Abstracts of Papers Presented at the 14th European Conference on Cyber Warfare and Security

ECCWS-2015

The University of Hertfordshire Hatfield, UK

2-3 July 2015

Papers submitted to this conference have been double-blind peer reviewed before final acceptance 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.

This Booklet of abstracts and other conference materials is provided to conference participants for use at the conference.

Conference Proceedings

The Conference Proceedings is a book published with an ISBN and ISSN. The proceedings have been submitted to a number of accreditation, citation and indexing bodies including Thomson ISI Web of Science and Elsevier Scopus for indexing.

The Electronic version of the Conference Proceedings is available to download from **DROPBOX**. (**http://tinyurl.com/ECCWS2015**) Select Download and then Direct Download to access the Pdf file. Free download is available for conference participants for a period of 2 weeks after the conference.

The Conference Proceedings for this year and previous years can be purchased from http://academic-bookshop.com

E-Book ISBN: 978-1-910810-29-3
E-Book ISSN: 2048-8610
Book version ISBN: 978-1-910810-28-6
Book Version ISSN: 2048-8602
CD Version ISBN: 978-1-910810-30-9
CD Version ISSN: 2048-8629

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

Contents

Preface

These proceedings represent the work of researchers participating in the 14th European Conference on Cyber Warfare and Security (ECCWS 2015) which is being hosted this year by the University of Hertfordshire, Hatfield, UK on the 2-3 July 2015.

ECCWS is a recognised event on the International research conferences calendar and provides a valuable platform for individuals to present their research findings, display their work in progress and discuss conceptual and empirical advances in the area of Cyberwar and Cyber Security. It provides an important opportunity for researchers and managers to come together with peers to share their experiences of using the varied and expanding range of Cyberwar and Cyber Security research available to them.

The conference this year will be opened with a keynote presentation by Professor Madjid Merabti from the School of Computing & Mathematical Sciences, Liverpool John Moores University (LJMU), UK. Majid will address *The Challenge of cascading effects of cyber-attacks in a network of critical infrastructures*.

The second day of the conference will be opened by Professor John Clark from the Department of Computer Science, University of York, UK - Royal Society Wolfson Research Merit Award Holder. John will be providing some insight to the question *Security: Is this the best we can do?*

With an initial submission of 107 abstracts, after the double blind, peer review process there are 38 academic Research papers and 9 PhD papers Research papers, 3 Master's research Papers and 2 Work In Progress papers published in these Conference Proceedings. These papers come from many different countries including: Australia, Austria, Czech Republic, Finland, France, Greece, Ireland, Israel, Istanbul, Italy, Norway, Pakistan, Portugal, Russia, South Africa, Sweden, Turkey, UK, USA

We wish you a most interesting conference.

Dr Nasser Abouzakhar
Conference Chair
July 2015

Conference Committee

Conference Executive

Dr. Nasser Abouzakhar, University of Hertfordshire, UK
Dr Joseph Spring, University of Hertfordshire, UK
Dr Colin Egan, University of Hertfordshire, UK
Dr Hannan Xiao, University of Hertfordshire, UK
Dr Martina Doolan, University of Hertfordshire, UK
Dr Edwin "Leigh" Armistead, Edith Cowen University, Perth, Australia

Mini track chairs

Dr Aki-Mauri Huhtinen, Finnish National Defence University, Finland
Dr Jari Rantapelkonen, Finnish National Defence University, Finland
Dr Mils Hills, The University of Northampton, UK
Captain Guy Batchelor, British Army, UK

