

The 3rd International Conference on Information Warfare and Security

Peter Kiewit Institute
University of Nebraska
Omaha
USA
24-25 April 2008

Edited by
Leigh Armistead Edith
Cowan University

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.

Further copies of this book and previous year's proceedings can be purchased from <http://academic-conferences.org/2-proceedings.htm>

ISBN: 978-1-906638-01-6 cd

Published by Academic Publishing Limited
Reading
UK
44-118-972-4148
www.academic-publishing.org

ICIW 2008

Contents

Paper Title	Author(s)	Guide Page	Page No.
Preface		iv	iv
Biographies of Conference Chairs, Programme Chair, Keynote Speaker and Mini-track Chairs		vi	vi
Biographies of contributing authors		viii	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	1-10
Adapting Information Operations to a Changing World: Future Options for the United States	<i>Edwin Armistead Edith Cowan University, Perth, Australia</i>	2	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>	3	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>	4	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>	5	37-44
Developing Cyber Warriors	<i>Jeff Boleng, Dino Schweitzer, and David Gibson United States Air Force Academy, Colorado Springs, CO, USA</i>	6	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>	7	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>	8	59-66

Paper Title	Author(s)	Guide Page	Page No.
Biometric Security Enhancements Through Template Aging Matching Score Analysis	<i>John Carls¹, Richard Raines¹, Michael Grimaila¹ and Steven Rogers²</i> <i>¹Air Force Institute of Technology, Wright-Patterson AFB, OH, USA</i> <i>²Air Force Research Laboratory, Wright-Patterson AFB, OH USA</i>	9	67-76
Outsourcing and the Insider Threat: An Increasing Security Risk	<i>Carl Colwill</i> <i>BT Design, Security Risk and Compliance, UK</i>	10	77-86
The Impact of Vista and Federal Desktop Core Configuration on Incident Response	<i>Daniel Cotton, Stephen Nugen, and William Mahoney</i> <i>University of Nebraska at Omaha, NE, USA</i>	11	87-96
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>	12	97-108
Religion, Ideology, and Information Warfare	<i>Geoffrey Darnton</i> <i>Bournemouth University, UK</i>	13	109-116
An Investigation of Negative Authentication Systems	<i>Dipankar Dasgupta and Rukhsana Azeem</i> <i>The University of Memphis, TN, USA</i>	14	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>	15	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>	16	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>	17	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>	18	153-162

Paper Title	Author(s)	Guide Page	Page No.
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>	19	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>	20	171-178
Information Asset Value Quantification	<i>Denzil Hellesen¹, 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>	21	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>	22	189-194
Computer Assisted Security Assessment through Fact Proposition Space	<i>Peter Hospodka, Qiuming Zhu, William Sousan and Ryan Nickell</i> <i>Department of Computer Science, University of Nebraska at Omaha, NE, USA</i>	23	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>	24	203-212
Advanced Manipulation Of Digital Evidence Using Memory Based Anti-Forensic Tools	<i>Hamid Jahankhani¹, Elidon Beqiri¹ and Kenneth Revett²</i> <i>¹University of East London, UK</i> <i>²University of Westminster, UK</i>	25	213-220
Analyzing Anonymity in Cyberspace	<i>Douglas Kelly, Richard Raines, Rusty Baldwin, Barry Mullins and Michael Grimaila</i> <i>Air Force Institute of Technology, Wright Patterson Air Force Base, OH, USA</i>	26	221-232
A Framework for Classifying Anonymous Networks in Cyberspace	<i>Douglas Kelly, Richard Raines, Rusty Baldwin, Barry Mullins and Michael Grimaila</i> <i>Air Force Institute of Technology, Wright Patterson Air Force Base, OH, USA</i>	27	233-244

Paper Title	Author(s)	Guide Page	Page No.
A Survey of Critical Infrastructure Control System Effects	<i>Michael Kolbe and Paul Williams Air Force Institute of Technology (AFIT), Wright-Patterson Air Force Base, OH, USA</i>	28	245-254
Pattern Matching Information Flow using GADT	<i>Eric Lindahl and Victor Winter University of Nebraska at Omaha, NE, USA</i>	29	255-262
Static and Dynamic Packet Filtering on Lightly Managed Systems	<i>James Lupo and Daniel Likarish Regis University, Denver, CO, USA</i>	30	263-268
Organizing the United States Government for the Contemporary Environment	<i>Steven Mains US Combined Arms Center, Fort Leavenworth, KS, USA</i>	31	269-276
Developing a Requirements Framework for Cybercraft Trust Evaluation	<i>Todd McDonald and Shannon Hunt Air Force Institute of Technology, Wright Patterson Air Force Base, OH, USA</i>	32	277-284
Use of Evaluation Criteria in Security Education	<i>Thuy Nguyen and Cynthia Irvine Naval Postgraduate School, Monterey, CA, USA</i>	33	285-292
Implementation of a Multilevel Wiki for Cross-Domain Collaboration	<i>Kar Leong Ong, Thuy Nguyen and Cynthia Irvine Naval Postgraduate School, Monterey, CA, USA</i>	34	293-304
Formal Models of a Least Privilege Separation Kernel in Alloy	<i>David Phelps, Mikhail Auguston, Timothy Levin Naval Postgraduate School, Monterey, CA, USA</i>	35	305-314
Using Deception to Facilitate Intrusion Detection in Nuclear Power Plants	<i>Julian Rushi^{1,2} and Roy Campbell¹ ¹University of Illinois at Urbana-Champaign, Urbana, IL USA ²Università degli Studi di Milano, Via Comelico Milano, Italy</i>	36	315-324
Establishing the Human Firewall: Improving Resistance to Social Engineering Attacks	<i>Jamison Scheeres, Robert Mills and Michael Grimaila Air Force Institute of Technology, Wright-Patterson Air Force Base, OH, USA</i>	37	325-334
An Architecture for Cyber Incident Mission Impact Assessment (CIMIA)	<i>David Sorrels¹, Michael Grimaila¹, Larry Fortson², and Robert Mills¹ ¹Air Force Institute of Technology, Wright-Patterson AFB OH, USA ²Air Force Research Laboratory, Wright-Patterson AFB OH, USA</i>	38	335-344
Tailored Information Delivery Services for Open Source Intelligence	<i>William Sousan, Ryan Nickell, Qiuming Zhu and Pete Hospodka University of Nebraska at Omaha, NE, USA</i>	39	345-352

Paper Title	Author(s)	Guide Page	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>	41	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>	41	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>	42	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>	43	379-386
Using Markov Models to Crack Passwords	<i>Renier van Heerden and Johannes Vorster DPSS, CSIR, Pretoria, South Africa</i>	44	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>	45	395-402
Common Errors in Incident Response	<i>Michael Staggs FireEye, Inc. Menlo Park, CA, USA</i>	46	Abstract only

Preface

Welcome to the Third International Conference on Information Warfare and Security (ICIW 2008), hosted this year by the Peter Kiewit Institute, University of Nebraska Omaha, USA. The Conference Chair is William Mahoney from the Peter Kiewit Institute and the Programme Chair is Leigh Armistead from Edith Cowan University in Perth, Australia.

Now in its third year, the conference is well established as a platform 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 Brian Lopez from the Lawrence Livermore Laboratories, Livermore, CA, on the topic of "*Persistence, Ambiance and New Maps*". On day two of the conference, the opening keynote speaker is Brigadier General Davis from the United States Strategic Command and later in the day Dr. Roger Schell from the Aesec Corporation, Palo Alto, CA will address the topic "*Are the System Security Watchmen Asleep?*"

An important benefit of attending this conference is the ability to share ideas and meet the people who hold them. The broad range of papers will ensure an interesting and enlightened discussion over the full two day schedule. 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.

With an initial submission of 75 abstracts, after the double blind, peer review process there are 49 papers published in these Conference Proceedings, including contributions from India, Portugal, South Africa the United Kingdom and the 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
[Dorothy Denning](#), Naval Postgraduate School, Monterey, CA, USA
[Andy Jones](#), Security Research Centre, BT, UK and Edith Cowan University, Australia
[William Mahoney](#), University of Nebraska Omaha, Omaha, USA
[Dan Kuehl](#), National Defense University, Washington DC, UK,
[Corey Schou](#), Idaho State University, USA

Committee Members:

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); [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); Nathan Clarke (University of Plymouth, 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); Simin Garfinkel (NPS, Pleasant Street, Belmont, 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); Arreymbi Johnnes (University of East London, UK); Andy Jones (British Telecom, UK); Dan Kuehl (National Defense Forces, USA); Tuija Kuusisto (National Defence College, Finland); Arun Lakhotia (University of Louisiana Lafayette, USA); Irving Lachow (National Defense University, USA); Michael Lavine (John Hopkins University, USA); Tara Leweling (Naval Postgraduate School, USA); Cherie Long (Clayton State University, Decatur, 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); Robert Mills (Air Force Institute of Technology, Ohio, USA); Don Milne (Buckinghamshire and Chiltern University College, UK); Evangelos Moustakas (Middlesex University, UK); Srinivas Mukkamala (New Mexico Tech, Socorro, USA); Barry Mullins (Air Force Institute of Technology, Wright-Patterson, USA); Andrea Perego (Università degli Studi dell'Insubria, Italy) ; 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), William Sousan (University of Nebraska, Omaha, USA); [Doug Twitchell](#) (Illinois State University, USA); Stylianos Vidalis (Newport Business School, UK); Douglas Webster (USSTRATCOM Global Innovation & Strategy Center, USA); Paul Williams (Air Force Institute of Technology, Ohio, USA); [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



Dr William (Bill) 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.

Programme Chair

Leigh Armistead is currently the Senior Program Manager for Information Operations and Information Assurance for Honeywell Technology Solutions Inc, Leigh is also the editor of Information Operations: Warfare and The Hard Reality of Soft Power and Information Warfare: Separating Hype from Reality. A retired U.S. Naval Officer and former Master Faculty of IO at the Joint Forces Staff College, he is currently enrolled in a PhD program at Edith Cowan University in Perth, Australia. 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 in 2006 and 2007, as well as the IQPC IO Conference in the United Kingdom from 2002 to 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.



Keynote Speakers



Dr Roger Schell is co-founder and President of Aesec Corporation, a new company focused on verifiably secure platforms for secure, reliable e-business. At Novell he led their Class C2 network evaluation and managed development of product security. He was VP for Engineering at Gemini Computers where he developed their highly secure (Class A1) commercial product. He served as the founding Deputy Director of the National Computer Security Center. He originated several key modern security design and evaluation techniques and holds patents in cryptography and authentication. Dr. Schell has more than 60 publications, and was Associate Professor of Computer Science at the Naval Postgraduate School. The NIST and NSA recognized him with the 1991 National Computer System Security Award. Dr. Schell is a retired USAF Colonel. He received a Ph.D. in Computer Science from the MIT, an M.S.E.E. from Washington State, and a B.S.E.E. from Montana State

Brian Lopez is a computer scientist at Lawrence Livermore National Laboratory (LLNL). For the past decade he has led LLNL's Vulnerability and Risk Assessment Program (VRAP) which provides in-depth, multi-disciplinary assessments of threat, vulnerability, and consequence. Past projects include field work in 28 US states and internationally across a variety of sectors such as electric power, oil, gas, water, chemical, aviation, rail, maritime, financial, telecommunications, national icons, and classified sites. Additionally Brian assembled and led security teams for the 2002 Winter Olympics, California Energy Crisis, and 9/11 response. He is the co-author of the recent book "Seeds of Disaster" (Cambridge University Press) regarding critical infrastructure security.



