

Proceedings of the 8th European Conference on Information Warfare and Security

Military Academy
Lisbon and the University of Minho
Braga
Portugal
6-7 July 2009

Edited by
Henrique Santos
University of Minho

Copyright The Authors, 2009. All Rights Reserved.

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

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

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

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

ISBN: 978-1-906638-34-4 Cd

Published by Academic Publishing Limited
Reading
UK
+44-(0) 118-972-4148
www.academic-publishing.org

ECIW 2009

Contents

Paper Title	Author(s)	Booklet Page No	Book Page No.
Preface		v	lv
Biographies of Conference Chairs, Programme Chair, Keynote Speaker and Mini-track Chairs		viii	vii
Biographies of contributing authors		ix	viii
Markov Process Based Steganalysis by Using Second-Order Transition Probability Matrix	<i>Ainuddin Wahid Abdul Wahab^{1,2}, Hans Georg Schaathun¹ and Anthony Ho¹</i> <i>¹University of Surrey, UK</i> <i>²University of Malaya, Malaysia</i>	1	1
A Real-Time Robust Decision Support System for Network Centric Warfare	<i>Arundhati Bhattacharyya¹, Chandan Mazumdar² and V.K. Saraswat³</i> <i>¹Research Centre Imarat, Hyderabad, India</i> <i>²Jadavpur University, Kolkata, India</i> <i>³Defence Research and Development Organization, New Delhi, India</i>	2	9
A Security Architecture to Model Destructive Insider Attacks	<i>Clive Blackwell</i> <i>Royal Holloway University of London, Egham, UK</i>	3	20
A Secured Multi-Party Computational Protocol to Protect Cyberspace for Defense Applications	<i>Manohar Chandwani¹ and Durgesh Kumar Mishra²</i> <i>¹Institute of Engineering and Technology, Devi Ahilya Vishwavidyalaya, India</i> <i>²Acropolis Institute of Technology and Research, Indore, India</i>	4	30
Individual Factors Impact on Pirating Digital Media in Thailand	<i>Nawarat Chullasang and Nitaya Wongpinunwatana</i> <i>Thammasat University, Bangkok, Thailand</i>	5	35
How to Cooperatively Improve Broadband Security	<i>Tiago Cruz¹, Thiago Leite¹, Patricio Baptista¹, Rui Vilão¹, Paulo Simões¹, F. Bastos² and Edmundo Monteiro¹</i> <i>¹CISUC - DEI, University of Coimbra, Portugal</i> <i>²PT Inovação – Aveiro, Portugal</i>	6	42
Challenging Nato's Security Operations in Electronic Warfare: The Policy of Cyber-Defence	<i>Marios Panagiotis Efthymiopoulos</i> <i>Strategy Internationa.org, Greece</i>	7	52

Paper Title	Author(s)	Booklet Page No	Book Page No.
A National RACI Chart for an Interoperable “UNUational UCUyber USecUurity” Framework	<i>Mohamed Dafir Ech-Cherif El Kettani¹ and Taïeb Debbagh²</i> <i>¹University Mohammed V-Souissi, Rabat, Morocco</i> <i>²Ministry of Industry, Commerce and NT, Rabat, Morocco</i>	8	60
Operational aspects of cyberwarfare or cyber-terrorist attacks: what a truly devastating attack could do	<i>Eric Filiol</i> <i>ESIEA - Operational virology and cryptology laboratory, Laval, France</i>	9	71
Information Security and Data Protection: The Role of the “Human Factor” in Organizations	<i>Ulrike Hugl</i> <i>University of Innsbruck, Innsbruck School of Management, Austria</i>	10	80
Messy Wars - Postmodern Way to see a War	<i>Aki-Mauri Huhtinen¹ and Jari Rantapelkonen²</i> <i>¹National Defence College, Helsinki, Finland</i> <i>²Finnish Defence Forces, Riihimäki, Finland</i>	11	88
From Visible to Discreet and Interactive Management – Controlling in a Military Organisation in the Information Battle Space	<i>Aki-Mauri Huhtinen</i> <i>National Defence College, Helsinki, Finland</i>	12	95
Assessing the Usability of Personal Internet Security Tools	<i>Tarik Ibrahim¹, Steven Furnell^{1, 2}, Maria Papadaki¹ and Nathan Clarke^{1, 2}</i> <i>¹University of Plymouth, UK</i> <i>²Edith Cowan University, Perth, Western Australia</i>	13	102
Information Security Policies in Small Finnish Companies	<i>Ilona Ilvonen</i> <i>University of Technology, Tampere, Finland</i>	14	112
The Dark Side of Complex Information Technology Intensive Firms: Reconciling the Imperative of Social Value Creation With Controversial Quasi-Regulatory Practices	<i>Jonatan Jelen¹ and Marko Kolakovic²</i> <i>¹Parsons The New School for Design, New York, USA</i> <i>²University of Zagreb, Faculty of Economics, Zagreb, Croatia</i>	15	118
Tamper Resistance of Contactless IC Card to Side-Channel Attacks	<i>Tetsutarou Kanno, Keisuke Iwai and Takakazu Kurokawa</i> <i>National Defense Academy, Yokosuka city Japan</i>	16	126

Paper Title	Author(s)	Booklet Page No	Book Page No.
Multilevel Security in a Network-Centric Environment	<i>Anssi Kärkkäinen and Catharina Candolin The Finnish Defence Forces, Helsinki, Finland</i>	17	134
Applying a Cost Optimizing Model for IT Security	<i>Jyri Kivimaa Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia</i>	18	142
Application and Analysis of Private Matching Schemes Based on Commutative Cryptosystems	<i>Zbigniew Kwecka, William Buchanan and Duncan Spiers Napier University, Edinburgh, UK</i>	19	154
Security Framework for Information Systems	<i>José Martins¹, Henrique dos Santos² and Paulo Nunes³ ¹Academia Militar - Cinamil, Lisboa, Portugal ²University of Minho - Department of Information Systems, Guimarães, Portugal</i>	20	164
Theoretical Model for Creating a Nation-State Level Offensive Cyber Capability	<i>Rain Ottis Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia</i>	21	177
Applying Poker Strategies, Tactics and Rapid Decision Making Methods to Military Decision Making on the Tactical Level	<i>Evert Paas Estonian Defence Forces, Tallinn, Estonia</i>	22	183
Cellular Warfare	<i>Karlis Podins Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia</i>	23	192
Security Analysis and Modelling Framework for Critical Infrastructure Systems	<i>Graeme Pye and Matthew Warren School of Information Systems, Faculty of Business and Law, Deakin University, Geelong, Australia</i>	24	198
Network Centric Operations: the “SIVICC” Case Study	<i>Nuno Rosário and Paulo Nunes CIIWAC, Guarda Nacional Republicana, Largo do Carmo 1200-092 Lisboa, Portugal CIIWAC, CINAMIL, Academia Militar, Paço da Rainha 29 1169-203 Lisboa, Portugal</i>	25	208
White Force Tracking (WFT)	<i>Tapio Saarelainen National Defence University, Helsinki, Finland</i>	26	216

Paper Title	Author(s)	Booklet Page No	Book Page No.
Computer-Aided Warriors for Future Battlefields	<i>Tapio Saarelainen and Jorma Jormakka National Defence University, Helsinki, Finland</i>	27	224
RFID: Big Brother Global?	<i>Cristina Sousa¹, Pedro Teixeira Pereira¹, Sérgio Tenreiro de Magalhães¹, Leonel Santos², and Henrique Santos² 1) Universidade Católica Portuguesa, Braga, Portugal 2) Universidade do Minho, Guimarães, Portugal</i>	28	234
Supply Chain Management Security: The Weak Link of Australian Critical Infrastructure Protection	<i>Matthew Warren and Shona Leitch Deakin University, Victoria, Australia</i>	29	240

Preface

The Eighth European Conference on Information Warfare and Security (ECIW 2009) is jointly hosted by the University of Minho and the Military Academy in Lisbon, Portugal. The Conference Co-Chairs are Henrique Santos from the University of Minho and Col. Fernando Freire from the Military Academy. The Programme Chair is Dr Sérgio Tenreiro de Magalhães from the Universidade Católica Portuguesa.

The main aim of this Conference continues to be an opportunity 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 is given by Dr. Paulo Veríssimo, from the University of Lisboa who will talk about “Strategic Cyber Defense for Critical Infrastructures” and the second day will be opened by Rear-Admiral António Marques, IT directorate, Portuguese Navy together with Captain João Ribeiro, Chairman - NATO Ad-hoc Working Group for Maritime Force Protection, who will talk on the topic of “The importance of network centricity in obtaining overall awareness and understanding of the Portuguese maritime engagement space and outreaching the decision making process.”

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.

With an initial submission of 60 abstracts, after the double blind, peer review process there are 29 papers published in these Conference Proceedings. These papers come from all parts of the globe including Australia, Austria, Estonia, Finland, France, Greece, India, Japan, Morocco, Portugal, Thailand and the United Kingdom.