Committee Members

Dr. Mohd Faizal Abdollah (University Technical Malaysia Melaka, Melaka); Dr. Nasser Abouzakhar (University of Hertfordshire, UK); Dr. Kari Alenius (University of Oulu, Finland); Chaminda Alocious (University of Hertfordshire, UK); Prof. Antonios Andreatos (Hellenic Air Force Academy, Greece); Dr. Olga Angelopoulou (University of Derby, UK); Dr. Leigh Armistead (Edith Cowan University, Australia); Colin Armstrong (Curtin University, Australia, Australia); Johnnes Arreymbi (University of East London, UK); Debi Ashenden (Cranfield University, Shrivenham, UK); Dr. Darya Bazarkina (Sholokhov Moscow State Humanitarian University, Russian Federation); Laurent Beaudoin (ESIEA, Laval, France); Ass Prof. Maumita Bhattacharya (Charles Sturt University, Australia); Prof. Matt Bishop (University of California at Davis, USA); Andrew Blyth (University of Glamorgan, UK); Colonel (ret) Colin Brand (Graduate School of Business Leadership, South Africa); Dr. Svet Braynov (University of Illinois at Springfield, USA); Prof. Larisa Breton (University of the District of Columbia, USA); Bill Buchanen (Napier University, UK); Dr. Joobin Choobineh (Texas A&M University, USA); Bruce Christianson (University of Hertfordshire, UK); Dr. Maura Conway (Dublin City University, Ireland); Dr. Paul Crocker (Universidade de Beira Interior, Portugal); Prof. Tiago Cruz (University of Coimbra, Portugal); Dr. Christian Czosseck (CERT Bundeswehr (German Armed Forces CERT), Germany); Geoffrey Darnton (Bournemouth University, UK); Josef Demergis (University of Macedonia, Greece); Dr. Martina Doolan (University of Hertfordshire, UK); Paul Dowland (University of Plymouth, UK); Marios Efthymio-

poulos (Political Science Department University of Cyprus, Cyprus); Dr. Colin Egan (University of Hertfordshire, Hatfield, UK); Dr. Ramzi El-Haddadeh (Brunel University, UK); Daniel Eng (C-PISA/HTCIA, China); Prof. Dr. Alptekin Erkollar (ETCOP, Austria); Prof. Robert Erra (ESIEA PARIS, France); John Fawcett (University of Cambridge, UK); Prof. Eric Filiol (Ecole Supérieure en Informatique, Electronique et Automatique, France); Dr. Chris Flaherty (University of New South Wales, Australia); Prof. Steve Furnell (University of Plymouth, UK); Assoc. Professor Javier Garci'a Villalba (Universidad Complutense de Madrid, Spain); Kevin Gleason (KMG Consulting, MA, USA); Dr. Michael Grimaila (Air Force Institute of Technology, USA); Prof. Stefanos Gritzalis (University of the Aegean, Greece); Dr. Marja Harmanmaa (University of Helsinki, Finland); Ulrike Hugl (University of Innsbruck, Austria); Aki Huhtinen (National Defence College, Finland); Bill Hutchinson (Edith Cowan University, Australia); Dr. Berg Hyacinthe (State University of Haiti, Haiti); Dr. Abhaya Induruwa (Canterbury Christ Church University, UK); Hamid Jahankhani (University of East London, UK); Dr. Helge Janicke (De Montfort University, UK); Joey Jansen van Vuuren (CSIR, South Africa); Saara Jantunen (University of Helsinki, Finland); Andy Jones (BT, UK); Dr. Audun Josang (University of Oslo, Norway); James Joshi (University of Pittsburgh, USA); Nor Badrul Anuar Jumaat (University of Malaya, Malaysia); Maria Karyda (University of the Aegean, Greece); Ass Prof. Vasilis Katos (Democritus University of Thrace, Greece); Dr. Anthony Keane (Institute of Technology Blanchardstown, Dublin, Ireland); Jyri Kivimaa (Cooperative Cyber Defence and Centre of Excellence, Tallinn, Estonia); Dr. Spyros Kokolakis (University of the Aegean, Greece); Prof. Ahmet Koltuksuz (Yasar University, Dept. of Comp. Eng., Turkey); Theodoros Kostis (Hellenic Army Academy, Greece); Prashant Krishnamurthy (University of Pittsburgh, USA); Dan Kuehl (National Defense University, Washington DC, USA); Peter Kunz (Diamler, Germany); Pertti Kuokkanen (Finnish Defence Forces, Finland); Dr. Erikk Kurkinen (University of Jyväskylä, Finland); Takakazu Kurokawa (National Defence Acadamy, Japan); Rauno Kuusisto (Finnish Defence Force, Finland); Tuija Kuusisto (National Defence University, Finland); Dr. Laouamer Lamri (Al Qassim University and European University of Brittany, Saudi Arabia); Michael Lavine (John Hopkins University's Information Security Institute, USA); Martti Lehto (National Defence University, Finland); Tara Leweling (Naval Postgraduate School, Pacific Grove, USA); Paul Lewis (technology strategy board, UK); Peeter Lorents (CCD COE, Tallinn, Estonia); James Malcolm (University of Hertfordshire, UK); Hossein Malekinezhad (Islamic Azad University,Naragh Branch, Iran); Mario Marques Freire (University of Beira Interior, Covilhã, Portugal); Ioannis Mavridis (University of Macedonia, Greece); Rob McCusker (Teeside University, Middlesborough, UK); Jean-Pierre Molton Michel (Ministry of Agriculture, Haiti); Durgesh Mishra (Acropolis Institute of Technology and Research, India); Dr. Yonathan Mizrachi (University of Haifa, Israel, Israel); Edmundo Monteiro (University of Coimbra, Portugal); Evangelos Mousta-

