

**Proceedings
of the
6th International
Conference on Information
Warfare and Security**

**The George Washington University
Washington, DC, USA**

17-18 March 2011

Edited by
Leigh Armistead
Edith Cowan University
Programme Chair

Copyright The Authors, 2011. 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.

These Conference Proceedings have been submitted to Thomson ISI for indexing.

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

ISBN:97-1-906638-93-1 CD

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

Contents

Paper Title	Author(s)	Guide Page	Page No.
Preface		vi	v
Biographies of Conference Chairs, Programme Chair, Keynote Speaker and Mini-track Chairs		vi	iv
Biographies of contributing authors		vii	v
Using the Longest Common Substring on Dynamic Traces of Malware to Automatically Identify Common Behaviors	<i>Jaime Acosta</i>	1	1
Modeling and Justification of the Store and Forward Protocol: Covert Channel Analysis	<i>Hind Al Falasi and Liren Zhang</i>	2	8
The Evolution of Information Assurance (IA) and Information Operations (IO) Contracts across the DoD: Growth Opportunities for Academic Research – an Update	<i>Edwin Leigh Armistead and Thomas Murphy</i>	3	14
The Uses and Limits of Game Theory in Conceptualizing Cyberwarfare	<i>Merritt Baer</i>	4	23
Who Needs a Botnet if you Have Google?	<i>Ivan Burke and Renier van Heerden</i>	4	32
Mission Resilience in Cloud Computing: A Biologically Inspired Approach	<i>Marco Carvalho, Dipankar Dasgupta, Michael Grimaila and Carlos Perez</i>	5	42
Link Analysis and Link Visualization of Malicious Websites	<i>Manoj Cherukuri and Srinivas Mukkamala</i>	6	52

Paper Title	Author(s)	Guide Page	Page No.
The Strategies for Critical Cyber Infrastructure (CCI) Protection by Enhancing Software Assurance	<i>Mecealus Cronkrite, John Szydluk and Joon Park</i>	6	68
Building an Improved Taxonomy for IA Education Resources in PRISM	<i>Vincent Garramone, Daniel Likarish</i>	7	76
Using Dynamic Addressing for a Moving Target Defense	<i>Stephen Groat, Matthew Dunlop, Randy Marchany and Joseph Tront</i>	8	84
Changing the Face of Cyber Warfare with International Cyber Defense Collaboration	<i>Marthie Grobler, Joey Jansen van Vuuren and Jannie Zaaiman,</i>	8	92
Cyber Strategy and the Law of Armed Conflict	<i>Ulf Haeussler</i>	9	99
eGovernance and Strategic Information Warfare – non Military Approach	<i>Karim Hamza and Van Dalen</i>	9	106
Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains	<i>Eric Hutchins, Michael Cloppert and Rohan Amin</i>	10	113
The Hidden Grand Narrative of Western Military Policy: A Linguistic Analysis of American Strategic Communication	<i>Saara Jantunen and Aki-Mauri Huhtinen</i>	11	126
Host-Based Data Exfiltration Detection via System Call Sequences	<i>Brian Jewell and Justin Beaver</i>	12	134
Detection of YASS Using Calibration by Motion Estimation	<i>Kesav Kancherla and Srinivas Mukkamala</i>	12	143
Developing a Knowledge System for Information Operations	<i>Louise Leenen, Ronell Alberts, Katarina Britz, Aurna Gerber and Thomas Meyer</i>	13	151

Paper Title	Author(s)	Guide Page	Page No.
CAESMA – An On-Going Proposal of a Network Forensic Model for VoIP traffic	<i>Jose Mas y Rubi, Christian Del Carpio, Javier Espinoza, and Oscar Nuñez Mori</i>	14	160
Secure Proactive Recovery – a Hardware Based Mission Assurance Scheme	<i>Ruchika Mehresh, Shambhu Upadhyaya and Kevin Kwiat</i>	14	171
Identifying Cyber Espionage: Towards a Synthesis Approach	<i>David Merritt and Barry Mullins</i>	15	180
Security Analysis of Webservers of Prominent Organizations in Pakistan	<i>Muhammad Naveed</i>	16	188
International Legal Issues and Approaches Regarding Information Warfare	<i>Alexandru Nitu</i>	16	200
Cyberwarfare and Anonymity	<i>Christopher Perr</i>	17	207
Catch Me If You Can: Cyber Anonymity	<i>David Rohret and Michael Kraft</i>	18	213
Neutrality in the Context of Cyberwar	<i>Julie Ryan and Daniel Ryan</i>	19	221
Labelling: Security in Information Management and Sharing	<i>Harm Schotanus, Tim Hartog, Hiddo Hut and Daniel Boonstra</i>	19	228
Information Management Security for Inter-Organisational Business Processes, Services and Collaboration	<i>Maria Th. Semmelrock-Picej, Alfred Possegger and Andreas Stopper</i>	20	238
Anatomy of Banking Trojans – Zeus Crimeware (how Similar are its Variants)	<i>Madhu Shankarapani and Srinivas Mukkamala</i>	21	252

Paper Title	Author(s)	Guide Page	Page No.
Terrorist use of the Internet: Exploitation and Support Through ICT Infrastructure	<i>Namosha Veerasamy and Marthie Grobler</i>	22	260
Evolving an Information Security Curriculum: New Content, Innovative Pedagogy and Flexible Delivery Formats	<i>Tanya Zlateva, Virginia Greiman, Lou Chitkushev and Kip Becker</i>	23	268
PhD Research Papers			
Towards Persistent Control over Shared Information in a Collaborative Environment	<i>Shada Alsalamah, Alex Gray and Jeremy Hilton</i>	27	279
3D Execution Monitor (3D-EM): Using 3D Circuits to Detect Hardware Malicious Inclusions in General Purpose Processors	<i>Michael Bilzor</i>	28	289
Towards An Intelligent Software Agent System As Defense Against Botnets	<i>Evan Dembskey and Elmarie Biermann</i>	29	299
Theoretical Offensive Cyber Militia Models	<i>Rain Ottis</i>	30	308
Work in Progress			
Large-scale analysis of continuous data in cyber-warfare threat detection	<i>William Acosta</i>	33	317
A System and Method for Designing Secure Client-Server Communication Protocols Based on Certificateless PKI	<i>Natarajan Vijayarangan</i>	34	320

Preface

These Proceedings are the work of researchers contributing to the 6th International Conference on Information Warfare and Security (ICIW 2011), hosted this year by the George Washington University, Washington DC, USA. The Conference Chair is Dr. Julie Ryan from the George Washington University, Washington, DC, USA and I am again the Programme Chair.

The opening keynote address this year is given by Matthew A. Stern, General Dynamics Advanced Information Systems, USA. The second day will be opened by Mathew “Pete” Peterson from the Naval Criminal Investigative Service, USA.

An important benefit of attending this conference is the ability to share ideas and meet the people who hold them. The range of papers will ensure an interesting and enlightened discussion over the 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 97 abstracts, after the double blind, peer review process there are 38 papers published in these Conference Proceedings, including contributions from Austria, Bangladesh, Estonia, Finland, India, Iran, Pakistan, Peru, Romania, South Africa, the Netherlands, United Arab Emirates, United Kingdom and the United States.

I wish you a most enjoyable conference.

March 2011
Leigh Armistead
Edith Cowan University
Programme Chair

Biographies of Conference Chairs, Programme Chairs and Keynote Speakers

Conference Chairs



Dr. Julie Ryan currently teaches and directs research in Information Assurance at The George Washington University. Prior to joining academia, she worked in various positions in industry and government. Her degrees are from the US Air Force Academy, Eastern Michigan University, and The George Washington University.

Programme Chairs

Dr Edwin “Leigh” Armistead is the Director of Business Development for Goldbelt Hawk LLC, the Programme Chair for the International Conference of Information Warfare and an Adjunct Lecturer for Edith Cowen University in Perth, Australia. He has written nine books, 18 journal articles, presented 17 academic papers and served as a Chairman for 16 professional and academic conferences. Formerly a Master Faculty at the Joint Forces Staff College, Leigh received his PhD from Edith Cowen University with an emphasis on Information Operations. He also serves as a Co-Editor for the *Journal of International Warfare*, and the Editorial Review Board for European Conference on Information Warfare.



Keynote Speakers



Mathew “Pete” Peterson has served in a variety of positions within US government agencies since 1989, to include 13 years on active duty in the U.S. Army. He has experience in a wide range of domains, including information assurance/information protection, research, development & acquisition (RDA)/research & technology protection (RTP), cyber analysis issues, critical infrastructure protection, and threat analysis. He currently serves as Cyber Analysis Division Chief within the Naval Criminal Investigative Service, while working towards completion of his dissertation in the Executive Leadership Doctoral Program at George Washington University’s Virginia Campus.