Biographies of contributing authors (in alphabetical order)

Gail-Joon Ahn is an Associate Professor of Software and Information Systems Department at UNC Charlotte and Director of Center for Digital Identity and Cyber Defense Research which has been designated as a National Center of Academic Excellence in Information Assurance Education. His principal research and teaching interests are in information and systems security. His research foci include vulnerability and risk management, access control, and security architecture for distributed systems. His research has been supported by NSF, NSA, DoD, DoE, Bank of America, Hewlett Packard, Microsoft and Robert Wood Johnson Foundation. Dr. Ahn is a recipient of Department of Energy CAREER Award and the Educator of the Year Award from the Federal Information Systems Security Educators' Association (FISSEA)

Eric Ashe is currently attending the Air Force Institute of Technology at Wright-Patterson AFB, OH where he is working on his M.S. in Information Resource Management. He received a B.B.A from the University of New Mexico and is currently serving as a communications officer in the United States Air Force.

William Bahn is a researcher for the Academy Center for Information Security (ACIS), a research center within the Department of Computer Science at the United States Air Force Academy, where he focuses on the applied aspects of the center's jam resistance project. To this effort he brings his experience as a Senior Engineer for Black Forest Engineering, a small company that designs fully custom high-performance mixed-signal application-specific integrated circuits. Mr. Bahn is presently completing both a Masters of Science degree in Computer Science and a Ph.D. in Electrical Engineering at the University of Colorado at Colorado Springs.

Jeff Boleng LtCol. is the Deputy Department Head and an Assistant Professor of Computer Science at the US Air Force Academy. He teaches a variety of Computer Science courses in computer networks, security, and operating systems. He is an active researcher in Mobile Ad-hoc Networks, Sensor Networks, Software Defined Radio applications, and Computer Security topics. LtCol Boleng is a 1991 graduate of the US Air Force Academy, and earned a Master's and Doctorate in Mathematical and Computer Sciences from Colorado School of Mines in Golden Colorado. His operational experience ranges from a deployed networks engineer with the 1st Combat Communications Squadron in Germany, to the chief of Command and Control Interoperability for Combined Forces Command Korea, and the chief of net-centric integration for Air Force Space Command. He has commanded at the flight and squadron level having served most recently as the Commander of the 21st Mission Support Squadron, Peterson Air Force Base, Colorado.

Adam Bryant is a Ph.D. student at the Air Force Institute of Technology at Wright-Patterson Air Force Base, Ohio. He served as a missile maintenance technician and a communications and information officer in the U.S. Air Force for nine years and holds a bachelor's degree in Social Psychology from Park University and two master's degrees, in Information Resource Management and Computer Science, from the Air Force Institute of Technology.

John Carls received a BS Computer Science from Old Dominion University in 1998 and a MS Computer Science from the U.S. Naval Postgraduate School in 2003. He is currently a PhD Student at the U.S. Air Force Institute of Technology. He has served over 20 years Active Duty in the U.S. Navy.

Carl Colwill is a Principal Consultant, at the Security Risk Management. Carl joined BT in 1980 and since 1990 has been involved with security and risk management; he was a founder member of BT's Information Assurance team established to assess emerging risks from a national infrastructure perspective. Carl's current focus is outsourcing risks; he leads security risk and compliance reviews for BT and is also responsible for the application of best practice risk management methods.

Daniel Cotton is a resident of Omaha and a student in Computer Science at the University of Nebraska at Omaha. He is interested in the areas of information assurance, and has been specifically conducting research into OpenPGP encryption for OVAL, and research in the area of computer forensics. His forensics work has dealt specifically with the Federal Desktop Core Configuration. Mr. Cotton has also worked at the Defense Intelligence Agency in the area of Intelligence Community Vulnerability Alerts. In addition to his information assurance studies, Mr. Cotton has completed the two year Cisco CCNA course and has completed the CISSP examination.

Robert Cowan is a Captain in the United States Air Force, he is a Communications Officer currently assigned to Headquarters US Air Force Europe A6. His educational background includes a Bachelor of Science Degree from Louisiana Tech University and a Masters Degree in Information Resource Management from Air Force Institute of Technology with focus in Information Assurance and Strategic Information Management.

Geoffrey Darnton is Head of knowledge Transfer and a Business Fellow at the Business School of Bournemouth University, England. He has spent many years in industry in the computer field dealing primarily with information systems, and not just the technology. He has had a stream of research and activity in matters of peace and war for more than 30 years, including dealing with the philosophical problems of defining peace, using econometric techniques to monitor arms agreements, assessing the lawfulness of the possession and use of nuclear weapons, and more recently and exploration of the legal implications of information warfare and applications of content analysis in IW. He has a distinct preference for multi-disciplinary approaches to difficult problems. His interests in information systems and information warfare come together in recent research looking at the roles of religion, ideology, and culture in, and as targets of, information operations

Dipankar Dasgupta, Professor of Computer Science has been doing research in applying computational intelligence in Cyber Security, and received funding from different federal organizations including NAVY, NSF, DARPA and DHS for his research. He published more than 130 research papers in book chapters, journals, and international conferences. He published one book, two edited volumes and co-edited several conference proceedings over the last 10 years. Prof. Dasgupta, the founding Director of the Center for Information Assurance (<http://cfia.memphis.edu>), is spearheading the information security research, education and training efforts of the University of Memphis.

Evan Dembskey worked in the IT industry for more than ten years, starting out by installing network hardware and ending as a senior programmer. In 2005 he made the switch to the Tshwane University of Technology in Pretoria, South Africa, where he lectures programming and AI. He is currently busy with his doctorate, and intends to make a career of academics. In his spare time he likes to read science fiction novels, non-fiction books about the Greco-Romans and physics, and make beer.

David Fahrenkrug is currently the Chief Strategist at Eighth Air Force located at Barksdale Air Force Base in Louisiana. He is responsible for developing concepts and

strategies for air, space, and cyberspace operations in support of US Strategic Command missions. He is a senior pilot with more than 2000 hours in the T-38 and F-15C. He has flown combat operation in support of Operations Northern and Southern Watch and served as the Detachment Commander for Operation Northern Guardian. He is a graduate of the Air Force's advanced strategy school, The School of Advanced Air and Space Studies and also completed graduate studies at the University of Chicago where he received a Doctorate in Political Science. His dissertation showed how certain political strategies can extend the longevity of empires by overcoming nationalist resistance to imperial control. His was the lead author for the Eighth Air Force's Concept of Cyber Warfare and his current projects include developing strategies for warfare in cyberspace.

James Gorsuch is currently serving as a captain in the US Air Force at Maxwell AFB AL. He is assigned to the Air Force Wargaming Institute where he is the program manager for multiple software development programs. Previously he was assigned to the Headquarters of Air Force Materiel Command in the network operations security center as the network security commander maintaining the viability of network access. His research interests continue to include the understanding of malicious logic operation and the protection of networks from malicious actors.

Dennis Guster is a Professor in Computer Information Systems at St. Cloud State University. He has been involved in computer security for 30 years and has devised and taught numerous courses related to information assurance. Further, he has published numerous articles and undertaken sponsored research projects in the area. His current research emphasis is security within a distributed computing environment. Recently he has taught courses in Computer Security Policy, Client/Server Security and Security Management.

Nicholas Haan is a graduate student at the Air Force Institute of Technology at Wright-Patterson AFB, Ohio. His degree of study is Master of Science in Information Resource Management with an emphasis on Information Assurance in the Department of Systems and Engineering Management. His thesis research is focused on insider threat detection within military weapons systems

Andrew Hansen (Major) is an Intermediate Developmental Education (IDE) student at the Air Force Institute of Technology (AFIT), Wright-Patterson AFB, Ohio. He is studying to achieve a Master's Degree in Computer Science with emphasis on Information Assurance. His research focus is the establishment of a realistic training environment for Cyberspace. Prior to attending AFIT, Major Hansen was the Assistant Operations Officer and an F-16 Instructor Pilot in the 64th Aggressor Squadron Nellis AFB, Nevada. He is an experienced instructor with over 1,500 fighter hours. Major Hansen was commissioned in 1992 as a distinguished graduate of the University of Colorado ROTC program and has served in various operational and staff assignments in Europe and the United States.

Denzil Helleesen enlisted in the United States Air Force in 1991. He received training at the 81st Communications Training Squadron, Keesler Air Force Base, Mississippi, in August 1996. He completed his undergraduate studies at Park University of Parkville, Missouri, in 2003. He is currently attending the Air Force Institute of Technology for graduate studies at, Wright-Patterson Air Force Base, Ohio.

Thomas Holt is an Assistant Professor in the Department of Criminal Justice at the University of North Carolina at Charlotte. He received his Ph. D. in criminology from the University of Missouri-Saint Louis, and his research focuses on computer hacking,

malware, and the role that technology and the Internet play in facilitating all manner of crime and deviance. Dr. Holt is also a member of the editorial board of the International Journal of Cyber Crimes and Criminal Justice.

Peter Hospodka completed his B.S. in Computer Science from the University of Nebraska at Omaha in 2006. He is now working on his M.S. in Computer Science also at the University of Nebraska at Omaha. His interests are directed towards Artificial Intelligence and its applications, which so far has been involving decision support systems.

Berg Hyacinthe holds a PhD from Florida State University. He concentrated his studies on Information Warfare, Social Informatics, and Emergent Technologies. His multidisciplinary research activities encompass global security threats and autonomous response systems. Author of several U.S. patent publications, Dr. Hyacinthe is conducting research in Europe around the concept of an autonomous biochemical neutralization system, which is considered as a revolutionary attempt to secure next-generation aroma-embedded information systems (e.g., scented emails and aroma-enabled browsers) and, in the area of homeland security, to avail an autonomous response to airborne biochemical threats (attacks or accidents) in confined spaces such as: aircrafts, subway systems, and other at-risk critical infrastructures.

Cynthia Irvine is the Director of the Center for Information Systems Security Studies and Research (CISR) and a Professor of Computer Science at the Naval Postgraduate School, where she has worked since 1994. Her research centers on the design and construction of high assurance systems and multilevel security. She is an author on over 125 papers and reports on security and has supervised the research of over 100 Masters and PhD students. She has served on numerous government committees and review boards. She is a member of the ACM, a lifetime member of the ASP, and a Senior Member of the IEEE. She is currently serving as Chair of the IEEE Technical Committee on Security and Privacy.

Michael Kolbe graduated from The Pennsylvania State University as a member of the class of 2003 with a Bachelors of Science in Computer Engineering. His research interests and previous assignments focus on critical infrastructure control system security. He is currently a Lieutenant working toward his Masters of Science in Cyber Operations at the Air Force Institute of Technology at Wright-Patterson Air Force Base, OH.

Nitin Kumar Dhiman has been working in Center For Artificial Intelligence and Robotics (CAIR), Defence Research and Development Organization (DRDO), India for the past three years. He has a degree of Bachelor of Technology in Computer Science from Kurukshetra University, India. He has contributed towards development of GIS applications and is currently working on knowledge representation and geo-spatial and temporal reasoning methodologies.

Stuart Kurkowski: Colorado school of mines, PhD in Mathematical and Computer Sciences, 2006. AIR Force insitute of technology, MS in Computer Science, 2000. Troy state university ms in Management Information Systems, 1994. US air force Academy bs in Computer Science, 1991. Current Faculty at AFIT.

Thuy Nguyen is a senior researcher of Computer Science at the Naval Postgraduate School. She has over 20 years of engineering and technical management experience in high assurance systems development, network security, trusted OS and security evaluation. She also oversees the construction of a multilevel security testbed, develops

Common Criteria protection profiles, serves as advisor to graduate students, and teaches security requirements engineering.