Group work and sharing of ideas are not confined to seminar sessions alone. On the second day participants will have the opportunity of participating in one of two interactive sessions aimed at stimulating leadership capabilities through a role play exercise and experimenting with technology used by some groups at the Pentagon to improve the decision making process.

I wish you a most interesting conference.

Henrique De Santos
Conference Chair
June 2009

Conference Executive:

Debi Ashenden, Cranfield University, UK
Dr Andrew Blyth, University of Glamorgan, Wales, UK
Professor Steven Furnell, University of Plymouth, UK
Professor Aki Huhtinen, Finnish Defence Forces, Finland
Dr Andy Jones, British Telecom, UK and Edith Cowan University, Australia
Dr Sérgio Tenreiro de Magalhães, Universidade Católica Portuguesa, Portugal
Tim Parsons, BAE Systems, UK
Dr Jari Rantapelkonen, Finnish Defence Forces, Finland
Dr Henrique Santos, University of Minho, Portugal
Dr Jill Slay, University of South Australia
Dr Iain Sutherland, University of Glamorgan, UK

Committee Members

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

Abiola Abimbola (Napier University, UK); Gail-joon Ahn (University of North Carolina, Charlotte, USA); Leigh Armistead (Edith Cowan University Australia); Colin Armstrong (Curtin University, Australia); Debi Ashenden (Cranfield University, Shrivenham, UK); Richard Baskerville (Georgia State University, USA); Maumita Bhattacharya (Charles Sturt University, Australia); John Biggam (Glasgow Caledonian University, UK); Andrew Blyth (University of Glamorgan, UK); Martin Botha (South African Police, South Africa); Svet Braynov (University of Illinois, Springfield, USA); Bill Buchanan (Napier University, UK); Catharina Candolin (Finnish Defence Forces, Helsinki, Finland); Jerome Carrere (Telindus, Luxembourg); Rodney Clare (EDS and Open University, UK); Maura Conway (Dublin City University, Ireland); Michael Corcoran (DSTL, UK); Geoffrey Darnton (Bournemouth University, UK); Dorothy Denning (Naval Postgraduate School, USA); Paul Dowland (University of Plymouth, UK); Marios Efthymiopoulos (Special Envoy of the Hellenic Foreign Ministry to Nato, Italy); Ramzi El-Haddadeh (Brunel University, UK); John Fawcett (University of Cambridge, UK); Eric Filiol (Ecole Superior Informatique, France); Chris Flaherty (University of New South Wales, Australia); Steve Furnell (University of Plymouth, UK); Javier Garci'a Villalba (Universidad Complutense de Madrid, Spain); Kevin Gleason (KMG Consulting, Massachusetts, USA); Stefanos Gritzalis (University of the Aegean, Greece); Barry Horne (QinetiQ TIM, UK); Ulrike Hugl (University of Innsbruck Austria); Aki Huhtinen (National Defence College, Finland); Bill Hutchinson (Edith Cowan University, Australia); Berg P Hyacinthe (Assas School of Law, Universite Paris, France); Hamid Jahankhani (University of East London, UK); Helge Janicke (De Montfort University, Leicester, UK); Andy Jones (BT UK); James Joshi (University of Pittsburgh, USA); Nor Badrul Anuar Jumaat (University of Malaya, Malaysia); Maria Karyda (University of the Aegean Greece); Auli Keskinen (National Defence College, Finland); Jyri Kivinaa (Co-operative Cyber Defence and Centre of Excellence in Tallinn, Estonia); Spyros Kokolakis (University of the Aegean, Greece); Prashant Krishnamurthy (University of Pittsburgh USA); Dan Kuehl (National Defense University, Washington DC, USA); Peter Kunz (Diamler Chrysler Germany); Pertti Kuokkanen (University of Helsinki Finland); Takakazu Kurokawa (National Defence Academy, Japan); Tuija Kuusisto (Finnish Defence Force, Finland); Rauno Kuusisto (Finish Defence Force, Finland); Michael Lavine (John Hopkins University's Information Security Institute, USA); Martti Lehto (FiAF, Finland);

Tara Leweling (Naval Postgraduate School, Pacific Grove, USA); Paul Lewis (Technology Strategy Board, UK); Sharman Lichtenstein (Deakin University, Australia); David Llamas (University of St Andrews, UK); Keith Martin (Royal Holloway, University of London, UK); Bill Martin (RMIT, Australia); Eduardo Medina (Universidad de Castilla-La Mancha, Spain); Don Milne (Buckinghamshire Chilterns University, UK); Yonathan Mizrahi (University of Haifa, Israel); Evangelos Moustakas (Middlesex University, London, UK); Kara Nance (University of Alaska Fairbanks, USA); Dan Ophir (Academic College of Judea and Samaria, Israel); Rain Ottis (Co-operative Cyber Defence and Centre of Excellence in Tallinn, Estonia); Juhani Paavilainen (University of Tampere, Finland); Maria Papadaki (University of Plymouth, UK); Tim Parsons (BAE Systems, Bristol, UK); Maria Papadaki (University of Plymouth, UK); Tim Parsons (DETICA, UK); Andrea Perego (Università degli Studi dell'Insubria, Italy); Michael Pilgermann (University of Glamorgan UK); Fred Piper (Royal Holloway, University of London, UK); Jari Rantapelkonen (National defense University, Finland); Andrea Rigoni (Booze & Company, Italy); Raphael Rues (DigiComp Academy Switzerland); Henrique Santos (University of Minho, Portugal); Damien Sauveron (University of Limoges, France); Richard Sethmann (University of Applied Sciences, Bremen, Germany); Jill Slay (University of South Australia, Australia); Anna Squicciarini (University of Milano, Italy); Iain Sutherland (University of Glamorgan, Wales, UK); Jonas Svava Iversen (Danish Broadcast Corporation, Denmark); Phil Taylor (University of Leeds, UK); Sérgio Tenreiro de Magalhães (Universidade Católica Portuguesa, Portugal); Theodore Tryfonas (University of Glamorgan, UK); Craig Valli (Edith Cowan University, Australia); Rudi Vansnick (Internet Society, Belgium); Richard Vaughan (General Dynamics UK); Stilianos Vidalis (Newport Business School, UK); Teemupekka Virtanen (Helsinki University of Technology, Finland); Marja Vuorinen (University of Helsinki, Finland); Michael Walker (Vodafone, UK); Mat Warren (Deakin University, Australia); Kenneth Webb (Edith Cowan University, Australia); Peter Wild (Royal Holloway, University of London, UK); Trish Williams (Edith Cowan University, Australia); Patricia Williams (Edith Cowan University, Australia); Tom Wilsdon (University of South Australia); Simos Xenitellis (Royal Holloway University, London, UK); Omar Zaafrany (Ben-Gurion University of the Negev, Israel); Omar Zakaria (University of Malaya, Malaysia).

Biographies of Conference Chairs, Programme Chair and Keynote Speaker

Conference Chairs



Dr Henrique Santos is an Associate Professor in the department of Information Systems at the University of Minho in Guimarães, Portugal. He lectures on Computer architecture, Information system security and computer programming. His research interests include security models, security policies and security evaluation issues. Public Key Infrastructures and its applications are also a central topic of interest. He is the Director of the Algoritmi research centre at the University.

Colonel Fernando Freire is an Military Professor in the Department of Exact and Natural Sciences at the Military Academy in Lisbon, Portugal. He lectures on Operational Research, Information, Uncertainty and Risk and Decision Theory and Management. His research interests include support decision, uncertainty, knowledge management and information warfare, in general. He is one of the coordinators of Posgraduate Studies on Information Warfare/Competitive Intelligence. Fernando holds a Master of Science degree



Programme Chair



Dr Sérgio Tenreiro de Magalhães teaches IT Project, Computer Architecture and Information Security related topics in the Universidade Católica Portuguesa. He is also a member of the Knowledge and Information Systems and Services research group in the Algoritmi Research Centre of the University of Minho. Sérgio has also collaborated as a manager and as a consultant with several organizations and he has also participated in the development of the National Science and Technology Platform for the Ministry of Science

and Technology and in the National Defence Ministry's project Security in the Digital Data Distribution Network for the Armed Forces. He is a member of the Editorial Board of the International Journal of Electronic Security and Digital Forensics and reviewer of the IEEE Transactions on Systems, Man and Cybernetics – Part C: Applications and Reviews. He is also a member of several international conferences' programme committees and has published several security related book chapters and more than 20 security related papers in both international journals and conferences.

Keynote Speakers

Dr Paulo Veríssimo is currently a professor of the Department of Informatics (DI) of the University of Lisboa Faculty of Sciences (<http://www.di.fc.ul.pt/~piv>), and Director of LASIGE, a research laboratory of the DI (<http://lasige.di.fc.ul.pt>). He is Fellow of the IEEE. He is associate editor of the Elsevier Int'l Journal on Critical Infrastructure Protection, and past associate editor of the IEEE Tacs. on Dependable and Secure Computing. He belonged to the European Security & Dependability Advisory Board. He is past Chair of the IEEE



Technical Committee on Fault Tolerant Computing and of the Steering Committee of the DSN conference, and belonged to the Executive Board of the CaberNet European Network of Excellence. He was coordinator of the CORTEX IST/FET project (<http://cortex.di.fc.ul.pt>). Paulo Veríssimo leads the Navigators research group of LASIGE, and is currently interested in: architecture, middleware and protocols for distributed, pervasive and embedded systems, in the facets of real-time adaptability and fault/intrusion tolerance. He is author of more than 145 refereed publications in international scientific conferences and journals in the area, and co-author of five books (ex. <http://www.navigators.di.fc.ul.pt/dssa/>).



