

ECIW 2007
The 6th European
Conference on Information
Warfare and Security
Defence College of Management and
Technology, Shrivenham, UK
2-3 July 2007

Edited by

Dr Dan Remenyi
Trinity College Dublin, Ireland

Copyright The Authors, 2007. All Rights Reserved.

No reproduction, copy or transmission may be made without written permission from the individual authors.

Papers have been double-blind peer reviewed before final submission to the conference. Initially, paper abstracts were read and selected by the conference panel for submission as possible papers for the conference.

Many thanks to the reviewers who helped ensure the quality of the full papers.

ISBN: 978-1-905305-49-0 Cd

Published by Academic Conferences Limited
Reading
UK
44-118-972-4148
info@academic-conferences.org

ECIW 2007

Contents

Paper Title	Author(s)	Guide Page	Proceedings Page
Preface		v	v
Biographies of Conference Chairs, Programme Chair, Keynote Speaker and Mini-track Chairs		vii	vii
Biographies of contributing authors		viii	viii
Minimizing Network Risk with Application to Critical Infrastructure Protection	<i>Waleed Almannai and Ted Lewis Naval Postgraduate School, Monterey, CA, USA</i>	1	1-16
A Proposed Cyber-terrorism SCADA Risk Framework Concept for Australia	<i>Christopher Beggs¹ and Matt Warren² ¹Monash University, Berwick, Victoria, Australia ²Deakin University, Burwood, Victoria Australia</i>	2	17-26
The Layered Security Model: Analysis of Systems from the Conceptual, Logical and Physical Viewpoints	<i>Clive Blackwell Information Security Group University of London, Egham, UK</i>	3	27-36
A Roadmap Towards Content Based Information Security	<i>Catharina Candolin¹ and Mikko Kiviharju² ¹The Finnish Defence Forces, Helsinki, Finland ²The Finnish Defence Forces, Riihimäki, Finland</i>	4	37-46
The Design of Information Security Management Systems for Small-to-Medium Size Enterprises	<i>Elizabeth Coles-Kemp and Richard Overill King's College London, Strand, London, UK</i>	5	47-54
Developing Information Security Culture in Small and Medium Size Enterprises: Australian Case Studies	<i>Sneza Dojkovski, Sharman Lichtenstein and Matthew Warren School of Information Systems, Deakin University, Australia</i>	6	55-66
Fighting Shadows and Ignoring the Elephant: Lessons for PsyOps Strategy from Organisational Responses to Risk and Crisis	<i>Mils Hills Analytic Red LLP, Milton Keynes, UK</i>	7	67-76
The Forensic Utility of Detecting Disruptive Electromagnetic Interference	<i>Richard Hoad¹ and Iain Sutherland² ¹QinetiQ Ltd, Cody Technology Park, Farnborough, UK ²University of Glamorgan, Pontypridd, Wales</i>	8	77-88
Strategically Leading for Identity in War on Terror– The Transformation and Meaning (Lessness) of Motivation in Western Male Militarized Culture	<i>Aki-Maur Huhtinen National Defence University, Helsinki, Finland</i>	9	89-98

Paper Title	Author(s)	Guide Page	Proceedings Page
Lethal Mutation Versus Messianic Singularity: "A New Multidimensional Perspective on the Reciprocal Function of Digital Information Technologies as Offensive and Defensive Weapon Systems."	<i>Berg Hyacinthe¹, Mourad Debbabi², Abdeslem Boukhtouta³, Zia Hayat⁴ and Yves Anglade⁵</i> ¹ Florida State University, Tallahassee, Florida, USA ² Concordia University, Montreal, Quebec, Canada ³ Defence Research and Development Canada, Quebec, Canada ⁴ BAE systems, UK ⁵ Florida A&M University, Tallahassee, Florida USA	10	99-108
Security Policies: Making it Work	<i>Anushia Inthiran and Andrew Seddon</i> University College of Technology and Innovation, Kuala Lumpur, Malaysia	11	109-114
Digital Anti Forensics: Tools and Approaches	<i>Hamid Jahankhani¹, Bouras Anastasios¹ and Kenneth Revett²</i> ¹ University of East London, UK ² University of Westminster, UK	12	115-120
The Role of Dynamic Security Policy in Military Scenarios	<i>Helge Janicke¹ and Linda Finch²</i> ¹ De Montfort University, Leicester, UK ² General Dynamics United Kingdom Limited, Newbridge, UK	13	121-130
Critical Infrastructure Protection – Developments Since the Inception of the Concept	<i>Andrew Jones</i> BT Security Research Centre, UK Edith Cowan University, Australia	14	131-138
A Novel Approach to Offline Signature Verification using Gaussian Empirical Rule	<i>Dakshina Ranjan Kisku, Ajita Rattani and Phalguni Gupta</i> Indian Institute of Technology Kanpur, India	15	139-150
Simplifying Security Management of Cross-Organisation Collaborative Decision Making	<i>Ulrich Lang and Rudolf Schreiner</i> Object Security Ltd., St John's Innovation Centre, Cambridge, UK	16	151-162
Development of Command and Control in Air Force – Transformation or Gradual Evolution	<i>Martti Lehto¹ and Pertti Kuokkanen²</i> ¹ Finnish Air Force Headquarters, Tikkakoski, Finland ² Defence Command Finland Helsinki, Finland	17	163-170
A Subliminal Channel Scheme Based on Random Numbers Approximation Sequence	<i>Gang Luo¹, Xing-ming Sun^{1,2}, and Jun-wei Huang¹</i> ¹ Hunan University, Changsha, China ² University College London, London, UK	18	171-180
The Role of Knowledge Centres in Information Warfare	<i>Károly Nagy</i> The Hungarian Prime minister's Office, Budapest	19	181-186

Paper Title	Author(s)	Guide Page	Proceedings Page
Body Movement Identification (BMI)	<i>Dan Ophir, Itzhak Schlissel and Benyamin Tamir Faculty of Scientific Studies, the College of Judea and Samaria, Ariel, Israel</i>	20	187-196
A Flexible Threat Model for Computer Based Systems	<i>Venkat Pothamsetty Critical Infrastructure Assurance Group, Cisco Systems ,Austin, Texas, USA</i>	21	197-206
Benchmarks for Critical Infrastructure Systems Modelling	<i>Graeme Pye and Matthew Warren School of Information Systems, Deakin University, Geelong, Australia</i>	22	207-216
An Investigation into the Suitability of Unidirectional Networks for use in e-Commerce Security	<i>Vanja Radjenovich and Jill Slay University of South Australia, Mawson Lakes, South Australia</i>	23	217-226
Scenario Analysis using Out-of-Line Firewall Evaluation Framework	<i>Lionel Saliou, William Buchanan, Jamie Graves, and Jose Munoz Napier University,Edinburgh, UK</i>	24	227-236
Hybrid Intelligent Intrusion Detection/Prevention System using Fuzzylogic and Data Mining	<i>Bharanidharan Shanmugam and Norbik Bashah Idris University Teknologi, Kuala Lumpur, Malaysia</i>	25	237-244
An Intrusion Detection Countermeasure for 4th-Generation TLB-Assisted Rootkits and Self-Hashing Attacks	<i>Dave Sharp and Carlisle Adams University of Ottawa, Ottawa, Ontario, Canada</i>	26	245-252
Greater is our Terror of the Unknown the Diasporic Internet Networks and their Inference with Global Security	<i>Marina Shorer-Zeltser and Galit . Ben-Israel Institute for Identity research in Media and Politics, Israel</i>	27	253-262
SQL Infections Through RFID	<i>Anthonius Sulaiman, Vignesh Venkataramana, Srinivas Mukkamala and Andrew Sung Institute for Complex Additive Systems Analysis, NM, USA</i>	28	263-272
Information Technologies for the Information Agent	<i>Sérgio Tenreiro de Magalhães¹, Henrique Santos¹, Leonel Duarte Santos¹, Kenneth Revett² and Paulo Viegas Nunes³ ¹University of Minho, Guimarães, Portugal ²University of Westminster, London, UK ³Military Academy Research Center (CINAMIL), Lisboa, Portugal</i>	29	273-280
Malicious Software and System Damages: Is There a Case for Liability of Software Vendors?	<i>Theodore Tryfonas, Paul Owen and Paula Thomas Faculty of Advanced Technology, University of Glamorgan, U K</i>	30	281-290

Paper Title	Author(s)	Guide Page	Proceedings Page
Network Forensics of SSL/TLS Encrypted Channels	<i>Meng-Da Wu and Stephen Wolthusen Information Security Group, Royal Holloway, University of London, UK</i>	31	291-302
Lexical Natural Language Steganography Systems with Human Interaction	<i>Brecht Wyseur, Karel Wouters and Bart Preneel K.U. Leuven, Heverlee, Belgium</i>	32	303-312
Experiential Operations: An Information-Based Operational Management Approach for Managing National Security Operations	<i>Ken Webb Edith Cowan University, Perth, Western Australia</i>	33	313-320
Public Key Usage Model in Converge Network	<i>Lee Fueng Yap¹ and Andy Jones^{2,3} ¹British Telecommunications plc., Asian Research Centre, Kuala Lumpur, Malaysia ²British Telecommunications plc., Security Research Centre, Ipswich, UK ³Adjunct, Edith Cowan University, Perth, Australia</i>	34	321-326
Investigating the Evasion-Resilience of Network Intrusion Detection Systems	<i>Jarle Ytreberg and Maria Papadaki University of Plymouth, Plymouth, UK</i>	35	327-334
Identifying Computers Hidden Behind a NAT using Machine Learning Techniques	<i>Ori Zakin, Metal Levi, Yuval Elovici, Lior Rockach, Nir Shafir, Guy Sinter and Ofer Pen Ben-Gurion University of the Negev, Beer-Sheva, Israel</i>	36	335-340
NATO's war on Terror and the Electronic Medium: A Retrospective Analysis on Combating Terrorist linsurgence	<i>Marios-Panagiotis Efthymiopoulos¹ and Josef Demergis² ¹University of Crete, Greece ²University of Macedonia, Greece,</i>	37	341-348
Corporate Data Loss at Thirty Thousand feet	<i>Grigorios Fragkos, iain Sutherland, and Konstantinos Xynos University of Glamorgan, Wales</i>	38	Abstract only

Preface

The Sixth European Conference on Information Warfare and Security (ECIW 2007) is hosted by the Defence College of Management and Technology at Shrivenham in the UK this year. The Conference Chair is Debi Ashenden from the Defence College and the Programme Chair is Iain Sutherland from the University of Glamorgan.