kas (Middlesex University, London, UK); Dr. Kara Nance (University of Alaska Fairbanks, USA); Muhammad Naveed (IQRA University Peshawar, Pakistan, Pakistan); Mzukisi Njotini (University of South Africa, South Africa); Rain Ottis (Cooperative Cyber Defence Centre of Excellence, Estonia); Tim Parsons (Selex Communications, UK); Michael Pilgermann (University of Glamorgan, UK); Engur Pisirici (govermental - independent, Turkey); Dr Bernardi Pranggono (Glasgow Caledonian University, UK); Dr. Muttukrishnan Rajarajan (City University London, UK); Andrea Rigoni (Booz & Company,, USA); Dr. Neil Rowe (US Naval Postgraduate School, Monterey, USA); Raphael Rues (DigiComp Academy, Switzerland); Prof Vitor Sa, (Catholic University of Portugal, Portugal); Filipe Sa Soares (University of Minho, Portugal); Dr Char Sample (Carnegie Mellon University/CERT, USA); Prof. Henrique Santos (University of Minho, Portugal); Prof. Chaudhary Imran Sarwar (Mixed Reality University, Pakistan); Dr. Damien Sauveron (Mathematics and Computer Sciences, University of Limoges, France); Sameer Saxena (IAHS Academy, Mahindra Special Services Group , India); Prof. Dr. Richard Sethmann (University of Applied Sciences Bremen, Germany); Dr. Yilun Shang (Singapore University of Technology and Design, Singapore); Prof. Paulo Simoes (University of Coimbra, Portugal); Prof. Jill Slay (University of South Australia, Australia); Dr Joseph Spring (University of Hertfordshire, UK); Anna Squicciarini (University of Milano, Italy); Iain Sutherland (Noroff University College, Kristiansand, Norway.); Jonas Svava Iversen (Danish Broadcast Corporation, Denmark); Anna-Maria Talihärm (Tartu University, Estonia); Dr. Selma Tekir (Izmir Institute of Technology, Turkey); Prof. Sérgio Tenreiro de Magalhães (Universidade Católica Portuguesa, Portugal); Prof. Dr. Peter Trommler (Georg Simon Ohm University Nuremberg, Germany); Betrand Ugorji (University of Hertfordshire, UK); Craig Valli (Edith Cowan UniversitY, Australia); Rudi Vansnick (Internet Society, Belgium); Richard Vaughan (General Dynamics UK Ltd, UK); Stilianos Vidalis (Newport Business School, Newport, UK); Dr. Natarajan Vijayarangan (Tata Consultancy Services Ltd, India); Dr Sune von Solms (Council for Scientific and Industrial Research, South Africa); Marja Vuorinen (University of Helsinki, Finland); Prof Mat Warren (Deakin University, Australia, Australia); Dr. Kenneth Webb (Edith Cowan University, Australia); Dr. Santoso Wibowo (Central Queensland University, Australia); Dr. Trish Williams (Edith Cowan University, Australia); Simos Xenitellis (Royal Holloway University, London, UK); Dr Hannan Xiao (University of Hertfordshire, UK); Dr. Omar Zakaria (National Defence University of Malaysia, Malaysia)

Biographies

Conference Chair

Dr. Nasser Abouzakhar is a senior lecturer at the University of Hertfordshire, UK. Currently, his research is mainly focused on critical infrastructure security, industrial control systems security and applying machine learning solutions to various Internet and Web security related problems. He received PhD in Computer Sci Engg in 2004, University of Sheffield, worked as a lecturer at the University of Hull in 2004-06 and a research associate at the University of Sheffield in 2006-08. He is a technical studio guest to various BBC World Service Programmes such as Arabic 4Tech show, News hour programme and Breakfast radio programme. Nasser is a BCS assessor for the accreditation of Higher Education Institutions (HEIs) in the UK, BCS chartered IT professional (CITP), CEng and CSci.

Conference Co-Chair

Dr. Martina A. Doolan is a UK National Teaching Fellow and a Principal Lecturer in Computer Science at the University of Hertfordshire in the UK. Martina's research interests include: technology mediated communication and collaboration, social media and security.