Rear-Admiral António Marques joined the Navy in 1976. After a tour on board frigates and patrol boats as Navigation Officer and Executive Officer, he attended the Communications Specialization Course in the Navy followed by a MSEE degree in Electrical and Computer Engineering which he has attended in the Naval Postgraduate School in Monterey, California, between 1984 and 1987. Returning to Portugal, he was involved in the Vasco da Gama Class Frigates project, namely in the development and maintenance of the frigate's Combat System, and has lead several IT projects in

the Portuguese Navy. In 2003 he attended the NATO Defence College course and from 2004 to 2007 he was the Portuguese Navy counsellor to Portugal's Ambassador to NATO where he was the Portuguese permanent representative to the NATO C3 Board. After returning to Portugal, he attended the Flag Officer's Course in the National Defence College and was promoted to the current rank in November of 2008. He currently leads the IT directorate of the Portuguese Navy.

Captain João Ribeiro joined the Navy in 1981. He attended the Communications Specialization Course and served as Principal Warfare Officer on board frigates NRP Cte Hermenegildo Capelo and NRP Álvares Cabral and as Executive Officer of frigate NRP Vasco da Gama. Meanwhile, he served as staff officer of the Portuguese Naval and Joint Task Groups, as well as NATO Standing Naval Force Atlantic. He has been involved in several real world operations, namely, Embargo Operations to Former Yugoslavia, Non-Combatant Evacuation in Republic of Guinea-Bissau, and Global War on Terrorism. He served ashore as Director of Navy Communications School, Staff Officer for Navy Staff CIS Division, Public Affairs Officer and Navy Spokesman to the Chief of Navy Staff Private Office, Staff Officer for Joint Staff CIS Division and National Liaison Representative to Supreme Allied Commander Transformation and the United States Joint Forces Command . Currently he serves as Head of Operations Division in the Navy Staff. He is chairman of NATO Ad-hoc Working Group for Maritime Force Protection, and Navy's representative to the National Maritime Coordination Center.



Biographies of contributing authors (in alphabetical order)

Arundhati Bhattacharyya is a postgraduate in Physics from University of Hyderabad, and in “Software Systems” from Birla Institute of Technology & Science, Pilani, India. She joined the Defence Research & Development Organization, India in 1987 and is involved in the R&D work in challenging fields for the military services.

Clive Blackwell received an EPSRC award for his PhD in network security at Royal Holloway under the supervision of Professor Chris Mitchell. He has developed a practical scheme to model the security architecture of computer networks such as the Internet and other complex systems such as critical infrastructure. He is developing a new process calculus called spygraphs from a process calculus called bigraphs to model security architecture. Clive has recently written a book on the insider threat and is working on another book on data protection. He holds a degree in Mathematics from Warwick University and in Computer Science from Royal Holloway where he passed out top of his class, and an MSc in Information Security also from Royal Holloway.

Mishra Durgha Ph.D. (Computer Engineering) – specialization in Privacy preserving Data Mining, Secure Multi-party Computation, Security, Privacy, Databases, Data mining. M. Tech. (Computer Science) Secretary, IEEE MP-subsection Published around 50+ papers in International/National Journal and reviewed conferences. Invited speakers in IEEE International workshop on Data Mining and Artificial Intelligence. Invited Speaker in various Conference and faculty development program in nationwide.

Nawarat Chullasang is currently studying Master’s Degree programme in Management Information System at Thammasat University in Bangkok, Thailand. At the same time, she is also working as a Software Developer at Tilleke & Gibbins International Ltd, one of leading law firms in Thailand. She has an extensive 6 years experience in system analysis and design. Her research interests include software and digital piracy, digital purchasing decision and mobile commerce.

Tiago Cruz is a researcher working on his PhD thesis at the Communications and Telematics group at the Centre of Informatics and Systems of the University of Coimbra. Its interests spawn from Desktop Management to O&M Organization and Distributed Management. He is presently focusing on the subject of borderline security mechanisms in access networks.

Marios Panagiotis Efthymiopoulos is a Scholar of the Onassis Foundation. He holds a PhD in International Relations from the Political Sciences Department University of Crete Greece. Holds a BA Hons in International Relations and Politics from the University of Lincolnshire and Humberside, attended the MSc in Russian and Post-Soviet Studies LSE, holds an MA in Advanced International Relations, the Diplomatic Academy of Vienna. Appointed by the Ministry of Foreign Affairs of Greece, as an academic envoy at the NATO Defence College, NADEFCOL during 2004-2005 periods. Diploma by the Academic programme of NADEFCOL, Senior Course 105 on NATO policies.

M.D. El Kettani is a professor of Computer Science at ENSIAS-University Mohammed V-Souissi. He teaches « System and Network Security ». He has many publications in « eGovernment security » field. He is the coordinator of « Juniper Networks Academic Alliance » in ENSIAS. He is member of ITU High-Level Experts Group n°3. This working group assisted ITU’s Secretary-General in developing strategic proposals to Member States, within the process of development of a national cybersecurity plan.

Ulrike Hugl Studies: economics and social sciences, University of Innsbruck (further studies: pedagogics; law). Industry affiliations (several years): in the fields of personnel development, organization, and marketing. University affiliations: Institute of Public Sector Management (University of Innsbruck); project coordinator of an entire university reform project (for the Senate of the University of Innsbruck); researcher and lecturer at the University of St. Gallen (Institute for Information Management). Ongoing: Innsbruck School of Management (University of Innsbruck). Research/project experiences: privacy / information security issues; technology implementation processes; e-learning. Miscellaneous: membership of several international research associations; lecturer at diverse universities; reviewer of international journals; keynote speeches at international conferences (informatics / management).

Aki-Mauri Huhtinen on the Department of Leadership and Military Pedagogy Studies at Finnish National Defence College are also the docent on the Department of Social and Moral Philosophy at University of Helsinki and the docent of social consequences of media and information technology in Faculty of Art and Design at University of Lapland in Rovaniemi.

Nathan Clarke Dr graduated with a BEng (Hons) degree in Electronic Engineering in 2001 and a PhD in 2004 from the University of Plymouth. He has remained at the institution and now is a senior (principal) lecturer in Information Systems Security within the Centre for Information Security and Network Research. Dr Clarke is also an adjunct scholar at Edith Cowan University, Western Australia. His research interests reside in the area of user identity, mobility and intrusion detection; having published 40 papers in international journals and conferences.

Eric Filiol Lt Colonel (ret) has spent 21 years in the army first in marine corps regiments then in computer security and cyberwarfare. His area of expertise and research are computer virology and cryptology. He currently heads the operational cryptology and virology lab at the ESIEA Laval in France. He holds a engineer diploma in cryptology, a PhD in mathematics and a habilitation thesis in computer science.

Ilona Ilvonen is a doctoral student at Tampere University of Technology, department of Business Information Management and Logistics. She earned her master degree from the program of information and knowledge management on 2006. She has published conference articles on the management of information security in small and middle size companies since the year 2003.

Keisuke Iwai received the B.E. degree in Electrical Engineering from Waseda University in 1996, the M.E. and the Dr. Eng. degree in Computer Science from Keio University in 1998 and 2001. He is Research Associate in the Dept. of Computer Science, National Defense Academy of Japan. His research interests include Differential Power Analysis, Parallel Processing, Reconfigurable computer and its application, and Parallelizing Compilers

Jonatan Jelen A former executive manager with companies in Paris and New York, Dr. Jonatan Jelen is currently a business owner, entrepreneur, Assistant Professor of Business at Parsons The New School for Design – School of Design Strategies, and visiting faculty at USST in Shanghai, China, and the Faculty of Economics of the University of Zagreb, Croatia.

Tetsutarou Kanno received the B.E. degree in Electronic Science from National Defense Academy in 2003, He is Master Course of Dept. of Computer Science, National Defense Academy of Japan and First Lieutenant of Japan Maritime Self Defense Force. His research interests include power analysis and EM analysis.

Jyri Kivimaa is currently at NATO Cooperative Cyber Defence Center of Excellence, Estonia. Education: 1972 Tallinn Technical University: graduated engineer (equal to master's degree), electronics. Languages Estonian, Finnish, English, Russian Employment record 2007–.NATO CCD CoE, scientist, 1998–2007 Union Bank of Estonia, data security expert.

Takakazu Kurokawa received the B.E., M.E., and Dr. Eng. degree in Electrical Engineering from Keio University in 1983, 1985, and 1988. He is Professor in the Dept. of Computer Science, National Defense Academy of Japan, His research interests include parallel architectures and reconfigurable systems.