Eric Lindahl holds a Bachelor of Science Degree in Computer Science with Minors in Mathematics and Physics from the University of Nebraska at Omaha. His university research includes information assurance using information flow, ontological concept graph development and designing belief fusion operators as SQL stored procedures for summarizing homeland security threats. Mr. Lindahl has a diverse 15 year career in software engineering and architectural background in both theoretical scientific and high performance business environments. Mr. Lindahl is a veteran object-oriented software engineer and architect at such corporations as Canon Research and Development, ARINC, Caliper Microfluidics, Chevron, Lockheed Martin Mission Systems, and Wells Fargo.

James Lupo has over 30 years experience in high performance computing and computational physics, 20 of those years in parallel processing. A 20 year USAF career sharpened his early interest in communication security. As Senior Research Scientist for Massively Parallel Technologies Inc, he was instrumental in forming advanced communication and service delivery architectures. He has been associated with Regis Univ. for 6 year, and helped establish the Systems Engineering and Application Development Practicum.

Steven Mains is a Colonel in the United States Army with almost 28 years of active service. Commissioned in Armor from the US Military Academy, he has served in Tank and Cavalry units and is a veteran of Desert Storm and Operation Iraqi Freedom. He holds a PhD in Computer Science from the College of William and Mary and is a graduate of the British Staff College and the Indian National Defence College.

Todd McDonald is Lieutenant Colonel in the U.S. Air Force and an Assistant Professor in the Department of Electrical and Computer Engineering at the A.F. Institute of Technology. He received his doctoral degree in Computer Science from Florida State University in 2006, his Master of Science degree in Computer Engineering from the Air Force Institute of Technology in 2000, and his Bachelor of Science degree in Computer Science from the U. S. Air Force Academy in 1990.

Kar Leong Ong is civilian employee of the Ministry of Defense, Singapore. He received a B. Eng. with honors from the National University of Singapore in 1997 and a M.S. in Computer Science from the Naval Postgraduate School in 2007. His expertise is in the area of application architectures.

David Phelps studied computer science at Portland State University located in the gorgeous Pacific Northwest. After completing a Bachelor of Science degree in Computer science David continued his studies at the Naval Postgraduate School in scenic Monterey, California, where he completed a Master of Science degree in Computer Science with an emphasis in information assurance. David now works for SPAWAR Systems Center in Charleston, SC.

Julian Rrushi is a research scholar at the Department of Computer Science, University of Illinois at Urbana-Champaign, USA, and a final year PhD candidate in Computer Science at Università degli Studi di Milano, Italy. His research interests lie in system and network security, and cryptology. Rrushi has been an (ISC)² scholarship recipient for the years

2005 and 2007, and has carried out research at the Joint Research Center of the European Commission in Ispra, Italy.

Jamison Scheeres graduated from the United States Air Force Academy graduate in 2001 with a BS in Social Sciences. Upon graduation, he was commissioned as a Second Lieutenant, and assigned to Keesler AFB, Mississippi where he served for two years in a variety of roles as a communications officer, including creating weekly information security intelligence briefings for 18 months post 9/11. From Keesler AFB, he was assigned to the Information Technology Wing of the NATO E-3 AWACS Component in Geilenkirchen, Germany for three years, where he served as the supervisor for the configuration management section, as well as the site security officer for a major simulation system. In August 2006, he entered the Graduate School of Engineering and Management, Air Force Institute of Technology, where he graduated with a MS in Information Resource Management in March 2008. He separated from active duty in January 2008.

William Sousan is a PhD at the University of Nebraska, Omaha. His interests are semantic web, web intelligence, ontologies, knowledge modeling, information retrieval and extraction. Presently he is working on the Tailored Information and Delivery System"

Dennis Strouble is an assistant professor at the Air Force Institute of Technology at Wright-Patterson Air Force Base where he teaches Systems Engineering Management, Law, and Information Technology. He has a BS degree from Pennsylvania State University, a Masters from the University of Southern California, and a PhD. and JD from Texas Tech University. He has taught at several institutions, practiced law, co-founded a high tech company and served on active duty with the U.S Army.

Renier van Heerden works as a senior researcher at Council for Scientific and Industrial Research (CSIR) in South Africa in the field of Information Warfare. Before working at the CSIR he worked as a software engineer at Denel Optronics and as a Lecturer at the University of Pretoria. He has obtained a degree in Electronic Engineering and a Masters in Computer Engineering at the University of Pretoria.

Dorsey Wilkin is a captain in the United States Air Force and hails from Greenville, Michigan. He obtained a BS in Computer Science from Seattle University in Seattle Washington and is currently working on an MS in Computer Science from the Air Force Institute of Technology in Dayton Ohio. His research interests focus on critical infrastructure control system security.

Understanding IRC Bot Behaviors in Network-centric Attack Detection and Prevention Framework

Gail-Joon Ahn, Napoleon Paxton, and Kevin Pearson
University of North Carolina at Charlotte, NC, USA

Abstract: Botnets are one of the most threatening adversaries over the Internet due in large part to the difficulty of identifying botnet traffic patterns. Also, botnets are a prevalent and continuously growing method for conducting distributed attacks and identity theft. These attacks can include email spamming, distributed denial of service, port scanning, remote exploitation of vulnerabilities, and self-propagation to expand the botnet's size. The botnets can be used to scan infected hosts' machines and log keystrokes for sensitive data such as credit card and banking information, then relay gathered information to the botmasters. We have witnessed that existing signature-based detection and protection methods are ineffective in dealing with unknown bots. For these situations, a more proactive approach must be taken to gather and analyze botnets. In this paper, we introduce a network-centric attack management framework to learn more information about the bots by identifying malicious characteristics through the network traffic. Based on our framework, this paper focuses on our analysis method of IRC bots using IRC monitoring tool called IRC Sandman that observes IRC traffic and automatically downloads secondary injections from a command and control center. In addition, we briefly elaborate our findings and lessons learned.

Keywords: Network-centric attack, IRC bot, botnets

Adapting Information Operations to a Changing World: Future Options for the United States

Edwin Armistead

Edith Cowan University, Perth, Australia

Abstract: We now live in an Information Age, which has been called 'an era of networks' (Copeland, 2000; Arquilla and Ronfeldt, 1996, 2001). Loudly proclaimed to be a transformational period, it is especially interesting to compare and contrast the differences between the rhetoric and reality. Information Operations (IO), is a relative newly defined activity, which proposes to revolutionise the manner in which warfare, diplomacy, business and a number of other areas are conducted. Yet in the United States government, a significant gap exists in regards to the conduct of IO. While strategic policy and doctrine have been developed and promulgated, in most cases, the actual conduct of IO activities and campaigns, are normally performed at a more tactical level. This delta between theory and reality exists because the federal bureaucracy is unwilling or unable to make the transformational changes that are needed to best utilise information as an element of power. In his research, the author has developed definitions and models that articulate not only why this delta exists, but also specific strategies for utilising IO in a manner that best optimises the inherent capabilities of this element of power. Specific recommendations are noted below, and will be laid out in greater detail throughout the paper: Develop an Academic Theoretical Construct for IO, Understand that Different Approaches and Processes are Needed to Support IO, Establish an International IO Standards Effort, Meeting the IO Training Needs. These ideas were taken from 100 interviews conducted over a five-year period as part of a PhD dissertation from practising mid-level officials of the interagency organisations in the United States that are involved in conducting information campaigns. It is hoped that these conclusions developed in this paper may be useful for future IO planners, as well as senior level decision makers.

Keywords: Information operations, training, standards, theory, process

A Framework for Improving Consistency of the Protection of Critical Technologies

Eric Ashe¹, Michael Grimaila¹, and Brian Carter²

¹Air Force Institute of Technology, Wright-Patterson Air Force Base, OH USA

²Air Force Research Laboratory, Wright-Patterson Air Force Base, OH USA

Abstract: In this paper, we propose a framework to assure the consistent application of anti-tamper measures to protect critical technologies in Department of Defense programs. The proposed framework utilizes a secure multilevel security database to provide the capability to accurately document critical technologies and their associated protection measures; enable auditing across and between services to ensure the consistent application of anti-tamper protection measures across all Department of Defense organizations; and provides visibility of baseline critical technologies protective measures while maintaining compartmentalization of program specific information.

Keywords: Critical technology protection, anti-tamper, multilevel security database, auditing

Interactive Visualization of Fused Intrusion Detection Data

Serafin Avitia, Stuart Kurkowski, and Luke van der Hoeven

Air Force Institute of Technology, Wright Patterson Air Force Base, OH, USA

Abstract: Today's complex networks with their large traffic volume and increased malicious activity, make intrusion detection awareness difficult. The traditional analyst-based review of stand-alone intrusion detection system (IDS) alerts is rapidly exceeding human capability. Several different areas of research focus on reducing the number of alerts. One example would be the reduction of the number of false positive alerts generated by these IDS tools. However, the number of alerts remains large. Recent research focuses on aggregating alerts for a single tool or even the fusion of data between alerts from multiple tools and system logs, all with the goal of reducing duplicates and shortening the analysis loop across different tool sets. The research in this paper targets this fused set of alerts and log entries as our basis for developing interactive visualizations. This fused data is an aggregation of several sources providing more "information" than the raw alert data. The presence of "information" allows our visualizations to provide the analyst with more context and knowledge than traditional IDS-level data visualizations such as parallel axis plots, etc. Providing both increased context and interaction for data exploration enables an analyst to achieve increased situational awareness quicker and easier. Linking multiple views of the information to maintain focus and context allows the analyst to see not only malicious activity, but also what assets are affected and where activities may be directed next. The traditional approach of an analyst working in isolation with a single tool's output and then passing brief reports to others to correlate are limiting activities. Synergistic visualizations of the network data aggregated from alerts and logs can lead to the elimination of an entire layer or phase of analysis operations. Visualizations of the fused data allow direct analysis across tools thus improving the analysis process.

Keyword: IDS visualization, network situational awareness, IDS analysis, network defence, network information visualization

Jam Resistance Communications without Shared Secrets

William Bahn, Leemon Baird III and Michael Collins

United States Air Force Academy, Colorado Springs, CO, USA

Abstract: As the United States develops the Global Information Grid (GIG), cryptographic key management will be a challenging problem. Information security is attained only when all four of the classic goals - confidentiality, integrity, authenticity, and availability – are attained. Hostile jamming is a direct attack on the availability of an information resource. While much progress has been made utilizing asymmetric cryptography and a Public Key Infrastructure (PKI) to protect keys that encrypt, decrypt, and authenticate data, the same cannot be said for keys used to protect the physical communication layer from hostile jamming. In particular, battlefield ad hoc wireless networks appear to be at significant risk. Preferred methods for jam resistance rely on highly-directional links (e.g., high-gain antennas, lasers, or physical cable), but realistic operational environments will heavily utilize omnidirectional radio frequency (RF) links as well. Presently, jam-resistance in omnidirectional links relies on spread spectrum techniques, all current forms of which require symmetric keys (i.e., secret keys pre-shared by users). While shared-secret schemes are workable in small networks, the scale and nature of theater-wide, mobile, ad-hoc wireless networks will quickly overwhelm any practical key management strategy. Not only will the initial distribution of keys be difficult, but preventing keys from being compromised and re-keying when the inevitable compromises occur will place extreme burdens on the system. In addition commercial systems, such as cellular phone networks, face similar challenges as their growing need for jam resistance becomes more evident. Furthermore, public-access systems such as the civilian side of the Global Positioning Satellite (GPS) system preclude reliance on secret keys at all since, by definition, the pool of authorized users includes everyone. Yet while civilian GPS is recognized as having little jam-resistance, the present trend calls for increased reliance on it for civil aviation. The key management problem in such systems can only be alleviated if the physical layer link can remain available even without a shared secret in place. Such a physical layer can then serve as the foundation upon which well established asymmetric techniques can be used to construct a secure channel. We propose the first algorithms that make this possible: the BBC encoding and decoding algorithms. We describe these algorithms and how they can be implemented in suitable physical layers.

