

**ICIW 2007**  
**2nd International**  
**Conference on i-Warfare**  
**and Security**  
**Naval Postgraduate School, Monterey,**  
**California, USA**  
**8-9 March 2007**

Edited by

Dr Dan Remenyi  
Trinity College Dublin, Ireland

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.

ISBN: 978-1-905305-41-4

Published by Academic Conferences Limited  
Reading  
UK  
44-118-972-4148  
[info@academic-conferences.org](mailto:info@academic-conferences.org)

# ICIW 2007

## Contents

Paper Title	Author(s)	Guide Page	Proceedings Page
Preface		v	v
Biographies of Conference Chairs, Programme Chair, Keynote Speaker and Mini-track Chairs		vii	vii
Biographies of contributing authors		ix	ix
The Evolution of Information Operations, Contracts across the DoD: Opportunities for Growth in the Future for Academics	<i>Edwin Leigh Armistead<sup>1</sup> and Thomas Murphy<sup>2</sup></i> <i><sup>1</sup>Edith Cowan University, Australia</i> <i><sup>2</sup>Northlight Technologies, USA</i>	1	1-8
On Manipulability of Algorithms	<i>Sviatoslav Braynov</i> <i>University of Illinois at Springfield</i> <i>IL USA</i>	2	9-16
Developing a Framework to Improve Information Assurance Battlespace Knowledge	<i>Adam Bryant and Michael Grimaila</i> <i>Air Force Institute of Technology,</i> <i>Fairborn, OH, USA</i>	3	17-24
Security Risks in USAF Geospatial Information Sharing	<i>Scott Bryant and Michael Grimaila</i> <i>Air Force Institute of Technology</i> <i>Fairborn, OH, USA</i>	4	25-32
Performance Impact of Connectivity Restrictions and Increased Vulnerability Presence on Automated Attack Graph Generation	<i>James Cullum, Cynthia Irvine and Tim Levin</i> <i>Naval Postgraduate School,</i> <i>Monterey, CA, USA</i>	5	33-46
Analyzing Security Measures for Mobile Ad Hoc Networks Using Attack and Protection Trees	<i>Kenneth Edge, Richard Raines, Rusty Baldwin, Michael Grimaila, Christopher Reuter and Robert Bennington</i> <i>Wright-Patterson AFB, Fairborn, Oh,</i> <i>USA</i>	6	47-56
A Study of DNS Traffic Patterns on a Large Autonomous System	<i>Sid Faber<sup>1</sup> and Bert Lundy<sup>2</sup></i> <i><sup>1</sup>Software Engineering Institute,</i> <i>Pittsburgh, PA, USA</i> <i><sup>2</sup>Naval Postgraduate School,</i> <i>Monterey, CA, USA</i>	7	57-68
Development of a Defensive Cyber Damage Assessment Framework	<i>Larry Fortson and Michael Grimaila</i> <i>Air Force Institute of Technology,</i> <i>Fairborn, OH, USA</i>	8	69-76
Anti-Forensics: Techniques, Detection and Countermeasures	<i>Simson Garfinkel</i> <i>Naval Postgraduate School,</i> <i>Monterey, CA, USA</i>	9	77-84
IPv6: World Update	<i>Kenneth Geers and Alexander Eisen</i> <i>NCIS Washington, DC, USA</i>	10	85-94
Leap in the Dark: An Attempt to Theorize Personnel Anomaly Detection for Countering Insider Threats	<i>Shuyuan Mary Ho</i> <i>Syracuse University, NY, USA</i>	11	95-100

Paper Title	Author(s)	Guide Page	Proceedings Page
Conceptual Design of a Microfluidics Suppressor to Protect against Potentially Lethal Printing Devices: A Scenario-based Physical Cyber Security Measure	<i>Berg Hyacinthe<sup>1</sup> and Yves Anglade<sup>2</sup></i> <i><sup>1</sup>Florida State University, Tallahassee, FL, USA</i> <i><sup>2</sup>Florida A&amp;M University, Tallahassee, FL, USA</i>	12	101-110
'Virtual' Security Teaching Techniques – Teaching IA methods using VMWare Teams	<i>Derek Isaacs</i> <i>Colorado Technical University, and Boecore Inc, Colorado Springs CO, USA</i>	13	111-116
Differential Power Analysis Attacks against AES Circuits Implemented on a FPGA	<i>Keisuke Iwai, Minoru Sasaki and Takakazu Kurokawa</i> <i>National Defense Academy, Japan</i>	14	117-122
Categorization of Profiles for PSYOPs: Can Technology Help?	<i>Magdi Kamel, Mark Eramo, and Christopher Sutter</i> <i>Naval Postgraduate School, Monterey, CA, USA</i>	15	123-132
Implications of Information Flow Priorities for Interorganizational Crisis Management	<i>Tuija Kuusisto<sup>1</sup>, Rauno Kuusisto<sup>2</sup> and Mark Nissen<sup>3</sup></i> <i><sup>1</sup>Ministry of Defence, Helsinki, Finland</i> <i><sup>2</sup>National Defence University, Helsinki, Finland</i> <i><sup>3</sup>Naval Postgraduate School, Monterey, CA, USA</i>	16	133-140
Thinking Strategically About Information Operations	<i>Irving Lachow and Robert Miller</i> <i>National Defense University, Washington, DC, USA</i>	17	141-146
Intrusion Detection in open Source Software via Dynamic Aspects	<i>William Mahoney and William Sousan</i> <i>University of Nebraska at Omaha, NE, USA</i>	18	147-154
Fine-Grain Security for Military-Civilian-Coalition Operations Through Virtual Private Workspace Technology	<i>R William Maule and Shelley Gallup</i> <i>Naval Postgraduate School, Monterey, CA, USA</i>	19	155-162
Creating Hardware-based Primitives that Facilitate the Exposure of State Information Useful for Security Related Monitoring	<i>Stephen Mott and Paul Williams</i> <i>Air Force Institute of Technology, Fairborn, OH, USA</i>	20	163-170
Graphical Based user Authentication with Embedded Mouse Stroke Dynamics	<i>Ken Revett<sup>1</sup>, Sergio Tenreiro de Magalhaes<sup>2</sup> and Henrique Santos<sup>2</sup></i> <i><sup>1</sup>University of Westminster, London, Uk</i> <i><sup>2</sup>University do Minho, Portugal</i>	21	171-176
Planning Cost-Effective Deceptive Resource Denial in Defense to Cyber-Attacks	<i>Neil Rowe</i> <i>U.S. Naval Postgraduate School, CA, USA</i>	22	177-184
Experiments with a Testbed for Automated Defensive Deception Planning for Cyber-Attacks	<i>Neil Rowe, Han Goh, Sze Lim, and Binh Duong</i> <i>U.S. Naval Postgraduate School, CA, USA</i>	23	185-194

Modified RSL as a Countermeasure Against Differential Power Analysis	<i>Minoru Sasaki, Keisuke Iwai and Takakazu Kurokawa National Defense Academy, Japan</i>	205-216
A Framework for Relating Cyberspace Operations to the Cognitive and Physical Domains	<i>Tiffany Smith<sup>1</sup>, Pamela Woolley<sup>2</sup>, Robert Mills<sup>1</sup>, and Richard Raines<sup>1</sup> <sup>1</sup>Air Force Institute of Technology, Fairborn, OH, USA <sup>2</sup>Fairchild AFB WA, USA</i>	217-224
Similarity Analysis of Malicious Executables	<i>Anthonius Sulaiman, Sandeep Mandada, Srinivas Mukkamala and Andrew Sung New Mexico Tech, Socorro, NM, USA</i>	225-232
Using Deception for assuring Security	<i>Stilianos Vidalis, Eric Llewellyn and Chrostopher Tubbs University of Wales, Newport ,UK</i>	233-240
The Design Space of Metamorphic Malware	<i>Andrew Walenstein<sup>1</sup>, Rachit Mathur<sup>2</sup>, Mohamed Chouchane<sup>1</sup>, and Arun Lakhota<sup>1</sup> <sup>1</sup>University of Louisiana at Lafayette, LA, U.S.A. <sup>2</sup>McAfee Avert Labs, Beaverton, OR, U.S.A.</i>	241-248
Information Terrorism in the New Security Environment	<i>Ken Webb RNSA and Edith Cowan University, Perth, Western Australia</i>	249-256
Inter-Network Operations Center Dial-By-ASN (INOC-DBA), a Hotline for Critical Internet Infrastructure Management	<i>Bill Woodcock<sup>1</sup> and Ross Stapleton-Gray<sup>2</sup> <sup>1</sup>Packet Clearing House, Berkeley, CA, USA <sup>2</sup>Internet Awareness, Inc., Berkeley, CA, USA</i>	257-262
SME Security in the Digital age	<i>Don Milne<sup>1</sup>, John McCarthy<sup>2</sup>, and Bryan Mills<sup>2</sup> <sup>1</sup>Buckinghamshire Chilterns University College, High Wycombe, UK <sup>2</sup>Service Tec Global Services Ltd, UK</i>	263-270

## Preface

Welcome to the Second International Conference on Information Warfare and Security (ICIW 2007), hosted this year by the Naval Postgraduate School in Monterey, California. The Conference Chair is Dr Dorothy Denning from the Naval Postgraduate School and the Programme Chair is Leigh Armistead from Edith Cowan University in Perth, Australia.