Rain Ottis is a researcher at the Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia. He has a MSc in Informatics and is pursuing a PhD from the Tallinn University of Technology. His research interests include cyber conflicts and cyber attack attribution.

Evert Paas has been working in Estonian Defence Forces for 10 years researching information warfare and information operations. His main research interests are connected with asymmetric warfare. His current research focuses on implementing poker decision making models to military decision making process.

Karlis Podins is affiliated with Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia. He has Bachelors and Masters Degrees from University of Latvia.

Nuno Miguel da Silva Rosário is a Republican National Guard's Officer, a Portuguese Police with military statute. He's graduated in Military Sciences and post-graduated in Competitive Intelligence and Information Warfare in the Military Academy of the Portuguese Army. He is also a founding member of the Competitive Intelligence and Information Warfare Association – Club (CIWAC), which was created in 2008 to develop and discuss themes related with this area.

Tapio Saarelainen, Major Born: 1966, MMSc (Master in Military Sciences). Working in National Defence University at Department of Military Technology as a researcher and lecturer. Participates in Finnish Future Warrior develop program since 2004. Post graduate student in National Defence University since 2006. Topic "Data and sensor fusion in Future Dismounted Warrior Concept".

Markov Process Based Steganalysis by Using Second-Order Transition Probability Matrix

Ainuddin Wahid Abdul Wahab^{1,2}, Hans Georg Schaathun¹ and Anthony Ho¹

¹University of Surrey, UK

²University of Malaya, Malaysia

Abstract: In this paper, we analyse and extend the steganalysis technique employed by Shi et al. (2006), where they used a first-order Markov model to generate second order statistics from the JPEG 2-D array. They have suggested that a second order Markov model should improve the performance, but did not proceed with the implementation due to its computational complexities. We have implemented a steganalysis based on the proposed second-order model, and found that the classification result was significantly improved at the expense of computational cost (2916 features). Interestingly, we find improved detection of embedding by the F5 software, but this seems to be entirely due to the detection of double compression and not due to the embedding itself.

Keywords: Steganalysis, F5, SVM

A Real-Time Robust Decision Support System for Network Centric Warfare

Arundhati Bhattacharyya¹, Chandan Mazumdar² and Vijay.Kumar. Saraswat³

¹Research Centre Imarat, Defence Research and Development Organization, Hyderabad, India

²Centre for Distributed Computing, Jadavpur University, Kolkata, India

³Defence Research and Development Organization, New Delhi, India

Abstract: Modern Battle Management System protecting a nation's defended assets in a theatre of war from varied threats, at strategic, operational and tactical levels, demands faster reaction and quick commander response. Threats of different severities could approach from geographical areas different from the areas where the weapons are deployed. Thus for defending assets, the nation states need to be networked to gather intelligence about the threats for the central command and control in order to decide on the type and the number of weapons to be engaged to neutralize the threats, assigning weapons to prioritized threats and finally assessing the battle damage, all in real-time. Information superiority and decision dominance are the key factors of modern warfare. This modern warfare is the Network Centric Warfare (NCW). Worldwide, a problem faced by the defence-planners is how to design nationwide Central Information Grid (CIG) and software, which will be inter-operable, sustainable and scalable and still can provide the robustness and time critical decisions. In order to be real-time compliant, the overall system should allow decentralized decision-making, which may be overridden by centralized command and control depending on the demand of the situation. The diversity and volume of online data overwhelms the cognitive capabilities of human commanders, which necessitate the use of a Decision Support System (DSS). A real-time robust DSS is an essential requirement of modern warfare. This paper presents the design approach of a multi-tier DSS Architecture pertaining to a nation's C4I characterized high performance Central Information Grid (CIG) connecting several interacting networks for the NCW environment, which can be seamlessly integrated with the CIG, for robust and time critical decision-making from intelligence gathered by itself and by the heterogeneous networks of the component C2I systems spread over the nation.

Keywords: network centric warfare, c4i, decision support system, central information grid, information superiority, battlespace

A Security Architecture to Model Destructive Insider Attacks

Clive Blackwell

University of London, Egham, UK

Abstract: The insider threat poses a significant and increasing problem for organisations. This is shown by the regular stories of data loss in the media such as the 25 million personal records mailed out on a CD by Revenue and Customs in the UK. There is a need to provide comprehensive protection from insider attacks at the physical, logical and social levels. We have developed a three-layer security architecture that we use to examine the insider threat systematically, which is very difficult to analyse manually because of its complexity. We investigate destructive insider attacks, but the model has straightforward application to the other main classes of insider threat from financial fraud and information theft. Our security model appears to have widespread application in other areas, as it allows the analysis of systems in their entirety including human and physical factors, not just as technical systems.

Keywords: Insider threat, multilevel security model, security architecture, attack and defence taxonomy, destructive attack, sabotage

A Secured Multi-Party Computational Protocol to Protect Cyberspace for Defense Applications

Manohar Chandwani¹ and Durgesh Kumar Mishra²

¹Institute of Engineering and Technology, Devi Ahilya Vishwavidyalaya, India

²Acropolis Institute of Technology and Research, Indore, India

Abstract: Secured multi-party computation (SMC) is a problem of information security when large organizations interact with one another for huge data sharing and data exchange. It is quite possible that during sharing and exchange, the private data also gets hacked. In order to protect and secure the private data, the protocols of SMC need to be deployed in the large computer networks on which the organizations work. The protocols work at the micro-level in terms of cryptography with which the data is encrypted and then shared while allowing the keys to be used for sharable data while keeping the keys untouched for private data. At macro level, the multilevel architectures are used for different types of security to be achieved. The computation part of the secured multi-party computation is based on the algorithmic complexity theory. The algorithms realize the protocols in such a way that it is tedious to break (decrypt) the keys to hack the private data. Computational complexities of such algorithms are non-polynomial and the computers may take long time to break the keys. In this paper, we will show how our SMC protocols prevent the data of an organization during the war from the cyberspace when a large number of defense units interact with one another, while hiding the identity and computations done by them.

Keywords: Correctness, cyberspace, privacy, secure multi-party computation (SMC), security, trusted third party (TTP)

Individual Factors Impact on Pirating Digital Media in Thailand

Nawarat Chullasang and Nitaya Wongpinunwatana
Thammasat University, Bangkok, Thailand

Abstract: The primary objective of this research is to identify the individual factors which influence the intention to pirate software and digital media in Thailand. An increasing of the speed of internet and the high technologies of digital compression are factors that made a digital piracy happen easily. Moreover, the lower cost of hi-speed internet is the incentive of the software and digital media piracy occurrences. This is only one of many reasons which cause digital piracy. As Thailand was ranked 13th in the most software piracy in the world in 2003, there are a lot of concerns about the high increasing of the digital piracy in Thailand. This study focuses on one of the digital piracy model, and uses The Theory of Planned Behavior (TPB) as a based theory to determine the factors influencing software and digital piracy. Attitude, Subjective norms and Perceived Behavioral Control are the factors described in TPB as they affect to the intention to create the behavior. Past Behavior is another factor added in this study apart from TPB, which has an impact to the piracy intention. The digital piracy behavior model was developed in this study, and the five hypotheses were proposed. A survey is used to collect data for testing the constructs of the research. Almost four hundred people in Thailand were asked to answer the questionnaire which was developed from an effective guideline to examine the constructs in TPB. Attitude, subjective norms, perceived behavioral control and past behavior were found significantly to be predictors of digital piracy intention. Moreover, the digital piracy intention was a greatest determinant of digital piracy behavior as described in TPB. The implication of this study is to identify the digital piracy factors which relate to people's behavior and to model the digital piracy behavior framework for better understanding of digital piracy behavior. In addition, using the result of this research, a better understanding of the cause of the piracy intention emerges. These can be used to help fighting with a software and digital media piracy in Thailand.

Keywords: Software piracy; pirate digital media; theory of planned behavior; digital piracy behavior model

How to Cooperatively Improve Broadband Security

Tiago Cruz¹, Thiago Leite¹, Patricio Baptista¹, Rui Vilão¹, Paulo Simões¹,
F. Bastos² and Edmundo Monteiro¹

¹CISUC - DEI, University of Coimbra, Portugal

²PT Inovação – Aveiro, Portugal

Abstract: The growth in the number of customers served by broadband connections (cable, xDSL) raises new concerns about potential security threats for ISPs, customers and third parties. A rapidly expanding customer base, mostly without adequate technical expertise, provided with permanent, high bandwidth connections constitute a risk scenario which the traditional security model adopted by ISPs, centered on their own internal infrastructure, is incapable of dealing with. As an alternative, we propose a new architecture based in a *shared security* model with close cooperation between ISPs and customer resources, taking advantage of the specific role and location of home gateways – as devices standing between the ISP and the customer network – to build a scalable, distributed intrusion detection and prevention system.