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

The opening keynote "War of the web" this year is given by Brian Collins, Defence College of Management and Technology, Cranfield University and the second day will be opened by Martin Gill, Perpetuity Research & Consultancy International, UK who will address the subject of "How do offenders assess security?".

A key aim of the conference is about sharing ideas and meeting the people who hold them. The range of papers will ensure an interesting two days. The topics covered by the papers this year illustrate the depth of the information operations' research area, with the subject matter ranging from the highly technical to the more strategic visions of the use and influence of information. To further enhance the networking opportunities Ken Webb from Edith Cowan University in Perth, Australia will lead a participatory session on Monday afternoon.

With an initial submission of 59 abstracts, after the double blind, peer review process there are 37 papers published in these Conference Proceedings. These papers come from all parts of the globe including Australia, Belgium, Canada, China, Finland, Germany, Greece, Hungary, India, Ireland, Israel, Malaysia, the United Kingdom (England, Scotland and Wales), and the United States.

I wish you a most interesting conference.

Dan Remenyi
dan.remenyi@tcd.ie
July 2007

Conference Executive:

Debi Ashenden, Defence College of Management and Technology, Shrivenham, UK
John Biggam, Glasgow Caledonian University, UK
Andrew Blyth, University of Glamorgan, Wales, UK
Steve Furnell, University of Plymouth, UK
Aki Huhtinen, Finnish Defence Forces, Finland
Andy Jones, British Telecom, UK
David Llamas, University of St. Andrews, Scotland, UK
Jari Rantapelkonen, University of Helsinki and Finnish Defence Forces, Finland
Jill Slay, University of South Australia
Iain Sutherland, University of Glamorgan, UK

Conference Committee:

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

Abiola Abimbola, (Napier University, Scotland, UK); Gail-joon Ahn, (University of North Carolina at Charlotte, USA); Muhammad Arif, (Allama Iqbal Open University, Lahore, Pakistan); Leigh Armistead, (Edith Cowan University, Australia); Colin Armstrong, (Curtin University, Australia); Debi Ashenden, (Defence College of Management and Technology, UK); Eelker Bakker, (Ministry of the Interior and Kingdom Relations, The Netherlands); Richard Baskerville, (Georgia State University, USA); Elisa Bertino, (CERIAS, Purdue University, USA); Maumita Bhattacharya, (Charles Sturt University, Australia); John Biggam, (Glasgow Caledonian University, UK); Andrew Blyth, (University of Glamorgan, UK); Svet Braynov, (University of Illinois at Springfield, USA); Jérôme Carrère, (Telindus, Luxembourg); Rodney Clare, (EDS and Open University, UK); Maura Conway, (Dublin City University, Ireland); Noah Curthoys, (Cabinet Office, London, UK); Geoffrey Darnton, (Bournemouth University, UK); Dorothy Denning, (Naval Postgraduate School, USA); Marios Efthymiopoulos, (Special Envoy of the Hellenic Foreign Ministry to NATO, Italy); Jean-Noel Ezingear, (Henley Management College, UK); John Fawcett, (University of Cambridge, UK); Elena Ferrari, (University of Como, Italy); Steven Furnell, (University of Plymouth, UK); Javier Garcia Villalba (Complutense University of Madrid, Spain); Kevin Gleason, (KMG Consulting, USA); Stefanos Gritzalis, (University of the Aegean, Greece); Barry Horne, (QinetiQ TIM, UK); Ulrike Hugl, (University of Innsbruck, Austria); Aki Huhtinen, (Finnish Defence Forces, Finland); Bill Hutchinson, (Edith Cowan University, Australia); Hamid Jahankhani, (University of East London, UK); Andy Jones, (British Telecom, UK); James Joshi, (University of Pittsburgh, USA); Maria Karyda, (University of the Aegean, Greece); Auli Keskinen, (National Defence College, Finland); Spyros Kokolakis, (University of the Aegean, Greece); Prashant Krishnamurthy, (University of Pittsburgh, USA); Dan Kuehl, (National Defence University, USA); Peter Kunz, (DaimlerChrysler, Germany); Pertti Kuokkanen, (University of Helsinki, Finland); Takakazu Kurokawa, (National Defence Academy, Japan); Rauno Kuusisto, (Finnish Defence Forces, Finland); Tuija Kuusisto, (Finnish Defence Forces, Finland); Thomas Lauer, (Oakland University, USA); Michael Lavine, (John Hopkins University, USA); Tara Leweling, (Naval Postgraduate School, USA); Sharman Lichtenstein, (Deakin University, Australia); David Llamas, (University of St. Andrews, UK); Bill Martin, (RMIT University, Australia); Keith Martin, (Royal Holloway, University of London, UK); Don Milne, (Buckinghamshire Chilterns University, UK); Yonathan Mizrahi, (University of Haifa, Israel); Evangelos Moustakas, (Middlesex University, UK); Shishir Nagaraja, (University of Cambridge, UK); Juhani Paavilainen, (University of Tampere, Finland); Maria Papadaki, (University of Plymouth, UK); Tim Parsons, (BAE Systems, UK); Michael Pilgermann, (University of Glamorgan, UK); Fred Piper, (Royal Holloway, University of London, UK); Jari Rantapelkonen, (University of Helsinki and Finnish Defence Forces, Finland); Raphael Rues, (Digicomp Academy, Switzerland); Henrique Santos, (University of Minho, Portugal); Jill Slay, (University of South Australia); Anna Squicciarini, (University of Milano, Italy); Iain Sutherland, (University of Glamorgan, Wales, UK); Jonas Svava Iversen, (Danish Broadcasting Corporation, Denmark); Phil Taylor, (University of Leeds, UK); Theodore Tryfonas, (University of Glamorgan, UK); Patrick Tyrell, (Royal Navy (retired), UK); Craig Valli, (Edith Cowan University, Australia); Rudi Vansnick, (Internet Society, Belgium); Stilianos Vidalis, (Newport Business School, UK); Teemupekka Virtanen, (Helsinki University of Technology, Finland); Michael Walker, (Vodafone, UK); Mat Warren, (Deakin University, Australia); Peter Wild, (Royal Holloway, University of London, UK); Patricia Williams, (Edith Cowan University, Australia); Tom Wilsdon, (University of South Australia); Simos Xenitellis, (Royal Holloway, University of London, UK); Omar Zakaria, (University of Malaya, Malaysia).

Biographies of Conference Chairs, Programme Chair and Keynote Speaker

Conference Chair

Debi Ashenden is a Senior Research Fellow within the Defence College of Management and Technology at Cranfield University. Prior to taking up this post she was a Managing Consultant within QinetiQ's Trusted Information Management Department (formerly the Defence Evaluation Research Agency). Specialising in information assurance in general, and risk assessment in particular, other specific areas of interest include building trust for information sharing, governance processes for information assurance and information security awareness. Debi has worked extensively across government, defence and the finance sector as a consultant and her work concentrates on understanding the role of individuals in ensuring that security risks are mitigated. Debi has had a number of articles on information security published, presented at a range of conferences and has co-authored a book for Butterworth Heinemann 'Risk Management for Computer Security: Protecting Your Network & Information Assets'. Her current research examines the practice of information operations using discourse analysis.



Programme Chair

Dr Iain Sutherland is a member of the Information Security Research Group and Senior Lecturer in the Faculty of Advanced Technology at the University of Glamorgan. He has been involved in a variety of research projects in the area of information security including secure XML transactions and reverse engineering metrics. Dr. Sutherland's main field of interest is computer forensics. He currently maintains Glamorgan University's Forensics Computing Laboratory, and has acted as a consultant and Expert Witness on civil and criminal cases.



Keynote Speaker



Professor Brian Collins is Professor of Information Systems at DCMT, Cranfield University, Shrivenham. He has also recently been appointed as Chief Scientific Adviser to the Department of Transport. His current interests centre on the design and engineering of structured, secure and dependable knowledge and information management processes and systems using next generation information and communications technology. He was an adviser to the House of Commons Science and Technology Committee on ID Cards and was special adviser to the Home Office Select Committee on the same subject. He was technical adviser to the DTI on a Foresight Cybertrust and Crime Prevention project and has been an Associate Fellow of RIIA Chatham House on Future Global Security issues. He was

International Director of Information Technology at Clifford Chance, Head of Information Systems at the Wellcome Trust and at GCHQ was Chief Scientist and Director of Science and Technology. He is a graduate of Oxford University.