Keywords: Spread spectrum, jam-resistance, physical layer

Developing Cyber Warriors

Jeff Boleng, Dino Schweitzer, and David Gibson
US Air Force Academy, Colorado Springs, CO, USA

Abstract: The US Department of Defense defines cyberspace as a “domain characterized by the use of electronics and the electromagnetic spectrum (EMS) to store, modify, and exchange data via networked systems and associated physical infrastructures.” Cyberspace is a warfighting domain on par with air, space, land, and sea, and the US Air Force has accepted the challenge of controlling it, defending it, and operating in it. The US Air Force Academy (USAFA) in cooperation with Air University, the AF Institute of Technology and AF Cyber Command (provisional) is developing the education and training requirements for our future cyber warriors. Much of this work builds on an already established curriculum being taught at USAFA and national training standards defined by the National Security Agency and the Department of Homeland Security. Our approach is a two-pronged effort. On one hand we provide a multi-disciplinary foundation for every graduate. We accomplish this by identifying and adding specific cyber content to our existing broad based core curriculum. On the other hand we also provide a smaller number of highly skilled, very technical, cyber warriors to support the required missions in the domain of network attack (NetA), network defense (NetD), network surveillance (NetS), and network support. We accomplish this through our accredited Computer Science major and the addition of a three course sequence including Computer Security and Information Warfare, Network Security, and Cryptography. This paper will outline the vision and broad educational requirements required for 21st century officers and provide details on our two-pronged approach to developing cyber warriors.

Keywords: Education, training, cyberspace, warfare, information

Sensor Collection and Analysis of Radio Frequencies (SCARF)

Jeff Boleng¹, Thorsten Wirges¹, Dino Schweitzer¹, Seana Hagerman² and Ramakrishna Thurimella²

¹US Air Force Academy, Colorado Springs, CO, USA

²University of Denver, Colorado , USA

Abstract: In today's net-centric warfare environment, effective management and use of the electromagnetic spectrum is critical. Increasing demands on wireless spectrum from radio traffic, unmanned aerial vehicle (UAV) communication, wireless networks, improvised explosive device (IED) jammers, and sensor networks result in sources competing for, and at times conflicting over, limited frequency spectrum. From an intelligence perspective, having a clear understanding of the RF environment, both friendly and foe, is an important essential of battlefield management. This paper presents the Sensor Collection and Analysis of Radio Frequencies (SCARF) system with a focus on the information processing requirements of the sensors and various system components. The overall architecture, sensor processing and fusion challenges, visualization algorithms, and current implementation status are discussed.

Keywords: RF collection, visualization, data fusion, system integration

Toward Detecting Novel Software Attacks by Using Constructs from Human Cognition

Adam Bryant

Air Force Institute of Technology, Wright-Patterson Air Force Base, OH, US

Abstract: Preventing code reverse engineering is a different type of problem than preventing infection from computer viruses or other malware. While most malware is blocked by software using rule-based signature systems or heuristics to determine functionality and respond, malware detection mechanisms are limited by the robustness of their classification systems and existing definitions. Software cracking and code reverse engineering, by contrast, are creative activities where an attacker typically employs novel solutions to circumvent protection systems and to prevent his own actions from being detected. Currently, there is no capability that totally prevents or detects code reverse engineering activities. To perfectly prevent reverse engineering of software, a system designer would have to be able to completely specify all potential attack vectors and then to implement countermeasures which address each type of attack vector.

The first part of autonomically responding to a threat action is to detect it. Potential answers to the detection problem lie in artificial intelligence research, but even the most advanced artificial intelligence and machine learning technologies are currently unable to produce a system which can detect a completely novel attack vector. Human cognition abilities, on the other hand, allow a person to recognize a novel event like an attack even if it does not fall into the typical categories of what that person expects for that given event.

This paper discusses Jean Piaget's cognitive development model and maps the phases of that model to different representations in computational intelligence. This mapping highlights the current state of the art of artificial intelligence and autonomic problem solving and highlights limitations of currently available approaches. This mapping will enable researchers to move toward developing theoretical and technological improvements in the hopes of detecting even novel code reverse engineering activities. This paper explores some different paths to be able to replicate the ability in a computer to detect a novel attack, classify novel events and circumstances, develop classification systems on-the-fly, and cross boundaries of classifications.

Keywords: Cognitive science, information security, reverse engineering, artificial intelligence, computational intelligence

Biometric Security Enhancements Through Template Aging Matching Score Analysis

John Carls¹, Richard Raines¹, Michael Grimaila¹ and Steven Rogers²

¹Air Force Institute of Technology, Wright-Patterson Air Force Base, OH, USA

²AFRL, Wright-Patterson Air Force Base, OH, USA

Abstract: Biometric technology and systems are revolutionizing identity capabilities. With biometrics maturing and in full, rapid development, there is a requirement to have a higher accuracy of identity verification. This higher accuracy will provide improvements to the security of biometric verification systems; ultimately reducing fraud, theft, and loss of resources from unauthorized personnel. With previous biometric systems, a higher acceptance threshold to obtain higher accuracy rates increased false rejection rates and user unacceptability. However, maintaining the higher accuracy rate enhances the security of the system. Through the methods presented in this paper, higher accuracy rates are obtained without lowering the acceptance threshold, therefore improving the security level, false rejection rates, and user acceptability. One area of biometrics that has a paucity of research is template aging and the adult age-progression, particularly in regards to facial aging. This paper presents methods of modeling and predicting facial template aging based on matching score analysis. A novel foundational framework for facial template aging is presented and provides a methodological framework. The groundwork discusses the techniques used in the template aging framework, to include similarities to the “perfect recognition similarity score” and “actual recognition similarity score” concepts. The matching scores are calculated using commercially available matching algorithms/SDKs against publicly available facial databases. This new framework improves performance error rates while maintaining or improving upon the overall matching and/or rejection levels. Using such scores, we can predict a timeframe if or when an individual needs to be re-enrolled with a new template. Additionally, experimental results demonstrate a significantly higher accuracy of identity verification using the presented methods. This framework ultimately enhances the security of the biometric system.

Keywords: Biometric security, template aging, matching scores

Outsourcing and the Insider Threat: An Increasing Security Risk

Carl Colwill

BT Design, Security Risk and Compliance, UK

Abstract: Critical National Infrastructures are no longer under the direct control of Governments and infrastructure protection has become increasingly dependent upon commercial organisations. However, the globalisation of business and the growth of the digital networked economy means that virtually any business process can be undertaken by someone else, somewhere in the world. This has resulted in a rapid and substantial increase in the outsourcing of a wide range of activities and operational processes. In turn, this means that components of national infrastructures and information security are also effectively outsourced. Whether the sourcing is in country or offshore this commercial reality results in a growing number of third parties and contractors (many of whom will be foreign nationals) who are given long term access to critical assets, systems and information. These people work within the extended boundaries of companies, often with privileged access rights and varying levels of operational control, but typically with lower levels of company and country affinity, loyalty and trust. The threat of attack from insiders is therefore growing and appropriate risk assessments and security controls must be implemented in a consistent and agile fashion.

This paper describes the tools and techniques used by BT to ensure that the core factors relating to insider threats are prominent in security risk assessments and lists a set of security countermeasures pertinent to most cases. The global sourcing environment is dynamic and risk assessments must not be one-off tactical exercises but part of an ongoing process to develop risk management strategies and compliance regimes.

Keywords: Insider threat, outsourcing, critical national infrastructure, security risk assessments

The Impact of Vista and Federal Desktop Core Configuration on Incident Response

Daniel Cotton, Stephen Nugen, and William Mahoney
University of Nebraska at Omaha, NE, USA

Abstract Detecting and responding to successful exploitation of Windows hosts depends on the skill and preparedness of first responders and the effectiveness of their tool sets. The release of and transition to Vista presents a potential challenge with respect to those skills and tools. The adoption of a new federal standard FDCC (Federal Desktop Core Configuration) specifying the configuration for desktop and laptop computers in federal agencies presents a second challenge to first responders and their tool sets. This paper explores those potential challenges by: (1) Identifying additional requirements for preparing to examine Windows hosts; and (2) Comparing the effectiveness of tool sets executed against two different Windows operating systems, configured to two different standards, resulting in these four cases:

Windows XP, default configuration.

Windows XP, configured to FDCC standards.

Windows Vista, default configuration.

Windows Vista, configured to FDCC standards.

Keywords Windows vista, incident response, federal desktop core configuration (FDCC), forensics, operating systems

Using Attack and Protection Trees to Evaluate Risk in an Embedded Weapon System

Robert Cowan¹, Michael Grimaila¹ and Raju Patel²

¹Air Force Institute of Technology, Wright Patterson Air Force Base, OH USA

²Aeronautical Systems Center, Wright Patterson Air Force Base, OH USA

Abstract: Previous research has demonstrated the benefits of using attack trees and protection trees to evaluate system risks. Attack and protection trees are useful in documenting and quantifying risks, determining the maximum protection capability in the presence of all control measures, and evaluating the tradeoffs between the costs of control measures and their effectiveness at mitigating risk. However, example applications of evaluating risks using attack trees and protection trees in the literature has largely been in narrow in scope, limited to simple textbook examples, and have not been proven in the analysis of complex systems.

In this paper, we consider the use of attack trees and protection trees for risk quantification during the risk management process conducted on an embedded weapon system. Specifically, we will evaluate the effectiveness of attack and protection trees in documenting the threats and vulnerabilities present in a generic Unmanned Aerial Systems (UAS) architecture. Existing methods for risk quantification used tend to be highly subjective, depend on the knowledge of analyst, and provide very little documentation to justify protection selection decisions. Our working hypothesis is that the application of attack trees and protection trees during the risk management process can provide an efficient and effectively means to quantify system risk, justify the selection among control measures, and provide the ability to build a library of trees that can be reused in similar systems and architectures. To test our hypothesis, we will build canonical attack and protection trees, assigning probabilities and losses, and conducting a trade off analysis of control measures in order to determine the utility of the methodology. The application of this methodology potentially will provide both a framework and a visual representation of both potential risks to a weapons system and also the costs of both protecting and defending that weapons system.

Keywords: Attack trees, protection trees, embedded weapons systems

Religion, Ideology, and Information Warfare

Geoffrey Darnton

Bournemouth University,UK

Abstract: This paper is primarily conceptual, but it also provides a summary of key prior research on the causes of war and statistical analyses of the relationships between religion and warfare. It proposes that religion, ideology, and belief systems are the ultimate preferred targets of information warfare. An operational definition of religion is proposed, which merges ideas of religion and ideology. Beliefs in things such as the desirability of allowing market forces to prevail, or preference for representative democracy, have the same characteristics as religions, and the creation and maintenance of such beliefs are key objectives of information warfare. Epidemiological theory is proposed as one framework for understanding how to achieve the spread of ideas, and how populations can also develop a 'natural' resistance to ideas about the desirability of the objectives of information warfare. A key proposition is that at present economic ideology probably kills far more people today than the total of religious extremism.