Keywords: Security architecture for broadband services, distributed IDS, home networks

Challenging Nato's Security Operations in Electronic Warfare: The Policy of Cyber-Defence

Marios Panagiotis Efthymiopoulos
Strategy International, Greece

Abstract: NATO is evolving. It is changing. It is estimated that in the end of 2009 or 2010, Allied member-states will hold or will have requested a renewed Strategic Concept as the current is considered no longer viable. In 21st century asymmetrical warfare, NATO requires to be technologically updated. This entails NATO to continue its effort to change. In terms of Electronic warfare, NATO is steadily unfolding its policy of Cyber-Defence. NATO needs to be operationally ready to counter all kinds of attacks, whether from the inside or the outside of its operational sphere of influence. It is the aim of this paper to provide the reader with the necessary information to firstly learn what has been done up to this date, in relations to NATO's operational preparations and in relations to its Cyber-Defence policy. In a second part, this paper shall examine and evaluate current policy decisions, if so made by the time of the paper's publication, as to understand whether a) NATO will actually take a major step into becoming involved into a new form of self-defensive or offensive war b) whether a political-military organisation of international members, such as NATO can actually afford working together. C) Whether the unfolding of Cyber-Defence policy will be implemented in NATO's operational environments, as to counter new phenomena of terrorism via the web. An explanation on network preparations and operations shall be made. At the same time an explanation shall be provided, why should the internet be so important to NATO's network centric operations and why does NATO need a Cyber-Defence policy. This paper is part of the author's wider topics of research made on NATO and its policies in the 21st century.

Keywords: NATO Cyber Defence Concept, NATO Cyber-Defence centre of excellence, North Atlantic council, transformation

A National RACI Chart for an Interoperable “National Cyper Security” Framework

Mohamed Dafir Ech-Cherif El Kettani¹ and Taïeb Debbagh²

¹University Mohammed V-Souissi, Rabat, Morocco

²Ministry of Industry, Commerce and NT, Rabat, Morocco

Abstract: Governments worldwide have faced serious Cyberterrorism threats, in a context where interoperability of “TransNational CyberSecurity Plans” is quite absent, in order to deal with incidents. It is important to know which agency or agencies should be given the responsibility for “National Cybersecurity”, in order to ensure that computer security will receive government-wide attention. Therefore, sectors and lead agencies should assess the reliability, vulnerability, and threat environments of the infrastructures and employ appropriate protective measures and responses to safeguard them. Responsibility Charting is a technique for identifying functional areas where there are process ambiguities, bringing the differences out, and resolving them through a cross-functional collaborative effort. We provide in this paper a “National RACI chart” that defines for each National Cyber Security process, who is “Responsible”, “Accountable”, “Consulted” and “Informed”. The “RACI chart” defines in detail what has to be delegated and to whom, and what kind of responsibility will be affected to one stakeholder instead of another. Thus, it will aid organisations and teams identifying the responsibility for specific elements at the national level.

Keywords: National cybersecurity, "RACI Chart", COBIT

Operational Aspects of Cyberwarfare or Cyber-Terrorist Attacks: What a Truly Devastating Attack Could do

Eric Filiol

ESIEA - Operational virology and cryptology laboratory, Laval, France

Abstract: Cyberwarfare and cyber-terrorism (mainly e-jihad) are nowadays a fashion topic. Since the Estonian attack in May 2007 and some intents of computer attacks by Al-Qaida, many papers have addressed, discussed not so say disputed about this. But those papers, for the most interesting ones, have just explained the effects of those attacks, drawn some conclusion and give only a very few technical details. But no paper has ever presented and pro-actively addressed the problem of operational and planning aspects of such cyber-attacks. In other words, how a terrorist group or a nation state could plan, organize, launch and conduct a real, large scale attacks? In this paper we present an in-depth reflection of how an attacker could plan such a wide-scale attack against a country, its infrastructure and its population, simply with a few clicks of a mouse. Based on real-cases analysis, military planning techniques and technical proactive research, we present a multi-step attack with the operational planning in mind (e.g. the attacker's view) without forgetting to explain how to technically execute each of the different phases of the attack. We will restrict to the case of attacks against a nation state conducted by a terrorist group or another country.

Keywords: IPSec tunnel, malware, encryption, eavesdropping, IPSec Security.

Information Security and Data Protection: The Role of the “Human Factor” in Organizations

Ulrike Hugl

University of Innsbruck, Innsbruck School of Management, Austria

Abstract: Information has become the new currency of organizations. The protection of corporate information assets is equally critical. Hence, information security continues to present a challenge for managers and IT professionals. Security and privacy incidents and further risks in organizations are influenced by the technological environment as well as by the behavior of staff. But a large part of information security research is technical-oriented with limited consideration of behavioral and organizational issues. An analysis of diverse studies presented in this paper adopts a broader perspective and shows a better understanding of information security with regard to the “human factor”. To ensure this broader perspective of information security this paper first focuses on a literature review analyzing influences on people’s behavior whilst also taking related organizational issues into account. The literature review concentrates on the one hand on a more internal-oriented level (security awareness approaches, policies and programs as well as support from top management) and on the other hand on a more external-oriented level (training of managers and employees). In a next step empirical studies—worldwide and covering European countries—are presented and analyzed regarding influences of the “human factor” on information security. The paper closes with a summary of the findings, a critical view on possible limitations and managerial implications. Results show that beside technical requirements the “people factor” plays a crucial role to secure and protect organizations’ critical information and data. Dangerous aspects on information security within organizations are being underestimated from both the management as well as from employees themselves. Awareness training is still less pronounced and implemented as well as in a large part not being consistent with organizations’ security policies, awareness programs, and other specific circumstances of each organization.

Keywords: Information security, data protection, information security policy/program/training, human factor, empirical study analysis, managerial implications

Messy Wars - Postmodern Way to see a War

Aki-Mauri Huhtinen¹ and Jari Rantapelkonen²

¹National Defence College, Helsinki, Finland

²Finnish Defence Forces, Riihimäki, Finland

Abstract: According to Douglas Kellner, the youth of the new millennium are the first generation to live the themes of postmodern theory. Entropy, chaos, indeterminacy, contingency, simulation, and hyper reality are not just concepts they might encounter in a seminar, but forces that constitute the very texture of their experience, as they deal with corporate downsizing and the disappearance of good jobs, economic recession, information and media overload, the demands of a high-tech computer society, crime and violence, identity crises, terrorism, war, and increasingly unpredictable future. For youth, contemporary life is a wild and dangerous ride, a rapid roller coaster of thrills and spills plunging into the unknown. Security authorities in western countries are highly productive and result oriented and they can be very effective when goal achievement is primary focus. For example, the stereotypical requirement of military leaders is also to be logical and rational who insist on covering all alternatives in decision making situation. Instead the inspirational style and radical new ideas or the supportive leadership dimension have often quite marginal. Typically, military organisations find itself up against serious deadline challenges, so command-and-control (C2) methods are quite natural leadership culture. In generally, in information age organisations has changed long C2 culture and move toward a more network-centric, asymmetric, and empowering environment. In military culture, this change will be a strategically issue. Security authorities of today will increasingly find themselves pitted against adversaries who “fight” without any rules or restraints. The applications of rational decision theory are worthless when dealing with those who are ready, if not anxious, to sacrifice their lives for the cause. In classical situation, “warriors” had to prepare to get kill. Today, terrorist in live and virtually, wants to get killed. Therefore, the whole planning, tactical and strategical doctrine is fundamentally undermined. In this article we examine the essential element of information time “warrior’s code”, i.e. the definite limits on what security authorities can and cannot do on extreme circumstance, has been changed by using new high-technological solutions.

Keywords: Postmodern, information war, media, C2

From Visible to Discreet and Interactive Management – Controlling in a Military Organisation in the Information Battle Space

Aki-Mauri Huhtinen

National Defence College, Helsinki, Finland

Abstract: We have travelled a long way from barbed wire to surveillance camera to the power of control in Western organisations. Barbed wire as a metaphor of control has a different order than Bentham's Panopticon or Michel Foucault's knowledge/power model. The barbed wire metaphor does not apply to general behaviour or educating the "better" individuals among those being observed, but is concerned simply with their position with respect to their boundary. The combination's sole purpose is preventing people from leaving an authorised area and entering a forbidden one. (Razac 2002, 97) Today, according to Oliver Razac, social control no longer relies on heavy barriers such as fences; they are too visible, and they offer too many vulnerable points of attack. The control of the information space has become discreet and interactive. Network-centric power is a way of empowering control. Of course, there is still a lot of use for barbed wire and classical visible power mechanisms, for example at the border between countries, like between the United States and Mexico, Chechnya and Russia and the Palestinian territories and Israel. (Razac 2002, 99, 107) This article examines the transformation of Western military organisations, their internal organisation, their external operational environments and their threats as they shift from visible to more invisible exercise of power. The central goal of armed forces in the information age is to organise themselves more on expertise and more like a networked society, which also affects the internal power structures of military organisations. An amazing revolution is taking place on the battlefield, starting to change not just how wars are fought, but also the politics, economics, laws, and ethics that surround war itself. Wars will become easier to start, that the traditional moral and psychological barriers to killing will fall, and that the "warrior ethos" the code of honour and loyalty which unites soldiers will erode. (Coker 2002 & 2007) Paradoxically, these new unmanned technologies will also seemingly bring war closer to our doorsteps, including even with videos of battles downloaded for entertainment. (Singer 2009)