Keynote Speaker

Professor Martin Gill is Director of Perpetuity Research and Consultancy International and a Professor of Criminology at the University of Leicester. He has published over 100 journal and magazine articles and 11 books including Commercial Robbery, CCTV, and Managing Security and the Handbook of Security. He is co-editor of the Security Journal and founding editor of Risk Management: an International Journal. Professor Gill is a Fellow of The Security Institute, a member of the Risk and Security Management Forum, the Company of Security Professionals (and therefore a Freeman of the City of London), the ASIS International Foundation Board, an overseas representative on the ASIS International Academic Programs Committee and the ASIS International Security Body of Knowledge Task Force. With PRCI colleagues he is currently involved with a range of projects related to different aspects of crime in organizations and private security, this includes shop theft, frauds, staff dishonesty, burglary reduction, robbery, the effectiveness of security measures, money laundering, policing, violence at work, to name but a few. He also led the Home Office national evaluation into the effectiveness of CCTV.



Biographies of contributing authors (in alphabetical order)

Waleed Almannai is a PhD Candidate, MOVES (Modeling, Virtual Environment, and Simulation) Institute, Naval Postgraduate School, Monterey, California

Christopher Beggs has been researching cyber-terrorism at Monash University for the last 4 years. And is currently at the completion of his PHD which has a specific focus towards cyber-terrorism and the threat to Australia. He has also worked on various security and defence projects outside Monash for the Australian government.

Clive Blackwell is currently writing-up his PhD at Royal Holloway, which unites the various existing Internet attack and defence taxonomies. The work can be applied to many other types of security system and can be formalised using graph theory. His other interests include Internet architecture, critical infrastructure protection and Trusted computing. He holds a BSc in Mathematics from Warwick University, and a BSc in Computer Science and an MSc in Information Security from Royal Holloway.

Catharina Candolin currently works as a Chief of Information Management at the Defence Staff of the Finnish Defence Forces. Her main areas of interest include information warfare, network-enabled defence, and security.

Lizzie Coles-Kemp has worked in information security since 1989, working in a range of both technical and management posts. Lizzie now works for a UK certification body auditing to both ISO 27001 and tScheme and for the Information Security Group, Royal Holloway, as tutor and module leader. She is completing a PhD in information security management at King's College, London.

Yuval Elovici is a senior lecturer at the department of Information Systems Engineering, Ben-Gurion University. He holds B.Sc and M.Sc degrees in Computer and Electrical Engineering from the Ben-Gurion University of the Negev, and Ph.D in Information Systems from Tel-Aviv University. His main research interests are information warfare, data mining, information retrieval, and detection of malicious code. Currently he is the director of Deutsche Telekom Laboratories at Ben-Gurion University.

Grigorios Fragkos has a Diploma and a B.Sc. in Software Engineering. He has a M.Sc. in Computer Systems Security. Currently, he is part of the Information Security Research Group (ISRG) of the University of Glamorgan undertaking his Ph.D. research in the area of Real-Time Threat Assessment of Intrusion Detection System's (IDS) data

Richard Hoad MSc. C.Eng, C.Sci, MInstP, MIET, MIEEE is a Technical Leader within the QinetiQ Electromagnetic and Environmental Services (EMES) team. His specific areas of interest include, Electromagnetic (EM) aspects of Information Security, EMC and EM hardening and protection of installations. Richard has many years of experience of EM Security issues including EM protection design and verification of large installations predominantly within the military environment. Richard is the secretary of IEC SC77C, an International committee developing standards for the protection of installations against the effects of High Power Transient Phenomena. Richard is also a part-time PhD. Student at the University of Glamorgan.

Berg Hyacinthe, Ph.D. (candidate) is conducting a multidisciplinary research focusing on cyber-olfaction security technologies at Florida State University. Along with a minor in Religious Studies, he holds degrees in several disciplines including Computer Science,

Modern Languages, and Educational Technology. His doctoral profile is symbolically built on Information Warfare, Social Informatics, and Emergent Technologies. He held several U.S government positions (local and state) in the areas of Information Technology. Author of several published patent applications in the U.S., he has a particular interest in futuristic modeling of global defense and security systems.

Anushia Inthiran completed her education at Monash University Melbourne Australia where she studied Computing with a specialism in Computer Technology and obtained a degree with distinction. She then progressed to complete a Masters of Science degree in Technology Management with merit from Staffordshire University United Kingdom. Her interests are in the areas of networking, management of technology, information systems security and computer forensics. Upon completing her degree, she began her career as an analyst programmer, then moved on to become a security analyst at the Information Technology department of Standard Chartered Bank Malaysia. Anushia is now a lecturer and programme leader for Staffordshire University's computing and information technology degree programmes at Asia Pacific Institute of Information Technology / University College of Technology and Innovation Malaysia (APIIT/UCTI). She lectures subjects relating to design of corporate networks, computer security and operating systems. Anushia is also a life time member with Golden Key National Honour Society.

Andy Jones is the Head of Security Technology research at the BT Security Research Centre. He is also a visiting adjunct at Edith Cowan University in Australia. His background research is into information Security, Information Warfare and computer forensics.

Dakshina Ranjan Kisku received his BEng and MEng degrees in Computer Science and Engineering from Jadavpur University India in 2001 and 2003 respectively. Currently he is research associate at Indian Institute of Technology Kanpur and carrying on research activities for PhD degree. His research interests include pattern recognition, machine learning, image processing and biometrics.

Ulrich Lang, CEO of Object Security - Ph.D. Univ. Cambridge Computer Lab (Security Group) on middleware security; M.Sc. Information Security Royal Holloway (Univ. London) on CORBA security; Business Marketing Strategy, Kellogg School of Management (Northwestern Univ.); computer science & management Univ. Munich and Royal Holloway; Author of a middleware security book and many publications; Co-founder of Object Security

Martti Lehto His officer career started in 1978 in Air Force C3 Systems School. He was on a General Staff Officer Course in the National Defence College from 1985 to 1987. The topic of his final study was "Information Security in the Air Command". Then he was appointed the Chief of Signals Office in the Air Force HQ. In 1992 he was transferred to Satakunta Air Command as Chief of the SOC. In the beginning of 1993 he was transferred back to the C3 Systems School, now as the Commandant of the School. After a five-year period at the C3 Systems School he took up the post of the Chief of the C4IS Systems Division of the Air Force HQ. In September 1999 he was posted to the Defence Staff as Deputy Chief of Operations Division. The beginning of 2003 saw him transferred back to the Air Force HQ where he resumed his duties as the Chief of C4IS Systems Division. In January 2007 he is started as Deputy Chief of Staff in FiAF. Colonel Lehto is currently writing a dissertation on "Transformation of management in Network Enable Air Defence" in the Finnish National Defence University.

Luo Gang is a PH.D degree candidate in computer application of Hunan University. His current research interests include information security, steganography and steganalysis .

Olli Mäkinen PhD, defended his theses on Kierkegaard's philosophy and repetition at University of Oulu. At the moment Mäkinen is working as an information specialist and a publisher at University of Vaasa. During the past year Mäkinen has published the following three books in commercial publishers: Academic Writing, Internet and Ethics and Research Ethics. Mäkinen has participated in several conferences dealing with Internet and virtuality and written many articles on the same subject.

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

Karoly Nagy Engineer-economist, Doctor of economic sciences. Experience obtained on information security in the Hungarian Army and various governmental agencies. Worked as a CEO of an information security consulting joint-stock company for more than a decade. Recently interested in cyber security issues. Several studies published on the security of virtual worlds and the global information society.

Dan Ophir Schissel. Ph.D. in Computer Science (72 and 79 Israel, Weizmann Institute of Science); Employment History: Mainly Defense and High-tech Industry: geo-positioning, electro-optic optimizations, . gene's sequence. Accademic: Research and lecturing.

Paul Owen is a PhD student with the Information Security Research Group at the Dept. of Electronics & Computer Systems Engineering, University of Glamorgan. He holds an MSc in Information Security & Corporate Intelligence and a BSc in Computing. His current research interests include high-tech ID theft and mobile forensics. He is an associate member of the British Computer Society.

Maria Papadaki is a Lecturer in Network Security at the University of Plymouth. Prior to returning to academia, she worked as a Security Analyst for Symantec Managed Security Services. Dr Papadaki's current research interests mainly focus around the area of intrusion prevention, detection and response.

Venkat Pothamsetty is a security research engineer in Critical Infrastructure Assurance Group (CIAG), Cisco Systems. His primary research interests include network protocol security, control systems security, security education and physical security. In his earlier role, he is a lead engineer in Security Technologies Assessment team (STAT), Cisco Systems, whose primary responsibility is to systematically evaluate Cisco products for security vulnerabilities. Venkat did his masters in computer security from Wright State Univerity and his master's thesis is titles "A laboratory setup for courses in computer security".

Lionel Saliou received his B.Eng of Electronics & Computer Engineering, along with medals for academic achievement and best electronic design, from Napier University in 2003. He currently is set to complete his Ph.D in fall 2007, at Napier School of Computing. His research interests include computer network security, security policies, and dynamically reconfigurable network devices.

Bharanidharan Shanmugam is currently pursuing towards Phd in Network Security. His interests include Network Security and management, Forensics and network infrastructure development.

Dave Sharp has been active professionally and academically in the area of secure software, steganography, and other covert activities for close to 10 years working in both the private sector and different agencies. He has recently taken his interests to the next level in pursuing a Ph.D. in the area of provably secure software.

Marina Shorer-Zeltser is a PhD Candidate at the Department of Political Science at Tel-Aviv University. She teaches at the Department of Israel and the Middle East at Judea and Samaria College at Ariel and at the Department of Public Policy at Beit-Berl College.