Matthew Stern is the director of cyber accounts for General Dynamics Advanced Information Systems. He also provides subject matter expertise in

cyber space operations to the company and its customers. Stern also represents the company on several boards and advisory groups providing thought leadership to the cyber security community. He spent 22 years in positions of increasing responsibility in the U.S. Army culminating with command of 2nd Battalion, 1st Information Operations Command and the Army Computer Emergency Response Team (ACERT). This is the first unit in U.S. Army history dedicated to cyberspace operations. Stern is an established expert on information technology, network security, information operations and special information operations. He is also a recognized visionary regarding the military conduct of cyberspace operations. He has developed his knowledge and expertise through practical experience leading his command, the U.S. military data communication services in Iraq, support to the technical architecture of the U.S. Army's digitized Armored Corps, and the systems integration for the Land Information Warfare Activity Information Dominance Center. Stern is also a decorated combat veteran of Operations DESERT SHIELD /STORM and IRAQI FREEDOM. Matt holds a Masters degree in Information Systems and Computer Resource Management from Webster University and a Bachelor's of Science degree in Political Science from Northern Illinois University.

Biographies of contributing authors (in alphabetical order)

Jaime Acosta completed his Ph.D. in Computer Science at the University of Texas at El Paso. Dr. Acosta's research has received awards and recognition including the outstanding dissertation award by the University of Texas at El Paso. Jaime is currently working at the United States Army Research Laboratory conducting security research.

William Acosta, Ph.D. received his Ph.D. from the University of Notre Dame in 2008 and is currently an assistant professor at the University of Toledo teaching in the Computer Science and Engineering Technology Program. His prior work included peer-to-peer search and distributed systems. He is currently working on experimental data systems research focusing on large-scale data analysis.

Hind Al Falasi, is currently pursuing a PhD in Information Security at the United Arab Emirates University, Al Ain, UAE. He received a Bachelors of Science in Information Security from the United Arab Emirates University. Where the main focus is Security of Vehicular Ad hoc Networks.

Rohan Amin is a member of Lockheed Martin's CIRT, who helped grow the team from 5 charter members with limited responsibilities to an industry-leading entity with global scope. His contributions to the team have ranged from deeply technical to broadly organizational.

Shada Al-Salamah is a doctoral candidate at the Department of Computer Science & Informatics, Cardiff University, UK. She received her MSc in Strategic Information Systems with Information Assurance from Cardiff University and received a BSc in Information Technology from the College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia.

Merritt Baer is a graduate of Harvard Law School and Harvard College. She has conducted clinical cyberlaw research at Harvard's Berkman Center for Internet and Society and has published a number of pieces at the intersection of cybercrime, Constitutional Internet issues and national security. She currently serves as a judicial clerk at the United States Court of Appeals for the Armed Forces.

Michael Bilzor is a PhD student at the Naval Postgraduate School. He has a B.S. in Computer Science from the U.S. Naval Academy and an M.S. in Computer Science from Johns Hopkins University. He served in F-14 and F/A-18 squadrons as a Naval Flight Officer until 2005. His research interest is in hardware security.

Ivan Burke is a Msc student in the department of Computer Science at the University of Pretoria, South Africa. He also works full time at the Council of Scientific and Industrial Research South Africa in the department of Defense Peace Safety and Security, where he works within the Command, Control and Information Warfare research group.

Marco Carvalho is a research Scientist at Florida Institute for Human and Machine Cognition (IHMC). He received his Ph.D. from Tulane University, New Orleans, following a M.Sc. in Computer Science from University of West Florida, a M.Sc. in Mechanical Engineering from Federal University of Brasilia (UnB), and a B.Sc. in Mechanical Engineering, also from UnB. His research interests are primarily in the areas of biologically inspired security and tactical networks.

Mecealus Cronkrite is studying for a M.S in Information & Security Management at Syracuse University, School of Information Studies, He is a DHS Career Development Grant fellow, Graduate Engineering Minority (GEM) fellow. He gained a B.S degree in 2009 in Computer Science, from the State University at Brockport NY. He has spent 7 years in industry in systems integration programming and analysis, and IT disaster management roles.

Mike Cloppert is a member of Lockheed Martin's CIRT, who helped grow the team from 5 charter members with limited responsibilities to an industry-leading entity with global scope. His contributions to the team have ranged from deeply technical to broadly organizational.

Evan Dembskey is a senior lecturer at UNISA in Pretoria, South Africa. He currently lectures in the area of computer security. His research interests include IW and technology and science in Ancient Greece and Rome.

Javier Espinoza was born in Lima, Peru, on August, 1971. He studied Electronic Engineering in Pontificia Universidad Catolica del Peru. He studied specialization in Cisco Certified Network Associate (CCNA), in Structured Wiring and Information System Security. Javier is studying a Telecommunications Engineering master at Pontificia Universidad Catolica del Peru in Lima, Peru

Stephen Groat is a PhD student at Virginia Tech in the Bradley Department of Electrical and Computer Engineering focusing on network security and IPv6. Working in coordination with the Information Technology Security Office and Lab, Stephen is researching the security implications of IPv6.

Ulf Haeussler is a Legal Advisor in the German Armed Forces and currently seconded to HQ SACT. Prior to this assignment, Ulf served in multiple German Armed Forces positions as well as at NATO HQ, and was deployed to NATO operations as a reservist on active duty. Ulf is widely published on international law.

Karim Hamza works as an Academic Researcher at the Maastricht school of Management (Netherlands), Part Time Professor at the American University (Egypt) and Approved Tutor for Edinburgh Business School (UK). Additionally, he works as a Business Development Manager in one of the leading information technology companies specialized in Enterprise Resource Planning applications for governments and private sectors.

Tim Hartog graduated in 2005 at the Technical University of Twente, in the Netherlands. Since then he has been active in the field of Information Security. During his work at TNO, the Dutch Organization for Applied Scientific Research, Tim has been working in the areas of Trusted Computing, Trusted Operating Systems and Cross Domain Solutions.

Saara Jantunen studies leadership as a doctoral student in the Finnish Defence University. She has studied English language and culture at the University of Groningen in the Netherlands and English philology in the University of Helsinki, Finland. Her research interests include language & identity and military discourse. Jantunen currently works in education.

Brian Jewell is a graduate student with an emphasis on Information Security at Tennessee Technological University. He received his B.S. in Computer Science from Murray State University. During summer 2010 he interned at Oak Ridge National Laboratory in the Applied Software Engineering

Research group. His research is in the area of host intrusion detection and response.

Louise Leenen is a Senior Researcher at the South African Council for Scientific and Industrial Research in the Defence, Peace, Safety and Security (DPSS) unit which focuses on defence related research and development. She holds a PhD in Computer Science from the University of Wollongong in Australia.

Dan Likarish is a Director of the Center on Information Assurance Studies and faculty at Regis University School of Information and Computer Science. For many years he has been the advisor for undergraduate and graduate students with an interest in IS and IT problems. His research interests are in rapid curriculum development and deployment in conjunction with virtual worlds.

Jose Luis Mas y Rubi studied Systems Engineering at the Instituto Universitario Politecnico Santiago Mariño in Barcelona, Venezuela. He has a Cisco CCNA certification in networking. He is currently studying for a Telecommunications Engineering Master degree at Pontificia Universidad Catolica del Peru in Lima, Peru.

Ruchika Mehresh is a doctoral student of Computer Science and Engineering at the State University of New York at Buffalo. Her research focuses on reliability and security in fault-tolerant computing. She has worked on research projects funded by U.S. Air Force Research Laboratory

David Merritt received his B.S. in computer engineering from the U.S. Air Force Academy. He is an Undergraduate Network Warfare Training graduate, holds CISSP and GSEC certifications, and spent 3 years on the Air Force Computer Emergency Response Team. David is an active duty officer attending the Air Force Institute of Technology in Ohio.

Srinivas Mukkamala is a senior research scientist with ICASA (Institute for Complex Additive Systems Analysis), Adjunct Faculty of Computer Science Department of New Mexico Tech, advisor Cyber Security Works, and co-founder/managing partner of CAaNES LLC. He received his Ph.D. from New Mexico Tech in 2005. He is a frequent speaker on information assurance in conferences and tutorials across the world.

Muhammad Naveed completed B.Sc degree in Electrical Engineering (with majors in communication), University of Engineering and Technology (UET), Peshawar, Pakistan 2010. Currently a lecturer at Department of Computer Science, IQRA University, Peshawar, Pakistan. Research interests include information security and cryptography.

Alexandru Nitu is a legal counselor at the Romanian Intelligence Service, with nine years of experience in matters regarding human rights protection. He is involved in legal studies referring to the impact of the intelligence activities on respecting citizens' fundamental rights and liberties.

Rain Ottis is a scientist at the Cooperative Cyber Defence Centre of Excellence. He is a graduate of the United States Military Academy and Tallinn University of Technology (MSc, Informatics). He continues his studies at a PhD program in Tallinn University of Technology, where he focuses on politically motivated cyber attack campaigns by non-state actors.

Christopher Perr is currently a PhD candidate at Auburn University studying computer and network security. He holds a B.S. in Computer Science from the Air Force Academy and a Masters of Software Engineering from Auburn University.

David Rohret, CSC, Inc. Joint Information Operations Warfare Center (JIOWC). For over fifteen years he has pursued network security interests to include developing and vetting exploits for use on established red teams and adversarial research. He holds degrees in Computer Science from the University of Iowa and La Salle University.

Shambhu Upadhyaya is Professor of Computer Science and Engineering at the State University of New York at Buffalo. His research interests are computer security, information assurance, fault-tolerant computing, distributed systems and reliability. His research has been funded by federal agencies such as National Science Foundation, U.S. Air Force Research Laboratory, DARPA, National Security Agency and industries such as IBM, Intel, Cisco and Harris Corporation.

