and Ramakrishna Thurimella² ¹United States Air Force Academy, Colorado Springs, CO USA ²University of Denver, Colorado, USA</i>	51-58
Toward Detecting Novel Software Attacks by Using Constructs from Human Cognition	<i>Adam Bryant Air Force Institute of Technology, Wright-Patterson Air Force Base, OH, US</i>	59-66
Biometric Security Enhancements Through Template Aging Matching Score Analysis	<i>John Carls¹, Richard Raines¹, Michael Grimaila¹ and Steven Rogers² ¹Air Force Institute of Technology, Wright-Patterson AFB, OH, USA ²Air Force Research Laboratory, Wright-Patterson AFB, OH USA</i>	67-76
Outsourcing and the Insider Threat: An Increasing Security Risk	<i>Carl Colwill BT Design, Security Risk and Compliance, UK</i>	77-86
The Impact of Vista and Federal Desktop Core Configuration on Incident Response	<i>Daniel Cotton, Stephen Nugen, and William Mahoney University of Nebraska at Omaha, NE, USA</i>	87-96

Paper Title	Author(s)	Page No.
Using Attack and Protection Trees to Evaluate Risk in an Embedded Weapon System	<i>Robert Cowan¹, Michael Grimaila¹ and Raju Patel²</i> <i>¹Air Force Institute of Technology, Wright Patterson Air Force Base, OH, USA</i> <i>²Aeronautical Systems Center, Wright Patterson Air Force Base, OH, USA</i>	97-108
Religion, Ideology, and Information Warfare	<i>Geoffrey Darnton</i> <i>Bournemouth University, UK</i>	109-116
An Investigation of Negative Authentication Systems	<i>Dipankar Dasgupta and Rukhsana Azeem</i> <i>The University of Memphis, TN, USA</i>	117-126
Software Agent framework for Computer Network Operations in Information Warfare	<i>Evan Dembskey and Elmarie Biermann</i> <i>Tshwane University of Technology, Pretoria, South Africa</i>	127-134
Cyber Warfare: Rethinking Strategy in the Information Age	<i>David Fahrenkrug</i> <i>8th Air Force, Barksdale Air Force Base, LA, USA</i>	135-142
Analysis of Routing Worm Infection Rates on an IPv4 Network	<i>James Gorsuch, Barry Mullins, Rusty Baldwin and Richard Raines</i> <i>Air Force Institute of Technology, Wright-Patterson Air Force Base, OH, USA</i>	143-152
A Comparison of Popular Global Authentication Systems	<i>Dennis Guster, Charles Hall, Suthantha Herath, Brittany Jansen and Lukasz Mikluch</i> <i>St. Cloud State University, St. Cloud, MN, USA</i>	153-162
Insider Threat Detection within Embedded Weapon Systems	<i>Nicholas Haan¹, Michael Grimaila¹ and Raju Patel²</i> <i>¹Air Force Institute of Technology, Wright Patterson Air Force Base, OH, USA</i> <i>²Aeronautical Systems Center, Wright Patterson Air Force Base, OH, USA</i>	163-170
Cyber Flag: A Realistic Training Environment for the Future	<i>Andrew Hansen, Paul Williams, Robert Mills and Mark Kanko</i> <i>Air Force Institute of Technology, Wright-Patterson Air Force Base, OH, USA</i>	171-178
Information Asset Value Quantification	<i>Denzil Helleesen¹, Michael Grimaila¹, Larry Fortson² and Robert Mills¹</i> <i>¹Air Force Institute of Technology, Wright-Patterson AFB, OH, USA</i> <i>²Air Force Research Laboratory, Wright-Patterson AFB, OH, USA</i>	179-188
Characterizing Malware Writers and Computer Attackers in Their own Words	<i>Thomas Holt, Joshua Soles and Lyudmila Leslie</i> <i>The University of North Carolina at Charlotte, NC, USA</i>	189-194
Computer Assisted Security Assessment through Fact Proposition Space	<i>Peter Hospodka, Qiuming Zhu, William Soutan and Ryan Nickell</i> <i>Department of Computer Science, University of Nebraska at Omaha, NE, USA</i>	195-202
Initial Supports to Regulate Information Warfare's Potentially Lethal Technologies and Techniques	<i>Berg Hyacinthe¹ and Larry Fleurantin²</i> <i>¹Infosense Technologies and Research Inc., Sunrise, FL, USA</i> <i>²Fleurantin and Associates, Miami Beach, FL, USA</i>	203-212