Keywords: Military organization, C2, transformation management, information warfare

Assessing the Usability of Personal Internet Security Tools

Tarik Ibrahim¹, Steven Furnell^{1,2}, Maria Papadaki¹ and Nathan Clarke^{1,2}

¹University of Plymouth, UK

²Edith Cowan University, Perth, Western Australia

Abstract: The popularity of the Internet and all the services it provides has driven the demand for computers in the home. Unfortunately, these home users typically represent a group of users who are generally poorly educated about the dangers and threats that exist when connected to the Internet. To this end, security vendors have provided a variety of integrated security solutions that provide Anti-Virus, Firewalls and Intrusion Detection Systems to enable home users to become better protected. However, the need to rely upon users to make decisions about potential threats they have little or no information about is concerning at best. An analysis of user interfaces that relate to security have shown they frequently lack in providing usable interfaces that users are able to make informed decisions from. The aim of the paper is to support these home users by proposing a set of novel design criteria to enable the development of usable security alerts which are triggered by home security mechanisms. Drawing from literature, the criteria that are proposed take into account the unique usability issues that exist when dealing with information security: explicit and useful information, the ability to make a timely response and a consistent presentation of information. A walkthrough using a potentially problematic dialog from Norton 360 is used as a case study to highlight the current issues with the interfaces and to evaluate the proposed criteria. The findings of the evaluation reveal that the novel criteria are promising and the assessment of other security tools are required to make consistent and valuable recommendations.

Keywords; Security, usability, human computer interaction, intrusion detection systems, home users, Norton 360

Information Security Policies in Small Finnish Companies

Ilona Ilvonen

University of Technology, Tampere, Finland

Abstract: Existing literature presents many information security management frameworks for large companies. Information security policy is often described as part of these frameworks. Information security policy is therefore considered an essential tool for information security management by most relevant sources. Though information security in small companies faces the same requirements as in large companies, some differences do exist. Companies generally dispose of limited resources (e.g. time and money) to spend on information security measures. At the same time the amount and type of information to be protected is different. Most information security policies are drafted from the viewpoint of large companies. Small companies often have to translate policies that had been written for major companies in order to fit their needs: a costly contextual adjustment. However, how these policies can be applied, and which parts can be left out (due to the size of the company) is not much discussed in literature. Empirical materials show that small companies often simply choose not to document information security policies. This paper introduces work inspired by the parallel established between the literature and existing practice in small companies. The paper analyses several information security policy guidelines from the viewpoint of small companies. The guidelines are analyzed on how they instruct the documentation of information security policy, and whether they offer any alternatives. Empirical findings from interviews in small Finnish companies are reflected upon based on this analysis. Through a series of interviews conducted in support of the comparative analysis, the reasons for documenting or not documenting information security policy are discussed, along with other information security management issues. The ultimate goal of the paper is to offer an informative discussion on how certain information security policy guidelines could be applied to meet the needs of small companies.

Keywords: Information security policy, information security management, small company

The Dark Side of Complex Information Technology Intensive Firms: Reconciling the Imperative of Social Value Creation With Controversial Quasi-Regulatory Practices

Jonatan Jelen¹ and Marko Kolakovic²

¹Parsons The New School for Design, New York, USA

²University of Zagreb, Croatia

Abstract: The prominent Complex Information Technology-Intensive (CITI) firms of the likes of Google, eBay, Amazon, Facebook, Myspace, Craig's List and their foreign equivalents, such as the Chinese QQ and Baidu, for example, are becoming increasingly controversial, conflicted, and contradictory: In a noble way, on one hand, benefitting a wide variety of stakeholders via some original and novel business models, they have been creating presumably significant amounts of social value, far above and beyond the immediate private wealth they return to their stockholders. Their strategies are ostensibly cooperative and collaborative rather than combative, their structures accentuate resilience and nimbleness instead of monolithic hierarchies, their immediate focus is not on sheer scale but on intelligent scope, and their social position sets new benchmarks in terms of complex transformational effectiveness and leadership impact, i.e. deemphasizing simple transactional and productive efficiency. But there is a dark side to this graciousness: Some substantial portion of this new benevolent image and laudable reputation rests on a very specific framework of self interest and self preservation with three central tenets: regulatory capture, regulatory arbitrage, and regulatory opportunism. Carefully connecting the three stand-alone economic principles of monopolistic competition, intellectual property rights protection, and voluntary preemptive regulatory forbearance they have created power and control structures rivaling forms of command economies and statism. While some vocal critics of the legal community are primarily concerned with the legal and regulatory implications of the formation of code of the *business mode* (i.e. the way they *behave*), we will expose the elements of a framework grounding this new ambivalent attitude in - and explaining it from the underresearched perspective of - the *business model* (i.e. the way they *exist*).

Keywords: CITI firms, regulatory opportunism, regulatory arbitrage

Tamper Resistance of Contactless IC Card to Side-Channel Attacks

**Tetsutarou Kanno, Keisuke Iwai and Takakazu Kurokawa
National Defense Academy, Yokosuka city Japan**

Abstract: Information technology has been making rapid progress and is spreading through our daily life. Especially, RFID is becoming a popular device with its special features as its light weight, small size and link ability to database systems. RFID is now used as electronic money, and is taking the role of currency. For this usage, security technology equipped with cryptographic algorithms is necessary. For example, DES, Triple-DES, AES and RSA are equipped in many contactless IC cards. Cryptanalysis by many research reports the strength of these cryptographic algorithms is proved not to be deciphered in realistic time. This paper studies tamper resistance of a contactless IC card named "FeliCa". Although FeliCa is used mainly in our country, its precious information on tamper resistance is not published. We first observed the internal structure of FeliCa by measuring EM (Electronic Magnetic) amplitude over the whole area of this card. Then leaked information at the encryption process in FeliCa was observed. As a result, by eliminating carrier wave at 13.56MHz from observed EM waves with band eliminate filter, SEMA (Simple Electric Magnetic Attack) as well as SPA (Simple Power Attack) succeeded in finding out 16 pulses according to the rounds process of DES algorithm. Focusing on the last pulse, we experimented with DEMA (Differential Electric Magnetic Attack) and DPA (Differential Power Attack) against S-BOX consisting of combinatorial circuits in FPGA to simulate the cryptographic circuit. Although both attacks clearing showed efficient, DEMA marked its peak amplitude 15% higher than that of DPA.

Keywords: RFID, side-channel attacks, SEMA, DEMA, SPA, DPA

Multilevel Security in a Network-Centric Environment

Anssi Kärkkäinen and Catharina Candolin

The Finnish Defence Forces, Helsinki, Finland

Abstract: Effect based operations require information to be highly available and reliable, which in turn places demands on security of the network centric environment. The task of the network environment is to support information sharing among heterogeneous users, services and processes. However, the users of the network centric environment have various kinds of demands for information security, resulting in a variety of security domains. The purpose of multilevel security is to allow users from different security domains to share and process classified information using a common network infrastructure. The main objective of this paper is to define a multilevel security framework for network centric environments and propose some solutions for secure information sharing. Multilevel security is discussed considering content, communication, and network security levels. Multilevel security on the content level includes cross domain information sharing and accessibility issues. On the communication level, communication protocol and signaling issues are discussed. The network level deals with authentication and physical network access challenges. Multilevel security in network centric environment is not only limited to computer security issues but also includes policy, trust management and technical challenges. The paper also discusses limitations and challenges in implementing multilevel security.

Keywords: Multilevel security, protected core networking, content based information security

Applying a Cost Optimizing Model for IT Security

Jyri Kivimaa

Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia

Abstract: In real life good solution today is quite often better than perfect solution after month(s). That's the reason why we are developing IT Security/Cyber Security Graded Security Expert System - for quick and economically rational/optimal specifying needed security measures to protect concrete information accordingly to its concrete needed/required security goals/goals levels. Graded Security Expert System is based on the high level risk analysis (gives mainly a required levels of information security goals), on the Graded Security methodology (DOE 1999, NISPOM 2006) and on an IT security costs optimizing function/model.