Jill Slay holds a degree in Mechanical Engineering, graduate diplomas in applied computing and further education and a PhD from Curtin University of Technology. Jill spent several years as an engineer in the UK before beginning a career in applied computing and spent many years living and working in Asia before settling in Australia. She is a fellow of the Australian Computer Society and a member of the Institute of Electrical and Electronic Engineers and is a Certified Information Systems Security Professional. Currently, she carries out collaborative research in Forensic Computing and IT Security with industry and government partners in Australia and focuses on 3 major grant funded projects in varying issues in Forensic Computing. She leads the Systems For Safeguarding Australia Theme of the Defence and Systems Institute at the University of South Australia, where she also heads the Forensic Computing Lab. She is also an affiliate faculty member at Idaho State University and is a Board Member of the Colloquium on Information Systems Security Education – Asia Pacific. Jill has published one book and numerous book chapters, journal articles and research papers in complex systems, CIP, information assurance and forensic computing. She is also a member of several editorial boards and conference committees.

Sérgio Tenreiro de Magalhães teaches Computing Systems and Computer Technologies in the University of Minho, Portugal and he is a researcher in the group of Information Systems Security, mainly in biometric technologies. He has also collaborated in the project “Security of the Digital Data in The Armed Forces Network”, a project with the Portuguese Army and Ministry of Defense.

Matt Warren is the Head of School at the School of Information System, Deakin University, Australia. He has gained international recognition for his scholarly work in the areas of Information Security, Risk Analysis, Electronic Commerce and Information Warfare. He has authored/co-authored over 180 books, book chapters, journal and conference papers.

Ken Webb is a graduate of the Royal Military College and qualified Commando and Special Air Service (SAS) Regiments’ officer, has just completed sponsored doctorate level research examining how to enhance national security from asymmetric threats,

particularly terrorism and information warfare. He is also the Counter-Terrorism Research Leader for the Australian Government's Research Network for a Secure Australia.

Meng-Da Wu received a BSc from Central Police University (Taiwan, 2004). He then joined the Information Department of Coast Guard Administration in Taiwan. He was awarded CISSP(Associate), CHFI(Computer Hacking Forensic Investigation), and CEH(Certified Ethical Hacker). He is currently studying for a Ph.D degree. His research interests include digital forensics, in particular network evidence issues.

Brecht Wyseur is a PhD student at the research group COSIC of the university of Leuven, Belgium. He is an expert in white-box cryptography, a novell technique to hide cryptographic keys in block cipher implementations (e.g. DES and AES). The author is furthermore involved in designing and securing DRM architectures.

Lee Fueng Yap is a researcher at British Telecom Asian Research Centre. Formerly she was with Intel Corporation as Technical Marketing Engineer supporting IXP2000 Series Network Processors. Her research interests include mobile forensic, network security, authentication, and public key cryptography. She received a Bachelor Degree in Electronic Engineering Major in Computer and a Master in engineering from Multimedia University, Cyberjaya Malaysia. Yap is also a certified Computer Hacking and Forensic Investigator .

Minimizing Network Risk with Application to Critical Infrastructure Protection

Waleed Almannai and Ted Lewis

Naval Postgraduate School, Monterey, CA, USA

Abstract: The risk posed by natural disasters and terrorist attacks on critical infrastructure sectors such as the power grid, water supply, and telecommunication systems can be modeled by network risk. However, there is currently no definition of risk for a network. We propose a new definition of network risk and apply it to optimal allocation of a fixed budget such that network risk is minimized for two cost models: Linear and non-linear. We show that in both cases, risk minimization is achieved by ranking nodes and links according to their damage value and degree sequence. Furthermore, we identify the critical nodes and links as those with the highest allocation of funds.

Keywords: Vulnerability, allocation cost, elimination cost, availability, critical infrastructure, network risk

A Proposed Cyber-terrorism SCADA Risk Framework Concept for Australia

Christopher Beggs¹ and Matt Warren²

¹Monash University, Berwick, Victoria, Australia

²Deakin University, Burwood, Victoria Australia

Abstract: Terrorist groups are in theory currently using information and communication technologies (ICTs) to orchestrate their conventional attacks. More recently, terrorists have been developing a new form of capability within the cyber arena to coordinate cyber based attacks. This paper examines a proposed cyber-terrorism SCADA risk framework concept. The paper proposes a conceptual framework which is designed to measure and protect the threat of cyber-terrorism against SCADA systems within Australia. The findings and results of a focus group will be examined to help validate the framework concept.

Keywords Cyber-terrorism, cyber-capability, SCADA, framework, security risk

The Layered Security Model: Analysis of Systems from the Conceptual, Logical and Physical Viewpoints

Clive Blackwell

Information Security Group University of London, Egham, UK

Abstract: Most security models are only suitable for limited problem domains, and are incomplete, as they do not consider all the ways security issues can arise. We have developed a practical security model that can be used to analyse systems more systematically, match more faithfully to their requirements, and which has widespread application. The model has three layers, which are the semantic (involving people), logical (computers) and physical layers including the relationships and interactions between them. This allows the analysis of systems in their entirety including human and physical factors, not just as technical systems. The model also has a horizontal constituent to represent the separate conceptual scope and connectivity of systems and entities at different layers. The model is intended to help in analysing, designing and configuring systems that can possibly be compromised at all three layers. It has application to broad problem domains such as critical infrastructure protection and specific business contexts such as banking applications. In addition, it can be used on a smaller scale to analyse components of systems or to investigate specific vulnerabilities. We examine the system of credit card transactions on the Internet to demonstrate the benefits of the model.

Keywords: Security model, architecture, fraud, financial transaction

A Roadmap Towards Content Based Information Security

Catharina Candolin¹ and Mikko Kiviharju²

¹The Finnish Defence Forces, Helsinki, Finland

²The Finnish Defence Forces, Riihimäki, Finland

Abstract: Content based information security (CBIS) as a concept refers to the possibility to protect the information at its source and to integrate access control in a managed way. The need for CBIS emerged as most armed forces have to deal with several different network environments with different security classifications. This becomes a problem both with respect to cost efficiency and usability. Deploying CBIS, however, would make it possible to rely on only one physical network while maintaining several logical environments on top. As the information is encrypted at its source according to its classification level and “need to know” criteria, then access control is about managing who is able to decrypt the information and under what circumstances. This means that the information, in its encrypted form, can be freely distributed over the physical network. Furthermore, the granularity of information access can be controlled in such a way that e.g. a document may contain parts with various security classifications; the user is able to see only the parts to which his classification level allows. This paper defines CBIS as part of a functional security architecture and investigates how information (a document and its metadata) consisting of multiple parts, each having their specific requirements to access control, integrity and non-repudiability, can be cryptographically constructed. The cryptographical construction is necessary, since the document is distributed freely without an active system enforcing security properties. A large part of the document security management procedures is related to key management. The paper outlines, how identity based PKI can efficiently be used to implement document life cycle management for confidentiality, integrity and non-repudiability.

Keywords: Content based information security, access control, key management, identity based PKI, XML

The Design of Information Security Management Systems for Small-to-Medium Size Enterprises

Elizabeth Coles-Kemp and Richard Overill
King's College London, Strand, London, UK

Abstract: Information security management systems (ISMSs) are often regarded as unnecessarily bureaucratic and for small-to-medium size enterprises (SMEs) they can be so bureaucratic that certification to information security management standard ISO 27001 becomes unrealistic. The bureaucracy arises largely as a result of misinterpretation of the standard and results from poor information security management process design and the use of inappropriate language in the risk assessment phase. ISO 27001 mandates the implementation of the following information security management processes: risk assessment, risk treatment, management review, internal audit, training and awareness, and incident management. However, in a SME these processes can be combined in a number of different ways to reduce the bureaucratic overhead and yet still construct an ISO 27001 compliant management system. The bureaucratic burden can be further reduced by tight implementation within the existing business processes. In particular, the bureaucracy of risk assessment can be reduced in two ways: by using linguistic metaphors appropriate for SMEs instead of the specialist language that is traditionally employed for information security risk assessment, and by combining risk assessment with a reflexive management review process. This paper presents a number of models for combining information security management processes and provides a number of case studies to show how these combined information security management processes can be implemented within standard business processes. The paper also offers a taxonomy of linguistic metaphors designed to be used in information security risk assessment in the SME.

Keywords: Information security management system; ISMS, small-to-medium size enterprise, SME

Developing Information Security Culture in Small and Medium Size Enterprises: Australian Case Studies

**Sneza Dojkovski, Sharman Lichtenstein and Matthew Warren
School of Information Systems, Deakin University, Australia**

Abstract: Ideally, information security practices in Small and Medium Size Enterprises (SMEs) should be non-intrusive and intuitive to employees. Previous research has largely overlooked the development of an information security culture for SMEs, and the potential influence of the national context in which the companies operate. This paper provides insights on the key issues involved in developing an information security culture in Australian SMEs from case studies of three Australian SMEs. The paper provides understandings of business owner and employee viewpoints on the issues, and suggests that the main challenges in developing such a culture relate to business owner awareness and countering the Australian laissez-faire attitude of employees. Implications for practice and theory are discussed.

Keywords: Information security culture; small and medium size enterprises; information security management

Fighting Shadows and Ignoring the Elephant: Lessons for PsyOps Strategy from Organisational Responses to Risk and Crisis

Mils Hills

Analytic Red LLP, Milton Keynes, UK

Abstract: yOps activities seek to shape - or force - specific, desired decision outcomes. The concept of unrestricted (total) warfare makes all areas of modern life a target-rich environment for business or other adversaries. Business continuity (including crisis management, risk assessment and resilience) are just some of the areas that provide insight into how planning and operations of organisational structures and processes are disrupted by uncertainty, incomplete and inconsistent information, situational delusion and self-inflicted wounds. The cultural and psychological context of an organisation and its constituent teams (at operational or strategic level) offer all manner of exploit opportunities to adversaries. Direct and indirect government dependence on the private sector makes no one immune from inclusion in conflict. Beyond the remit of technical countermeasures and the control of pre-emptive and formal plans and training, the argument is that the deliberate targeting of the human factor by determined and creative adversaries could produce effects of strategic significance to all sectors of the economy and administration.