Paper Title	Author(s)	Page No.
Advanced Manipulation Of Digital Evidence Using Memory Based Anti-Forensic Tools	<i>Hamid Jahankhani¹, Elidon Beqiri¹ and Kenneth Revett²</i> ¹ University of East London, UK ² University of Westminster, UK	213-220
Analyzing Anonymity in Cyberspace	<i>Douglas Kelly, Richard Raines, Rusty Baldwin, Barry Mullins and Michael Grimaila</i> Air Force Institute of Technology, Wright Patterson Air Force Base, OH, USA	221-232
A Framework for Classifying Anonymous Networks in Cyberspace	<i>Douglas Kelly, Richard Raines, Rusty Baldwin, Barry Mullins and Michael Grimaila</i> Air Force Institute of Technology, Wright Patterson Air Force Base, OH, USA	233-244
A Survey of Critical Infrastructure Control System Effects	<i>Michael Kolbe and Paul Williams</i> Air Force Institute of Technology (AFIT), Wright-Patterson Air Force Base, OH, USA	245-254
Pattern Matching Information Flow using GADT	<i>Eric Lindahl and Victor Winter</i> University of Nebraska at Omaha, NE, USA	255-262
Static and Dynamic Packet Filtering on Lightly Managed Systems	<i>James Lupo and Daniel Likarish</i> Regis University, Denver, CO, USA	263-268
Organizing the United States Government for the Contemporary Environment	<i>Steven Mains</i> US Combined Arms Center, Fort Leavenworth, KS, USA	269-276
Developing a Requirements Framework for Cybercraft Trust Evaluation	<i>Todd McDonald and Shannon Hunt</i> Air Force Institute of Technology, Wright Patterson Air Force Base, OH, USA	277-284
Use of Evaluation Criteria in Security Education	<i>Thuy Nguyen and Cynthia Irvine</i> Naval Postgraduate School, Monterey, CA, USA	285-292
Implementation of a Multilevel Wiki for Cross-Domain Collaboration	<i>Kar Leong Ong, Thuy Nguyen and Cynthia Irvine</i> Naval Postgraduate School, Monterey, CA, USA	293-304
Formal Models of a Least Privilege Separation Kernel in Alloy	<i>David Phelps, Mikhail Auguston, Timothy Levin</i> Naval Postgraduate School, Monterey, CA, USA	305-314
Using Deception to Facilitate Intrusion Detection in Nuclear Power Plants	<i>Julian Rushi^{1,2} and Roy Campbell¹</i> ¹ University of Illinois at Urbana-Champaign, Urbana, IL USA ² Università degli Studi di Milano, Via Comelico Milano, Italy	315-324
Establishing the Human Firewall: Improving Resistance to Social Engineering Attacks	<i>Jamison Scheeres, Robert Mills and Michael Grimaila</i> Air Force Institute of Technology, Wright-Patterson Air Force Base, OH, USA	325-334
An Architecture for Cyber Incident Mission Impact Assessment (CIMIA)	<i>David Sorrels¹, Michael Grimaila¹, Larry Fortson², and Robert Mills¹</i> ¹ Air Force Institute of Technology, Wright-Patterson AFB OH, USA ² Air Force Research Laboratory, Wright-Patterson AFB OH, USA	335-344
Tailored Information Delivery Services for Open Source Intelligence	<i>William Sousan, Ryan Nickell, Qiuming Zhu and Pete Hospodka</i> University of Nebraska at Omaha, NE, USA	345-352

Paper Title	Author(s)	Page No.
Legal Aspects of Warfare in Cyberspace	<i>Dennis Strouble and Michael Grimaila Air Force Institute of Technology, Wright Patterson Air Force Base, OH USA</i>	353-360
Voice Based Authentication Using the Null Frequencies	<i>Sérgio Tenreiro de Magalhães¹, Carlos Guimarães², Henrique Santos², Kenneth Revett³ and Hamid Jahankhani⁴ ¹Universidade Católica Portuguesa, Portugal ²University of Minho, Guimarães, Portugal ³University of Westminster, London, UK ⁴University of East London, London, UK</i>	361-364
Towards Faster Execution of the OODA Loop Using Dynamic Decision Support	<i>Shyni Thomas, Nitin Dhiman, Pankaj Tikkas, Ajay Sharma, Dipti Deodhare Centre for Artificial Intelligence and Robotics (CAIR), Bangalore, India</i>	365-378
Creating Hardware-based Primitives to Enhance Digital Forensics in a Novel Computing Architecture	<i>Al-Nath Tuting and Paul Williams Air Force Institute of Technology, Wright-Patterson Air Force Base, OH USA</i>	379-386
Using Markov Models to Crack Passwords	<i>Renier van Heerden and Johannes Vorster DPSS, CSIR, Pretoria, South Africa</i>	387-394
Designing and Implementing a Critical Infrastructure Lab for Educational Research	<i>Dorsey Wilkin, Michael Kolbe, Richard Raines, Paul Williams and Kenneth Hopkinson Air Force Institute of Technology, Wright-Patterson Air Force Base, OH, USA</i>	395-402