Namosha Veerasamy obtained a BSc:IT Computer Science Degree, and both a BSc: Computer Science (Honours Degree) and MSc: Computer Science with distinction from the University of Pretoria. She is currently employed as a researcher at the Council for Scientific and Industrial Research (CSIR) in Pretoria. Namosha is also qualified as a Certified Information System Security Professional (CISSP).

Natarajan Vijayarangan is a senior scientist in TCS. He obtained his Ph.D in Mathematics in 2001 from RIASM, University of Madras. He received 'Best Research Paper Award' of Ramanujan Mathematical Society in 2000. He has published patents, papers and books in the field of Information Security. He has participated in NIST SHA-3 competition and received 'AIP Anchor Award'.

Jannie Zaaiman (B Comm, B Proc, HBA, MBA, PhD) is Deputy Vice Chancellor: Operations at the University of Venda, and is the former Executive Dean, Faculty of Information and Communication Technology at the Tshwane University of Technology (TUT). Before joining TUT, Jannie was Group Company Secretary of Sasol, Managing Executive: Outsourcing and Divestitures at Telkom and Group Manager at Development Bank of Southern Africa.

Tanya Zlateva completed her doctorate at the Dresden University of Technology, Germany, and postdoctoral training at the Harvard-MIT Division for Health Sciences and Technology. Her research interests include application level security, biometrics, and new educational technologies. She currently serves as director of Boston University's Center for Reliable Information Systems and Cyber Security

Using the Longest Common Substring on Dynamic Traces of Malware to Automatically Identify Common Behaviors

Jaime Acosta

Army Research Laboratory, White Sands, NM, USA

Abstract: A large amount of research is focused on identifying malware. Once identified, the behavior of the malware must be analyzed to determine its effects on a system. This can be done by tracing through a malware binary using a disassembler or logging its dynamic behavior using a sandbox (virtual machines that execute a binary and log all dynamic events such as network, registry, and file manipulations). However, even with these tools, analyzing malware behavior is very time consuming for an analyst. In order to alleviate this, recent work has identified methods to categorize malware into “clusters” or types based on common dynamic behavior. This allows a human analyst to look at only a fraction of malware instances—those most dissimilar. Still missing are techniques that identify similar behaviors among malware of different types. Also missing is a way to automatically identify differences among same-type malware instances to determine whether the differences are benign or are the key malicious behavior. The research presented here shows that a wide collection of malware instances have common dynamic behavior regardless of their type. This is a first step toward enabling an analyst to more efficiently identify malware instances’ effects on systems by reducing the need for redundant analysis and allowing filtration of common benign behavior. This research uses the publicly available Reference Data Set that was collected over a period of three years. Malware instances were identified and assigned a type by six anti-malware scanners. The dataset consists of dynamic trace events of 3131 malware instances generated by CWSandbox. For this research, the dataset is separated into two sets: small and large. The small set contains 2071 instances of malware that are less than 100 KB in size. The large set contains 1060 instances of malware that are between 100 KB and 3.4 MB in size. In order to measure the common behavior between the small and large sets, common sequential event sequences within each malware instance in the small set are identified using a modified version of the longest common substring algorithm. Once identified, all appearances of these common event sequences are removed from the large set to determine shared behavior. Most common sequences are between length 2 and 60 events. Results indicate that when using length 2 event sequences and higher, on average, the large set instances share 96% of event sequences, with length 6 and higher event sequences—66%, and with length 12 and higher event sequences—50%. This indicates that an analyst’s workload can be largely reduced by removing common behavior sequences. Furthermore, it shows that malware instances may not always fall into exclusive categories. It may be more beneficial to instead identify behaviors and map them to malware instances, for example, as with the

Malware Attribute Enumeration and Characterization (MAEC). Future efforts may look into attaching semantic labels on long sequences that are common to many malware instances in order to aid the analyst further.

Keywords: Malware, similarity, dynamic, analysis, substring

Modeling and Justification of the Store and Forward Protocol: Covert Channel Analysis

Hind Al Falasi and Liren Zhang

United Arab Emirates University, Al Ain, United Arab Emirates

Abstract: In an environment where two networks with different security levels are allowed to communicate, a covert channel is created. The paper aims at calculating the probability of establishing a covert channel between the high security network and the low security network using Markov Chain Model. The communication between the networks follows the Bell-LaPadula (BLP) security model. The BLP model is a “No read up, No write down” model where *up* indicates an entity with a high security level and *down* indicates an entity with a low security level. In networking, the only way to enforce the BLP model is to divide a network into separate entities, networks with a low security level, and others with a high security level. This paper discusses our analysis of the Store and Forward Protocol that enforces the BLP security model. The Store and Forward Protocol (SAFP) is a gateway that forwards all data from a low security network to a high security network, and it sends acknowledgments to the low security network as if they were sent from the high security network; thereby achieving reliability of the communication in this secure environment. A timing covert channel can be established between the two networks by using the times of the acknowledgments to signal a message from the high security network to the low security network. A high security network may send acknowledgments immediately or with some delay where the time of the acknowledgments arrival is used to convey the message. The covert channel probability is found to be equal to the blocking probability of the SAFP buffer when analyzing the problem using Markov Chain Model. Increasing the size of the buffer at the SAFP decreases the covert channel probability. Carefully determining the size of the buffer of the SAFP ensures minimizing the covert channel probability.

Keywords: Covert channel, access model, Markov Chain Model, store and forward protocol

The Evolution of Information Assurance (IA) and Information Operations (IO) Contracts across the DoD: Growth Opportunities for Academic Research – an Update

Edwin Leigh Armistead¹ and Thomas Murphy²

¹Goldbelt Hawk LLC and Norwich University, USA

²NorthLight Technologies, USA

Abstract: Four years ago, the authors presented a paper at the ICIW conference in Monterey, CA (Armistead & Murphy, 2007) that outlined opportunities for academics and researchers with regard to IO (Information Operations), IW (Information Warfare) and IA (Information Assurance) contracts across the Department of Defense (DoD) and Federal government (USG). The original paper highlighted a differential in contracts available and the current opportunities were at that time. Specifically, that paper predicted what the future may hold for further growth in these areas and how growth of IO, IA and IW contract vehicles can benefit universities and academics from a funding aspect. Finally, the original paper also suggested future areas of research that academics may be interested in exploring, to best optimize their ability to secure grants and contracts over the next few years. This paper is not only an update to the original research, to review the original hypothesis and determine if the predictions from four years ago were correct, but it also mines new data sources to take a fresh look at current contracts. In this research, the authors analyze the growing new opportunities in cyber warfare, strategic communications, psychological operations and cyber security. The scope of IO / IA is also expanding farther into areas of diplomacy, economics, and homeland security, while growing even more central to complex unconventional and conventional warfare applications. In addition, organizational change is accompanying these doctrinal and application area changes, which has led to a subsequent revision of the contract opportunities available. Likewise, new revisions of policy and documentation are also expected to arrive in the foreseeable future, which could lead to a deeper understanding and appreciation of cultural values and psychological roles among the multiple political players. In this review, we explore what new and promising opportunities for collaboration exist for academics, and we hope that this paper can alert researchers to alternate opportunities for funding in the IO and IA arena that they may not have considered previously.

Keywords: Information assurance, information operations, Department of Defense, contracts, proposals

The Uses and Limits of Game Theory in Conceptualizing Cyberwarfare

Merritt Baer

Harvard Law School, Cambridge, USA

Abstract: In cyberwarfare, there are obstacles to reaching minimax stasis: unlike in checkers, game theory cannot follow each decision path to its conclusion and then trace the right decisions back. However, I contend that because the rational predictability of game theory will continue to drive decisions and seek out patterns in them, game theory may identify (and intelligently weight) nodes of a decision tree that are not immediately recognizable to or favored by human decision-makers. While we can't create a network that is maximally resistant to random faults and maximally resistant to targeted faults, we can take into account the particular weaknesses and likelihoods of attack so that the weaknesses overlap in resistant ways-- ways that correspond to risk preferences and security priorities. Moreover, using game theory to make a security strategy that is a calculated derivative of mapped potential outcomes will help us to avoid human biases and to respond to threats proportionately/economically. Rather than a process of continual growth, cyber evolution, like biological evolution, seems more aptly characterized as punctuated equilibrium—periods of relative stasis followed by quick, drastic periods of breakthrough. Reaching Nash equilibrium is unlikely in the cyberwar context because under unstable conditions, evolutionarily stable strategies don't run a typical course. While there may be no set of moves that is a "solution" in cyberwar strategy, game theory allows human decisionmakers to intelligently identify and weight decision paths to transcend cognitive biases. This paper seeks to change the way of thinking about cyberwar-- from one of stockpiling weapons, to one of looking for patterns-- thinking about the problem of cyber insecurity more holistically. The paper challenges some of the myopia in thinking about cyber in existing "warfare" terms and proposes that organic models' tendency toward game theoretic equilibrium may help us conceive of the cyberwar decisionmaking landscape more effectively.

Keywords: Cyberwarfare, game theory, layered defense, Nash equilibrium

Who Needs a Botnet if you Have Google?