The main aim of this Conference is for individuals working in the area of Information Warfare and Information Security to come together to share knowledge with peers interested in the same area of study.

The opening keynote address this year is given by Tim Thomas, Foreign Military Studies Office, Army Command and Staff College, Fort Leavenworth, USA on the topic of "*Decoding the Virtual Dragon*". On day two of the conference the keynote speaker is John Arquilla from the Naval Postgraduate School, who will talk on "*Information Warfare Today*".

An important benefit of attending this conference is the ability to share ideas and meet the people who hold them. The range of papers will ensure an interesting two days. The topics covered by the papers this year illustrate the depth of the information operations' research area, with the subject matter ranging from the highly technical to the more strategic visions of the use and influence of information. To further enhance the conference experience Leigh Armistead will lead an interactive session encouraging debate and discussion the current status of research in the I-Warfare and Security area.

With an initial submission of 60 abstracts, after the double blind, peer review process there are 33 papers published in these Conference Proceedings. These papers illustrate the true International spread of the conference, coming from Australia, Finland, Japan, United Kingdom, United States.

I wish you a most enjoyable conference.

Leigh Armistead  
Edith Cowan University  
Programme Chair

### *Conference Executive:*

[Edwin Leigh Armistead](#), Edith Cowan University, Australia  
[Sviatoslav Braynov](#) University of Illinois at Springfield, IL, USA  
[Dorothy Denning](#), Naval Postgraduate School, Monterey, CA, USA  
[Steve Iatrou](#), Naval Postgraduate College, Monterey, CA, USA  
[Andy Jones](#), Security Research Centre, BT, UK and Edith Cowan University, Australia  
[Dan Kuehl](#), National Defense University, Washington DC, UK,  
[Tara Leweling](#), Naval Postgraduate School, Monterey, CA, USA  
[Corey Schou](#), Idaho State University, USA  
[Stylianios Vidalis](#), University of Glamorgan, UK

### *Conference Committee:*

The conference programme committee consists of key people in the information systems, information warfare and information security communities around the world. The following people have confirmed their participation:

Leigh Armistead (Edith Cowan University, Australia); John Arquila (Naval Postgraduate School, USA); [Richard Baskerville](#) (Georgia State University, USA); Elisa Bertino (CERIAS, Purdue University, USA); Matt Bishop (University of California, USA); Alexander Bligh (College of Judea and Samaria, Israel); [Sviatoslav Braynov](#) (University of Illinois, USA); Rodney Clare (EDS and the Open University, UK); Geoffrey Darnton, (University of Bournemouth, UK); [Dipankar Dasgupta](#) (University of Memphis, USA); Dorothy Denning (Naval Postgraduate School, USA); Glenn Dietrich (University of Texas, USA); [Xinwen Fu](#) (Dakota State University, USA); Kevin Gleason (KMG Consulting, MA, USA); [Sanjay Goel](#) (University at Albany, USA); [Drew Hamilton](#) (Auburn University, USA); Dwight Haworth (University of Nebraska at Omaha, USA); Philip Hippensteel (Penn State University, USA); Bill Hutchinson (Edith Cowan University, Australia); Berg P Hyacinthe (Florida State University, USA); Cynthia Irvine (Naval Postgraduate School, USA); Andy Jones (British Telecom, UK); Dan Kuehl (National Defense Forces, USA); Tuija Kuusisto (National Defence College, Finland); Arun Lakhotia (University of Louisiana Lafayette, USA); Michael Lavine (John Hopkins University, USA); Tara Leweling (Naval Postgraduate School, USA); [Bin Lu](#) (West Chester University, USA); Bill Mahoney (University of Nebraska, USA); John McCarthy (Buckinghamshire and Chiltern University College, UK); Anne McGee (Industrial College of the Armed Forces, USA); [Don Milne](#) (Buckinghamshire and Chiltern University College, UK); [Evangelos Moustakas](#) (Middlesex University, UK); [Richard Raines](#) (Airforce Institute of Technology, USA); [Ken Revett](#) (University of Westminster, UK); [Neil Rowe](#) (US Naval Postgraduate School, USA); Julie Ryan (George Washington University, USA); Corey Schou (Idaho State University, USA); [Dan Shoemaker](#) (University of Detroit Mercy, USA); [Kevin Streff](#) (Dakota State University, USA), [Doug Twitchell](#) (Illinois State University, USA); Stylianios Vidalis (University of Glamorgan, UK); [Tom Wilsdon](#) (University of South Australia, Australia); William Yurcik (University of Illinois at Urbana-Champaign, USA); Zehai Zhou (Dakota State University, USA).

## Biographies of Conference Chairs, Programme Chair and Keynote Speaker



### Conference Chair

**Dorothy Denning** is a Professor in the Department of Defense Analysis and a member of the Center on Terrorism and Irregular Warfare at the Naval Postgraduate School. Her current research and teaching encompasses the areas of conflict and cyberspace, trust and influence, terrorism and crime, and information operations and warfare. She is author of *Information Warfare and Security* and over 130 articles, and has testified before the U.S. Congress on encryption policy and cyberterrorism.

### Programme Chair

**Leigh Armistead** is the Strategic IO/IA Development Manager for Honeywell Technology Solutions Inc. He has written two books, the most recent *Information Operations: Warfare and The Hard Reality of Soft Power* (Brassey's, August 2003) which serves as a textbook for a number of DoD organizations. Formerly a Master Faculty at the Joint Forces Staff College, Leigh is currently enrolled in a PhD program at Edith Cowan University with an emphasis on Information Operations, where he also serves on the Editorial Review Board for European Conference on Information Warfare, is a Co-Editor for the *Journal of International Warfare* and the Chairman for the IQPC annual conference on Information Operations.



### Keynote Speaker

**Dr John Arquilla** earned his degrees in international relations from Rosary College (BA 1975) and Stanford University (MA 1989, PhD 1991). He is professor of defense analysis at the Naval Postgraduate School, where he has taught in the special operations curriculum since 1993. He also serves as director of the Information Operations Center. His teaching interests revolve around the history of irregular warfare, terrorism, and the implications of the information age for society and security. His books include: *Dubious Battles: Aggression Defeat and the International System* (1992); *From Troy to Entebbe: Special Operations in Ancient & Modern Times* (1996), which was a featured alternate of the Military Book Club; *In Athena's Camp* (1997); *Networks and Netwars: The Future of Terror, Crime and Militancy* (2001), named a notable book of the year by the American Library Association; and *The Reagan Imprint: Ideas in American Foreign Policy from the Collapse of Communism to the War on Terror* (2006). His next book will be about military innovation.

Dr. Arquilla is also the author of more than one hundred articles on a wide range of topics in military and security affairs, with his work appearing in both the leading academic journals and in more general publications like *Wired* and *The New Republic*. He is best known for his concept of "netwar" (i.e., the distinct manner in which those organized into networks fight), a term which former defense secretary Donald Rumsfeld used on several occasions to describe the ongoing conflict in Iraq. His vision of "swarm tactics" was selected by *The New York Times* as one of the "big ideas" of 2001. In terms of policy experience, Dr. Arquilla worked as a consultant to General Norman Schwarzkopf during

Operation Desert Storm, as part of a small team of RAND analysts. During the Kosovo War, he assisted deputy secretary of defense John Hamre on a range of issues in international information strategy. Since the onset of the war on terror, Dr. Arquilla's policy contributions have included a brief period of service on the Information Operations Task Force, followed by more extended involvement with the 1<sup>st</sup> Marine Expeditionary Force, and other units, on practical, information-related "field problems." Currently, he guides an initiative at the request of the vice chairman of the joint chiefs.