Keywords: Information warfare, religion, ideology, peace, information space

An Investigation of Negative Authentication Systems¹

Dipankar Dasgupta and Rukhsana Azeem
The University of Memphis, TN, USA

Abstract This work explores a new concept in user authentication to improve security on login process. Most authentication systems use some form Positive Identification (PI) to identify legitimate users. Specifically, these systems use a password profile containing all the user passwords that are authorized to access the system (or the server). The negative counterpart (non-self/anti-password space) represents all strings that are not in the password file, which can possibly be exploited by hackers (using password guessing or cracking tools). While this Anti-Password (Anti-P) space appears to be very large, our technique utilizes a form of implicit clustering to generate a small set of Anti-P detectors to cover this password guessing space. The developed system demonstrated it is hard (if not impossible) to discover any individual password even though Anti-P detectors are being compromised. Moreover, experiments show that these detectors work as a password immunizer, filtering out all illegitimate users (hackers, crackers, etc.) before allowing the legal users to access the positive identification system.

Keywords Secure authentication, password protection, positive identification, negative authentication

Software Agent framework for Computer Network Operations in IW

Evan Dembskey and Elmarie Biermann

Tshwane University of Technology, Pretoria, South Africa

Abstract: It is imperative for countries and companies alike to protect their information and the parallels in doing so are very similar. A company is likely to gain a competitive advantage on its opponent by not only protecting its own information but also by modifying or obliterating its opponent's information. Network globalization and the very nature of the Internet have established a foothold for small scale IW opportunities. This makes it possible for companies with small budgets to engage in information warfare operations. For this purpose, effective tools are required to analyze and protect the digital battlefield, and if necessary, to retaliate. This paper presents a software agent framework (TELUM) that addresses the problems of defending against multiple external attack vectors, while simultaneously launching attacks against adversaries over public networks. The flexibility of the framework allows it to cater for existing as well as emerging technology.

Keywords: Information warfare, software agent, cyber crime, cyber terrorism, information security

Cyber Warfare: Rethinking Strategy in the Information Age

David Fahrenkrug

8th Air Force, Barksdale Air Force Base, LA, USA

Abstract: This paper examines some of the strategic and operational considerations for using cyberspace in the conduct of modern warfare. Understanding the role of cyberspace will lead to greater clarity on the long anticipated revolution in military affairs that is fueled by the explosion in information technology. Unfortunately, without a clear understanding of cyberspace there is often hyperbole and exaggerated claims as to the impact that information technologies will have on the conduct of war or even the very nature of war itself. The Department of Defense recently codified its definition of cyberspace as a networked environment that is more than the internet but is nonetheless bounded. This description has led to the realization that nearly every aspect of American society is permeated by cyberspace. From cell phones, to computers, to satellite television, government, businesses, and individuals depend on the use of cyberspace. Similarly, US military operations increasingly rely on cyberspace and the networking of sensors, command and control elements, and weapons systems to conduct warfare. Adversaries are very much aware of this dependence on cyberspace and they are actively seeking ways to exploit it and gain an advantage. In the same way that air power transformed the battlefield and exposed a nation's centers of gravity to direct attack, cyberspace is breaking down the physical barriers that shield nations from attacks on commerce and communication. National defense must, therefore, include an integrated strategy founded on the principle of protecting and exploiting the use of cyberspace. This paper will also identify potential strategic advantages that result from an ability to use cyberspace to create new and different types of effects against an adversary.

Keywords: Cyberspace, information warfare, strategy, information operations, military

Analysis of Routing Worm Infection Rates on an IPv4 Network

**James Gorsuch, Barry Mullins, Rusty Baldwin and Richard Raines
Air Force Institute of Technology, Wright-Patterson Air Force Base, OH**

Abstract: Malicious logic, specifically worms, cost network users an enormous amount of resources in the form of time and money. Worms, like Slammer and Code Red, infect thousands of systems and ultimately deny whole networks access to the Internet. This paper describes the evaluation of worm propagation speeds using models developed in Matlab. Specifically, the paper examines the rate at which the original Slammer worm, a Slammer based routing worm, and a new Single Slash Eight (SSE) routing worm infect vulnerable systems within a given IP address space. A comparison of the propagation speeds from a worm on a computing system in 2003 to those available today is performed.

This paper shows that both the Slammer-based routing worm and the SSE routing worm spread faster than the original Slammer. The SSE routing worm proved to be faster than any of the worms evaluated. The SSE routing worm was more than three times faster than the original Slammer worm and more than two times faster than the Slammer routing worm. Thus, the release of a similar worm on today's architecture would spread faster and cause even greater congestion than has been observed previously. As the capabilities of computer systems continue to grow, the speed of worm propagation should increase with it as their scan rates directly relate to their infection rate.

Keywords: Worm propagation, malicious code, matlab simulation

A Comparison of Popular Global Authentication Systems

Dennis Guster, Charles Hall, Suthantha Herath, Brittany Jansen and Lukasz Mikluch

St. Cloud State University, St. Cloud, MN, USA

Abstract: Distributed processing offers many benefits, most notably replication and enhanced processing performance. Key elements in cost effective distributed processing are grids and clusters in which the processor interconnectivity is supported by a computer network. Providing effective authentication among the many nodes involved is challenging in a private network, not to mention if the internet is used. From an end-user perspective, global authentication is a must, as it is both easy and convenient. With this convenience comes a problem: if compromised, it is not just the resources on one node but 64 nodes that are vulnerable. Typically, the grid or cluster is supported by some form of the Unix operating system; certainly a hacker would love to take over a 64 node cluster testbed and use it break encrypted passwords. This paper is designed to help make organizations that are using cluster/grid computing either in a LAN or WAN aware of the importance of using secure global authentication. The authors originally selected NIS in an effort to get their cluster/grids up and running as fast as possible. It was during the process of teaching security courses, which had auditing components, that the degree of vulnerabilities became exposed. This is when it was suggested by the literature that there are advantages to adapting to the LDAP structure, and the results of further investigation indicate these advantages. For example, the extra capabilities of LDAP to provide more secure authentication are especially warranted in these hostile environments. The following paper focuses on the advantages/disadvantages of using each as a global authentication system on either NIS or LDAP to support an instructional based distributed processing laboratory in a university setting. This paper will address some of the potential problems as well as might serve as a template to those seeking to upgrade their global directory services.

Keywords: Distributed processing, internet, testbed, attack, global authentication

Insider Threat Detection within Embedded Weapon Systems

Nicholas Haan¹, Michael Grimaila¹ and Raju Patel²

¹Air Force Institute of Technology, Wright Patterson Air Force Base, OH, USA

²Aeronautical Systems Center, Wright Patterson Air Force Base, OH, USA

Abstract: As security conscious organizations mature their information security capabilities to protect their information infrastructure from external attacks, risk management inevitably leads them to consider the risks associated with insider threats. The need for effective insider threat detection, prevention, and mitigation is driven by the growing number and magnitude of reported losses resulting from both malicious and non-malicious insider information incidents. Insiders have a significant advantage in that they are trusted; possess elevated privileges when compared to external users; have knowledge about technical and non-technical control measures; and, in some cases, can bypass security measures designed to prevent unauthorized access. Traditional security architectures focusing only upon perimeter defenses often do not provide the capability to efficiently identify and attribute fraud, information exfiltration, and sabotage to a trusted insider. Given this combination of insider access, knowledge, and the lack of insider threat detection measures, identifying and mitigating insider threats is a challenging task. The problem is further complicated by the difficulty in quantifying the costs and benefits when making risk tradeoff decisions to mitigate insider risk.

In this paper, we conduct an analysis of a generic, Unmanned Aerial Vehicle (UAV) weapon system architecture in order to identify risks arising from susceptibility to insider attacks; consider the application of insider threat detection technologies, policies, and processes to mitigate risks; and discuss challenges that program managers face when making risk trade-off decisions in embedded weapons systems. Embedded weapon systems present several unique challenges when assigning controls to mitigate insider risks. Operational requirements, budget, schedule, and culture often constrain the application of “best practice” security solutions and drive the need to develop alternate layered security strategies to mitigate insider risks. Through our analysis, we intend to identify appropriate insider threat security control measures that can enhance a generic UAV weapon systems architecture and security posture.

Keywords: Insider, insider threat, detection, threat indicators, malicious insider, weapon system

Cyber Flag: A Realistic Training Environment for the Future

Andrew Hansen, Paul Williams, Robert Mills and Mark Kanko

Air Force Institute of Technology, Wright-Patterson Air Force Base, OH, USA

Abstract: Now is the time for Cyber Flag – initiating and implementing an effective, comprehensive and coordinated training environment in the relatively new and quickly developing cyberspace domain. As is well understood, the rapidly unfolding challenges of cyberspace is a fundamental warfare paradigm shift revolutionizing the way future wars will be fought and won. A significant test for the Air Force (indeed any organization with a credible presence in cyberspace) will be providing a realistic training environment that fully meets this challenge. Why create another Flag level exercise? Realistic training (that which is effective, comprehensive and coordinated) is crucial to success in time of war. Red Flag provides dominant training within the air domain and now with the evolution of cyberspace, a comprehensive training environment is necessary to meet this growing and broadening threat. This paper builds on the Red Flag tactical training exercise in order to define a future environment that combines the air, space and cyberspace domains with specific emphasis on cyberspace capabilities and threats. Red Flag has and continues to be a great tactical training exercise; Cyber Flag would use the best practices of Red Flag (and other realistic training venues) to define a future training environment for the cyberspace domain. The Virtualized Intranet Platform for Exercise Realism (VIPER) combines portability with realistic replication of network architectures and traffic to enhance computer network operations during Cyber Flag. Using virtualization technology, VIPER provides a small-scale network with simulated users to act as either a target of computer network attack or a network defense problem. There is no better training than the hands-on realism associated with participation in an exercise such as Red Flag. Secretary Michael W. Wynne has a vision for dominant operations in cyberspace “comparable to the Air Force’s global, strategic omnipresence in air and space.” This bold vision requires a combination of joint coordination, skilled forces and a realistic training environment to bring them all together; Cyber Flag is the suggested vehicle for accomplishing this.

Keywords: Cyberspace, training, red flag, network warfare, information operations, LARIAT

Information Asset Value Quantification

Denzil Hellesen¹, Michael Grimaila¹, Larry Fortson² and Robert Mills¹

¹Air Force Institute of Technology, Wright-Patterson Air Force Base, OH, USA

²Air Force Research Laboratory, Wright-Patterson Air Force Base, OH, USA

Abstract: In this paper, we present the development of an Information Asset Valuation (IAV) process to identify factors and attributes which collectively are used to assign value to information asset (InfoA) within a military context. Information asset valuation is composed of a summation of tangible and intangible valuation measures that attempt to quantify how the InfoA supports the organizational mission. We review existing non-military information valuation methodologies used in the accounting and law disciplines to determine their applicability in a military context as well as examine existing military information valuation methodologies to understand the effectiveness of each discipline as adaptable models for IAV. The objective of this work is to identify measures that can account for context, environment, and temporal factors which impact information valuation. A standardized taxonomy of information valuation measures would help improve consistency, reduce uncertainty, promote documentation of information value during the risk assessment process, and enable the aggregation of information asset value in support of higher level decision making processes.