Ivan Burke and Renier van Heerden

Council for Scientific and Industrial Research, Pretoria South Africa

Abstract: Botnets have become a growing threat to networked operations in recent years. They disrupt services and communications of vital systems. This paper, gives an overview of the basic anatomy of a Botnet and its modus

operandi. In this paper, we present a Proof of Concept of how Google gadgets may be exploited to achieve these basic components of a Botnet. We do not provide a full fledged Botnet implementation but merely to mimic its functionality through Google Gadget API. Our goal was to have Google act as proxy agent to mask our attack sources, establish Command and Control structure between Bots and Botherders, launch attacks and gather info while at the same time maintaining some degree of stealth as to not be detected by users.

Keywords: Botnet; Google Gadget; Command and Control; DDoS

Mission Resilience in Cloud Computing: A Biologically Inspired Approach

Marco Carvalho¹, Dipankar Dasgupta², Michael Grimaila³ and Carlos Perez¹

¹Florida Institute for Human and Machine Cognition, Pensacola, USA

²University of Memphis, USA

³Air Force Institute of Technology, Wright-Patterson AFB, USA

Abstract: With the continuously improving capabilities enabling distributed computing, redundancy and diversity of services, Cloud environments are becoming increasingly more attractive for missioncritical and military operations. In such environments, mission assurance and survivability are key enabling factors for deployment, and must be provided as an intrinsic capability of the environment. Mission-critical frameworks must be safe and resistant to localized service failures and compromises. Furthermore, they must be able to autonomously learn and adapt to the environmental challenges and mission requirements. In this paper, we present a biologically inspired approach to mission survivability in cloud computing environments. Our approach introduces a multi-layer infrastructure that implements threat detection and service failure coupled with distributed assessments of mission risks, automated re-organization, and re-planning capabilities. Our approach leverages some insights from developmental biology at the service orchestration level, and takes failures and risk estimations as weighting functions for resource allocation. The paper first introduces and formulates the proposed concept for a simple single mission environment. We then propose a simulated scenario for proof-of concept demonstration and preliminary evaluation, and conclude paper with a brief discussion of results and future work.

Keywords: Mission assurance, cloud computing, mission survivability, biologically-inspired resilience

Link Analysis and Link Visualization of Malicious Websites

**Manoj Cherukuri and Srinivas Mukkamala
(ICASA)/CAaNES)/New Mexico Institute of Mining and Technology, USA**

Abstract: In this paper we present web crawling, Meta searches, geo location tools, and computational intelligent techniques to assess the characteristics of a cyber-incident to determine if an incident is likely to be caused by a certain group, geographical location of the source, intent of the attack, and useful behavioral aspects of the attack. The malicious websites extracted from the identified sources acted as seeds for our crawler and were crawled up to two hops traversing through all the hyperlinks emerging out from these pages. After crawling, all the websites were translated to their geographic locations based on the location of the server on which the website is hosted using the Internet Protocol (IP) address to the geographical location mapping databases. We applied social networking analysis techniques to the link structure of the malicious websites to put forward the properties of the malicious websites and compared them with that of the legitimate websites. We identified the potential sources or websites that publish malicious websites using the meta-searches. Our approach revealed that the behavior of the malicious websites with respect to their indegrees, outdegrees and the clustering coefficient differ from that of the legitimate websites and some malicious websites acted as promoters for other malicious websites. The link visualization showed that the links traversing across the malicious websites are not confined to the region where the website was hosted.

Keywords: Link analysis, link visualization, malicious websites, social networking analysis techniques

The Strategies for Critical Cyber Infrastructure (CCI) Protection by Enhancing Software Assurance

**Mecealus Cronkrite, John Szydlik and Joon Park
Syracuse University, USA**

Abstract: Modern organizations are becoming more reliant on complex, interdependent, integrated information systems. Key national industries are the critical infrastructure (CI) and include telecommunications, energy, healthcare, agriculture, and transportation. These CI industries are becoming more dependent on a critical cyber infrastructure (CCI) of computer information systems and networks, which are vital to the continuity of the economy. Organized attackers are increasing in number and power with more powerful computing resources that increasingly threaten CCI software systems. The motivations for attacks range from terrorism, fraud, identity theft, espionage, and political activism. Government and industry research

have found that most cyber attacks exploited known vulnerabilities and common software programming errors. Software publisher vendors have been unable to agree or implement a secure coding standard for two main reasons. The on-technical consumer is ill informed to demand secure quality products. These current conditions perpetuate preventable risk. As a result, software vendors do not implement security unless specifically required by the customer, leaving many systems full of gaps. Since most of exploited vulnerabilities are preventable, the implementation of a minimum level of software quality is one of the key countermeasures for protecting the critical information infrastructure. Government and industry can improve the resilience of the CI in an increasingly interdependent network of information systems by protecting the CCI with stronger software assurance practices and policies and strengthening product liability laws and fines for non-compliance. In this paper we discuss the increasing software and market risks to CCI and address the strategies to protect the CCI through enhancing software assurance practices and policies.

Keywords: Critical cyber infrastructure, secure programming quality, software assurance

Building an Improved Taxonomy for IA Education Resources in PRISM

Vincent Garramone and Daniel Likarish
Regis University, Denver, CO

Abstract: To address a perceived lack of availability of educational resources for students and educators in the field of information assurance, Regis University and the United States Air Force Academy (USAFA) have begun development of a web portal to store and make available to the public information security-related educational materials. The portal is named the Public Repository for Information Security Materials (PRISM). In this paper, we begin with a review of the initial vision for PRISM. We then discuss the development and maintenance of a deterministic discipline-specific vocabulary, along with the results of mapping curricular content to our initial set of terms. Out of the eight material descriptions used in our evaluation, five could be clearly mapped to the initial vocabulary, one could partially be mapped, and three did not contain any clearly mappable terms.

Keywords: PRISM, security education, taxonomy, educational resources

Using Dynamic Addressing for a Moving Target Defense

**Stephen Groat, Matthew Dunlop, Randy Marchany and Joseph Tront
Virginia Polytechnic Institute and State University, Blacksburg, USA**

Abstract: Static network addressing allows for attackers to geographically track hosts and launch network attacks. While technologies such as DHCP claim dynamic addressing, the majority of network addresses currently deployed are static for at least a session. Dynamic addresses, changing multiple times within a session, disassociate a user with a static address. This disassociation is important since a static address can be used to identify a host and makes targeting the host for attack feasible. We propose using dynamic addressing, in which hosts' addresses change multiple times per session, to create a moving target defense. Analyzing the primary factors which contribute to the security of dynamic addressing, we statistically evaluate the validity of this technique as a network defense. We then identify the optimal characteristics of a network-layer moving target defense that uses dynamic addressing.

Keywords: Moving target defense, network address security, privacy, dynamic addressing

Changing the Face of Cyber Warfare with International Cyber Defense Collaboration

Marthie Grobler¹, Joey Jansen van Vuuren¹ and Jannie Zaaiman²

¹Council for Scientific and Industrial Research, Pretoria, South Africa

²University of Venda, South Africa

Abstract: The international scope of the internet and global reach of technological usage requires the South African legislative system to address issues related to the application and implementation of international legislation. However, legislation in cyberspace is rather complex since the technological revolution and dynamic technological innovations are often not well suited to any legal system. A further complication is the lack of comprehensive international cyber defense cooperation treaties. The result is that many countries are not properly prepared, nor adequately protected by legislation, in the event of a cyber attack on a national level. This article will address the international cyber defense collaboration problem by looking at the impact of technological revolution on warfare. Thereafter, the article will evaluate the South African legal system with regard to international cyber defense collaboration. It will also look at the influence of cyber defense on the international position of the Government, as well as cyber security and cyber warfare acts and the command and control aspects thereof. The research

presented is largely theoretical in nature, focusing on recent events in the public international domain.

Keywords: Collaboration, cyber defense, legislation, government responsibility

Cyber Strategy and the Law of Armed Conflict

Ulf Haeussler

National Defense University, Washington, USA

Abstract: At the time of writing, the author was Assistant Legal Advisor Operational Law, Headquarters, Supreme Allied Commander Transformation (NATO HQ SACT). The views expressed herein are the author's own and do not necessarily reflect the official position or policy of NATO and/or HQ SACT. Abstract: At its Lisbon Summit (November 2010), NATO has adopted its Strategic Concept. The U.S. may soon adopt its Cyberstrategy 3.0 (originally expected for December 2010). Both strategy documents will contribute to a growing policy consensus regarding cyber security and defence as well as provide better policy insights regarding cyber offence. In doing so, they will contribute to a better understanding of how NATO and the U.S. want to prepare for, and conduct cyber warfare in a manner congruent with the law of armed conflict. In addition, they will determine to what extent this branch of the law needs to be better understood, developed, or reformed. Accordingly, this paper indicates how the existing legal and policy frameworks intersect with practical aspects of cyber warfare and associated intelligence activities, analyses how the new strategy documents develop and change the existing policy framework, and what repercussions this may have for the interpretation and application of the law of armed conflict. It also demonstrates how the new strategy documents inform the policy and legal discourse and hence help confirm that NATO and U.S. as well as other NATO Nations' cyber activities are, and will continue to be, lawful and legitimate.