### **Keynote Speaker**

**Timothy Thomas** is an analyst at the Foreign Military Studies Office (FMSO) at Fort Leavenworth, Kansas. He retired from the U.S. Army as a Lieutenant Colonel in the summer of 1993. Mr. Thomas received a B.S. from West Point and an M.A. from the University of Southern California. He was a U.S. Army Foreign Area Officer who specialized in Soviet/Russian studies. His military assignments included serving as the Director of Soviet Studies at the United States Army Russian Institute (USARI) in Garmisch, Germany; as an inspector of Soviet tactical operations under CSCE; and as a Brigade S-2 and company commander in the 82nd Abn Division. Mr. Thomas has done extensive research and publishing in the areas of peacekeeping, information war, psychological operations, low intensity conflict, and political-military affairs. He is the assistant editor of the journal *European Security*; an adjunct professor at the U.S. Army's Eurasian Institute; an adjunct lecturer at the USAF Special Operations School; and a member of two Russian organizations, the Academy of International Information, and the Academy of Natural Sciences.



## Biographies of contributing authors (in alphabetical order)

**Edwin Armistead:** The Strategic Information Assurance Development Manager for Honeywell Technology Solutions Inc, Leigh was also the editor of Information Operations: Warfare and The Hard Reality of Soft Power (Brasseys, May 2004). A retired US Naval Officer and Master Faculty (IO) at the Joint Forces Staff College, he is currently enrolled in a PhD program at Edith Cowan University (Perth, AU). Leigh has published a number of articles on IO in addition to chairing numerous professional IO conferences around the world, including the International Conference on Information Warfare (2006) and the IQPC IO Conference in the United Kingdom (2002-2005). Selected five years in a row as a research fellow for the International National Security Studies program to conduct IO related research, he also helped to develop an online IO course for the National Security Agency.

**Richard Baskerville's** research and authored works regard security of information systems, methods of information systems design and development, and the interaction of information systems and organizations. He is a Chartered Engineer, holds a B.S. summa cum laude, from The University of Maryland, and the M.Sc. and Ph.D. degrees from The London School of Economics, University of London.

**Sviatoslav (Svet) Braynov** (Dr) is an Assistant Professor at the Computer Science Department at the University of Illinois at Springfield. He has published more than 40 papers in refereed conferences and journals. He was also an invited speaker to several conferences, delivered several tutorials, and has served as a co-chair and a program committee member of more than 15 international conferences and workshops. His research interests include computer security, information warfare, electronic commerce, artificial intelligence, and game theory.

**Adam Bryant** (Captain) completed a B.S. in Social Psychology from Park University in 2001 and was commissioned in 2002. He was promoted to Captain in May 2006. He is a candidate for dual M.S. degrees from the Air Force Institute of Technology in Information Resource Management and Computer Systems, specializing in IA management and database systems

**Scott Bryant** (Captain) USAF is currently working on his Masters degree in Engineering Management at the Air Force Institute of Technology, Wright-Patterson AFB, OH. He served as the initial GeoBase Integration Officer at Elmendorf AFB, AK and as the War Fighting Headquarters' Chief of Resource, Environment, and GeoBase; 7th Air Force, Osan, AB, Republic of Korea, from 2003-2005.

**Mohamed Chouchane** is working towards his Ph.D. in Computer Science at the Center for Advanced Computer Studies in University of Louisiana at Lafayette. In his PhD dissertation he is studying the computational, complexity theoretic and practical aspects of the recognition of the output of metamorphic engines. He is a co-author of the paper "Normalizing Metamorphic Malware Using Term Rewriting" that was awarded the Best Paper Award of the IEEE Workshop on Source Code Analysis and Manipulation, 2006

**James Cullum** holds a Masters of Computer Science, specializing in Information Assurance, from the Naval Postgraduate School. In his thesis work he examined automated attack graph generation software, with Dr. Cynthia E. Irvine. While an intern at the FAA he studied vulnerability analysis.

**Kenneth Edge** is a Major in the U.S. Air Force. He is currently a PhD candidate at the Air Force Institute of Technology in Dayton, Ohio. His research interests include software protection and algorithms. He received his B.S. degree from the U.S. Air Force Academy in Colorado Springs, Colorado and his M.S. from Wright State University in Dayton, Ohio.

**Sid Faber** is an analyst at CERT, at the Software Institute, Carnegie Mellon University. He is an experienced network security analyst, and has a BS in Electrical Engineering from Penn State and MS in Information Science from the University of Pittsburgh.

**Larry Fortson** (Captain) USAF served as a network security operations commander at the AFNOC NSD and was deployed in Baghdad, Iraq. He is currently working on his Master's degree at the Air Force Institute of Technology with a concentration in Information Assurance Management. Capt Fortson's research focuses on operational damage assessment to enable mission capability impact following cyber-information incidents.

**Simson Garfinkel** is an Associate Professor at the Naval Postgraduate School. Dr. Garfinkel has research interests in computer forensics, the emerging field of usability and security, and personal information management. Garfinkel is the author or co-author of fourteen books on computing.

**Kenneth Geers**, the Naval Criminal Investigative Service (NCIS) Cyber Division Chief, has worked for many years as a translator, programmer, Web developer, and analyst. He also waited tables in Luxembourg, harvested grapes in the Middle East, climbed Mount Kilimanjaro, was bitten by a deadly spider in Zanzibar and made Trappist beer at 3 AM in the Rochefort monastery. The oddest job he had was working on the John F. Kennedy Assassination Review Board (don't ask). Mr. Geers is the author of *Cyber Jihad* and the *Globalization of Warfare*; *hacking in a Foreign Language: A Network Security Guide to Russia*; *Sex, Lies, and Cyberspace: Behind Saudi Arabia's National Firewall*; and *Greetz from Room 101*.

**Berg Hyacinthe** is completing a PhD in Information at Florida State University. His research interests encompass: Social Informatics, Information Warfare, and Emerging Technologies. His current research on cyber-assisted olfaction technologies will encapsulate (a) users' adoption of these technologies and (b) potential applications of these technologies to global defence and security.

**Derek Isaacs**-CISSP has 24+ years of experience in the Computer Security / Information Assurance area. He has a strong technical knowledge of a variety of platforms, security administration and protocols. Derek is an IA Engineer for Boecore Inc at the Joint National Integration Center (JNIC). Derek provides Information Assurance support for DITSCAP/DIACAP on a variety of Programs. Tasks include developing detailed System Security Authorization Agreements (SSAA), Trusted Facilities Manuals (TFM), Security Features Users Guides (SFUG), Finite State Machine Documents (FSM) and Certification Test & Evaluation (CT&E) Plans and Procedures. He also performs security assessment and testing (DISA Gold and Platinum disk) as well as other vulnerability tools Retina, ISS, (Nessus/Nmap).

**Keisuke Iwai** received the B.E. degree in electrical engineering from Waseda University, Tokyo, Japan in 1996 and the M.E. degree in computer science from Keio University, Tokyo, Japan in 1998 respectively. He also received Dr. Eng. degree in Science for open and environmental systems from Keio University, Tokyo, Japan. Presently he is a research associate at the National Defense Academy of Japan. His research interests are

optimizing compilers, multiprocessor architectures, reconfigurable processors and differential power analysis against cryptographic circuits.

**Shuyuan Mary Ho** researches design, criteria and mechanisms in “Personnel Anomaly Detection (PAD) for countering Insider Threat” and conceptualizes a Security Architecture for management executives, at the School of Information Studies, Syracuse University. Shuyuan is a CISSP by (ISC)2, a CISM by ISACA, and has been actively involved in technologies such as VPN, CA, RBAC, FW, IDS, vulnerability assessment, and policy management

**Magdi Kamel** (Dr) is an Associate Professor of Information Systems in the Division of Computer and Information Sciences and Operations at the Naval Postgraduate School. His research interests are in the areas of database management and knowledge base systems. He is particularly interested in database models and languages, data modeling, data and text mining, and knowledge discovery in large databases.

**Tuija Kuusisto** works as a Chief Information Officer for Ministry of Defence in Finland and as an adjunct professor for National Defence College and Helsinki University of Technology in Finland. She has over 20 years experience in the information and knowledge management field and especially in the geographic information management area. She has published over 50 articles in international and national journals, conference proceedings and books.

**Irving Lachow** is a Senior Research Professor at the National Defense University’s Information Resources Management College. He has also worked for Booz Allen Hamilton, the RAND Corporation, and the Department of Defense. Dr. Lachow received his Ph.D. in Engineering & Public Policy from Carnegie Mellon University. He earned a B.A. Political Science and a B.S. in Physics from Stanford University.