Keywords: Business continuity, crisis management, resilience, decision-making, uncertainty, PsyOp

The Forensic Utility of Detecting Disruptive Electromagnetic Interference

Richard Hoad¹ and Iain Sutherland²

¹QinetiQ Ltd, Cody Technology Park, Farnborough, UK

²University of Glamorgan, Pontypridd, Wales

Abstract: The intentional malicious use of Electromagnetic (EM) interference as a way to compromise Information Security (INFOSEC) and commit a criminal act is an emerging technical concern. High power radio frequency generators possess the ability to disrupt, and deny service to information systems and processes by adversely affecting sensitive electronic hardware. The manifestation of such an attack form is ambiguous and open to misinterpretation and as such the attack or crime may go undetected, or be incorrectly diagnosed. Further, incorrect diagnosis of an EM disruption incident may lead to an incorrect or inappropriate response which could lead to magnification of the impact with potential cost penalties. An Electromagnetic Disruption Detection System (EMDDS) prototype has been developed similar in function to conventional cyber Intrusion Detection Systems (IDS). The EMDDS raises an alarm when hostile activity, EM disruption, is taking, or has taken place. This paper discusses; EM disruptive threat types; the impact on INFOSEC; the potential types of criminal activity; the merits of detection; and the application of the EMDDS to a forensic investigation and for incident response.

Keywords: Electromagnetic pulse weapons, forensics

Strategically Leading for Identity in War on Terror– The Transformation and Meaning (Lessness) of Motivation in Western Male Militarized Culture

Aki-Mauri Huhtinen

National Defence University, Helsinki, Finland

Abstract: In general, the understanding and self-awareness of the male and female roles are the main elements of ideas of value also in wars and conflicts. Strategic communication has two targets: its own military culture and global media audience. This article tries to bring up identity phenomena, which have often remained merely unconscious effects on an idea of the character of the war. The motivation of the global audience and single soldiers was a central part of perception management in the success of the strategic leadership and management in the militarized western culture. The military culture has generally moved from the area of the war to an area in which the image of the war is created by military culture itself. Strategic Communications and Military Psychological Operations (PSYOP) are based on a Cold War construct that has not been significantly overhauled since the end of that era. Today's most pressing challenge, the Global War on Terrorism (GWOT) requires a different solution set. The Quadrennial Defense Review, the Information Operations Roadmap, the National Strategy for Combating Terrorism and the Report of the 9/11 Commission all recognize this fact. But the soldiers are still more dependent on political support and economic resources. For example, persuasive language in propaganda is not a new phenomenon in warfare, although its form adapts to the technology. An advertising rhetoric is becoming a part of military language. Also protecting identity – western, male, wealth - has been a central part of fighting the industrial war in the first half of the 19th century and also on terror through citizenship policies and practices. The war on terror has largely been fought in the public eye, through images of male politicians and soldiers waging war in defence of their nations and on behalf of the “civilized world”. For example, one of the three main themes in President Bush’s administration was the liberation of Arabic women under the Taleban regime. The character of the war has changed more and more in the direction in which soldiers meet civilians and other opponents, not other soldiers. This change requires a new image and brand of military culture. In such a case there is tension built inside the soldier culture, which will lead to psychological difficulties and refusal of battle if the situation drags on. A group of soldiers that has lost motivation begins to become passive and to avoid battle.

Keywords: Military culture, sex, gender, war on terror, psychological operations, identity security

Lethal Mutation Versus Messianic Singularity: “A New Multidimensional Perspective on the Reciprocal Function of Digital Information Technologies as Offensive and Defensive Weapon Systems.”

Berg Hyacinthe¹, Mourad Debbabi², Abdeslem Boukhtouta³, Zia Hayat⁴ and Yves Anglade⁵

¹**Florida State University, Tallahassee, Florida, USA**

²**Concordia University, Montreal, Quebec, Canada**

³**Defence Research and Development Canada, Quebec, Canada**

⁴**BAE systems, UK**

⁵**Florida A&M University, Tallahassee, Florida USA**

Abstract: This paper presents four (conventional, offensive, unconventional, and defensive) dimensions of the majestic interplay between digital information technologies and revolutionary weapon systems according to a new mutation paradigm. Past, present, and emerging applications of computers-as-weapons are reviewed in parallel with a middleware solution to better anticipate, prepare, and defend against emerging threats and a network security solution that involves a dynamic threat assessment to control risk exposure through a prioritization process. In summary, through this exploratory, prescriptive endeavor, the authors leap beyond the “impact of computers on weapon systems” aphorism to offer an informative discourse on the quiet advantage taken by civilians, paramilitary forces, or terrorist groups to morph (in addition to computers) common substances and apparatus into very lethal weapons.

Keywords: Computers as weapons, computer network security, lethal mutation, nano air vehicles, network centric operations, terrorism, unconventional warfare

Security Policies: Making it Work

Anushia Inthiran and Andrew Seddon

**University College of Technology and Innovation, Kuala Lumpur,
Malaysia**

Abstract: Security policies are often viewed as a document defining explicit rules of do's and don'ts in an organisation. Policies can be created to fulfil various needs and purposes. Organisations now acknowledge benefits of having policies and have started drifting away from using technological means such as firewalls, intrusion prevention systems or biometric devices on their own to protect the organisation. It is believed that the culminated strength of policies and technological devices would indeed increase the immunity of the organisation. On the other hand, organisations will have to realise that having policies does not guarantee protection of its resources and reputation. The entire cycle of conceptualisation, employee involvement, enforcement and amendments will need to be preserved to prevent the organisation from being the victim of the policies wrath. The research was undertaken using literature reviews and an extensive survey. The results of this paper indicate that organisations and the general public are aware of security policies and are able to describe this document, however the questions that remain unanswered are how do you measure the returns of using a security policy and how do we measure the quality of the policy. This paper would be beneficial for beginners as well as experts in the security domain as it provides a holistic view of policies and at the same time attempts to ruffle calm waters by questioning quality performance indicators and standardisation.

Keywords: Security policies, procedures, legislation

Digital Anti Forensics: Tools and Approaches

Hamid Jahankhani¹, Bouras Anastasios¹ and Kenneth Revett²

¹University of East London, UK

²University of Westminster, UK

Abstract: Anti-forensics as a concept is as old as the traditional computer forensics. Someone that commit a punishable action use any possible way to get rid of any evidence connected with the prohibited action. The traditional forensics can have a range of anti-forensics that start from a trivial level (e.g. wiping fingerprints from a gun) and to a level where our fantasy can meet the implementation of an anti-forensic idea (e.g. alteration of DNA left behind in a crime). In digital anti-forensics the same rules exists, with the difference that they are fairly new with little research and development. Although Anti-Forensics is a field under development, however, there are already categories of available tools. This paper aims to present of the some current anti-forensic approaches along with some applicable solutions.

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

The Role of Dynamic Security Policy in Military Scenarios

Helge Janicke¹ and Linda Finch²

¹De Montfort University, Leicester, UK

²General Dynamics United Kingdom Limited, Newbridge, UK

Abstract: The military organisation is dependent on timely access to up-to-date, relevant and trustworthy information in order to conduct its business. Access to information is controlled by the user's security clearance and the classification or protective marking of the data. Whilst it is necessary to preserve data confidentiality and integrity, controls have resulted in strict separation between different levels of security. This regime not only constrains the type and level of information sharing that can be achieved, more critically the speed at which access may be realised is impeded. The military is moving towards Network Enabled Capability (NEC) where the emphasis is on resource sharing within national contingents and on a coalition basis, facilitated by the Network. Future capability is predicated on the core attribute of agility. NEC is expected to enable the dynamic formation of communities of interest and the rapid reorganisation of resources as required by military commanders. This paper tests the assertion that the ability to express, verify and implement flexible security policy is essential to achieve the agility required. The assertion is tested through the practical application of a suitable security policy framework to a small but representative case study, the results of which will be of interest to system architects and decision makers alike.

Keywords: NEC, dynamic, security, policy

Critical Infrastructure Protection –Developments Since the Inception of the Concept

Andrew Jones

BT Security Research Centre, UK

Edith Cowan University

Abstract: The concept of the Critical (National) Infrastructure was introduced to the public arena in the mid 1990s when the USA started to acknowledge that there were a set of facilities and services that, together, provide the elements that were ‘critical’ to the effective running of a country and the wellbeing of its citizens. The range of organisations that were initially included in the US Critical Infrastructure were those facilities and services that provide power, water, fuel supply, communications, transport, the finance sector, government and Public Services. While failure of individual systems may not be significant as long as the service is available to most of the people for most of the time (and some of them at specific times), there is a point at which the failure of one or more of them becomes a threat to the good governance of a nation and the well being of the populace. The fact that there are services and facilities that are critical to the government and the people is not new. During times of civil unrest and wars, it has long been recognised that it is essential to protect things such as food and water supplies. When the ruling classes lived in castles, they recognised that in order to survive, they needed to gather the crops in and bring the herds inside the castle walls and to protect the wells to ensure the supply of potable water if they were to be able to survive a siege.

In more recent times, the police and the armed forces have been used to protect physical installations such as the ports, power plants, railway stations, goods yards and airports. This was a suitable response to the perceived threats to those services and facilities. This is a well established process that provides increased protection to those physical assets that are considered important. What changed in the late 20th century was largely driven by advances in technology and in particular, the Internet, when people started to realise that this protection was not enough. With the connectivity that was taking place it became apparent that it was now possible for an attack to take place without an attacker ever visiting the target. This paper will examine changes that have taken place in the protection of critical infrastructures around the world and new developments since the attacks on the US infrastructure in 2001.