Keywords: NATO Strategic Concept 2010, U.S. Cyberstrategy 3.0, Law of Armed Conflict, collective security, collective defence

eGovernance and Strategic Information Warfare – non Military Approach

Karim Hamza and Van Dalen

Maastricht School of Management, Netherlands

Abstract: Most of the developed Governments, active in reaping the benefits of eGovernance, nowadays have discovered the threats of this new approach too. They invest massively to cope with the highly complex decision making systems of today, dramatic changes in economy, technology and Information

Warfare threats plus government's own changing strategies. This creates challenges with respect to matching decision-making structures. eGovernance Frameworks is defined by the UNESCO as "*the use of ICT (Information and communication technologies) by different actors of the society with the aim to improve their access to information and to build their capacities*". It may be expected that eGovernance will have more strategic importance for many governments and that its concepts and tools will develop dramatically in the coming decade. This will raise the urgencies and importance of protecting government decision making processes from non-solicited disturbing external or internal interferences. Security is critical to the success of any eGovernance framework. Since such governance frameworks somehow will be open to interactions with different "stakeholders" *Internally* (within the boundaries of the state, like pressure groups, political parties, business, citizens ..) or *Externally* (e.g. other states, multinational businesses, worldwide operating malicious organizations,..) who may influence the decision making process in government, create political pressure or even start a cyber-war, by making use of eGovernance frameworks. This raises a number of prevention issues to cope with, like instability of the decision making processes, or even instability of real development processes in states. This causes efforts to add to the design process of eGovernance frameworks a new dimension, popularly labeled "Information Warfare Strategy", with the aim to build in existing and future eGovernance Frameworks safeguarding tools; to prevent abuse of such frameworks in practical government decision cases. Traditionally there is a distinction between military vs. non-military approaches. The question has to be raised in how far a distinction between Technology (ICT) vs. non-Technology tools (like diplomacy, or legal) will be more appropriate. However we have to recognize that any line of distinction is arbitrary and will show the need for some dynamics, because parties involved will learn and improve.

Keywords: eGovernment, government transformation, public sector information systems, e governance framework, information warfare, non military strategies

Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains

**Eric Hutchins, Michael Cloppert and Rohan Amin
Lockheed Martin, USA**

Abstract: Conventional network defense tools such as intrusion detection systems and anti-virus focus on the vulnerability component of risk, and traditional incident response methodology presupposes a successful intrusion. An evolution in the goals and sophistication of computer network intrusions has rendered these approaches insufficient for certain actors. A

new class of threats, appropriately dubbed the “Advanced Persistent Threat” (APT), represents well-resourced and trained adversaries that conduct multi-year intrusion campaigns targeting highly sensitive economic, proprietary, or national security information. These adversaries accomplish their goals using advanced tools and techniques designed to defeat most conventional computer network defense mechanisms. Network defense techniques which leverage knowledge about these adversaries can create an intelligence feedback loop, enabling defenders to establish a state of information superiority which decreases the adversary's likelihood of success with each subsequent intrusion attempt. Using a kill chain model to describe phases of intrusions, mapping adversary kill chain indicators to defender courses of action, identifying patterns that link individual intrusions into broader campaigns, and understanding the iterative nature of intelligence gathering form the basis of intelligence-driven computer network defense (CND). Institutionalization of this approach reduces the likelihood of adversary success, informs network defense investment and resource prioritization, and yields relevant metrics of performance and effectiveness. The evolution of advanced persistent threats necessitates an intelligence-based model because in this model the defenders mitigate not just vulnerability, but the threat component of risk, too.

Keywords: Incident response, intrusion detection, intelligence, threat, APT, computer network defense

The Hidden Grand Narrative of Western Military Policy: A Linguistic Analysis of American Strategic Communication

Saara Jantunen and Aki-Mauri Huhtinen
National Defence University, Helsinki, Finland

Abstract: War engages civilians in a very different way than is traditionally understood. The military-industrial complex has rooted itself permanently into the civilian world. In the US, recruiters have long operated in university campuses, the Pentagon has funded the entertainment industry for decades, and the current trend in most militaries is to advertise military careers that are less about war and more about individual expertise in civilian professions. The key place for military recruiting is shopping malls, where teenagers can play war games and enlist. Strategic communication has replaced information warfare. In a complex world, strategic communication exploits all possible media. As Art of War has been replaced by science, the representations of war and the role of the military have changed. Both war and military forces are now associated with binary roles: destruction and humanity, killing and liberating. The logic behind 'bombing for peace' is encoded in the Grand Military Narrative. This narrative is hidden in American (and NATO) strategies such as Effects Based Operations, which rely heavily on technology. As

people aim to rationalize the world with technology, they fail to take into account the uncertainty it brings. In warfare, that uncertainty is verbalized as “friendly fire”, “collateral damage” or simply as “accident”. Success and failure are up to technology. Technology is no longer a tool, but an ideology and an actor that not only 'enables' the military to take action, but frees it of responsibility. This article analyzes American strategy discourse and the standard and trends of rhetoric they create. The article focuses on pinpointing some of the linguistic choices and discourses that define the so-called 'techno-speak', the product of modern techno-ideology. These discourses result in representations of techno-centered binary values, which steer military strategy and foreign policy.

Keywords: Military-industrial complex, revolution in military affairs, effects based operations, discourse analysis, military technology

Host-Based Data Exfiltration Detection via System Call Sequences

Brian Jewell¹ and Justin Beaver²

¹Tennessee Technological University, Cookeville, USA

²Oak Ridge National Laboratory, Oak Ridge, USA

Abstract: The host-based detection of malicious data exfiltration activities is currently a sparse area of research and mostly limited to methods that analyze network traffic or signature based detection methods that target specific processes. In this paper we explore an alternative method to host-based detection that exploits sequences of system calls and new collection methods that allow us to catch these activities in real time. We show that system call sequences can be found to reach a steady state across processes and users, and explore the viability of new methods as heuristics for profiling user behaviors.

Keywords: Data exfiltration, data security, intrusion detection

Detection of YASS Using Calibration by Motion Estimation

Kesav Kancherla and Srinivas Mukkamala

(ICASA) / (Canes) / New Mexico Institute of Mining and Technology USA

Abstract: Through this paper we propose a new approach to thwart defects of current blind steganalysis methods. “Yet Another Steganographic Scheme” (YASS) is a robust steganographic scheme that embeds data in random locations based on a secret key. Due to this randomization the current steganalysis schemes such as self calibration methods do not detect YASS. In this work, we present a new calibration method using Motion Estimation and extract higher order features. In our methodology motion estimation

technique is applied on an image, to estimate its actual image. We assume that the estimated image captures the features of the actual image, due to spatial redundancy in the images. We extract two sets of features; DCT based features from DCT domain and Markov model based features from spatial domain, and apply Support Vector Machines (SVMs) on these feature sets. Our approach against YASS using different block sizes (9, 10, 12, and 14), compression rates (50-50, 50/75, and 75/75) and coefficients used for embedding data (12 and 19) obtained an accuracy of about 95%, even for bigger block lengths and low embedding rates. This methodology can be used as blind steganalysis technique, as detection is based on modification of an image rather than steganographic scheme.

Keywords: Blind steganalysis, Discrete Cosine Transform (DCT), motion estimation, steganalysis, Support Vector Machines (SVM)

Developing a Knowledge System for Information Operations

Louise Leenen, Ronell Alberts, Katarina Britz, AURONA Gerber and Thomas Meyer

Council for Scientific and Industrial Research, Pretoria, South Africa

Abstract: In this paper we describe a research project to develop an optimal information retrieval system in an Information Operations domain. Information Operations is the application and management of information to gain an advantage over an opponent and to defend one's own interests. Corporations, governments, and military forces are facing increasing exposure to strategic information-based actions. Most national defence and security organisations regard Information Operations as both a defensive and offensive tool, and some commercial institutions are also starting to recognise the value of Information Operations. An optimal information retrieval system should have the capability to extract relevant and reasonably complete information from different electronic data sources which should decrease information overload. Information should be classified in a way such that it can be searched and extracted effectively. The authors of this paper have completed an initial phase in the investigation and design of a knowledge system that can be used to extract relevant and complete knowledge for the planning and execution of Information Operations. During this initial phase of the project, we performed a needs analysis and problem analysis and our main finding is the recommendation of the use of logic-based ontologies: it has the advantage of unambiguous semantics, facilitates intelligent search, provides an optimal trade-off between expressivity and complexity, and yields optimal recall of information. The risk of adopting this technology is its status as an emerging technology and therefore we include recommendations for the development of a prototype system.

Keywords: Information operations, knowledge representation, ontology, query language

CAESMA – An On-Going Proposal of a Network Forensic Model for VoIP traffic

Jose Mas y Rubi, Christian Del Carpio, Javier Espinoza, and Oscar Nuñez Mori

Pontificia Universidad Catolica del Peru, Lima, Peru

Abstract: In the near future, service convergence will be a reality, which presents us with a possible misuse problem of these technologies. One of these services is Voice over IP (VoIP), which provides the phone communication services in this scheme. Currently VoIP is a very popular technology, and could be use by malicious attackers related to informatics crimes, to perform their illicit actions, which will be difficult to track because of IP network's nature. Because of this, our approach is to achieve a preliminary analysis to create a forensic model for detection and tracing of VoIP traffic, which will allow us to make an adequate evidence recollection which could be used by the police authorities.