**Bert Lundy** is a faculty member at the Computer Science Dept, Naval Postgraduate School. He has done extensive work in network protocols. He has a PhD from Georgia Tech in computer science.

**William Mahoney** received his B.A. and B.S. degrees from Southern Illinois University, and his M.A. and Ph.D. degrees from the University of Nebraska. He is a Research Fellow and Graduate Faculty at the University of Nebraska at Omaha Peter Kiewit Institute. His primary research interests include compilers, hardware and instruction set design, and VLSI. Prior to the Kiewit Institute Dr. Mahoney worked for 20+ years in the computer design industry, specifically in the areas of embedded computing and real-time operating systems. During this time he was also on the part time faculty of the University of Nebraska at Omaha. His outside interests include bicycling, photography, and more bicycling.

**R. William Maule** is Research Associate Professor of Information Science at the Naval Postgraduate School in Monterey, CA

**Robert Mills** is an Assistant Professor of Electrical Engineering at the Air Force Institute of Technology (AFIT), Wright-Patterson Air Force Base, Ohio. He received his Ph.D. in electrical engineering from the University of Kansas in 1994, his MSEE from AFIT in 1987, and BSEE from Montana State University in 1983. His research interests include communication systems, network management and security, information warfare, and systems engineering.

**Stephen Mott** graduated the United States Air Force Academy in Colorado Springs, CO as a member of the class of 2005 with a Bachelors of Science in Electrical Engineering. He is currently working towards his Masters of Science in Electrical Engineering at the Air Force Institute of Technology at Wright-Patterson Air Force Base, OH.

**Ken Revett** is a researcher in biometrics with an emphasis on enhancing C2 level security systems. Although his focus has been on keystroke dynamics, he is investigating incorporating physiological biometrics within the graphical user authentication. This paper presents some of our preliminary research into this exciting new topic.

**Neil Rowe** is Professor of Computer Science at the Naval Postgraduate School where he has been since 1983. His primary interest is information security, and he has also done research on data mining, robotics, computer vision, and intelligent tutoring systems. He is the author of 120 research papers and a book.

**Minoru Sasaki** graduated from National Defense Academy. He joined the Japan Maritime Self Defense Force in 2001. His rank is lieutenant junior grade. He is enrolled in National Defense Academy as a senior graduate student. Moreover, he is interested in reconfigurable architecture as well as computer security.

**Srinivas Mukkamala** is a senior research scientist with ICASA (Institute for Complex Additive Systems Analysis, a statutory research division of New Mexico Tech performing work on information technology, information assurance, and analysis and protection of critical infrastructures as complex interdependent systems) and Adjunct Faculty of the Computer Science Department of New Mexico Tech. He is a frequent speaker on information assurance in conferences and tutorials. He leads a team of information assurance (IA) "first responders" who are deployed at the request of various government agencies and financial institutions around the state of New Mexico to perform vulnerability analysis, information system security audits, network analysis and forensic incident analysis. He has a patent pending on Intelligent Agents for Distributed Intrusion Detection System and Method of Practicing the Same.

**Stilianos Vidalis** (Dr) received his PhD in Threat Assessment in July 2004 from the University of Glamorgan. He is currently a lecturer in the University of Wales, Newport, at the department of Computing and Engineering, where he is lecturing in the subjects of information security and computer networks in both the undergraduate and postgraduate level. His research interests are in the areas of information security, Information operations, threat assessment, network security, effective computer defence mechanisms and intrusion detection systems.

**Andrew Walenstein** is a Research Scientist at the University of Louisiana at Lafayette. He received his Ph.D. in 2002 from Simon Fraser University. His research interests include reverse engineering and malware analysis, program comprehension, visualization and human-computer interaction, and software engineering.

**Ken Webb.** After graduating from the Royal Military College, Ken mainly served as a qualified commissioned officer with the SAS and other special operations units, such as commanding strategic counter-terrorist, intelligence-gathering and unconventional warfare elements, where he also focused on special operations in the information warfare area. Upon leaving the military he worked globally in the information operations field and is about to complete a doctoral level research project for the Government into enhancing national security from the information operations of terrorist groups. Ken is also the

counter-terrorism research leader for the RNSA, which is a Government initiative aimed at identifying and fostering academic, industry and government research into safeguarding Australia.

**Bill Woodcock** is research director of Packet Clearing House, a non-profit research institute dedicated to understanding and supporting Internet traffic exchange technology, policy, and economics. Bill has operated national and international Internet service provision and content delivery networks since 1989, and currently spends most of his time building Internet exchanges in developing countries.

# The Evolution of Information Operations Contracts across the DoD: Growth Opportunities for Academic Research

Edwin Leigh Armistead<sup>1</sup> and Thomas Murphy<sup>2</sup>

<sup>1</sup>Edith Cowan University, Australia

<sup>2</sup>NorthLight Technologies, USA

**Abstract:** The development of Information Operations (IO) as a major military area of concentration in the United States is a relatively new phenomenon, with the first unclassified doctrine only being released within the last ten years (Joint Publication 3-13, *Joint Doctrine for Information Operations*, 9 October 1998). IO is a superset of other military operations such as Psychological Operations (PSYOP), Electronic Warfare (EW), Operations Security (OPSEC) and Information Assurance (IA). Hence IO is often viewed as an overarching integrating strategy that is still maturing, when compared to the older legacy warfare communities mentioned above. This view has in the author's opinion led to an overall lack of support from a fiscal, personnel and policy perspective. The diffuse nature of IO may also lead to confusion or lack of awareness of research opportunities by academics, especially with regard to aligning oneself to Department of Defense (DoD) contracts. Normally a rich source of funding or grants, at first glance it appears that the DoD contract opportunities in the IO and Information Warfare (IW) areas, are more scattered than and not as numerous as the more specific skill sets such as IA and Information Technology (IT). For example, One can easily cite very large DoD and Federal IA contracts such as DISA I-Assure, ANSWER, Millenia, etc., that are all worth billions of dollars, which are available to the DoD to support IT and IA issues. But the same cannot often be readily be said of IO and IW, where the appearance is the contract vehicles that are available tend to be fewer and much smaller. The questions for this paper are then does this dichotomy really exist? Is so, why? If not, why is this assumption so readily accepted? Finally, where are the main DoD contracts in the IO and IW arena that are available to access for academic researchers? Are the majority of these opportunities based on the older legacy areas of EW, PSYOP, IA, etc or on the more broader issue area of IO and IW?. This paper will attempt to answer these questions as it addresses the evolution and development of IO and IW contracts across the DoD, and their potential for academic researchers. It will show why the differential has developed with other areas such as IA, and what are the current opportunities are that exist today. This paper will also show what the future may hold for further growth in this area and how the growth of IO, IW and IA contract vehicles can benefit universities and academics. Finally, this paper will also suggest future areas of research that academics may be interested in exploring, to best optimize their ability to secure grants and contracts over the next few years.

**Keywords:** Information operations, department of defense, contracts, information warfare, proposals

# On Manipulability of Algorithms

**Sviatoslav Braynov**

**University of Illinois at Springfield, IL, USA**

**Abstract:** In adversarial situations, the input data to an algorithm could be manipulated to make the algorithm produce erroneous output or to make a wrong decision. The paper presents a formal definition and a model of algorithm manipulation from a game-theoretic point of view. Algorithm manipulation is viewed as a game between a decision maker and an adversary. The decision maker runs an algorithm to make a decision, whereas the adversary manipulates the input data to his own advantage and to the disadvantage of the decision maker. The paper also proposes a method for decision making based on manipulated input. According to the method, the decision strategy and the manipulation must be in Nash equilibrium. In other words, the decision strategy is the best response to the manipulation and vice versa, the manipulation is the best response to the decision strategy.

**Keywords:** data manipulation, decision making, algorithm design, adversarial learning, adversarial planning, adversarial plan recognition.

# **Developing a Framework to Improve Information Assurance Battlespace Knowledge**

**Adam Bryant and Michael Grimaila**

**Air Force Institute of Technology, Fairborn, OH, USA**

**Abstract:** In any organization that operates in cyberspace, it is necessary to clearly understand the information battlespace. Defensive information battlespace knowledge can be provided by detailed analysis of carefully selected metrics using automated analysis, data mining, and data calls. Gathering data for metrics involves many of the same pitfalls as collecting data in research but also incurs the intra-organizational communication problems inherent in organizations. These factors make it difficult to turn data and metrics into decision-ready knowledge. This paper explores data gathering in an organization as a research program and a knowledge transfer activity.