Keywords: Graded security model, Pareto optimal security evaluation, high level risk analysis, information security metrics, information security requirements

Application and Analysis of Private Matching Schemes Based on Commutative Cryptosystems

Zbigniew Kwecka, William Buchanan and Duncan Spiers
Napier University, Edinburgh, UK

Abstract: Privacy issues are becoming a key focus with software systems. Surveys show that the invasion of privacy is among the things people fear the most from the coming years. These fears seem to be justified, in the light of recent events involving the UK government. Thus, according to the EU Telecoms Commissioner the UK government breach European privacy laws by allowing a group of UK based Internet Service Providers (ISPs) to intercept communications of their users for behavioural advertising purposes. In this case it was complaints from the concerned public that made the EU Commission examine the privacy implications. Yet, on the contrary, popularity of various social networking portals, where users publish their personal and sensitive data publicly, is growing. Therefore, some argue that users should not expect any level of privacy in the digital world. Such claims are backed-up by the fact that majority of Internet users are unconcerned about the *digital footprint* they leave behind. What is overseen is the control factor. Users want to have the right to decide what information about their lives is in the public domain. Consequently, 'one-size fits all' solution to privacy concerns does not exist, as everybody perceives privacy in a slightly different way. Therefore, parties involved in data-handling, including social networking portals, need to research and implement privacy technologies that can keep their customers happy and make the operation comply with local security and privacy directives in many locations around the globe. This paper gives an insight on how Privacy Enhancing Technologies (PETs) can be used to perform private matching operations in large datasets. These operations can be used by data-holders and individuals to compare or to retrieve information in a private manner in cases where trusted third party does not exist or trusted third party it is used trusted for authentication purposes only. Thus, they can provide users with greater control over how their data is used. They include equality tests, dataset intersections, dataset equijoins, and symmetric private information retrieval protocols. Application of such private operations lies in the area of pervasive computing, database interaction, auditing and data acquisition. Here it is shown that PETs based on commutative cryptosystems are most efficient in performing these operations. Therefore, these cryptosystems are examined in detail. Currently anyone wishing to implement PETs based on commutative cryptosystems will quickly notice that such cryptosystems cannot be found in any of the popular cryptographic suites. The reason for this is the fact that these cryptographic algorithms are expensive to run in comparison with other encryption technologies and have limited area of usage in security applications. Thus, the key contribution of this paper is a guide to implementing commutative cryptosystems, using common open-source cryptographic packages. Consequently, this should enable developers and researchers to further investigate the existing PETs and propose new systems employing the notion of the commutative cryptography.

Keywords: Commutative cryptography, data acquisition, privacy enhancing technologies, data mining, private matching

Security Framework for Information Systems

José Martins¹, Henrique dos Santos² and Paulo Nunes³

¹Academia Militar - Cinamil, Lisboa, Portugal

²University of Minho - Department of Information Systems, Guimarães, Portugal

³Academia Militar - Cinamil, Lisboa, Portugal

Abstract: Nowadays, information is one of the most important resources in an organization, supporting most of the business processes. So, organizations must try to guarantee at all times information's fundamental properties: confidentiality, integrity, and availability. Information Systems are a determining factor for the organization's capability, consisting of a tool that stimulates its productivity, indispensable in the decision making process at the various levels of management. The current network society supported primarily through Internet, presents new threats to information networks that support organizational Information Systems, independently of their dimension, nature, organization and technological resources. This scenario requires the utilization of a Security Framework in order to guarantee the information security, and also to integrate a set of different organizational views: a scientific community (conceptual model); decider's perception (behavioural model); and a technological model, as support for business processes. An established security policy and operational identification and evaluation methodology of risk must be distinguished in order to protect an organization from threats towards its information systems or information resources which it is responsible for. In this paper we propose a Security Framework for organizational Information Systems, to guarantee the security of the major information actives and to serve as a possible model of security information management, to supporting the decision making process on information security and management. We search to minimize the possible actions of Information Warfare / Competitive Intelligence, outlining in this framework the various standards of good information security practises. We have as an objective to guarantee the protection of Information Systems from the various methods of attack in use and types of weapons utilized.

Keywords: Information systems, information warfare, information security management and analysis and evaluation of risk

Theoretical Model for Creating a Nation-State Level Offensive Cyber Capability

Rain Ottis

Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia

Abstract: Recent events in Estonia and Georgia have elevated the threat of cyber attacks to the international consciousness. While this has added visibility to the topic, it has not brought more clarity to the discussion. Terms like cyber warfare and cyber terrorism are widely used, but their definitions are rarely agreed upon. As a result, there is a lot of skepticism about the true nature of cyber threats and whether governments are engaging in such attacks in cyberspace. It should be safe to assume that all governments are developing and using defensive cyber capabilities to some degree. Defending computer systems is considered a right and typically legal frameworks support such activity. As soon as one goes on the cyber offensive, however, they are off the map. There is little consensus, let alone legal guidance, regarding the use of cyber attacks to further a political or military goal. Very few nations have announced an offensive capability in cyber space, but it is reasonable to assume that more are covertly creating such a capability. In this paper the term offensive cyber capability is used instead of the better known computer network attack (CNA). Offensive cyber capability differs from CNA by including actors from outside the direct control of the government, such as freelance hackers, criminals and flash mobs as possible extensions to a nation-state's offensive capability. This paper offers a theoretical model composed of three approaches that a nation-state might use when creating an offensive cyber capability. First, the traditional use of 'own forces' is analyzed. The second way is to cultivate a volunteer force that can be guided to attack designated targets with little or no attribution to the government. The last approach is to outsource the problem to digital mercenaries. Each option has unique benefits and drawbacks, while some aspects remain universal across the board. In reality, the most effective approach is most likely a combination of all three.

Keywords: Offensive cyber capability, cyber attack, computer network attack, People's War

Applying Poker Strategies, Tactics and Rapid Decision Making Methods to Military Decision Making on the Tactical Level

Evert Paas

Estonian Defence Forces, Tallinn, Estonia

Abstract: Poker is a thoroughly researched and analyzed game where several competing adversaries must deal with risk management, opponent modeling, deception as well as using untrusted and incomplete information in order to succeed. This mirrors the complexities of the real world, whether in business, politics or warfare. As a consequence, poker has been used as a test environment for researching incomplete information handling, decision making, opponent behavior modeling and deception operations. In today's no limit poker games one can clearly recognize the classic military strategies and tactics that are to some degree based on modeling opponent behavior, various forms of deception and taking advantage of weaknesses identified in the enemy. And *vice versa*, one can often detect typical poker themes in military planning, decision making and leadership process. This research paper describes a very basic approach to implementing the poker modification *No Limit Texas Hold'em tournament model decision making process* (NTD) to *modern military operation decision making process* (MMD) in order to gain in speed, flexibility, adaptiveness and robustness in tactical level decision making process. Three main results are presented in this paper: (1) a system representing the corresponding military and poker terms in order to transfer information from one subject area to the other; (2) a system for describing tactical military situations using letter encoding; (3) and a table for making a suitable choice in a given tactical military situation based on the presence of factors that are defined as critical for the given problem. The paper consists of six main parts: (1) presenting arguments in support of using NTD for MMD; (2) identifying common critical factors for MMD and NTD; (3) finding corresponding elements in MMD and NTD in order to transfer information between the systems; (4) constructing a table for assessing a situation based on identified common critical factors; (5) constructing a table for making a suitable decision that allows using NTD strategies and tactics to be used in MMD based on the presence of critical factors; (6) remarks on future research on this topic. The results presented in this paper simplify the analysis of case studies of military operations. They allow the representation of military operations with a compact system of tactical moves, implemented with a simple letter encoding system.

Keywords: Military decision making process, poker decision making process, rapid decision making methods, strategy, tactics

Cellular Warfare

Karlis Podins

Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia

Abstract: In this paper we explore the possibilities of cyber warfare activities connected to cell phone networks. We analyze known attacks that originate in and/or target cellular phone networks as weapons of cyber warfare. The historic high reliability of cellular networks has caused a significant reliance on them as the sole means of communication in many developed countries, making it a part of national critical infrastructures. The growing popularity of smartphones opens up cellular network both to the advantages and disadvantages currently associated with the internet. The possibility that an attacker could deny cellular voice/SMS services to legitimate users is already widely discussed. Such attacks could begin by using internet services to send SMS messages or using a botnet consisting of smart cellular phones. Such attacks could be aimed at a core infrastructure to shut down or cripple a cellular network; even very small botnets could be used to launch attacks that disrupt or limit cellular services in targeted geographical areas. We evaluate the possible usage of such techniques both by nation-states and by non-state-actors that could be used as effective digital cover for their actions. The advantage of such attacks is that virtually no hardware is needed to launch them and all activities can be developed, tested and controlled remotely from a safe location. This makes them a good choice for parties seeking asymmetric advantages. Another technique we discuss is the use of cellular botnets to launch a denial of service attack against emergency call services or other phone lines in critical infrastructure. We note that the excellent record of cellular networks does not prove that cellular networks are reliable; we believe that there has simply been a lack of real-world attacks so far. An overview of current and possible countermeasures is provided to show the level of complexity of such a task. We estimate that the importance of this threat will increase together with the rise in both the popularity and the complexity of smartphones.

Keywords: Keywords: cellular networks, denial of service, cyber warfare, botnets

Security Analysis and Modelling Framework for Critical Infrastructure Systems

Graeme Pye and Matthew J. Warren
School of Information Systems, Faculty of Business and Law, Deakin University, Geelong, Australia

Abstract: The provision and delivery of many of the services that modern society enjoys are the result of ubiquitous critical infrastructure systems that permeate across many sectors of the Australian community. Moreover, the integration of technological enhancements and networking interconnections between critical infrastructure systems has heightened system interdependence, availability and resilience, including the efficient delivery of services to consumers within Australia's industrialised society.