Keywords: Network forensics, forensic model proposal, voice over IP

Secure Proactive Recovery – a Hardware Based Mission Assurance Scheme

Ruchika Mehresh¹, Shambhu Upadhyaya¹ and Kevin Kwiat²

¹State University of New York at Buffalo, USA

²Air Force Research Laboratory, Rome, USA

Abstract: Mission Assurance in critical systems entails both fault tolerance and security. Since fault tolerance via redundancy or replication is contradictory to the notion of a limited trusted computing base, normal security techniques cannot be applied to fault tolerant systems. Thus, in order to enhance the dependability of mission critical systems, designers employ a multi-phase approach that includes fault/threat avoidance/prevention, detection and recovery. Detection phase is the fallback plan for avoidance/prevention phase, as recovery phase is the fallback plan for detection phase. However, despite this three-stage barrier, a determined adversary can still defeat system security by staging an attack on the recovery phase. Recovery being the final stage of the dependability life-cycle, unless certain security methodologies are used, full assurance to mission critical operations cannot be guaranteed. For this reason, we propose a new methodology, viz. secure proactive recovery that can be built into future mission-critical systems in order to secure the recovery phase at low cost. The solution proposed is realized through a hardware-supported design of a consensus protocol. One of the major strengths of this scheme is that it not only detects abnormal behavior due to system faults or attacks, but also

secures the system in case where a smart attacker attempts to camouflage by playing along with the predefined protocols. This sort of adversary may compromise certain system nodes at some earlier stage but remain dormant until the critical phase of the mission is reached. We call such an adversary The Quiet Invader. In an effort to minimize overhead, enhance performance and tamper-proof our scheme, we employ redundant hardware typically found in today's self-testing processor ICs, like design for testability (DFT) and built-in self-test (BIST) logic. The cost and performance analysis presented in this paper validates the feasibility and efficiency of our solution.

Keywords: Security, fault tolerance, mission assurance, critical systems, hardware

Identifying Cyber Espionage: Towards a Synthesis Approach

David Merritt and Barry Mullins

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

Abstract: Espionage has existed in many forms for as long as humans have kept secrets. With the skyrocketing growth of digital data storage, cyber espionage has quickly become the tool of choice for corporate and government spies. Cyber espionage typically occurs over the Internet with a consistent methodology: 1) infiltrate a targeted network, 2) install malware on the targeted victim(s), and 3) exfiltrate data at will. Detection methods exist and are well-researched for these three realms: network attack, malware, and data exfiltration. However, formal methodology does not exist for identifying cyber espionage as its own classification of cyber attack. This paper proposes a synthesis approach for identifying targeted espionage by fusing the intelligence gathered from current detection techniques. This synthesis of detection methods establishes a formal decision-making framework for determining the likelihood of cyber espionage.

Keywords: Covert channel, cyber espionage, data exfiltration, intrusion detection, malware analysis

Security Analysis of Webservers of Prominent Organizations of Pakistan

Muhammad Naveed
Free Lance Research, Pakistan

Abstract: Insecure webservers are a serious threat to the organization's reputation and resources. Successful attack on webservers can destroy the trust of customers or people getting services from the organization. Webservers were selected for this study because they provide easily accessible entrance to the network from the Internet and security of webservers should be considered as an index to assess the organization's overall information security. This study analyzes the webservers of prominent organizations of Pakistan to assess their level of security. Webservers of different types of organizations were selected to provide a general view of security of Pakistani webservers. The selected webservers were of the organizations who should be first to secure their webservers as they are the leaders in their respective fields in the country. So, all the smaller organizations can be assumed to have much lesser concern for security. Benchmark for every type of organization was first established to compare the results of the analysis with it. Nmap scanner was used to scan the webservers for security threats. The results reveal that the webservers in Pakistan are not secure and there is extreme need of awareness about information security in the country. The lack of importance given to information security can lead to cyber terrorism and might create a lot of troubles for the country.

Keywords: Information security, analysis, security threats, Webserver, Pakistan, Nmap

International Legal Issues and Approaches Regarding Information Warfare

Alexandru Nitu
Romanian Intelligence Service, Bucharest, Romania

Abstract: In present times, societies and economies increasingly rely on electronic communications, becoming more vulnerable to threats from cyberspace. At the same time, states' military and intelligence organizations are increasingly developing the capability to attack and defend computer systems. The progress of information technology makes it possible for adversaries to attack each other in new ways, inflicting new forms of damage; technological change enables cyberwarfare acts that do not fit within existing legal categories, or may reveal contradictions among existing legal principles. The paper examines the relationship between information warfare and the law, especially international law and the law of war, as it is apparent that

some fundamental questions regarding this new and emerging type of security threat need to be explored. For example, what types of activities between nation states, could or should be called information warfare? What are 'force', 'armed attack', or 'armed aggression' - terms from the UN Charter - in the Information Age, and do they equate to information warfare? Information warfare is neither 'armed' in the traditional sense, nor does it necessarily involve conflict, so an important issue is if 'war' between states necessarily require physical violence, kinetic energy, and human casualties. A threshold question that arises from the development of information warfare techniques is thus the definitional one: has the development of information warfare technology and techniques taken information warfare out of the existing legal definition of war? Characteristics of information technology and warfare pose problems to those who would use international law to limit information warfare, and leave legal space for those who would wage such warfare. Consequently, there may be confusion over what limits may apply to the conduct of information warfare, and when information warfare attacks may be carried out. Prospects of new technological attacks pose problems for international law because law is inherently conservative. From this point of view, the paper examines how the law itself might change in response to the fast development of information technology and how will long-established legal principles such as national sovereignty and the inviolability of national borders be affected by the ability of cyberspace to transcend such concepts.

Keywords: International law, information warfare, use of force, Charter of the United Nations, Geneva conventions

Cyberwarfare and Anonymity

Christopher Perr
Auburn University, USA

Abstract: Public policy and strategy do not keep up to date with technology. There is generally a lag time between the release and application of a technology till a shortcoming is observed. Once a shortcoming is revealed it is a race to address that potential weakness with improved policy, updated strategy, a technological initiative to combat the shortcoming, or a necessary combination of all methods. The invent of computer reliant and networked systems has created a modern arms race which has seen more innovation and more need for updated policy and strategy than any other period in history, yet the United States continues to fall behind in this arms race. When security cannot be verified, but only risk mitigated, it is time to think deterrence. Unfortunately, deterrence falls apart when you cannot identify the perpetrator behind attacks. This paper will look at the role that information has played in previous conflicts, as well as the modern strategy towards protecting the United States in cyberspace, and will draw a singular conclusion as to the best course of action towards improving our security.

Through a mix of policy, strategy, and technology the anonymity which attackers use as a shield needs to be eliminated in order to allow room for a strong policy of deterrence with a verifiable response. In establishing the means to identify our attackers and provide serious recourse cybersecurity can be greatly improved for the United States.

Keywords: Information warfare, security, policy, strategy, history, information security

Catch Me If You Can: Cyber Anonymity

David Rohret and Michael Kraft

Joint Information Operations Warfare Center (JIOWC) Red Team, San Antonio, Texas, USA

Abstract: Advances in network security and litigation have empowered and enabled corporations to conduct Internet and desktop surveillance on their employees to increase productivity and their customers to gain valuable marketing data. Governments have spent billions to monitor cyberspace and have entered agreements with corporations to provide surveillance data on adversarial groups, competitors, and citizenry (Reuters, 2010). The Chinese government's monitoring of the Internet (Markoff, 2008), the United Kingdom's plan to track every email, phone call, and website visited (Whitehead, 2010), and the recent announcement from the United States that a program named the "Perfect Citizen" (Bradley, 2010) will be used to identify those committing cybercrimes and terrorist activities. These government surveillance programs have many concerned that anonymity on the Internet is non-existent and that real objectivity and candidness found on news, educational, and research websites is being replaced with a "big brother" atmosphere; preventing open discussion and information transfers between domains. Although the initial intent of network and Internet monitoring may be honourable; terrorists, hackers, and cyber-criminals already have access to the necessary tools and methodologies to continue in their activities unabated. State and non-state adversaries can use these same tools and methodologies to divert malicious and offensive actions towards a common adversary, avoiding attribution while increasing tensions among non-actors. Concerned educators, scientists, and citizens are rebelling against Internet monitoring providing the impetus for developers and entrepreneurs to create methods, tools, and virtual private networks that provide secrecy for those wishing to remain invisible; avoiding detection from employers, law enforcement, and other government agencies (Ultimate-Anonymity, 2010). The intent of this research is to first briefly identify the efforts required by governments to track and monitor individuals and groups wishing to remain anonymous within the cyber community. The authors define "cyber community" as the boundaries within any tool, process, or mechanism utilizing Transmission Control Protocol (TCP)/ Internet Protocol (IP), or similar

protocols that allow for the transfer and aggregation of information and data. In contrast, the authors will then identify a process to remain wholly anonymous in the context of an internet identity. This will be demonstrated in a step-by-step case study using a "paranoid" approach to remaining anonymous.