**Keywords:** Information assurance, metrics, strategic alignment

# Security Risks in USAF Geospatial Information Sharing

Scott Bryant and Michael Grimaila

Air Force Institute of Technology, Fairborn, OH, USA

**Abstract:** Technological advancements such as Geospatial Information Systems (GIS) and the Internet have made it easier and affordable to share information, thus enabling complex and time sensitive decisions to be made with higher confidence. However, the sharing of information also increases the likelihood that an adversary can gain illicit access to the information. Today's military leaders are faced with the challenge of deciding how to make geospatial information collected on military installations and organizations available to authorized communities of interest while simultaneously restricting access to protect operational security. In this paper, we explore the security implications of the US Air Force's applied Geospatial Information System (GeoBase) program. We examine the rapid expansion of the use of GeoBase to communities outside of the civil engineering field; examine the intrinsic and extrinsic security risks of the unconstrained sharing of geospatial information; and explore difficulties encountered when attempting to facilitate sharing geospatial information sharing while minimizing the associated operational risks.

**Keywords:** Geospatial information security, USAF geoBase, terrorism, targeting, information sharing

# Performance Impact of Connectivity Restrictions and Increased Vulnerability Presence on Automated Attack Graph Generation

James Cullum, Cynthia Irvine and Tim Levin  
Naval Postgraduate School, Monterey, CA, USA

**Abstract:** The current generation of network vulnerability detection software uses databases of known vulnerabilities and scans target networks for these weaknesses. The results can be voluminous and difficult to assess. Thus, the success of this technology has created a need for software to aid in network vulnerability analysis. Although research has shown the effectiveness of automated attack graph generation tools in displaying potential attack paths in a network, research involving the performance of these tools has been limited. The performance impact of connectivity restrictions and the number of vulnerabilities present on a network for these tools is not well understood. Using empirical testing, we have collected quantitative data using CAULDRON, an attack graph generation tool developed at George Mason University, on a collection of simulated networks defined to modulate connectivity at certain points in our networks and represent the number of vulnerabilities present per node. By defining our model to include sets of nodes, which allow connectivity from all nodes to all vulnerable nodes in the set; the number of nodes present in each set, the number of connections between sets; and the number of vulnerabilities per node as our variables, we are able to observe the performance impact on CAULDRON of both connectivity restrictions and the increased presence of vulnerabilities in our networks. The effect of these variables on processing time and memory usage is presented and can be used as a metric to assess the scalability of this tool within various customer environments.

**Keywords:** Attack graph, network, exploits, vulnerability analysis, performance.

# Analyzing Security Measures for Mobile Ad Hoc Networks Using Attack and Protection Trees

Kenneth Edge<sup>1</sup>, Richard Raines<sup>1</sup>, Rusty Baldwin<sup>1</sup>, and Michael Grimaila<sup>1</sup>

<sup>1</sup>Air Force Institute of Technology, Fairborn, OH, USA

Christopher Reuter<sup>2</sup> and Robert Bennington<sup>2</sup>

<sup>2</sup>Air Force Research Laboratory, Fairborn, OH, USA

**Abstract:** Mobile Ad Hoc Networks (MANETs) consist of multiple individual wireless nodes that together form a mobile computing network without any centralised control. MANETs are desirable for various applications due to their inherent mobility and connectivity. A major disadvantage of MANETs is their complex security issues. This paper explores these security issues using a methodical process that implements attack and protection trees. Attack trees are an established method of conducting a risk analysis on a MANET. This paper builds on this methodology by also incorporating protection trees. Protection trees are derived from attack trees and provide a means to allocate limited resources to defend against specific attacks. Protection trees are produced systematically by first developing an attack tree, computing metrics for each node of an attack, and developing a corresponding protection tree with similar metrics. In this paper, a generic MANET is implemented and attack and protection trees are used to analyze the security of this network. This analysis of the MANET is a multi-objective problem with competing objectives of cost and performance. Methods are developed to use protection trees while determining the most efficient types of protection to implement depending on the application. Using the results of this analysis, a security scheme can be implemented which obtains the best results with the least amount of resources.

**Keywords:** Protection tree, attack tree, MANET, security, risk analysis, multi objective

# A Study of DNS Traffic Patterns on a Large Autonomous System

Sid Faber<sup>1</sup> and Bert Lundy<sup>2</sup>

<sup>1</sup>Software Engineering Institute, Pittsburgh, PA, USA

<sup>2</sup>Naval Postgraduate School, Monterey, CA, USA

**Abstract** In this report DNS (Domain Name System) traffic on a major autonomous system is analyzed for unusual or malicious traffic patterns. DNS nodes inside the network are classified according to function. One finding is that DNS security concerns stem primarily from improperly configured DNS clients and servers. Many DNS servers leak private addressing information, some DNS Clients forward all queries to a DNS server that is outside of the autonomous system, and many DNS servers allow public recursion. Although some of these issues have been previously identified, quantitative detection of their existence in a large real-world autonomous system is provided, and methods for mitigating the threat of these misconfigurations are presented.

**Keywords:** Network security, intrusion detection, traffic anomaly, domain name system, recursion, [prisoner.iana.org](http://prisoner.iana.org)

# **Development of a Defensive Cyber Damage Assessment Framework**

**Larry Fortson and Michael Grimaila**

**Air Force Institute of Technology, Fairborn, OH, USA**

**Abstract:** Information is a vital resource used in all aspects of modern military operations. Information is collected, processed, analyzed, and distributed to support situational awareness, operations planning, intelligence, and command decision making. The dependence upon information creates significant operational risk to the organizational mission when an information incident occurs. In this paper, we discuss the findings of a US Air Force research project focused on improving the defensive cyber damage assessment process. We identify gaps in the risk management process, discuss the existing incident response and damage assessment process, and propose changes to the damage assessment process as well as identify organizational implementation challenges. The results of the research provide a roadmap for the implementation of a real-time situational awareness tool that maps the technical impact of an information incident to an impact on mission capability.

**Keywords:** Damage assessment, information asset valuation, decision making

# Anti-Forensics: Techniques, Detection and Countermeasures

**Simson Garfinkel**

**Naval Postgraduate School, Monterey, CA, USA**

**Abstract:** Computer Forensic Tools (CFTs) allow investigators to recover deleted files, reconstruct an intruder's activities, and gain intelligence about a computer's user. Anti-Forensics (AF) tools and techniques frustrate CFTs by erasing or altering information; creating "chaff" that wastes time and hides information; implicating innocent parties by planting fake evidence; exploiting implementation bugs in known tools; and by leaving "tracer" data that causes CFTs to inadvertently reveal their use to the attacker. Traditional AF tools like disk sanitizers were created to protect the privacy of the user. Anti-debugging techniques were designed to protect the intellectual property of compiled code. Rootkits allow attackers to hide their tools from other programs running on the same computer. But in recent years there has been an emergence of AF that directly target CFTs. This paper categorizes traditional AF techniques such as encrypted file systems and disk sanitization utilities, and presents a survey of recent AF tools including Timestomp and Transmogrify. It discusses approaches for attacking forensic tools by exploiting bugs in those tools, as demonstrated by the "42.zip" compression bomb. Finally, it evaluates the effectiveness of these tools for defeating CFTs, presents strategies for their detection, and discusses countermeasures.

**Keywords:** 42.zip; anti-computer forensics; cybercrime; EnCase; hacker tools; privacy enhancing tools.

# IPv6: World Update

**Kenneth Geers and Alexander Eisen**  
**NCIS Washington, DC, USA**

**Abstract:** Governments around the world are setting deadlines for IPv6 compliance. While there is still room for debate regarding specific dates for deployment, there is no question but that your organization must begin to prepare for the Next-Generation Internet, and it should start today. This paper is based on wide-ranging, in-depth research, including interviews with the top thinkers on the most crucial issues surrounding the sleeping giant known as IPv6. It will give you the facts you need in order to plan for what may be difficult times ahead. The tactical, down-in-the-weeds take on IPv6 is examined in detail. This paper includes technical details that will inform the reader of the challenges that await as he or she attempts to keep pace not only with their government mandates, but also with economic competitors from around the world. This paper also explains how hackers can exploit this new technology, and how security administrators can stop black hats from taking advantage of the necessarily long-lasting, heterogeneous environment that will be required during the transition to IPv6. Many nation-states view IPv6 as crucial to their national security plans for the future. This paper will make stops at the White House, Tokyo, Beijing, and Red Square, and cover in detail the most current IPv6 research and deployment events from around the world. It discusses how, if some governments get their way, most of us could well lose our last byte of anonymity on the Internet. Finally, the corporate side of Internet addressing is addressed: what do the Xbox, IPTV, and the number of beers I have left in my fridge at home have in common? Answer: IPv6!