This research delivers a system security analysis and system modelling framework tool based on an associated conceptual methodology as the basis for assessing security and conceptually modelling a critical infrastructure system incident. The intent is to identify potential system security issues and gain operational insights that will contribute to improving system resilience, contingency planning development applicable to disaster recovery and ameliorating incident management responses for Australian critical infrastructure system incidents.

Keywords: Critical infrastructure, system, security, analysis, modelling

Network Centric Operations: the “SIVICC” Case Study

Nuno Rosário and Paulo Nunes

CIIWAC, Guarda Nacional Republicana, Largo do Carmo 1200-092

LISBOA, Portugal

CIIWAC, CINAMIL, Academia Militar, Paço da Rainha 29 1169-203

LISBOA, Portugal

Abstract: The aim of this paper is to analyze the application of the Network Centric Operations (NCO) Conceptual Framework within the scope of a Command and Control (C2) Maritime Surveillance System. This system, designated as *Sistema Integrado de Vigilância, Comando e Controlo* (SIVICC), will be implemented in the near future along the West Portuguese Coastline. The main question to clarify is to know how the NCO tenets may influence and enhance the operational use of a technological system like SIVICC, converting it on a dynamic learning system. Being SIVICC still a prototype system, available information about its design and future field deployment is sometimes scarce and incomplete. In order to support a possible adoption of NCO tenets some SIVICC project assumptions are assumed. The SIVICC implementation will be based on the idea of a centralized integration of maritime surveillance sensors throughout the Portuguese coast and aims to strengthen the Guarda Nacional Republicana (GNR) overall operational capability on the fulfillment of its Mission in the area of surveillance, patrolling and land and maritime interception of boats which may be committing a criminal offense, such as drug traffic, people traffic or smuggling. Starting by presenting a theoretical background of NCO related concepts, this paper highlights the advantages associated to the adoption of NCO principles and how historically they have evolved. Afterwards, some additional information about other European Maritime Surveillance Systems (like the French, the Spanish and the current Portuguese System) is presented, in order to frame these systems as operating processes which demand an adequate and quick answer to improve its operational performance. Finally, some answers to the questions initially raised will be derived, based upon the fact that the adoption of NCO tenets will bring operational benefits to SIVICC, such as a reduction of response times, better agility, higher level of interoperability and the overall quality enhancement of the System. Concluding remarks will highlight the added value of adopting the NCO conceptual framework in Law Enforcement Maritime Surveillance Systems in order to improve its responsiveness to face the threat dynamics and increase its mission effectiveness.

Keywords: Network Centric operations, interoperability, agility, flexibility and maritime surveillance systems

White Force Tracking (WFT)

Tapio Saarelainen

National Defence University, Helsinki, Finland

Abstract: This paper focuses on the possibilities of locating the White Force using the available COTS-technology along with the Blue and Red Force tracking on the battlefield. White Force Tracking (WFT) is an issue that has not been studied earlier nor discussed in non-classified scientific forums. The term 'White Force' covers individuals working in crises areas for specific aid agendas, and determining the location of White Forces, such as members of Non-Governmental Organizations (NGOs), is crucial in all theatres. Currently, several options are available for utilizing unused sensors to gain optimal results needed in location services. As asymmetric warfare replaces traditional battlefields, it is necessary to be able to recognize and classify the impartial actors in the theatre, since there are no front lines and recognition of friend and foe is an insecure process. The White Force needs to be recognized in asymmetric warfare, Peace Support Operations (PSO), Peace Forcing Operations (PFO), unconventional warfare, especially in built-up urban areas. Particularly, in PSOs, PFOs, and in military operations other than war (MOOTW), the given situation varies from riot control to pre-war situations in an unpredicted pace, and thus it is crucial to avoid fratricide and impartial casualties. This study introduces few technical principles and methods available for locating different types of White Force actors while there is an ongoing war in the vicinity. The outcome of using the presented techniques will be measured as reduction of impartial casualties. White Force Tracking (WFT) is an unused key for winning the hearts and minds in the military theatre. Soldiers constantly need to locate and, if possible, to pinpoint the White Forces in relation to friendly maneuvers. This aims at avoiding unnecessary collateral damage in the crises area. The locating of White Forces becomes significant when using weapons with great destruction power, especially beyond the horizon. Similarly, the level of Situational Awareness has to remain high, for before executing the use of weapon systems, the Commanding Officer has to be in control of the situation to avoid both fratricide (Blue Force [BF]) and impartial casualties (White Force [WF]).

Keywords: White Force tracking, Situational Awareness (SA), Combat Identification (CID), Target Identification (TID), sensors

Computer-Aided Warriors for Future Battlefields

Tapio Saarelainen and Jorma Jormakka

National Defence University, Helsinki, Finland

Abstract: This paper describes a new perspective on discussions related to the Future Dismounted Infantry Warrior. The present approach is based on system optimization and on defining precise levels for the Warrior. Currently, world militaries are facing new threats while not being able to afford to provide all their Warriors with the newest gear. Equipping and training Warriors is a time- and money-consuming process, which means that it is useless and too expensive to equip every Warrior with top-gear. Thereby system requirements and system engineering provide the tools for determining the need of the novel tools for Command, Control, Communications, Computer, Intelligence and Information (C⁴I²) environment at each Warrior level. The level and versatility of Network Centric Operations (NCO) in battlefields have increased in the present wars. In order to increase Situation Awareness (SA) in all Warrior levels, versatile and optimized network solutions have been adopted. Computer-aided Warriors utilize all means available to enhance their SA to complete the mission tasked with minimum or zero casualties. This paper argues for the efficiency of the hierarchy-based Warrior system instead of the principle of equipping all the Warriors with the newest Commercial off the Shelf (COTS) gear. This study demonstrates that in Human Machine Interface (HMI) -based Warrior solutions the key relationship is between different Warrior levels and proposes that the Future Warrior is based on the three production line Warriors equipped with precise, task- and level-dependent gear. This paper, furthermore, discusses the interconnectedness of the trained Warriors and their gear in the light of the following three Warrior levels: 1) The basic Warrior at the bottom level, 2) the Readiness Brigade Warrior, and 3) the Special Forces Warrior.

Keywords: Future Warrior, production line Warrior, HMI, computers, COTS, network centric operations

RFID: Big Brother Global?

Cristina Sousa^{1,2}, Pedro Teixeira Pereira¹, Sérgio Tenreiro de Magalhães¹, Leonel Santos³ and Henrique Santos³

¹Universidade Católica Portuguesa, Braga, Portugal

²Escola Sec. de Fontes Pereira de Melo, Porto, Portugal

³Universidade do Minho, Guimarães, Portugal

Abstract: Nowadays, one of the most utilized technologies, which simplifies the daily life of millions of people, is the RFID (Radio Frequency Identification). This technology works on a radio frequency emission that automatically and without the necessity of human intervention identifies “tags” placed on people, animals, equipment and packages that contain information about hosts. This technology first appeared during the Second World War due to the necessity of authentication. It has since proved to have many varied uses but it also has many vulnerabilities that could be taken advantage of by evil doers. The main one obviously, being the violation of the right to privacy of citizens everywhere. Nowadays this technology is used in many of our daily routines. In the near future, there are many different areas which will seek to avail of its usefulness, such as health care, safety and security, commerce, industry or common services. In a world full of computers, all kinds of objects and even people will be tagged for easy automatic recognition. Nevertheless, the excessive and abusive use of this technology by business people and governments has raised important concerns that need to be studied and discussed. This article revises the areas and forms in which this technology is used, so it is possible to understand how the combination of the available information provided by RFID represents a threat to people and systems, whether they are private or public. The study developed shows that RFID have the potential to be used by individuals, organizations and governments with evil intentions to implement systems that could represent threats, such as violation of privacy, the strengthening of control by government dictatorships and other criminal acts, like theft, industrial espionage or even terrorist attacks. These potential threats are the scope of this work.

Keywords: RFID, privacy, big brother, security, technology

Supply Chain Management Security: The Weak Link of Australian Critical Infrastructure Protection

**Matthew Warren and Shona Leitch
Deakin University, Victoria, Australia**

Abstract: Secure management of Australia's commercial Critical Infrastructure presents ongoing challenges to both the owners of this infrastructure as well as to the Australian Federal government. The security management process is currently managed through high-level information sharing via collaboration, but does this situation suit the commercial sector? One of the issues facing Australia is that the majority of critical infrastructure resides under the control of the business sector and certain aspects such of the critical infrastructure such as Supply Chain Management (SCM) systems are distributed entities that span a number of commercial organisations. Another issue is that these SCM systems can be used for the transportation of varied items, such as retail items or food. This paper will explore the security issue related to food SCM systems and their relationship to critical infrastructure. The paper will focus upon the security and risk issues associated with SCM system protection within the realms of critical infrastructure protection. The paper will review the security standard ISO 28000 - Supply Chain Security Management Standard. The paper will propose a new conceptual security risk analysis approach that will form the basis of a future Security Risk Analysis approach. This new approach will be aimed at protecting SCM systems.

Keywords: Critical infrastructure protection, risk and supply change management