Keywords: Anonymity, network, internet surveillance, foreign proxy, Hacker, Big Brother

Neutrality in the Context of Cyberwar

Julie Ryan¹ and Daniel Ryan²

¹The George Washington University, Washington, USA

²National Defense University, Washington, USA

Abstract: This paper will examine the legal antecedents of the concepts of neutrality and current enforceability of declarations of neutrality in the context of information operations amongst belligerents. This is a non-trivial point of understanding, given the potential for belligerents to use and abuse infrastructure elements owned and/or operated by nation states desiring to remain neutral. The analysis will consider the instantiated concepts of neutrality, the potential for expanding or contracting the concepts of neutrality in the context of cyberwar, and the possibility of erosion of neutrality in cyberwar scenarios. We have a notion enshrined in international law that says that you don't lose your neutrality if belligerents use your telephone lines or telegraph lines to communicate even if they are crossing your territory, even if they are passing operational orders. The problem with cyberwar is that they are potentially not just transferring orders but also potentially weapons -- cyber-weapons. So it becomes a more complex problem and the challenge is to understand at what point the nation state should be required to act, or if such a point exists at all. This analysis will examine the intersection between technology and law in regards to this issue.

Keywords: Neutrality; law of armed conflict; international humanitarian law; cyberwar

Labelling: Security in Information Management and Sharing

Harm Schotanus, Tim Hartog, Hiddo Hut and Daniel Boonstra
TNO Information and Communication Technology, Delft, The Netherlands

Abstract: Military communication infrastructures are often deployed as stand-alone information systems operating at the System High mode. Network-Enabled Capabilities (NEC) and combined military operations lead to new requirements for information management and sharing which current

communication architectures cannot deliver. This paper informs information architects and security specialists about an incremental approach introducing labelling of documents by users to facilitate information management and sharing in security related military scenarios.

Keywords: Labelling, meta-information, information security, cross-domain solutions, information sharing, need-to-protect, duty-to-share

Information Management Security for Inter-Organisational Business Processes, Services and Collaboration

Maria Semmelrock-Picej¹, Alfred Possegger² and Andreas Stopper²

¹eBusiness Institute, Klagenfurt University, Austria

²Infineon IT-Services GmbH Austria, Austria

Abstract: Web-based collaborations and cross-organizational processes typically require dynamic and context-based interactions between involved parties and services. Due to temporary nature of collaboration and an evolving of competencies of involved companies over time security issues like trust, privacy and identity management are of a high interest for a long lasting success of virtual collaborations. This paper addresses this issue by presenting some results of an international research project. The vision of this project is to implement a virtual cooperation system for SMEs to be used for realizing competitive advantages through virtual cooperations. The paper describes some results of this system. Especially we will discuss issues concerned with identity management. Identity Federation is one of the key concepts of SPIKE to support “virtual organizations”, their fast setup, comfortable maintenance and orderly closing. This paper describes the mechanisms from which collaboration partners, registered at the SPIKE platform, will be authenticated by using a standardized identity federation protocol – Shibboleth. It is shown how the identity data of a company, using its own IDMS, can be integrated into the SPIKE platform and what a company has to setup from a technical point of view so that its employees can be authenticated via Shibboleth. Further an approach is presented suitable for mostly SMEs which do not have an own IDMS.

Keywords: eCollaboration, security, identity management, phases of cooperation

Anatomy of Banking Trojans – Zeus Crimeware (how Similar are its Variants)

**Madhu Shankarapani and Srinivas Mukkamala
(ICASA)/(CAaNES)/New Mexico Institute of Mining and Technology, USA**

Abstract: To add complexity to existing cyber threats; targeted Crimeware that steals personal information for financial gains is for sale as low as \$700 dollars. Banking Trojans have been notoriously difficult to kill and to date most antivirus and security technologies fail to detect or prevent them from causing havoc. Zeus which is considered as one of the most nefarious financial and banking Trojans targets business and financial institutions to perform unauthorized automated clearinghouse (ACH) and wire transfer transactions for check and payment processing. Zeus is causing billions of dollars in losses and is facilitating identity theft of innocent users for financial gains. Zeus Crimeware does one thing very well that every security researcher envy's – obfuscation. Zeus kit conceals the exploit code every time a binary is created. Zeus Crimeware has an inbuilt binary generator that generates a new binary file on every use that is radically different from others; which evades detection from antivirus or security technologies that rely on signature based detection. The effectiveness of an up to date antivirus against Zeus is thus not 100%, not 90%, not even 50% – it's just 23% which is alarming. No matter how smart and how different Zeus binaries are, most of them share a few common behavioral patterns such as an ability to take screenshots of a victim's machine, or control it remotely, hijacking E-banking sessions and logging them to the level of impersonation or add additional pages to a website and monitor them, or steal passwords that have been stored by popular programs and use them. In this paper we present detection algorithms that can help the antivirus community to ensure a variant of a known malware can still be detected without the need of creating a signature; a similarity analysis (based on specific quantitative measures) is performed to produce a matrix of similarity scores that can be utilized to determine the likelihood that a piece of code or binary under inspection contains a particular malware. The hypothesis is that all versions of the same malware family or similar malware family share a common core signature that is a combination of several features of the code (binary). Results from our recent experiments on 40 different variants of Zeus show very high similarity scores (over 85%). Interestingly Zeus variants have high similarity scores with other banking Trojans (Torpig, Bugat, and Clampi) and a well know data stealing Trojan *Qakbot*. We present experimental results that indicate that our proposed techniques can provide a better detection performance against banking Trojans like Zeus Crimeware.

Keywords: Zeus Crimeware, banking Trojans, Torpig, Bugat, Clampi, malware similarity analysis, anatomy of Zeus, malware analytics

Terrorist use of the Internet: Exploitation and Support Through ICT Infrastructure

Namosha Veerasamy and Marthie Grobler

Council for Scientific and Industrial Research, Pretoria, South Africa

Abstract: The growth of technology has provided a wealth of functionality. One area in which Information Communication Technology (ICT), especially the Internet, has grown to play a supporting role is terrorism. The Internet provides an enormous amount of information, and enables relatively cheap and instant communication across the globe. As a result, the conventional view of many traditional terrorist groups shifted to embrace the use of technology within their functions. The goal of this paper is to represent the functions and methods that terrorists have come to rely on through the ICT infrastructure. The discussion sheds light on the technical and practical role that ICT infrastructure plays in the assistance of terrorism. The use of the Internet by terrorist groups has expanded from traditional Internet usage to more innovative usage of both traditional and new Internet functions. Global terrorist groups can now electronically target an enormous amount of potential recipients, recruits and enemies. The aim of the paper is to show how the Internet can be used to enable terrorism, as well as provide technical examples of the support functionality and exploitation. This paper summarises the high-level functions, methods and examples for which terrorists utilise the Internet. This paper looks at the use of the Internet as both a uni-directional and bi-directional tool to support functionality like recruitment, propaganda, training, funding and operations. It also discusses specific methods like the dissemination of web literature, social-networking tools, anti-forensics and fund-raising schemes. Additional examples, such as cloaking and coding techniques, are also provided. In order to analyse how ICT infrastructure can be used in the support of terrorism, a mapping is given of communication direction to the traditional Internet use functions and methods, as well as to innovative Internet functions and methods.

Keywords: Anti-forensics, internet, terrorism, ICT, propaganda, social-networking

Evolving an Information Security Curriculum: New Content, Innovative Pedagogy and Flexible Delivery Formats

**Tanya Zlateva, Virginia Greiman, Lou Chitkushev and Kip Becker
Boston University, USA**

Abstract: In the last ten years information security has been recognized as a most relevant new trend by academia, government and industry. The need for educating information security professionals has increased dramatically and is not being met despite recent growth of cyber security programs. The challenge is to design and evolve multi-disciplinary curricula that provide theoretical as well as hands-on experience and are also available to a broad student audience is of strategic importance for the future of reliable and secure systems. We present our experience in designing and evolving information security programs that have grown to over 650 students per year since their inception eight years ago and have graduated more than 250 students. We discuss three major directions in the evolution of the program: the increased focus of the core and growth of concentration electives, the design of cyber law curriculum and coordination with the business continuity programs, and the introduction of new educational technologies such as virtualization and video-collaboration and flexible online and blended delivery formats. The rapid growth of the program, the changes in the discipline and the great diversity of professional interests of our students required broadening of the curriculum with courses and modules on emerging technologies such as digital forensics, biometrics, security policies and procedures, privacy and security in health care, cyber law, as well as the coordination of the curriculum with existing programs in business continuity. Special efforts were expended to the introduction of more participatory pedagogy, more specifically by developing a series of virtual laboratories that brought real world situations into the class room and through video-collaboration tools that encourage team building. The accessibility of the programs was increased through the introduction of flexible delivery formats. After establishing the programs in the traditional classroom, we added an blended and online version that rapidly found a national audience.

Keywords: Information security education, digital forensics, cyber law, virtualization, business continuity, online and blended learning

PhD Research

Towards Persistent Control over Shared Information in a Collaborative Environment

**Shada Alsalamah, Alex Gray and Jeremy Hilton
Cardiff University, UK**

Abstract: In a complex collaborative environment, such as healthcare, where Multi-Disciplinary care Team (MDT) members and information come from independent organisational domains, there is a need for information-sharing across the organizations' information systems in order to achieve the overall goal of collaboration. Inability to provide a secure communication method, giving local/global protection is affecting inter-professional communications and hindering sharing among MDT members. This research aims to facilitate a secure collaborative environment enabling persistent control over shared information across boundaries of the organisations that own the data. This paper is based on the early stages of the research and its results will feed into following stages. It looks at the structure of a healthcare system to understand the types of inter-professional communication and information exchange that occur in practice. Additionally it presents an initial assessment identifying the Information Security (IS) needs and challenges faced in providing persistent control in a shared collaborative environment by using conceptual modelling of a selected medical scenario (breast cancer in Wales). The results show that a considerable number of professionals are involved in a patient's treatment. Each plays a well-defined role, but often uses different Healthcare Information Systems (HIS) to store sensitive and confidential patient medical information. These HIS cannot provide secure multi-organisational information-sharing to support collaboration among the MDT members. This causes inter-professional communication issues among team members that inhibit decision-making using the information. The findings from this study show how to improve information support from HIS stored information for MDT members. Also the resulting IS functions will be described which facilitate establishing secure collaborative environments guaranteeing persistent control over shared information.