**Keywords:** IPv6, Next-Generation Internet, protocol, management, national security

# **Leap in the Dark: An Attempt to Theorize Personnel Anomaly Detection for Countering Insider Threats**

**Shuyuan Mary Ho**  
**Syracuse University, NY, USA**

**Abstract:** Personnel Anomaly Detection (PAD) is a study that attempts to uncover the mechanism for detecting malicious personnel behaviour within the context of an organization. Human behaviour is polymorphous. Humans tend to hide their true intentions from their peers. Human behaviour tends to be self-modifying in response to changes in one's environment. This research attempts to propose a theoretical framework for identifying risk indicators in personnel anomalous behaviour. A socio-technical approach is used to derive the framework, which is designed to collect and analyze data through analysis of critical incident technique and natural language processing. This research will contribute to corporate personnel security for countering insider threats.

**Keywords:** Personnel anomaly detection, insider threat, corporate defence mechanism, personnel security, polymorphous human behaviour.

# Conceptual Design of a Microfluidics Suppressor to Protect against Potentially Lethal Printing Devices: A Scenario-based Physical Cyber Security Measure

Berg Hyacinthe<sup>1</sup>, Yves Anglade<sup>2</sup>

<sup>1</sup>Florida State University, Tallahassee, FL, USA

<sup>2</sup>Florida A and M University, Tallahassee, FL, USA

**Abstract:** This paper explores the potential misuse of print cartridges to diffuse lethal airborne substances to a massive population of computer users around the world. This issue touches on engineering design, cyber security, terrorism, and weapons of mass destruction (WMD). The design and implementation of fast and efficient micro biosensors have become a global defence and security priority due particularly to the widespread fear of potential bio-chemical attacks on civilian populations and due to bioterrorism in general. Evidently, a successful research on micro biosensors necessitates a solid background on bioinformatics, molecular and cell biology, and micro-electromechanical systems (MEMS) technology. As civilians, paramilitary forces, and terrorist groups continue to amplify the mutation of common substances and apparatus into very lethal weapons, a new computers-as-weapons paradigm has emerged. Hence, in order to anticipate future cyber-related threats, the authors relied on scenario planning (a method that combines detailed analyses with imagination to produce reports as though people might write them in the future). In summary, they conclude that the technologically plausible lethal printer scenario calls for a dual approach: (1) coupling digital forensics with human intelligence gathering to uncover hidden threats before they translate into attacks and (2) designing a microfluidics suppressor as a physical cyber security measure.

**Keywords:** Lethal weapons, computers-as-weapons, physical cyber security, microfluidics, autonomous systems, scenario planning

# Virtual' Security Teaching Techniques – Teaching IA methods using VMWare Teams

**Derek Isaacs**

**Colorado Technical University and Boecore Inc, Colorado Springs CO, USA**

**Abstract:** Teaching Security techniques and methods today requires that the instructor 'know' the student to a depth of trust and integrity that is often impractical in a University setting. Merely imparting instruction and hands on "how-to" information can sometimes put the instructor and potentially the educational institution at risk – as these tools and techniques for testing security are only a step removed from the methods and means of effecting security breaches or causing incidents. The need for training must therefore be balanced with the responsibility to provide an isolated and restrained environment in which to present material and hone new skills (or to use the vernacular '-skilz'). As a means of solving this, Virtual Machines (VM) and virtual network environments or team architectures offer a solution to these issues. They also provide, from an educational context, a set of 'known' problems and findings with which the student can study and develop the tools, techniques and knowledge to be an effective Information Assurance professional. This paper presents a series of architectures and scenarios proposed to effect such a learning environment that retains the viability of a 'real' network environment while providing an isolated and restricted learning area. This can be achieved through a series of scenarios and VM Team members (scenario players) in a virtual machine based learning environment.

This approach allows a number of benefits:

- Isolation of the learning environment

- Restrict potential issues (DoS / attack signature detection) to a secured space

- Provide limits on tool and technique usage and impact

- Limit and mitigate risk and liability issues for the educational institution

The VM environment also offers a unique opportunity to provide completely known interactions between the student and the learning environment – the software and the underlying virtual hardware. A detailed set of proposed scenarios and a learning environment architecture, including toolsets and targets of evaluation (TOE) systems is proposed. The applicability of the VM 'team' systems approach is discussed through a suite of scenarios designed to illustrate attack causation, monitoring, and detection.

**Keywords:** Information assurance, security education, virtual systems

# Differential Power Analysis Attacks against AES Circuits Implemented on a FPGA

**Keisuke Iwai, Minoru Sasaki and Takakazu Kurokawa**  
**National Defense Academy, Japan**

**Abstract:** Cryptosystems implemented in embedded systems are more and more increasing thus its tamper resistances are becoming much more important naturally. Differential power analysis (DPA) attacks presented by Kocher et al. are most attractive methods as side channel attacks. This article discusses results of DPA attack against AES cryptosystems implemented in embedded devices which are designed with three different methods. Two of them are designed as hardware circuit using Verilog and Handel-C, and another one is designed as software program on embedded CPU. As results of DPA attacks on them, leaks which include information of secret keys appeared in all circuits but a circuit designed with C-based language shows leaks less than others.

**Keywords:** DPA, side channel attacks, embedded systems, FPGA, AES

# **Categorisation of Profiles for PSYOPs: Can Technology Help?**

**Magdi Kamel, Mark Eramo and Christopher Sutter**  
**Naval Postgraduate School, Monterey, CA, USA**

**Abstract:** Influencing one's adversary has always been an objective in warfare. To date the majority of psychological influence operations have been geared toward the masses. A tailored approach of individual targeting is preferred, but this approach requires unattainable resources. This paper investigates whether state-of-the-art data and text mining tools can be used to automate the categorisation/segmentation of individual profiles for psychological operations. Five data and text mining software applications were tested and their results compared with those of a social psychologist. Using statistical analysis, it was concluded that current data and text mining tools are not mature enough to produce results comparable with those produced by psychologists.

**Keywords:** Information operations, psychological operations, data mining, text mining, text categorisation.

# Implications of Information Flow Priorities for Interorganizational Crisis Management

Tuija Kuusisto<sup>1</sup>, Rauno Kuusisto<sup>2</sup> and Mark Nissen<sup>3</sup>

<sup>1</sup>Ministry of Defence, Helsinki, Finland

<sup>2</sup>National Defence University, Helsinki, Finland

<sup>3</sup>Naval Postgraduate School, Monterey, CA, USA

**Abstract:** The aim of this paper is to increase understanding about the implications of information flow priorities for interorganizational crisis management. The paper is based on the main results of a prior study that addressed the information requirements of high-level decision-making activities during a sudden crisis situation. The study identified priorities of retrieved and delivered information flows from the perspectives of information content and information update frequency needs. The results about the information priorities based on update frequency needs provide novel insights into information flow priorities for decision-making in crisis management. These results show the most effective information categories to prioritize for decision-making in the context of interorganizational crisis management.

**Keywords:** Information flows, decision-making, homeland security, crisis management

# Thinking Strategically about Information Operations

Irving Lachow and Robert Miller

National Defence University, Washington, DC, USA

**Abstract:** There is widespread agreement that the Global War on Terrorism is, at least in part, a “war of ideas.” There is also a consensus among both academics and policymakers that the United States has done a poor job in fighting this war. While the U.S. has struggled to develop and implement a coherent strategy for influencing key target audiences, Islamic extremists have effectively used modern communications technologies like the Internet to inspire, frighten, and manipulate target audiences, media organisations, and even entire countries. However, their heavy reliance on technologies like the Internet also makes extremist groups vulnerable to countermeasures. This paper explores general steps the U.S. can take to exploit the vulnerabilities found in the current information operations (IO) approaches being followed by Islamic extremists. It also examines options at the physical, informational, and cognitive “layers” of the information environment and describes advantages and disadvantages for each. The result is a recommended series of actions the U.S. can pursue to further its own strategic IO goals while degrading the IO efforts of its adversaries.

**Keywords:** Information operations, influence, extremists, terrorism, strategic.

# Intrusion Detection in open Source Software via Dynamic Aspects

**William Mahoney and William Sousean**  
**University of Nebraska at Omaha, NE, USA**

**Abstract:** Aspect-Oriented Programming (AOP) is an emerging software engineering methodology, which has been used to assist in the removal of crosscutting concerns from traditional methods of software development. As an example, software used to determine whether a user has appropriate security clearance might be scattered throughout the many modules, which require this check. Utilising AOP, “aspects” are “woven” into the software either in a “static” method, during compilation, or a “dynamic” method while the program is executing. The “join points” in a program are the points where these aspects are applied. The “aspect” code is written once and “woven” in to the modules at join points. Typical aspects involve logging changes to a database and monitoring memory usage. Our focus is on aspects related to security and intrusion incident detection.