Keywords: Information valuation, asset, subjective assessment, information asset

Characterizing Malware Writers and Computer Attackers in Their own Words

Thomas Holt, Joshua Soles and Lyudmila Leslie
The University of North Carolina at Charlotte, NC, USA

Abstract: As the world comes to rely on computers and rapidly changing technologies, the threat posed by computer criminals has become increasingly significant. Despite the best efforts of security professionals, computer attackers are able to exploit vulnerabilities in systems and circumvent antivirus software to obtain all manner of sensitive personal and financial information. Attackers no longer need to rely on their abilities, as malware and automated tools quickly and efficiently perform attacks for them.

Individuals can buy access to sophisticated malware, including bots, Trojans, and worms via markets run in publicly accessible web forums around the world. Some individuals also release their tools to the public free of charge under the guise of sharing information and resources for penetration testing and security purposes. Regardless of method, the creators of malicious software enable individuals around the world to engage in all manner of cyberattacks and crime.

At the same time, the blogs, web-forums, and personal web-pages used by malware writers and attackers can provide information on their actions and connections to others. By analyzing the information provided, researchers can understand the motives and beliefs that drive attackers. This presentation explores the on-line personas of multiple malware writers and attackers using a variety of on-line resources. The role of individuals and groups in the spread of malicious software around the world are also discussed in some detail. The implications of these findings for information security and criminologists are also considered.

Keywords: Malware, hackers, profiling, cybercrime

Computer Assisted Security Assessment through Fact Proposition Space

Peter Hospodka, Quiming Zhu, William Sousan and Ryan Nickell
Department of Computer Science, University of Nebraska at Omaha, NE, USA

Abstract: In this age of Information Warfare, it is becoming increasingly important to make quick and informed decisions based on current information and knowledge gained from the past. Whether these decisions are used for assessing risk involved with an action, threat involved with an opponent's action, or impact of your decision on opponent's actions, it is a daunting process without support from advanced situational assessment systems. To provide such support and assistance, we have devoted our effort on an intelligent inference system operating based on a hierarchical fact-proposition space (FPS) model. Basic components of our FPS consist of a set of propositions or questions that need confirmation or answers at the levels of the hierarchy. Some propositions have relationships where the outcome of one affects the outcome of another. The FPS inference process tries to use the past knowledge to determine initial beliefs or strength of the relationships. Current knowledge is further used to identify some proposition confirmation or question answers which in turn are used to propagate up the hierarchy in the goal to return some recommended decision(s). Our FPS model has similar foundations of Bayesian Networks (BN) in that both base computations on Bayes' Theory and probabilistic inference. However, our FPS differs from BN in that it sub-divides a complicated multi-level, multi-variant decision problem into a number of hierarchically organized subspaces, where each space can be manipulated in terms of matrix computations in a simple form of Bayesian inference. By partitioning the solutions at the subspaces in the hierarchy, the total complexity of the problem is reduced. The system's objectives are to provide a valuable information fusion and belief integration engine to those making decisions on risk assessment, threat assessment, and similar tasks. Through the prototype implementations, we hope to demonstrate the capabilities and advantages of the hierarchical fact-proposition space model.

Keywords: Computer assisted assessment, decision making, fact proposition space, inference engine, information warfare

Initial Supports to Regulate Information Warfare's Potentially Lethal Technologies and Techniques

Berg Hyacinthe¹ and Larry Fleurantin²

¹Infosense Technologies and Research Inc., Sunrise, FL USA

²Fleurantin and Associates, Miami Beach, FL USA

Abstract: The information warfare paradigm is taking a perilous interstellar dimension, without the explicit rules necessary to protect cyberwarriors against war crimes or to address other related international humanitarian concerns. As a result, this report examines the international legal implications of involving weapons of mass destruction (WMD) and offers an early contribution to continuous efforts aimed at the regulation of the most lethal information technologies of the new millennium. With regard to the United States (U.S.), where information warfare plays a quintessential role in strategic defense and security, many scholars argue that foreign criminal statutes will most likely apply to crimes committed during information operations. Others suggest that "information attacks" occur in another dimension, and the general consensus is that current law is not applicable. In either case, the asymmetrical nature of information warfare makes any attempt to maintain "information dominance" very challenging. According to the authors' main line of argument concerning information operations, the current state of *legal ambiguity*, once perceived as an advantage, has become a threat to the U.S., the entire international community, and beyond (e.g., outer-space and celestial bodies). This report only offers a snapshot of a much broader research agenda to explore the applicability of existing conventions and treaties (e.g., the Biological Warfare Convention (BWC) of 1972, the Outer Space Treaty of 1972, the International Telecommunication Convention (ITC) of 1984, and the Chemical Warfare Convention (CWC) of 1993) to the quiet fusion of digital telecommunication networks and bio-microelectromechanical systems (BIO-MEMS) into potential diffusers, relays, or transport vehicles of WMD. Acknowledging the imperative to strike a fine balance between *humanitarian concerns* and *military necessity*, according to customary and international laws, the authors also discuss (1) the "physicality" and "lethality" of information warfare technologies and techniques, (2) the involvement of information warfare weapons in "armed conflicts", (3) the initiative of U.S. military officials to address humanitarian concerns and potential charges of war crimes, and (4) the military's responsibility to protect critical infrastructures (e.g., communication satellites, military bases, warships and other crafts). In synthesis, after a preliminary evaluation on the merits and demerits of an eventual *international convention on information warfare's most lethal technologies and techniques*, the authors concluded with the following observation: the evolution/survival of the *Homo sapiens* is threatened by the same "technologies" originally intended to secure the transition from terrestrial to interstellar living.

Keywords: Lethal information technologies, information warfare, WMD, cyberwarriors, information war crimes, interstellar law

Advanced Manipulation Of Digital Evidence Using Memory Based Anti-Forensic Tools

Hamid Jahankhani¹, Elidon Beqiri¹ and Kenneth Revett²

¹University of East London, UK

²University of Westminster, UK

Abstract: Criminals are exploiting now digital communications to commit a wide range of crimes such as identity theft, online piracy, financial fraud, terrorism and pornography distribution. Computer forensics is the discipline that deals with the acquisition, investigation, preservation and presentation of digital evidence in the court of law. Whereas anti-forensics is the terminology used to describe malicious activities deployed to delete, alter or hide digital evidence with the main objective of manipulating, destroying and preventing the creation of evidence. This paper aims to present some of the current anti-forensic approaches and in particular reports on memory-based anti-forensic tools and techniques. Memory-based bootable live CD's are specially built Linux operating systems that boot directly from the CD drive into the RAM (Random Access Memory) area. Live CD's are used mainly for penetration testing and other security related tasks and they include a variety of software packages that can be used for anti-forensic purposes.

Keyword: Anti-forensics, live CD, data hiding, wireless anti-forensics, memory-based anti-forensics

Analyzing Anonymity in Cyberspace

Douglas Kelly, Richard Raines, Rusty Baldwin, Barry Mullins and Michael Grimaila

Air Force Institute of Technology, Wright Patterson Air Force Base, OH, USA

Abstract: For any organization interested in securing anonymity in cyberspace, the ability to understand changes in anonymity levels during a cyber attack is crucial. To achieve anonymity actions should be separated from the agents who perform them, for some adversary. Anonymity in general as well as the anonymity of each particular agent or group is dependent upon several factors. Thus, numerous methods of analyzing anonymity in cyberspace exist. Typical approaches use simple quantifications and basic probabilistic models. This paper explores a variety of anonymity metrics. Practical applications of the metrics reveal how anonymity is defined and quantified in cyberspace. The objective is to provide a macro-level view of the systematic analysis of anonymity preservation, degradation, or elimination in existing and proposed wired and wireless anonymous communications networks.

Keywords: Anonymity, metrics, communications networks, cyberspace

A Framework for Classifying Anonymous Networks in Cyberspace

Douglas Kelly, Richard Raines, Rusty Baldwin, Barry Mullins and Michael Grimaila

Air Force Institute of Technology, Wright Patterson Air Force Base, OH, USA

Abstract: The desire for privacy in cyberspace drives research in the area of anonymous networks. Any entity operating in cyberspace is susceptible to debilitating cyber attacks. As part of the National Strategy to Secure Cyberspace, the United States acknowledges that the speed and anonymity of cyber attacks makes distinguishing among the actions of terrorists, criminals, and nation states difficult. Indeed, today's Internet is an incredibly effective, uncontrolled weapon for eavesdropping and spying. Therefore, anonymity and privacy are increasingly important issues. A plethora of anonymous networks achieve varying levels of anonymity against a wide range of adversarial attacks. However, very few conceptual frameworks exist to ease the classification of anonymity in the diverse set of wired and wireless anonymous communications networks. This paper proposes a novel cubic framework to facilitate the systematic definition and classification of anonymity in anonymous communications networks. Three key anonymity components: anonymity property, adversary capability, and network type are thoroughly explored. This framework highlights the subtle and expanding definition of anonymity and aids in the advancement of state-of-the-art technological privacy-preserving mechanisms in cyberspace against any adversary.

Keywords: Anonymity, privacy, communications networks, cyberspace, national security

A Survey of Critical Infrastructure Control System Effects

Michael Kolbe and Paul Williams

**Air Force Institute of Technology, Wright-Patterson Air Force Base, OH,
USA**

Abstract: The critical infrastructure control systems of the United States have long been shielded, through obscurity and the slow introduction of technology, from the onslaught of malicious crackers, worms and viruses that brought about security awareness and change to the Internet. Availability of information, access to attack tools, and the advantages of highly-networked organizations have created precarious links between the vital underpinnings of society and the security test range of the web. Remote or geographically dispersed nodes present high-value targets to a technology aware foe whose tactics thrive on attacks that do not require extensive resources. The common solution of layering a typical network security infrastructure upon a control system (CS) does not address the different perceptions held by the IT staff and control engineers. This paper examines the various implementations of control systems and explains how integration of modern technology has introduced security flaws. Plausible uses of cyberspace for physical effects are theorized with attention paid to the cascading (second and third order) effects of critical infrastructure disruption. Discussion of process control specific hardware, vulnerabilities, and practices unveil potential risks unprotected by incorporating a standard network / host based security structure into a critical infrastructure control system.

Keywords: Critical infrastructure, control system security, SCADA, distributed control, Cyber operations, terrorism

Pattern Matching Information Flow using GADT

Eric Lindahl and Victor Winter

University of Nebraska at Omaha, NE, USA

Abstract: Integrating security policies into security assurance mechanisms to ensure end-to-end behavior is still a challenge. Information flow analysis and type checking are effective methods for the analysis and verification of secure communications and processing. Language-based information flow security models use programming-language for specifying and enforcing security policy. Dependently typed programming is an efficient and powerful way to concisely communicate, represent, and then reason over security policies. In this paper we demonstrate an integration of policy elements in a subset of a language-based information flow security model implemented using dependent type programming. We illustrate how recent advances in type theory in secure domains make available enabling technologies for developing policy aware secure computing.

Keywords: GADT, information flow, non-interference, static analysis, type systems, security policies

Static and Dynamic Packet Filtering on Lightly Managed Systems

James Lupo and Daniel Likarish
Regis University, Denver, CO, USA

Abstract: Regis University operates servers that must be open to external access for a variety of educational purposes. These servers were managed by student and faculty, hence the experience level was generally low, and the time available for expert oversight was limited. In May of 2006 unauthorized attempts to gain access were noted and steps were taken to reduce risk of system compromise. The attempts increased in sophistication and severity with time. The pattern of access attempts seemed to follow a training curriculum from simple to more complex based on our responses to the attempts. The need to understand the threat profile resulted in the design of a HoneyNet to capture attack characteristics. When large numbers of login attempts were noted involving extremely long lists of pseudo user names and well known system account names, the following defensive measures were implemented. Password strength requirements were increased, IPTables was set up to block entire Class A network ranges, pinholes were defined to allow trusted host access, throttling was defined to slow down probes, and monitoring via swatch was implemented to block attempts from unexpected sources. The dynamic blocking process uses TCPWrappers and the *hosts.deny* file to immediately block the source address of the suspected activity. The addresses were then manually reviewed to determine both the location and associated network ranges. Depending on the circumstances, the host address was left in the *hosts.deny* file, or it was removed and the entire associated network range was permanently blocked by an IPTables filtering rule. Since the system was implemented, intrusion attempts have dropped from several thousand per day to approximately 1 per week. And after a year of operation, no legitimate access has been blocked.