Keywords: Information security, information system, Information sharing, multi-disciplinary team, persistent control, secure collaborative environment

3D Execution Monitor (3D-EM): Using 3D Circuits to Detect Hardware Malicious Inclusions in General Purpose Processors

Michael Bilzor

U.S. Naval Postgraduate School, Monterey, California, USA

Abstract: Hardware malicious inclusions (MIs), or "hardware trojans," are malicious artifacts planted in microprocessors. They present an increasing threat to computer systems due to vulnerabilities at several stages in the processor manufacturing and acquisition chain. Existing testing techniques, such as side-channel analysis and test-pattern generation, are limited in their ability to detect malicious inclusions. These hardware attacks can allow an adversary to gain total control over a system, and are therefore of particular concern to high-assurance customers like the U.S. Department of Defense. In this paper, we describe how three-dimensional (3D) multi-layer processor fabrication techniques can be used to enhance the security of a target processor by providing secure off-chip services, monitoring the execution of the target processor's instruction set, and disabling potentially subverted control circuits in the target processor. We propose a novel method by which some malicious inclusions, including those not detectable by existing means, may be detected and potentially mitigated in the lab and in fielded, real-time operation. Specifically, a target general-purpose processor, in one layer, is joined using 3D interconnects to a separate layer, which contains an Execution monitor for detecting deviations from the target processor's specified behavior. The Execution monitor layer is designed and fabricated separately from the target processor, using a trusted process, whereas the target processor may be fabricated by an untrusted source. For high-assurance applications, the monitor layer may be joined to the target layer, after each has been separately fabricated. In the context of existing computer security theory, we discuss the limits of what an Execution monitor can do, and describe how one might be constructed for a processor. Specifically, we propose that the signals which carry out the target processor's instruction set actions may be described in a stateful representation, which serves as the input for a finite automata-based Execution monitor, whose acceptance predicate indicates when the target processor's behavior violates its specification. We postulate a connection between Execution monitor theory and the proposed 3D processor monitoring system, which can be used to detect a specific class of malicious inclusions. Finally, we present the results of our first monitor experiment, in which we designed and tested (in simulation) a simple Execution monitor for a small open-source 32-bit processor design known as the ZPU. We analyzed the ZPU processor to determine which signals must be monitored, designed a system of monitor interconnects in the hardware description language (HDL) representation, developed a stateful representation of the microarchitectural behavior of the

ZPU, and designed an Execution monitor for it. We demonstrated that the Execution monitor identifies correct operation of the original, unmodified ZPU, as it executed arbitrary code. Having introduced some minor deviations to the ZPU processor's microarchitectural design, we then showed in simulation that the Execution monitor correctly detected the deviations, in the same way that it might detect the presence of some malicious inclusions in a modern processor.

Keywords: Processor, security, trojan, subversion, detection

Towards an Intelligent Software Agent System as Defense Against Botnets

Evan Dembskey and Elmarie Biermann

UNISA, Pretoria, South Africa

French South African Institute of Technology CPUT, Cape Town, South Africa

Abstract: Computer networks are targeted by state and non-state actors and criminals. With the professionalization and commoditization of malware we are moving into a new realm where off-the-shelf and time-sharing malware can be bought or rented by the technically unsophisticated. The commoditization of malware comes with all the benefits of mass produced software, including regular software updates, access to fresh exploits and the use of hack farms. To an extent defense is out of the hands of the government, and in the hands of commercial and private hands. However, the cumulative effect of Information Warfare attacks goes beyond the commercial and private spheres and affects the entire state. Thus the responsibility for defense should be distributed amongst all actors within a state. As malware increases and becomes more sophisticated and innovative in their attack vectors, command & control structures and operation, more sophisticated, innovative and collaborative methods are required to combat them. The current scenario of partial protection due to resource constraints is inadequate. It is thus necessary to create defence systems that are robust and resilient against known vectors and vectors that have not previously been used in a manner that is easy and cheap to implement across government, commercial and private networks without compromising security. We argue that a significant portion of daily network defence must be allocated to software agents acting in a beneficent botnet with distributed input from human actors, and propose a framework for this purpose. This paper is based the preliminary work of a PhD thesis on the topic of using software agents to combat botnets, and covers the preliminary literature survey and design of the solution. This includes a crowd sourcing component that uses information about malware gained from software agents and from human users. Part of this work is based on previous research by the authors. It is anticipated that

the research will result in a clearer understanding of the role of software agents in the role of defence against computer network operations, and a proof-of-concept implementation.

Keywords: Information warfare, Botnet, software agent

Theoretical Offensive Cyber Militia Models

Rain Ottis

Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia

Abstract. Volunteer based non-state actors have played an important part in many international cyber conflicts of the past two decades. In order to better understand this threat I describe three theoretical models for volunteer based offensive cyber militias: the Forum, the Cell and the Hierarchy. The Forum is an ad-hoc cyber militia form that is organized around a central communications platform, where the members share information and tools necessary to carry out cyber attacks against their chosen adversary. The Cell model refers to hacker cells, which engage in politically motivated hacking over extended periods of time. The Hierarchy refers to the traditional hierarchical model, which may be encountered in government sponsored volunteer organizations, as well as in cohesive self-organized non-state actors. For each model, I give an example and describe the model's attributes, strengths and weaknesses using qualitative analysis. The models are based on expert opinion on different types of cyber militias that have been seen in cyber conflicts. These theoretical models provide a framework for categorizing volunteer based offensive cyber militias of non-trivial size.

Keywords: Cyber conflict, cyber militia, cyber attack, patriotic hacking, on-line communities

Work in Progress Papers

Large-Scale Analysis of Continuous Data in Cyber-Warfare Threat Detection

William Acosta
University of Toledo, USA

Abstract: Combating cyber/information warfare threats requires analyzing vast quantities of diverse data. The data required to detect attacks as they occur (on-line analysis of live data) and predict future threats (forensic analysis/data mining) is not only large, but is growing at a staggering rate. Data such as network traffic logs, emails, and social networking posts, SMS message, and cell phone call logs are, by nature, continuous and growing. The problem addressed in this research is that current systems are not designed to handle either the scope or nature of the analysis or the data itself. For example, distributed data processing systems like Google's Map-Reduce provide the ability to process large data sets, but they are not designed to easily support processing of changing data sets or data-mining algorithms. In light of this, Google has itself recently stopped using MapReduce for building its web-index, opting instead for a custom mechanism that can more quickly respond to and process new content. Non-traditional databases, like vertically-partitioned/column-store databases, can efficiently support analysis algorithms on large quantities of data, but they are not designed to support continuously changing data sets. The goal of this research is to explore and design new data management system that can handle large quantities of incrementally growing data as well as direct support for data mining and analysis algorithms. Specifically, this research proposes a new distributed data processing system that exploits the parallel and distributed resources/computation of cloud computing infrastructures. It makes use of summary data structures that can be updated incrementally and continuous queries to support analysis and data mining algorithms natively. This approach allows for larger-scale and more robust analysis on continuously growing data that can help detect, predict and respond to cyber-warfare threats.

Keywords: Data-mining, databases, text-search, cloud computing, data integration

A System and Method for Designing Secure Client-Server Communication Protocols Based on Certificateless PKI

Natarajan Vijayarangan

Tata Consultancy Services Limited (TCS), Chennai, India

Abstract: Client-server networking is a distributed application architecture that partitions tasks or work loads between service providers (servers) and service requesters (clients), where the network communication is not necessarily secure. A number of researchers and organizations have produced innovative methods to ensure a secure communication in the client-server set up. However, in this paper, TCS has brought out a system of novel network security protocols for a generic purpose. Let us take a look into the brief history of client-server communication. In 1993 Bollovin and Merritte patented a strong Password-based Authentication Key Exchange (PAKE), an interactive method for two or more parties to establish cryptographic keys based on one or more party's knowledge of a password. Later, Stanford University patented Secure Remote Protocol (SRP) used for a new password authentication and key-exchange mechanism over an untrusted network. Then Sun Microsystems implemented the Elliptic Curve Cryptography (ECC) technology which is well integrated into the OpenSSL-Certificate Authority. This code enables secure TLS/SSL handshakes using the Elliptic curve based cipher suites. In this paper, we proposed a set of client-server communication protocols using certificateless Public Key Infrastructure (PKI) based on ECC. Then the protocols have identity based authentication without using bilinear maps, session key exchange and secure message transfer. Moreover, we showed that the protocols are lightweight and are designed to serve multiple applications.

Keywords: Certificateless public key cryptography, elliptic curve cryptography, jacobi identity, message preprocessing, lie algebras, challenge-response