Dynamic weaving allows aspects to be woven in and out as the program is executing. However the base code often must be compiled with additional “syntactic sugar” – additions that are required for the later connection of dynamic aspects. This paper presents a new technique to enable dynamically loaded security modules to be added into existing C/C++ code on the fly while the program is executing. Our tool is a Run-Time Event Monitoring System called “dynamicHook”, implemented on a standard Linux platform using existing Linux tools, which tests each potential join point for the required activation of advice. Our system does not need to modify the executable files, but instead we compile in special “linkage” between the base code and potential aspects which are then called as dynamically linked routines located in shared libraries. Our scheme does not require any new syntax or language extensions or rely on code transformations; we thus use it for adding intrusion detection methodologies to pre-existing off-the-shelf open source software.

**Keywords:** Open-source, intrusion detection, dynamic aspects, AOP.

# **Fine-Grain Security for Military-Civilian-Coalition Operations Though Virtual Private Workspace Technology**

**R William Maule and Shelley Gallup  
Naval Postgraduate School, Monterey, CA, USA**

**Abstract:** Next-generation service-oriented architectures provide a means for unprecedented levels of collaboration. Security built upon LDAPv3 when coupled with virtual private database technology can enable secure operations within a domain while retaining need-to-know thresholds with fine-grain security. This paper discusses such a technology in use for navnetwarcom trident warrior experimentation. A simulated scenario is discussed in which 12 officers involved in a mhq with moc in mda scenario prototyped an operational application of a comprehensive suite of xml web services that provided a personalised portal for each user, email, chat, presence, instant messenger, web conference, threaded discussions, and secured virtual workspaces with libraries, discussion area, and task management. The focus was on methods to secure communications across military, civilian and coalition operations preliminary to more extensive testing to occur in Trident Warrior 07. Along with an introduction to the technology the study results are presented, addressing methodology and protocols for highly collaborative sessions with varying levels of security in highly dynamic scenarios.

**Keywords:** military, security, collaboration, community of interest, coi, workspace, wiki

# Creating Hardware-based Primitives that Facilitate the Exposure of State Information Useful for Security Related Monitoring

**Stephen Mott and Paul Williams**

**Air Force Institute of Technology, Fairborn, OH, USA**

**Abstract:** The Co-processor Intrusion Detection System (CuPIDS) is an intrusion detection system (IDS) we are using to explore ways in which security-focused hardware primitives can improve the security of modern computer architectures without compromising performance. While focusing on intrusion detection, CuPIDS also allows for application focused security policy compliance monitoring (SPCM). Previous work on CuPIDS (CuPIDS-Purdue) proved that leveraging multiple CPUs in an asymmetrically parallel manner can reliably detect a multitude of attack/exploit types in real-time for real world applications – a sought after capability in the security monitoring field. Our research - the CuPIDS-AFIT project - furthers this effort by exploring novel hardware-based primitives that support parallel monitoring for real-time intrusion detection (ID) and SPCM tasks. The availability of processors embedded within a field programmable gate array (FPGA) afford us the opportunity to develop practical means by which we can implement these primitives to gain and transmit state information in hardware by methods not possible previously. From this, we have shifted CuPIDS' reliance on the host operating system (OS) to dedicated hardware for viewing and reporting system state information. This makes the IDS itself more secure from attack, tangibly improves runtime efficiency and time to detection, as well as enables new means by which real-time ID and SPCM are implemented.

**Keywords:** Intrusion detection (id), security policy compliance monitoring (spcm), parallel monitoring, asymmetric computing

# Graphical Based User Authentication with Embedded Mouse Stroke Dynamics

Kenneth Revett<sup>1</sup>, Asim Zia<sup>1</sup>, Sérgio Tenreiro de Magalhães<sup>2</sup>, and Henrique Santos<sup>2</sup>

<sup>1</sup>University of Westminster, London, UK

<sup>2</sup>Universidade do Minho, Portugal

**Abstract:** Research on character based login details reveal that they tend to be simple and relatively easy to guess. As an alternative, graphical user authentication schemes have been suggested, as research in cognitive psychology indicates that images are more memorable than characters. We combine this advantage that graphical passwords provide, along with an added layer of security which incorporates mouse stroke dynamics. In this paper, we examine a graphical user authentication scheme with respect to length as a function of embedded noise and image size to determine the optimal values for these parameters. We then add a mouse stroke dynamics biometric with the optimal graphical password length and graphic image size. The results indicate that a ratio of 1:4 may be optimal with respect to the number of elements in a graphical password and the total number of graphics presented to select from. The size of the images did not change the FRR. Lastly, mouse stroke dynamics did not produce any change in the FRR, but reduced false acceptance to levels approaching keystroke dynamics, depending on the acceptance threshold criteria employed. These results are quite promising – with FRR/FAR values in the range of 1-4% - consistent with the most accurate biometric systems reported for this technology. These results indicate that graphical based authentication schemes (with embedded mouse stroke dynamics) are viable alternatives to character based password schemes. In addition, our technology could be directly applicable to a mobile computing device that required a stylus for interaction.

**Keywords:** Graphical authentication, mouse stroke dynamics, biometrics, false acceptance, false rejection

# Planning Cost-Effective Deceptive Resource Denial in Defense to Cyber-Attacks

**Neil Rowe**

**U.S. Naval Postgraduate School, Monterey, CA, USA**

**Abstract:** Cyber-attacks against computer systems that provide valuable services can often be effectively defended by tactics of deliberately deceptive resource denial. Delaying in response to suspicious requests is one example; it permits time to develop a good defense, facilitates analysis of the attacks and formulation of a response, and may little affect legitimate users. But delays can look suspicious; a better tactic can be for the operating system to falsely claim unavailability of some critical resources that the attacker needs (files, directories, access rights, network connections, or software). This can be more effective than using “security policy” as an excuse to deny those resources because it is unexpected and more flexible. We formulate a decision-theoretic approach to the problem of deciding when to deceive by resource denial in a sequence of interactions with a user of an operating system, and provide general formulae for decisions in planning deceptions. Our theory covers both reactive and proactive deception, and both single-session and multi-session attacks. We also provide additional criteria to ensure logically consistent tactics. We provide some evidence from a survey of users to support our modeling.

**Keywords:** Deception, cyberspace, decision theory, resources, denial, lies

# Experiments with a Testbed for Automated Defensive Deception Planning for Cyber-Attacks

**Neil Rowe, Han Goh, Sze Lim, and Binh Duong**  
**U.S. Naval Postgraduate School, Monterey, CA, USA**

**Abstract:** A key problem in research in cyberwarfare is the difficulty of conducting experiments with real attackers; science requires experiments, and it is desirable to make information warfare scientific where we can. Some data is available regarding attacks but not much on countermeasures. We report on a testbed we are developing for conducting defensive deception experiments with the normal random background of attacks on the Internet. The testbed is built on top of a honeypot, a computer system that deliberately invites attack to yield useful intelligence about attack methods, but modified to use various deception methods to fool an attacker. Unlike earlier attempts at deception testbeds, ours permits full interaction of an attacker with our system, and thus a wide range of deceptions is possible. We present data obtained by running a partial implementation of our testbed, showing patterns in attacks over time and with system modifications. We show analysis of situations in which attackers may have been induced to leave by thinking the system was not attackable or not in their interest to attack. We also discuss design directions we are exploring.

**Keywords:** Deception, internet, testbed, attack, honeypot, statistics

# **Possible Risks Analysis Engine: A Prototype Tool for Managing IT Security Safeguards Acquisition**

**Robert Sainsbury and Richard Baskerville  
Georgia State University, Atlanta, GA, USA**

**Abstract:** Risk analysis provides a cost-benefit analysis of information security controls and safeguards in economic terms. Despite serious flaws in its fundamentals, approaches to calculating risk have changed little over the past decades. The publicly available frequency data that does exist is generally incompatible and unusable. Theories of mathematical evidence indicate that probability theory is inappropriate where frequency data is unavailable. While alternative theoretical frameworks have been suggested, practical vehicles for the use of such frameworks have yet to materialize. This paper reports on design science research that employs fuzzy sets and possibility theory as kernel theories to develop and demonstrate a prototype of such a practical vehicle. This vehicle opens avenues for testing and operating risk analysis methodologies based on alternative mathematical theories of evidence.