Keywords: intrusion detection protection filtering risk management

Organizing the United States Government for the Contemporary Environment

Steven Mains

US Combined Arms Center, Fort Leavenworth, KS USA

Abstract: The United States has ceded the informational aspects of the Global War on Terror through lack of a campaign plan and lack of organization to execute it. As a result our enemies are free to foster the perception of a dichotomy between the policies and ideals of the United States government to the detriment of the United States and its allies as well as their efforts to free people around the world. This paper outlines a plan for a strategic-level information campaign and proposes an interagency approach to support it led by a Deputy to the National Security Advisor for Strategic Communications and a Strategic Communications Task Force. The Deputy for Strategic Communications will incorporate Strategic Communications considerations into policy formulation at the highest level. As lead for a Strategic Communications Task Force made up of Undersecretary-level representatives from State, Defense, Education, Homeland Security, and US Agency for International Development (among others), he would be responsible for integration of Strategic Communications into policy execution. As communications with people is becoming much more important than communications with governments, Public Diplomacy will be strengthened through increased personnel and better training. A Corporation for Public Diplomacy will be established to conduct Public Diplomacy beyond Embassy efforts. A Public Diplomacy Institute will study Public Diplomacy methods and train practitioners. The US Information Agency will be revitalized and expanded to leverage all media including print, terrestrial and satellite television, radio and the Internet. A law similar to the 1986 Goldwater-Nichols act will make Public Diplomacy experience and training a requirement for advancement in the State and other Departments to senior supervisory positions. Public Affairs efforts will be expanded to make the government and its actions more transparent to the public of the United States and its allies. Public Diplomacy and Public Affairs practitioners will be assigned to all Department of Defense Combatant Commands and USAID missions. All Departments in the Government will be responsible to integrate information operations into all operations including military to military operations and training, counter-drug and law enforcement operations.

Keywords: Information warfare, organization, interagency cooperation, whole-of-government approach, strategic communications, national security council, information operations

Developing a Requirements Framework for Cybercraft Trust Evaluation

Todd McDonald and Shannon Hunt

Air Force Institute of Technology, Wright Patterson Air Force Base, OH, USA

Abstract: It should be no surprise that Department of Defense (DoD) and U.S. Air Force (USAF) networks are the target of constant attack. As a result, network defense remains a high priority for cyber warriors. On the technical side, trust issues for a comprehensive end-to-end network defense solution are abundant and involve multiple layers of complexity. The Air Force Research Labs (AFRL) is currently investigating feasibility for a holistic approach to network defense, called Cybercraft. We envision Cybercraft to be trusted computer entities that cooperate with other Cybercraft to provide autonomous and responsive network defense services. A top research goal related to Cybercraft centers around how we may examine and ultimately prove features related to this root of trust. In this work, we investigate use-case scenarios for Cybercraft operation with a view towards analyzing and expressing trust requirements inherent in the environment. Based on a limited subset of functional requirements for Cybercraft in terms of their role, we consider how current trust models may be used to answer various questions of trust between components. In this work we characterize generic model components that will help answer questions regarding Cybercraft trust and pose relevant comparison criteria as evaluation points for various (existing) trust models. Our contribution in this research provides a framework for comparing trust models that are applicable to similar network-based architectures.

Keywords: Network defense, trust, cybercraft, trust model, requirements, threat model, attack tree

Use of Evaluation Criteria in Security Education

Thuy Nguyen and Cynthia Irvine

Naval Postgraduate School, Monterey, CA, USA

Abstract: Success in information warfare will depend on resilient, reconstitutable cyber assets and the ability to assess and respond to attacks. A cornerstone of this success will be the ability of Information Assurance professionals to develop sound security requirements and determine the suitability of evaluated security products for mission-specific systems. Recognizing the pedagogical value of applying security evaluation criteria such as the Common Criteria (CC) to information security education, we recently introduced a graduate-level Computer Science course focusing on methodical security requirements engineering based on the CC. This course aims to provide students with an understanding of how security evaluation criteria can be used to specify system security objectives, derive security requirements from security objectives, establish life cycle and development processes, and provide an organizational framework for research and development. Although imperfect, the paradigmatic process of the CC provides a usable framework for in-depth study of various tasks relating to system requirements derivation and verification activities: system requirements elicitation, threat analysis, security objectives definition and security requirements expression. In-class discussions address fundamental security design principles and disciplines for information and software assurance (e.g., formal methods and life cycle management) as applied to security requirements derivation. Coverage of advanced CC topics includes high assurance evaluation, international and U.S. scheme interpretation processes, guidance for Protection Profile development, CC evaluation methodology, and composite evaluation. This paper describes the scope and design of a pilot course offering. Laboratory projects focus on the differences between security functional and assurance requirements, mock evaluation of a draft Protection Profile, examination of the interpretation process in the U.S. scheme, and development of a preliminary sketch of a Composed Assurance Package for a hypothetical composed target system that is suitable for use in operational environments requiring medium robustness. Lessons learned and planned refinements of course material and focus are also discussed.

Keywords: Security requirements engineering, security evaluation, security education, information assurance

Implementation of a Multilevel Wiki for Cross-Domain Collaboration

Kar Leong Ong, Thuy Nguyen and Cynthia Irvine
Naval Postgraduate School, Monterey, CA, USA

Abstract: The pace of modern warfare requires tools that support intensive, ongoing collaboration between participants. Wiki technology provides a hypertext content-based collaborative authoring and information sharing environment that includes the ability to create links to other web contents, relative stability, ease of use, and logging features for tracking contributions and modifications. Military environments impose a requirement to enforce national policies regarding authorized access to classified information while satisfying the intent of wikis to provide an open context for content sharing. The Global Information Grid (GIG) vision calls for a highly flexible multilevel environment. The Monterey Security Architecture (MYSEA) Test-bed provides a distributed high assurance multilevel networking environment where authenticated users securely access data and services at different classification levels. The MYSEA approach is to provide users with unmodified commercial-off-the-shelf office productivity tools while enforcing a multilevel security (MLS) policy with high assurance. The extensible Test-bed architecture is designed with strategically placed trusted components that comprise the distributed TCB, while untrusted commercial clients support the user interface.

We have extended the collaboration capabilities of MYSEA through the creation of a multilevel wiki. This wiki permits users who access the system at a particular sensitivity level to read and post information to the wiki at that level. Users at higher sensitivity levels may read wiki content at lower security levels and may post information at the higher security level. The underlying MLS policy enforcement mechanisms prevent low users from accessing higher sensitivity information. The multilevel wiki was created by porting a publicly available wiki engine to run on the high assurance system hosting the MYSEA server. A systematic process was used to select a wiki for the MYSEA environment. TWiki was chosen. To simplify identification of errors that might arise in the porting process, a three-stage porting methodology was used. Functional and security tests were performed to ensure that the wiki engine operates properly while being constrained by the underlying policy enforcement mechanisms of the server. An objective in designing the test plans was to ensure adequate test coverage, while avoiding a combinatoric explosion of test cases. Repeatable regression testing procedures were also produced. A conflict between the application-level DAC policy of the wiki and that of the MYSEA server was identified and resolved.

Keywords: Wiki, multilevel security, access controls, porting methodology

Formal Models of a Least Privilege Separation Kernel in Alloy

David Phelps, Mikhail Auguston and Timothy Levin
Naval Postgraduate School, Monterey, CA, USA

Abstract: We describe the specification of the formal security policy model and formal top-level specification for the Least Privilege Separation Kernel (LPSK) in Alloy, a relatively new modeling language and analysis tool. The state of the art for the formal verification of secure software requires representation of an abstract model, and one or more refinements (to the model), in a formal specification language. These specifications are then examined for self-consistency with their properties, as well as for consistency between levels of abstraction, all of which can be time consuming, and costly. Alloy provides a simple, intuitive logic framework, in contrast to many other formal languages that are intended to support general-purpose mathematics. In order to determine whether Alloy can improve the efficiency and effectiveness of the verification of secure computer systems, we used it to specify portions of the LPSK formal security policy model and formal top-level specification, and utilized the Alloy Analyzer to examine the consistency of the specifications. The security-critical system elements and predicates for security properties were defined in terms of a state model, and system operations were represented as state transitions. While Alloy does not support induction or proofs, it can be used to find counter examples in a small scope of state transitions. We conclude that Alloy has few limitations and is suitable, as measured by utility and ease of use, to include in the toolbox for rapid high-assurance system development. The primary concern with using Alloy for industrial, versus academic, security verification is the scalability of the Alloy Analyzer with respect to the state-space of the security model and formal top-level specification. For real system verification, Alloy must support a much larger scope. We found that the translation of an existing informal LPSK security policy model to Alloy provided insight for making the model clearer. It is also apparent that Alloy allows for the beginner to formal system verification to quickly climb its learning curve.

Keywords: Software verification; principles, least privilege; information flow controls, separation kernels; formal languages

Using Deception to Facilitate Intrusion Detection in Nuclear Power Plants

Julian Rushi^{1,2} and Roy Campbell¹

¹University of Illinois at Urbana-Champaign, Urbana, IL USA

²Università degli Studi di Milano, Via Comelico Milano, Italy

Abstract: In this paper we propose reactor mirage theory as a deception-based intrusion detection approach for digital I&C systems in nuclear power plants (NPPs). We draw from military deception techniques based on simulation of physical targets such as troops, radar-equipped air defense installations, tanks, bridges, airfields, etc. We propose the employment of genuine digital I&C systems to simulate physical components of a NPP via generation of Modbus protocol data units (PDUs) typical to the operation of these components. Communicating finite state machines are used to generate and recognize such deceptive PDUs. Artificially generated Modbus traffic is the reactor mirage theory counterpart of electromagnetic beam reflections, heat emitters, etc., commonly used as deceptive mechanisms by the military in warfare to indicate the existence of physical targets. These deceptive PDUs produce a drastic incrementation of the uncertainty which attackers may be subject to during the selection of target NPP components they plan to hit, hence increase by a high order of magnitude the probability of detection of attacks on NPP components.

Keywords: MILDEC, intrusion detection, digital I&C systems, nuclear power plants, signal detection theory, reactor mirage theory

Establishing the Human Firewall: Improving Resistance to Social Engineering Attacks

Jamison Scheeres, Robert Mills and Michael Grimaila

Air Force Institute of Technology, Wright-Patterson Air Force Base, OH,

Abstract: Hackers frequently use social engineering attacks to gain a foothold into a target network. This type of attack is a tremendous challenge to defend against, because the avenue of attack is through the human users and not through technology. Thus far, methods for dealing with this threat have included establishing better security policies and educating users on the threat that exists. Existing techniques simply are not working effectively as evidenced by the fact that auditing agencies consider it a given that they will be able to gain access via social engineering. This paper provides new insight into how organizations can improve their security posture by bolstering individual users' resistance to social engineering attacks. This is achieved by first establishing a connection between social engineering attacks and what social psychologists call "illegitimate persuasion". A content analysis is performed to show that social engineering and illegitimate persuasion target the same common psychological triggers. The paper then discusses how specific techniques shown to be effective in increasing an individual's resistance to illegitimate persuasion can be leveraged in the fight against social engineering. The paper concludes recommendations on implementing some of the techniques described.