Keywords: Critical national infrastructure, protection

A Novel Approach to Offline Signature Verification using Gaussian Empirical Rule

Dakshina Ranjan Kisku, Ajita Rattani and Phalguni Gupta
Indian Institute of Technology Kanpur, India

Abstract: This paper presents a novel approach to Off-line Signature Verification based on Gaussian empirical rule. The verification module extracts global and local features from the training signature images divided into two sets i.e., s_1 and s_2 . To have high discrimination ability, feature subset selection is done using Gaussian empirical rule. The proposed system calculates mean and standard deviation from the subset s_1 and then considers only the features extracted from s_2 that falls within the third standard deviation of the mean extracted from s_1 . The same process is applied for query image by considering only the corresponding features to the selected features of s_2 . The authenticity of the user is determined if the number of corresponding features in the query set lying within the third standard deviation of the mean of calculated on s_1 , is within some threshold empirically determined. The work reports an increase in the accuracy of the system in consideration to the state of arts. The system is tested on IIT-Kanpur database containing a total of 3600 signatures of 330 individuals showing promising results.

Keywords: Biometrics, pre-processing, global and local features, Gaussian empirical rule, signature verification

Simplifying Security Management of Cross-Organisation Collaborative Decision Making

Ulrich Lang and Rudolf Schreiner

Object Security Ltd., St John's Innovation Centre, Cambridge, UK

Abstract: The development of security-critical large-scale distributed software systems is a difficult and error prone process. As we learnt from practical experiences, it is especially difficult to manually define and manage security policies, for example for access control, with a sufficient level of assurance. The human security administrator is not able to cope with the high complexity of the interactions of the application and the low level, platform specific security policy. Therefore, a new approach is needed to improve the correctness of the security policies, and to make security policies manageable. This is particularly eminent in two areas: service-oriented architecture (SOA) style environments where agility support and reuse (also of policies!) are critical; and in environments where collaborative decision making (CDM) has to be implemented, which typically requires agile secure information sharing (especially sensitive cross-organisation between coalition partners). This paper shows how security engineering can be integrated into a model-driven software development process. In our approach, UML models of the application's functional properties are flexibly augmented with security relevant information. Together with a high level security policy defined by the security administrator, this augmented functional model is then used in an automatic model transformation to generate the platform specific security policy with high assurance. With this approach, which also supports the separation of concerns in model based software engineering, we can automatically generate security-critical applications for different middleware platforms like our SecureMiddleware, which is an extended implementation of the CORBA Components Model with improved support for properties like security. The concepts, platforms and tools presented in the paper are currently used for the development of several large-scale and secure applications, for example for building a Virtual Air-Space Management System with strong security requirements, and within the U.S. Naval Research Lab SINS project.

Keywords: security policy, policy management, cross-organisation security policy, collaborative decision making, model driven architecture, model driven security, secure information sharing, information assurance

Development of Command and Control in Air Force – Transformation or Gradual Evolution

Martti Lehto¹ and Pertti Kuokkanen²

¹Finnish Air Force Headquarters, Tikkakoski, Finland

²Defence Command Finland Helsinki, Finland

Abstract: Development processes in modern armed forces are based on the concept of transformation. Transformation is a process and a mind-set. It is not only about developing new weapons systems; it is also a change that has a significant impact on military doctrines, organizations, capabilities, training, education, and logistics. Its goal is to improve interoperability within a fundamentally joint, network-centric, distributed force capable of using information superiority to make timely and appropriate decisions and then effectively execute the appropriate tasks well within the decision cycle of an opponent.

There are remarkable change points in the evolution of transformation in which a development has given an entirely new direction for a change. Today's transformation was initiated by profound changes in information technology. As to air forces, they are now enjoying unprecedented global possibilities to employ their assets. World War I saw the evolution of air power from a tactical force into an efficacious operational tool while in World War II air power became a decisive factor in battles. Successful land and maritime operations were not possible without air superiority. Has the development of air power reached the point which enables winning a war only by using air power.

A transformation process requires major change inducers. The present change seems to be led by information technology that is primarily intended for non-military purposes. The essential objective of this study is to determine the key factors contributing to changes. Are changes brought about by technology or tactics? A commander wants to have superiority over the capability of his opponent, and this can be created by information superiority and more rapid cycle of decision-making supplemented with analysis patterns. This article provides patterns, discourse, and analyses of air power evolution from the standpoint of command and control.

Keywords: transformation, information technology, command and control

A Subliminal Channel Scheme Based on Random Numbers Approximation Sequence

Gang Luo¹, Xing-ming Sun^{1,2}, and Jun-wei Huang¹

¹Hunan University, Changsha, China

²University College London, London, UK

Abstract: A novel narrowband subliminal channel scheme based on random numbers approximation sequence is presented in this paper. This scheme has a better concealment, and the total efficiency of subliminal messages embedded and recovered exceed 5 times than that of the traditional narrowband subliminal channel schemes. The bandwidth of our subliminal channel only relies on the computing power of subliminal messages receiver. This scheme can not only be used to transfer secret information but also be applied to encryption algorithms to do information deception. This scheme is implemented within ECEIGamal encrypt algorithm and Schnorr signature scheme, and the experimental results are provided.

Keywords: Subliminal channel, steganography, random numbers approximation sequence, bandwidth, computing power, information deception

The Role of Knowledge Centres in Information Warfare

Károly Nagy

The Hungarian Prime Minister's Office, Budapest

Abstract: Below, I present the role of knowledge centres in terms of eliminating and mitigating the threats and risks arising from information warfare and outline its basic function which is to generate more efficiently than ever before, full information from incomplete, empty and false data.

By information warfare I mean deliberate, organized political actions and processes carried out or conducted in order to disrupt, destroy and annul conditions for meeting the needs for information vital for the inhabitants of the community (alliance) of a particular country or countries.

The basic thesis of this presentation is that knowledge centres and their developing global network have a major importance in mitigating the threat arising from information warfare. Organising knowledge centres into a network, the creation of harmony between civil control and state financing, and the network's global nature extending across country-borders seeks the dissolution and the exceeding of such contradictions, a condition of which is the development of a new security culture. The operation of knowledge centres requires interactive supervision for which civil associations should be made responsible.

The development of the global informational society came to a standstill following the events of 11th September 2001. The defence of individual rights has decreased due to the necessary security measures imposed by governments. For solving the security problems occurring on the side of privacy the spread of the new security culture is indispensable. With the promoting of the creation of new security knowledge, the knowledge centres play an important role in the field of the evolution of the new security culture.

Keywords: Knowledge centers, information security issues related to information retaining principle security of the virtual worlds cyber security, new security culture

Body Movement Identification (BMI)

Dan Ophir, Itzhak Schlissel and Benyamin Tamir

Faculty of Scientific Studies, the College of Judea and Samaria, Ariel, Israel

Abstract: Biometrics is nowadays a fast-developing domain (especially after the September 11th events) that facilitates identifying suspects in a crime. Herein we propose a new, complementary approach that may succeed when other conventional methods fail.

This new method is based on the fact that each person has its own manner of walking and moving (dynamic-signature). This observation may be used for (untouched, remote) identification and authentication (verification) of a person who tries to change his identity by disguising himself.

Several mathematical tools have been used for pattern recognition; these include the Fourier transform neural-network algorithms, the Kalman Filter (for prediction), morphological methods, and others. These may be implemented when utilizing the new behavioral biometrics: Body Movement Identification (BMI).

Keywords: Biometrics, behavioural-biometrics, body-language, mathematical-filtering, neural-network, image processing

A Flexible Threat Model for Computer Based Systems

Venkat Pothamsetty

**Critical Infrastructure Assurance Group, Cisco Systems, Austin, Texas,
USA**

Abstract: Threat modeling provides a systematic and repeatable approach for analyzing and assessing the security of systems, such as applications, protocols and devices. In this paper, we present a flexible threat modeling methodology for computer based systems called the 'system based threat model' (SBTM). First, we review the three prominent threat modeling approaches. We then present the difficulties that we faced when we tried to use the present threat modeling approaches for security and threat evaluations. We then describe the SBTM model in detail, continuing on to build the model for computer based systems. We then use the model for solving a few generic problems that security evaluators face. We conclude by evaluating the merits of the model, discuss its drawbacks, and present ideas for potential future enhancements.

Keywords: Threat modeling, security evaluation, attack modeling

Benchmarks for Critical Infrastructure Systems Modelling

Graeme Pye and Matthew Warren

School of Information Systems, Deakin University, Geelong, Australia

Abstract: This paper draws together previous security assessment research and builds upon the current systems modelling research investigation into the application of potential modelling styles that can be applied to model critical infrastructure systems, networks, their inter-relationships and functionality. The emphasis here is to develop appropriate benchmarks as a means of assessment to determine the appropriateness of various systems modelling styles and techniques and their suitability for modelling critical infrastructure systems. The benchmarks are applicable on a number of differing levels to determine the 'best fit' for modelling critical infrastructure systems, to aid in identifying potential system or inter-network vulnerabilities.