Dr. Joseph Spring is a senior lecturer at the University of Hertfordshire. His research interests include the application of mathematical and computer based concepts to the development of secure systems in cyber space. He has published internationally in areas relating to quantum voting, entanglement, probability, stochastic calculus, network intrusion, game theory and misbehaviour.

Programme Co-Chairs

Dr Colin Egan is a senior lecturer at the University of Hertfordshire, UK. His research area is mainly focused on Computer Architecture and he has a developing interest in Cyber Security especially from the hardware view point. He received his PhD in Computer Architecture in 2000, from the University of Hertfordshire and has continued his re-

search/teaching work there since. Earlier in Colin's career he worked in Neurotoxicology and he has a number of published papers in this area. Colin also has a number of research papers in the area of accessibility issues in Teaching and Learning. His research papers have been published in various international journals and conference

Dr. Hannan Xiao received her PhD from the Department of Electrical & Computer Engineering, the National University of Singapore in 2003, and B.Eng and M.Eng degrees from the Department of Electronics & Information System Engineering, the Huazhong University of Science & Technology, China. Dr Xiao has been with the University of Hertfordshire as a lecturer/senior lecturer since October 2003. Dr Xiao has been actively involved in research and development in the areas of mobile ad hoc and sensor networks. She proposed and developed one of the first Quality of Service models for mobile ad hoc networks (FQMM). The model has 400+ citations in google scholar as in January 2014 and has been used in several textbooks in computer networks. Dr Xiao is currently engaged in several research projects in the areas of distributed systems and security.

Mini Track Chairs

Dr Aki Huhtinen is a professor at Finnish National Defence University. His expertise areas are military leadership, and philosophy of war.

Dr Jari Rantapelkonen is a professor at Finnish National Defence University. His expertise areas are strategic communication and operational art and tactics.

Dr Mils Hills was the first social anthropologist to be employed by the UK Ministry of Defence, rising to be head of the UK capability in the human factors of Information Warfare. Later seconded to a strategic role in the UK Cabinet Office, Mils has also been a consultant specialising in helping organisations protect their decision-making capability against conventional and unconventional challenge.

Keynote Speakers

Professor Madjid Merabti is Director of the School of Computing & Mathematical Sciences, and a Professor of Networked Systems at Liverpool John Moores University (LJMU). Madjid has over 200 publications in these areas and he leads the Distributed Multimedia Systems Group which has a number of government and industry supported research projects. He is also Director of PROTECT – A Critical Infrastructure Research Centre that addresses the challenges of building and managing 21stcentury new critical infrastructure systems that are not only resilient to unpredicted changes, but are secure from external attacks. On the teaching and academic development front, he has acted as a reviewer for the UK Higher Education Quality Assurance Agency over a number of years in assessing degree standards. He regularly review BSc and MSc programme offerings at various UK Universities and overseas. He has graduated over 35 PhD students and receives many invitations to examine PhD theses.

Professor Madjid Merabti will be speaking at ECCWS 2015 on *"The Challenge of cascading effects of cyber-attacks in a network of critical infrastructures".*

Dr John Clark did Mathematics and then an MSc in Applied Statistics at Oxford. He then joined the security division of the software and systems house Logica in 1987 and in 1992 joined the University of York. John has been research active since around 1997 (with a few outputs before then). His personal and supervised research work concentrates on aspects of security and software engineering John was awarded a PhD in 2002 and promoted to a Personal Chair in January 2005. Since April 2009 he has been Deputy Head of Department (Responsible for Research). John views his research role largely as helping the people who work with him get on in their careers by producing excellent research. John is currently engaged in personal research that is exceptionally ambitious but with significant chances of nothing meaningful coming out of it, but then again, if something does.... Most would describe John's research work as largely applied. He don't distinguish too strongly between theory and applied.

Dr John Clark will be speaking at ECCWS 2015 on *"Security: Is this the best we can do?".*

Biographies of Presenting Authors

Muhammed Bello Abdulazeez is currently PhD Student in Computer Science at the University of Liverpool UK and a Senior Engineer, Technical at the Nigeria Communications Satellite Limited. His research is in the area of Intrusion Detection and Prevention Systems in the Cloud environment. His main area of interest is Dynamic protocol Analyses to defend against Denial of Service (DoS) attacks. His Other areas of interest are; Distributed Systems Security, Secure Payment Systems and Information Warfare.