Keywords: Social engineering; information warfare and security education

An Architecture for Cyber Incident Mission Impact Assessment (CIMIA)

David Sorrels¹, Michael Grimaila¹, Larry Fortson², and Robert Mills¹

¹Air Force Institute of Technology, Wright-Patterson Air Force Base, OH, USA

²Air Force Research Laboratory, Wright-Patterson Air Force Base, OH, USA

Abstract: Information is a critical asset to modern organizations, but especially so for the military which uses information to conduct all aspects of modern military operations. Information is collected, processed, analyzed, distributed, and aggregated to support situational awareness, operations planning, intelligence, and command decision making. When a cyber incident occurs which may compromise the confidentiality, integrity, and/or availability of a critical information asset, all decision makers who are dependent on the information must be immediately made aware of the potential impact of the incident. Previous research identified this need and proposed a conceptual framework to facilitate near real-time Defensive Cyber Damage Assessment following a cyber incident. We are continuing this research by developing an operational process to facilitate Cyber Incident Mission Impact Assessment (CIMIA).

In this paper, we propose an information architecture that operationalizes the CIMIA process. The proposed architecture is scalable, takes advantage of existing information infrastructure resources, and provides the building blocks necessary for mission impact assessment. This work will validate the previous research and is designed to meet the Department of Defense and United States Air Force guidance which requires detailed mission impact reporting. The proposed architecture utilizes current applications and resources augmented with end user input in order to automate a process that will be able to observe the network (processes and information flows between information sources and sinks), provide the ability to document information dependencies and their value, and enable the near real time notification of downstream information consumers when a cyber incident occurs.

Keywords: Situational awareness, cyber damage assessment, mission impact assessment, information architecture

Tailored Information Delivery Services for Open Source Intelligence

William Sousan, Ryan Nickell, Qiuming Zhu and Pete Hospodka
University of Nebraska at Omaha, NE, USA

Abstract: Open Source Intelligence (OSINT) consists of locating, harvesting, and analyzing information provided by, or available from, various public sources such as news media data, public records, academic publications, and other data sources for intelligence gathering purposes. With the advent of the internet, a plethora of unclassified freely accessible information exists across the world that provides many sources of possible intelligence value. Simultaneously this vast ocean of information creates a challenge to information systems in extracting and getting desired information from these sources. As a result, users and software systems are often overloaded with unrelated information while collecting data for open source intelligence operations. To assist in OSINT operations, we are developing a TIDS (Tailored Information Delivery Services) system to provide user selected information and reduce the amount of irrelevant information. Our TIDS system is based on semantic matching of concepts selected by users that are compared against the open source data tagged by using the same concepts. These concepts are part of a shared common ontology that can be extended through a collaborative effort of all users. As users discover new ontological instances, or concepts, they are added in an incremental process to the shared ontology, thus building a domain specific knowledge base for an OSINT operation. Furthermore, we leverage the benefits of existing upper-level ontologies for jump-starting the system. The TIDS system also provides a framework for research purposes in investigating how to best develop the components of an ontology-based information system such as semantic annotation, structure and creation of ontologies, and semantic information retrieval for the OSINT domain. The objective of our research is to create a semantics-based information delivery system that functions in a “What You Get Is What You Need (WYGIWYNTM)” fashion. Through the use of semantics matching, improved information relevancy can be achieved that supports military commanders and analysts with accurate information in their operational interests.

Keywords: Information overload, information retrieval, open source intelligence, ontology, semantic annotation, ontological indexing

Legal Aspects of Warfare in Cyberspace

Dennis Strouble and Michael Grimaila

**Air Force Institute of Technology, Wright Patterson Air Force Base, OH
USA**

Abstract: While the Department of Defense (DoD) has well defined rules of engagement and laws of war in the traditional physical domains (e.g., land, sea, air, and space); those in cyberspace are not as well defined or understood. In December 2005, the United States Air Force changed its mission statement to add a new domain, "Cyberspace," to its traditional operational domains. This change is significant and has resulted in the need for a detailed examination of the legal implications of warfare in this domain. For example, in the physical domains combatants wear uniforms for identification; vehicles with a Red Cross are off limits; and moving over the land, airspace, or territorial waters of neutral countries is forbidden. In contrast, in the cyberspace domain many entities are invisible; an Internet address can be accessed from any other Internet node; and both malicious and non-malicious traffic co-mingle on a common communications infrastructure. While attacks perpetrated in the physical world can often be attributed to specific entities based upon evidence and intelligence collected in the physical domain, the attribution of attacks to an entity in the cyber domain is much more difficult and complex. A cyber attack launched over the Internet could take multiple routes; use terrestrial, underwater, and satellite communication links; and travel through the information infrastructure of many different nations, including friendly, combatants and neutral states. The investigation and attribution of a cyber attack can be very difficult, requiring extensive time and resources. Even when the network source of the attack is positively identified, it does not mean that the system owner was complicit (or even aware) of the attack. In fact, systems are more frequently compromised by an adversary unknowingly and used as their "agent" to perpetrate attacks at a future time (e.g., as a bot in a larger botnet). Cyber attack investigations require the collection and integration of information from multiple communities (e.g., commercial, intelligence, and military) which introduces significant legal constraints. If an adversary is positively identified, the issue of proportionality of response and concerns about the potential for collateral damage must also be considered (ideally) before the need for a timely response. In this paper, we identify difficulties in the application of existing laws of warfare when conducting operations in the cyber domain; examine new legal issues that arise from warfare in cyberspace; and offer recommendations on changes that can be made in policy and law to reduce ambiguity in the rules of engagement and laws of warfare in cyberspace.

Keywords: Cyber warfare law, attribution, proportionality

Voice Based Authentication Using the Null Frequencies

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

Abstract: The human voice has many features that have been used for centuries for authenticating others. That was/is the case when someone calls for one other, but that is even more relevant when the communication is made at distance, like when using the phone. These facts served as inspiration for software designers that started to investigate how the voice can be used in an automatic way to provide or deny access to valuable places, physical or logical. The range of frequencies covered by the human voice is well known, although it is not the same for each person, and this data has been used to feed the several algorithms that have been developed in the past years. What we now have found is that one person, for each sentence, has some not used frequencies. In this paper we will present some studies that indicate that those unused frequencies alone can be used to authenticate and even to recognize the users.

Keywords: Authentication, voice patterns, security, biometrics

Towards Faster Execution of the OODA Loop Using Dynamic Decision Support

Shyni Thomas, Nitin Dhiman, Pankaj Tikkas, Ajay Sharma, Dipti Deodhare

Centre for Artificial Intelligence and Robotics (CAIR), Bangalore, India

Abstract: The OODA loop is a common framework in which military decision making is discussed and is an abstraction of the sequence of events that must take place in any military engagement. Of the four components of the OODA loop, the first three involve processing of information, comprising information gathering, information distribution, information analysis, information understanding and deciding how to act upon this information. To achieve higher operational tempo, all components of the OODA loop need to be accelerated. While speed-ups in information gathering and distribution can be attained by well implemented networking, information analysis, understanding and decision making can prove to be severe bottlenecks to the operational tempo. In this context, we discuss the importance of Decision Support Systems (DSS) that dynamically respond to changing scenarios. DSSs developed using Semantic Web techniques and conventional AI-based search mechanisms like A* have the potential to respond to evolving situations providing autonomous capabilities to military applications. This can contribute towards swifter execution of the OODA loop with little human intervention. This paper, discusses in detail, the design and implementation of a DSS for a prototypical problem of convoy scheduling. Convoy Scheduling is a common military operation involving planning a convoy move from one location to another. The problem domain of convoy scheduling has many complexities and various constraints to be satisfied. Several realistically defined scheduling constraints have been incorporated, including permissible convoy speed, movement time, availability of road *etc.*, to name a few. Thus Convoy Scheduling DSS in itself proves to be a self sufficient example to demonstrate the purpose of this paper. Further, the use of ontologies in representing information pertaining to military and geographical domains is demonstrated. The use of A*, a tree-based search algorithm, for optimal clash-free convoy scheduling has also been highlighted. Finally, a framework for a system incorporating this Convoy Scheduling DSS to respond dynamically to various events that may affect scheduled convoy plan is proposed. The responses may include diverting a convoy, inducing forced wait *etc.* depending on the trade-offs and overall implications

Keywords: OODA, dynamic DSS, demantic web, ontologies, A*

Creating Hardware-based Primitives to Enhance Digital Forensics in a Novel Computing Architecture

Al-Nath Tuting and Paul Williams

Air Force Institute of Technology, Wright-Patterson Air Force Base, OH, USA

Abstract: Adding hardware primitives to observe and preserve digital events and states of a computer will enhance the development of usable knowledge in digital forensic investigations. This will allow for trusted indirect observations of a computer's internal states producing evidence that will satisfy the evidence purists and the court system. Typically, traditional digital forensic techniques have focused on disk drives and other non-volatile data sources. Pulling the plug on a live system has been the long-established way to preserve digital evidence; however, this has the side effect of erasing volatile memory. Acquiring system memory and other volatile data leading up to an incident in a trusted fashion and independent of software running on the system can provide a great deal of relevant information about the system's state before, during and after an incident. This paper explores forensic hardware primitives via a socket-compatible field programmable gate array (FGPA) for motherboard processor sockets. This provides us the opportunity to develop practical means by which we can acquire volatile main memory as well as collect other volatile data independent of the operating system or other potentially compromised code.

Keywords: Volatile memory acquisition; digital evidence; digital investigation; incident response; computer forensics

Using Markov Models to Crack Passwords

Renier van Heerden and Johannes Vorster
DPSS, CSIR, Pretoria, South Africa

Abstract: We present a Markov Model for cracking and measuring quality of passwords. The Markov Model represents the transitions between specific characters. The Markov Model was built from a list of captured passwords, thus generating a password model with the frequency of passwords also incorporated. Traditional password quality measurement tests only against large dictionaries. We found that through the Markov Model character transition map we can optimise the search sequence for partially known passwords.

Keywords: Markov model, password cracking

Designing and Implementing a Critical Infrastructure Lab for Educational Research

Dorsey Wilkin, Michael Kolbe, Richard Raines, Paul Williams and Kenneth Hopkinson

Air Force Institute of Technology, Wright-Patterson Air Force Base, OH, USA

Abstract: Most educational institutions do not have access to critical infrastructure facilities or equipment to conduct information security research. Therefore, they often must build a lab to emulate the particular critical infrastructure sector of interest. This paper outlines the design and implementation used by the Air Force Institute of Technology to build a modular lab capable of being used by future students for any area of industrial control system research. Designed to imitate real life, the solution was developed using an integrated systems engineering design approach. The logical architecture, the network architecture, the low-level physical devices, to include equipment and software, were all chosen for their wide use within industry.

Keywords: SCADA systems, Computer network security, Educational research, Critical Infrastructure, Lab design

Common Errors in Incident Response

Michael Staggs

FireEye, Inc. Menlo Park, CA

Abstract: Computer Security Incident Response is a task that is most often implemented by personnel that have not been formally trained in this discipline acting under the extreme pressure of the moment. It is the intent of this paper to provide a set of guidelines and suggestions that the user may follow when under the pressure of an incident. Topics in incident definition, forensic rigor, sample data artifacts, tools and final presentations will be covered.

Keywords: Forensics, incident, computer, network, findings, legal