Keywords: Critical infrastructure, security, benchmark, systems modelling

An Investigation into the Suitability of Unidirectional Networks for use in e-Commerce Security

Vanja Radjenovich and Jill Slay

University of South Australia, Mawson Lakes, South Australia

Abstract Network security is vital to the survival of any e-commerce organisation. Any data theft, corruption or loss can easily result in severe consequences for the organisation. To prevent such loss occurring, almost all organisations apply the use of Firewalls, Anti Virus Tools and Intrusion Detection Systems (IDSs). However, recent surveys indicate that despite the use of these technologies, 63% of organisations reported losses due to security failure. Much work has been done on improving such tools, but very little research has been conducted into alternative ways of looking at network security, and in particular, the solutions military and intelligence organisations have implemented to protect their data. This paper examines the use of network separation and unidirectional networking technology as a new means of protecting networks of e-commerce institutions. As little research exists in the public domain regarding the possible use of unidirectional networking technology in e-commerce, businesses have not been able to take advantage of it. This work has explored current implementations of unidirectional networking technology, how these implementations can be adapted to e-commerce, and its potential benefits or limitations to e-commerce organisations. The study has concluded that unidirectional networking technology has great potential for the future of e-commerce security, but without significant demands from government or consumers, organisations are unlikely to spend the large resources and effort necessary to implement the technology.

Keywords: Network security; e-Commerce; unidirectional

Scenario Analysis using Out-of-Line Firewall Evaluation Framework

Lionel Saliou, William Buchanan, Jamie Graves, and Jose Munoz
Napier University, Edinburgh, UK

Abstract: Distributed Denial-of-Service (DDoS) attacks against corporate networks and assets are increasing, and their potential risk for future attacks is also a major concern. These attacks typically aim at disabling computer network infrastructure, and, since there is no one method to mitigate this type of threat, organisations must deploy adequate solutions, and assess the adequacy of their choices against their network requirements, through analysis, such as a simulation, or through network device modelling. A key factor is that DDoS is a dynamic type of attack, and thus device performance is a key parameter, especially for intermediate devices, such as network firewalls. Most of the modelling, though, for firewalls is focusing on static and logical performance attributes, such as whether traffic is denied or permitted. Thus existing models typically cannot deal with dynamic issues when related to intermediate devices. Simulation tools might be possible, but it is often difficult to cover a whole range of devices, thus this paper outlines a novel method of modelling the dynamic performance of network firewalls, and in measuring if they can cope with varying network loads.

Keywords: Dynamic evaluation, network firewall, analysis, security, out-of-line evaluation

Hybrid Intelligent Intrusion Detection/Prevention System using Fuzzylogic and Data Mining

Bharanidharan Shanmugam and Norbik Bashah Idris
Universiti Teknologi, Kuala Lumpur, Malaysia

Abstract: Intrusion Detection Systems are increasingly a key part of systems defense. Various approaches to Intrusion Detection are currently being used, but they are relatively ineffective. Artificial Intelligence plays a driving role in security services. This paper proposes a dynamic model Intelligent Intrusion Detection System, based on specific AI approach for intrusion detection. The techniques that are being investigated include fuzzy logic with network profiling, which uses simple data mining techniques to process the network data. The proposed hybrid system combines anomaly and misuse detection. Simple fuzzy rules, allow us to construct if-then rules that reflect common ways of describing security attacks. We use DARPA dataset for training and benchmarking.

Keywords: Data mining, fuzzy logic, intrusion detection, network security

An Intrusion Detection Countermeasure for 4th-Generation TLB-Assisted Rootkits and Self-Hashing Attacks

Dave Sharp and Carlisle Adams
University of Ottawa, Ottawa, Canada

Abstract: Kernel rootkits are a relatively recent and potentially very serious innovation in malware technology; they started life as simple Trojans embedded in static system executables and have evolved to the latest fourth generation of executables. Rootkits can be used to hide other forms of malicious software such as spyware. The spyware can, in turn, be injected into a running kernel and hidden by manipulation of Translation Look-aside Buffer (TLB) hardware in this latest form of 4th-generation rootkit, making the detection of spyware-infected executables extremely difficult. The spyware can then be used to capture passwords or credit card numbers, or to perform other criminal activity. An AOL study found that spyware had been detected on as many as 80% of the computers tested.

[Van Oorschot] and [Wurster] concurrently developed a generalized hardware-assisted circumvention attack using manipulation of the TLB; this attack can be used to defeat the self-hashing tamper resistance software used in anti-piracy techniques, malware, and other types of activities. (Note that the cost of software piracy alone is estimated in the tens of billions of dollars and the loss of hundreds of thousands of jobs annually, making the protection of software through the use of tamper resistance technologies a high priority.)

In this paper, we demonstrate a novel and simple intrusion detection counterattack against this latest fourth-generation rootkit and hardware-assisted circumvention attack; we show that this counterattack generalizes across different hardware platforms. We also demonstrate methods to mitigate the possibility of an attack by the very rootkit we are trying to detect.

Keywords: Rootkit, covert, spyware, malleability

Greater is our Terror of the Unknown the Diasporic Internet Networks and their Inference with Global Security

Marina Shorer-Zeltser and Galit Ben-Israel

Institute for Identity research in Media and Politics, Israel

Abstract: Regional and international security problems can be understood in more profound way if the research will take into account the relationship between terrorism and new media technologies. If the civilians are exposed to the information and technological revolution, there is no logic to assume that terrorist groups do not share the same benefits and advantages. The terrorists endeavor to mobilize local and international groups, trying to gain advantage by activating loyal civilians who are exposed to the cultural and technological resources of their targets. In this respect, special interest can be brought to the issue of Diasporic communities in the Internet.

The current research is a part of a broader investigation on patterns of political involvement of Diasporic Internet communities. The study has compared the Internet content of three religious groups (Muslim, Jewish and Sikhs) with an attempt to reveal certain cultural and religious codes that bring the potential terrorists to use the Internet as a tool for mobilization and coordination of their actions.

Keywords: Diaspora, internet, political mobilization, loyalty

SQL Infections Through RFID

Anthonius Sulaiman, Vignesh Venkataramana, Srinivas Mukkamala and Andrew Sung

Institute for Complex Additive Systems Analysis, New Mexico, USA

Abstract: Automatic identification and collection (AIDC) technologies have made the life of a man much easier on numerous platforms. Of the various such technologies the radio frequency identification devices (RFID) have become pervasive essentially because they can track from a greater physical distance than the rest. The back end that supports these RFID systems has always been working well until they encounter a badly-formatted RFID tag. There have hardly been any incidents where such tags, once identified by the back-end systems, can in fact wreak havoc via the interacting databases in the RFID infrastructure. Recently, there has been significant research in this area. In the previous work, the author managed to do an attack using a self-referential query on Linux, Oracle, and PHP. However, they have been unable to test it on SQL Server 2005. This paper differs from the previous work in the way that it extends the attack using a self-referential query to Windows, SQL Server 2005, and ASP with their respective latest updates installed. The query itself is more robust by making certain that the table can contain it.

Keywords: RFID Attacks, RFID Virus, SQL Infections, SQL Injections

Information Technologies for the Information Agent

Sérgio Tenreiro de Magalhães¹, Henrique M. D. Santos¹, Leonel Duarte Santos¹, Kenneth Revett² and Paulo Viegas Nunes³

¹University of Minho, Guimarães, Portugal

²University of Westminster, London, UK

³Military Academy Research Center (CINAMIL), Lisboa, Portugal

Abstract: The information agent has requirements in the Information Technology (IT) age that are in everything comparable to those of one hundred years ago. But, despite being similar, they require new forms of implementation due to the evolution of the communication platforms and protocols and to the increase in the amount of information that has to be known, stored, transmitted, and interpreted. Although, in many situations, the information agent will make use of everyday equipment, he will always require levels of trust in the processes that are far beyond those of the everyday citizen. But this cannot imply to carry huge infrastructures that will reveal the agent's intentions. In extreme situations the information agent is the soldier engaged in military activities in hostile environments. There, above all places, he requires light weight trustable equipment and protocols that can perform those tasks.

This work, while making the parallel with the traditional methods, proposes a technological environment able to give answer to the requirements of information agents dealing with the need for a competitive intelligence advantage through the correct use of IT, namely biometrics, alternative authentication processes, Public Key Infrastructures and anti-fishing technologies.

Keywords: Security infrastructure, wearable security, information activities

Malicious Software and System Damages: Is There A Case For Liability Of Software Vendors?

Theodore Tryfonas, Paul Owen and Paula Thomas

Faculty of Advanced Technology, University of Glamorgan, U K

Abstract: This discussion paper addresses the potential responsibility of the software vendors in the light of the changing nature of the threats originating from malicious software. The authors argue that our understanding of the conventional breed of rogue programs (viruses, worms and Trojan horses) highlighted the liabilities residing with those programs' creators or the end-users' negligence, overlooking the potential responsibility of the software vendor. However, because of the way contemporary forms of malicious software ('adware', spyware, botnets etc.) infect systems, primarily due to the faulty nature of the software end-product or its ineffective support, a question is raised about the emerging potential liability of the product provider, who advertises the safe and secure operation of the software – and receives revenues from its sales.

Keyword: Malware, software vendor, liability

Network Forensics of SSL/TLS Encrypted Channels

Meng-Da Wu and Stephen Wolthusen

Information Security Group, Royal Holloway, University of London, UK

Abstract: Network forensics is increasingly hampered by the ubiquitous use of encrypted channels by legitimate and illegitimate network traffic. Both types of traffic are frequently tunneled over application-layer encryption mechanisms, generally using the ubiquitous TLS (SSL) protocol. This results in traditional network forensics tools being largely limited to recording external characteristics (source and origin addresses and ports, time and traffic patterns), but with little insight into content and purpose of the traffic. We propose that a precise characterization of encrypted traffic not only in the form of the external characteristics but also through the analysis of the exact mechanisms, variants and options used for the encrypted channel but visible without access to key material along with a fine-grained analysis of the traffic patterns itself incorporating domain knowledge of the SSL/TLS protocol can yield valuable insights and help to classify traffic into legitimate traffic, illegitimate immediate traffic (e.g. as caused by a Trojan). It can also characterize traffic that is added to an existing data stream by an illegitimate source. In this paper, we therefore present and characterize different traffic types and subsequently analyze this traffic, including the SSL/TLS protocol data units using selected sequence mining techniques.