**Keywords:** Risk management, risk analysis

# Modified RSL as a Countermeasure Against Differential Power Analysis

**Minoru Sasaki, Keisuke Iwai and Takakazu Kurokawa**  
**National Defense Academy, Japan**

**Abstract:** Ever since embedded cryptosystems face threats arisen from side channel attacks such as Differential Power Analysis: (DPA), many countermeasures have been proposed. However, these countermeasures are usually vulnerable in the realistic circuits because of the distributions of gate delays. Among those, Random Switching Logic: (RSL) takes account of such delays, and masks internal variables with random numbers. This countermeasure is classified as the primitive gate level countermeasure against DPA, and has already been proved to have high resistant to DPA. However, a special circuit design for generating enable signals is necessary for RSL, which fact increases its circuit scale. This paper proposes an improved method of RSL named as "Modified Random Switching Logic: (MRSL)". MRSL requires no enable signals, which fact reduces a vast amount of time and effort to design RSL circuit, and also can reduce the circuit scale of MRSL drastically from that of RSL. Considering all possible state changes of MRSL gates, MRSL can be proved to accept any distributions of gate delays. As an evaluation for the proposed MRSL, 2-input MRSL NAND gate as well as multi-input MRSL gates are confirmed to have enough DPA resistance compared with other representative DPA countermeasures. Furthermore, S-BOX in DES circuit using composite fields on Field Programmable Gate Array: (FPGA) based on MRSL is proved to have an excellent ability to hide internal variables. The leakage voltage of the proposed MRSL after DPA is almost the same as that of RSL, and is confirmed to be far less than that of Trichina's gate, and normal gate. The circuit scale of MRSL can be reduced drastically from that of RSL as well as of Trichina's gate, which fact leads to its possible usage to the embedded cryptosystems.

**Keywords:** DPA, side channel attack, DES, FPGA

# **A Framework for Relating Cyberspace Operations to the Cognitive and Physical Domains**

**Tiffany Smith<sup>1</sup>, Pamela Woolley<sup>2</sup>, Robert Mills<sup>1</sup>, and Richard Raines<sup>1</sup>**

**<sup>1</sup>Air Force Institute of Technology, Fairborn, OH, USA**

**<sup>2</sup>Fairchild AFB WA, USA**

**Abstract:** The United States Air Force recently released a new mission statement adding cyberspace as an area of operations to achieve military goals and objectives. The ability to clearly articulate exactly what is and what is not cyberspace will greatly simplify the assignment of roles and missions, as well as the development of cyber warfare doctrine. With that said, there remains much debate about what cyberspace really is, and whether it is truly a domain in which warfare can be waged. In this paper we offer a new perspective on cyberspace that addresses many of the stumbling blocks of previous definitions. We begin with the network centric warfare model that identifies physical, cognitive, and information domains. By focusing on information flows, we develop a model of cyberspace which does not stand on its own but rather is part of a larger whole that encompasses both virtual and physical domains. We go on to show how this framework overcomes limitations of existing cyberspace definitions and will also help clarify discussions about cyber roles and missions, organizational responsibilities, and force development.

**Keywords:** Cyber warfare, information warfare theory.

# Similarity Analysis of Malicious Executables

**Anthonius Sulaiman, Sandeep Mandada, Srinivas Mukkamala and Andrew Sung**  
**New Mexico Tech, Socorro, NM, USA**

**Abstract:** Malware seemingly leads the myriad of security threats on the Internet today. In this paper, we categorize and examine numerous malwares in order to identify the parts that cause malicious activities. Our paper relies on the factor that malware with similar symptoms share a common signature. We analyze and extract snippets of API sequences that appear frequently in a number of malicious samples. Our technique uses Windows API as its basis. Hence, its usage is currently limited to Windows systems. Experimental results from a large set of recent spy ware, adware, and viruses are presented.

**Keywords:** Malware, adware, spy ware, anti virus, similarity analysis

# The Design Space of Metamorphic Malware

Andrew Walenstein<sup>1</sup>, Rachit Mathur<sup>2</sup>, Mohamed Chouchane<sup>1</sup>, and Arun Lakhotia<sup>1</sup>

<sup>1</sup>University of Louisiana at Lafayette, LA, U.S.A.

<sup>2</sup>McAfee Avert Labs, Beaverton, OR, U.S.A.

**Abstract:** A design space is presented for metamorphic malware. Metamorphic malware is the class of malicious self-replicating programs that are able to transform their own code when replicating. The raison d'etre for metamorphism is to evade recognition by malware scanners; the transformations are meant to defeat analysis and decrease the number of constant patterns that may be used for recognition. Unlike prior treatments, the design space is organized according to the malware author's goals, options, and implications of design choice. The advantage of this design space structure is that it highlights forces acting on the malware author, which should help predict future developments in metamorphic engines and thus enable a proactive defence response from the community. In addition, the analysis provides effective nomenclature for classifying and comparing malware and scanners.

**Keywords:** Metamorphic malware, virus scanner.

# **Information Terrorism in the new Security Environment**

**Ken Webb**

**RNSA and Edith Cowan University, Perth, Western Australia**

**Abstract:** Over the years there have been many interpretations of what constitutes Information Terrorism. This paper reviews literature on Information Warfare and Terrorism to deduce what the threat of Information Terrorism is considered to be now in the new security environment. It achieves this by outlining the threat itself, and its potential impact, capability and advantages. The positives that can be derived to counter it are then examined and, based on the literature reviewed, a deduced interpretation/definition of Information Terrorism is provided. The paper concludes with remarks that Information Terrorism is a major dynamic contributing to a new national security environment.

**Keywords:** Information terrorism, information warfare, counter-terrorism, national security, future terror

# **Inter-Network Operations Center Dial-By-ASN (INOC-DBA), a Hotline for Critical Internet Infrastructure Management**

**Bill Woodcock<sup>1</sup> and Ross Stapleton-Gray<sup>2</sup>**

**<sup>1</sup>Packet Clearing House, Berkeley, CA, USA**

**<sup>2</sup>Internet Awareness, Inc., Berkeley, CA, USA**

**Abstract:** The paper describes the nature and operation of INOC-DBA, a global VoIP-based hotline, a practical and effective means for inter-NOC coordination in response to Internet security and stability incidents. INOC-DBA is a response to threats to Internet operations, which has emerged organically from within the Internet operations community.

**Keywords:** NOC, VoIP, incident response, infrastructure protection

# Using Deception for Assuring Security

**Stilianos Vidalis, Eric Llewellyn and Christopher Tubb**  
**University of Wales, Newport, UK**

**Abstract:** For each layer of information security there are a number of techniques and tools that can be used to ensure information superiority. Indeed some experts would argue that you can not have the former without the later. In today's technological & interconnected world though, information superiority is very hard to achieve and almost impossible to maintain. This paper will argue that the art of deception is a reliable and effective technique that can ensure and maintain the security of an infrastructure. The paper will conclude by presenting a technical solution of the above statement.

**Keywords:** Information security, information superiority, deception, virtual honeypots

# **SME Security in the Digital Age**

**Don Milne<sup>1</sup>, John McCarthy<sup>2</sup>, and Bryan Mills<sup>2</sup>**

**<sup>1</sup>Buckinghamshire Chiltern University College, High Wycombe, England**

**<sup>2</sup>ServiceTec Global Services Ltd, UK**

**Abstract:** The past few years has shown an increasing level of concern by governments, policy makers and the ICT Industry over SME's reluctance to engage in the digital economy. This will have an impact on the economy as a whole. Current data shows the uptake in the use of ICT technology has not been expanding at the rate expected. The security issues and concerns of SME's owner managers have been shown to contribute to the lack of uptake of the more complex ICT required for e-business engagement. Many small organisations, in both the commercial and the not for profit sector have a different approach to prioritising and decision making. This is reflected in their use of ICT systems and as a consequence has an impact upon ICT security. Whilst some of this under performance in the digital economy may be related to the management style and lack of ICT expertise of the companies the part played by the ICT service suppliers must also be investigated. Evaluation of the traditional security threats to organisations and individuals is undertaken to recommend suitable responses to these threats. By evaluating, through a series of case studies continued from a previous work, how the ICT service industry currently provides support for such organisations and how the products they offer satisfy or fail to match the needs of the SME's. From this it is possible to take a new look at how the provision of security support for the smaller end of the market should be undertaken in the future. From this study security service providers can relate their products and services to the functional needs of the SME giving them the ability to respond better to the needs of the small organisation.

**Keywords:** SME's; security; distributed systems; digital economy