Key words: SSL/TLS, network forensics, traffic classification, sequence alignment

Experiential Operations: An Information-Based Operational Management Approach for Managing National Security Operations

Ken Webb

Edith Cowan University, Perth, Western Australia

Abstract: This paper outlines an information-based process for rationally managing national security operations. The approach arises because research conducted by the author into better managing asymmetric threats to national security shows that any purposeful national security system requires the interplay of constructs and categories that are dependent on a dynamic operating environment. The unpredictable nature of this means management must constantly mix the system components used in a way that achieves the desired result. An aligned approach is required to maximise the managerial effectiveness of information operations and *Experiential Operations* provides managers with a methodological map to do this.

Keywords: National security, asymmetric threats, information operations, terrorism, management approach

Lexical Natural Language Steganography Systems with Human Interaction

Brecht Wyseur, Karel Wouters and Bart Preneel
K.U. Leuven, Heverlee, Belgium

Abstract: This paper describes an implementation for linguistic steganography based on word substitution over an IRC channel. A typical problem with linguistic steganography is that it is difficult to pay attention to the semantic cohesion of the result. If automated, sentences can be ripped out of context or appear unnatural. Therefore, we propose a solution that involves human interaction with the steganographic engine. This results in sentences that fit perfectly into the context of the IRC conversation. To provide a continuous flow of parts of the message to be transferred, it is encrypted with a stream cipher while it is embedded. A challenging aspect of this work is the generation of the word substitution table based on a session (stego) key. This is because an acceptable number of synonyms must be available for each word such that the interacting user is able to choose synonyms that produce a credible sentence that fits into the context. As we are dealing with an IRC channel though, spelling errors and abbreviations can be introduced to generate more alternatives. We also indicate how our implementation is related to other steganographic systems, such as automated linguistic steganography systems.

Keywords: Linguistic steganography, IRC, human interaction, information hiding

Public Key Usage Model in Converge Network

Lee Fueng Yap¹ and Andy Jones²³

¹British Telecommunications plc., Asian Research Centre, Kuala Lumpur, Malaysia

²British Telecommunications plc., Security Research Centre, Ipswich, UK

³Adjunct, Edith Cowan University, Perth, Australia

Abstract: This paper proposes a usage model of public key cryptography in converged telecommunications networks environment to provide network domain independent registration, authentication, authorization and data confidentiality services. This implementation overcomes conventional PKI system limitations which hinder its wide deployment. The benefits and implementation considerations of the proposed public key cryptography application model is illustrated.

Keywords: Public key cryptography, public key infrastructure, converged network

Investigating the Evasion-Resilience of Network Intrusion Detection Systems

JarleYtreberg and Maria Papadaki
University of Plymouth, Plymouth, UK

Abstract: Network Intrusion Detection Systems provide an extra security precaution by detecting attacks that have bypassed the firewall. Knowledge-based intrusion detection systems rely upon rules to trigger alerts, mainly based upon the occurrence of certain keywords. However, attackers can send evading attack packets that will try to avoid detection by the IDS, and tools can be obtained to automate such attacks. A crucial question is therefore the extent to which modern IDS are resilient to evasion attempts of this type. This paper presents the results of experiments conducted using the Nikto evasion tool against the Snort IDS, with the aim of assessing Snort's alerting capabilities when mutated attack packets were sent to a web server. It was found that Snort alerted for about half of the attack packets. In addition, some weaknesses were identified in Snort's ability to detecting certain evasion attacks, which can be solved by creating customized rules. As a result of these findings, the paper also discusses a new detection method, based upon the division of large request strings into smaller ones, analyzing each of them against the rules. The total danger level of these combined strings could decide if the IDS would alert for the request.

Keywords: NIDS, Evasion, Snort, Nikto

Identifying Computers Hidden Behind a NAT using Machine Learning Techniques

Ori Zakin, Metal Levi, Yuval Elovici, Lior Rockach, Nir Shafrir, Guy Sinter and Ofer Pen

Ben-Gurion University of the Negev, Beer-Sheva, Israel

Abstract: Attackers may use computers hidden behind a Network Address Translator (NAT) in order to conduct malicious activities such as denial of service (DoS). In such cases law enforcement agencies are unable in many cases to single out an attacker from all the users hidden behind the NAT. In this paper we present an innovative approach for clustering the sessions emanating from the NAT in order to identify the attacker. Each cluster should ideally include only the sessions emanating from a specific computer. A system that implements the new approach was developed. It was used to evaluate the new approach performance in a real environment that included 24 computers hidden behind the NAT. The preliminary evaluation results have demonstrated the superiority of the new approach over existing solutions and its ability to assist in locating potential attackers hidden behind a NAT.

Keywords: Network address translator, security

NATO's war on Terror and the Electronic Medium: A Retrospective Analysis on Combating Terrorist Insurgence

Marios-Panagiotis Efthymiopoulos¹ and Josef Demergis²

¹University of Crete, Greece

²University of Macedonia, Greece

Abstract: The war on terror is highly publicised via the use of the internet. Along the same line, terrorists use the internet to disseminate their acts. Can the resilience of terrorist groups in using new technology /IT infrastructure in order to promote their aims/propaganda along with being able to maintain administrative/command lines, be used against them? Can NATO accordingly develop the technological/ IT infrastructure skills to fight the technological battle of e-terror? With the development of High-Tech preparation for open warfare can NATO use the necessary equipment to help fight terrorism? If so what should be this new IT equipment? Can national states promote such policy in a supranational level? Are all countries interoperable to each other to join a newly formed network of e-intelligence to counter terrorism?

Keywords: terrorism, counter-terrorism, internet, Propaganda, Polarisation, NATO internet strategy

Corporate Data Loss at Thirty Thousand Feet

Grigorios Fragkos and Andrew Blyth

**Faculty of Advanced Technology, University of Glamorgan,
Wales, UK**

Abstract: The purpose of this paper is to make organizations and corporations aware of the potential “controlled environment” threat and bring them one step ahead in protecting their assets. Computers and in general any type of device which has wireless capabilities is most vulnerable to be targeted for exploitation, while in an isolated environment. Isolated environment can be considered a train, an aircraft, a hotel and others which can offer a “controlled environment” by an attacker. Additionally, this paper goes through a list of probable reasons for being targeted and discusses the concept of an era of cyber battles and cyber wars.

Over the past few years companies have been made aware of security issues concerning their employees’ laptops. The manufacturers create laptops with all sorts of wireless technologies like Bluetooth, WiFi, etc as standard. Wireless is very convenient for home and in particular corporate use. The users need to be able to hook up on the network, from everywhere, anywhere, anytime. Large Corporations are doing really good job to ensure data integrity, confidentiality, and availability. Traveling around the world for business purposes is very common nowadays. Most of the times people are try to catch up with work even during a short flight. You can notice a number of people working on their laptops by a simply walking, up and down the airplane’s aisle. The purpose of this paper is to explore the potential threats from a security aspect, when using a wireless capable laptop within an aircraft during a flight. Due to the fact that most laptop manufacturers have wireless enabled by default, or do not provide a hardware switch, these computers are exposed into the aircraft’s cabin environment. This environment can be used and misused by a threat agent (hacker) for the duration of the flight. At thirty thousand feet there are no corporate firewalls, no Intrusion Detection Systems, most probably nothing that will log the activity and most importantly, nothing to raise the alarm and notify the user so as to take measures of protection. Finally, consequences from such attacks could lead to theft of personal data, retrieval of sensitive information or corporate intelligence, spyware drops for corporate espionage or blackmailing.

There are several places which can be considered isolated environments where it is easier for an attacker to commence an attack. Similar places to the in-flight example, where computers are more vulnerable, are ‘public’ places like trains, hotels, conference rooms etc. In the in-flight example there are two significant parameters that are true and benefit the attacker. Firstly, the flight provides a specific timeframe, when in a train the one that is being attack could get off in any of the stations (if the actual destination is not known in advance). Secondly, if the attack has been identified some how while in the aircraft, it is difficult for the police to press charges due to the fact the attacker was in international air space or international waters at the time of the attack. Consequently these are two very interesting reasons why the paper uses the in-flight example as a preferable isolated environment. One of the sections of the paper tries to expand the views of

the readers when considering the results of future targeted attacks. The collateral damage to computer infrastructures could be major without a specific or reasonable motive. A few years ago the police were trying to stop hooligans or gang members from vandalizing public property. Fights between gangs had an effect on public safety, affected businesses along with the increase or decrease of real estate prices. Along the same lines, hackers (threat agents) across the world have formed teams that one could say that they are similar to the street gangs.

The paper tries to merge motive with consequence by analyzing the today's actions of novice and expert threat agents. Taking under consideration different approaches of the current situations in the digital world it should be wised to try predict some parts of the future actions. What could be the outcome of such behavior at the current state? This prediction has a low percentage of being successful in a large scale but if in any case comes true it could lead to be a guideline for future way of thinking. It is difficult to understand the events taking place in present time that is why a step out of the box and a look to the bigger picture is always useful. Basically, the main idea for this paper is to make people think and discuss on how could different simple events today can be interlinked in order to form tomorrow's threats.

Keywords: Information assurance, data loss, wireless attacks, aircraft environment, threat agents