Shakeel Ahmed Habib, received his Ph.D. in Business Administration from the University of Arizona in 1993. Dr. Habib is currently the Dean of Prince Sultan College for Business at Al Faisal University - Jeddah, Saudi Arabia. His research interests include Human Resources, Performance Management, and Business Communication.

Ali Al Mazari, earned his PhD in Science from the School of Information Technologies, Sydney University (Australia), early 2007. Dr Al Mazari is currently Head of IT Department and Director of IT Centre at Al-Faisal University (Prince Sultan College in Jeddah Campus, KSA). His research interests include Data Mining, Bioinformatics, Information Security, and Cybercrime Management.

Dr Leigh Armistead is the President of Peregrine Technical Solutions, a cyber security company. His PhD (Edith Cowan University) focused on IW, he is Chief Editor for the *Journal of International Warfare*, the Vice-chair WG 9.10 - ICT Uses in Peace and War, on the ECCWS Editorial Review Board and is the ICCWS Programme Director.

Prof. Audun Jøsang works at the University of Oslo where he teaches and conducts research in cyber security. Before moving to Oslo in 2008 he was Associate Professor at QUT, research leader of the Security Unit at DSTC in Brisbane, worked in the telecommunications industry for Alcatel Telecom in Belgium and for Telenor in Norway. He received a Master's degree in Information Security from Royal Holloway College, University of London, and a PhD from NTNU in Norway

Adiel Aviad is a Ph.D. student and an industry savvy. Current research interests include cyber defence at system level, semantic technology, management systems and management methods.

Dr. Samsun M. Basarici works as a lecturer at Yasar University, Izmir, Turkey and is the Head of Computer Technologies Department at the same university. His main research and teaching areas are (medical) image processing, neurosciences, computer graphics and game programming. Basarici holds BSc in Computer Engineering and MSc in Informatics degrees from University of Hamburg, Germany and a Ph.D. at International Computer Institute at Ege University in Izmir.

José Borges is a mechanical engineer with a PhD in the field of systems, automation, control and robotics. His current R&D interests and projects are focused in developing and applying decision support systems to applications in military context, in particular information security. He holds a teaching and research position with the Portuguese Military Academy.

Christopher Brill is a Lieutenant in the Alaska Army National Guard. He holds a B.A. in History from Rutgers University and is completing his M.A. in Military Studies and Strategic Leadership from American Military University this summer. He has served as a Signals Intelligence Analyst during OIF and Target Area Reporter at the National Security Agency. Brill is a Program Analyst in the Planning, Budget, Operations, and Training directorate for the Alaska National Guard and Platoon Leader for a Long Range Surveillance communication platoon.

Joobin Choobineh is an associate professor of Information and Operations Management at Texas A&M University. His research areas include Management Information Systems and Information Security Management. He has authored or been a coauthor of more than fifty (50) articles. He has served as the chair of 8 and committee member of 11 Ph.D. students. Dr. Choobineh is on the editorial board of the International Journal of Business Information Systems.

Manuel Corregedor is the Operations Manager at Wolfpack Information Risk and has been involved in a number of research projects targeting organisations, industry sectors and various countries. He has done a significant amount of research in the area of malware and anti-malware techniques. He holds an MSc IT degree (Information Security) from the University of Johannesburg.

Lucia De Marco is a PhD candidate of the joint Information Systems and Software Engineering program held by University of Salerno and University College Dublin. She graduated with a B.Sc. in 2007 and an M. Sc. in 2011, both in Computer Science. She is working on Proactive and Reactive Cloud Forensics since 2012.

Giulia Droandi received a master's degree (com laude) in Mathematics at the University of Siena (Italy), in 2011, with a thesis on enumerative combinatory.

From 2012 she is a Ph.D. Student at the Department of Information Engineering. Her research focuses on fully and Somewhat Homomorphic Encryption and its possible applications to biometrics.

Jan Fesl has a M.Sc. Diploma received in Computer Science in 2007 at the Czech Technical University of Prague, Czech Republic. Currently, he is an assistant professor at the University of South Bohemia and he is a Ph.D. student at the Czech Technical University of Prague. His current research is focused on computer networks and distributed computing.

Courtney Falk is working on his doctorate of philosophy degree in information security at Purdue University. Between degrees he spent eight years working in first the government sector and then in private industry writing secure code. His current research goal is to apply natural language processing to information security problems.

Cécilia Gallais After five years of university studies in mathematics and cryptography in Rennes and an internship at Orange Labs Caen, I joined TEVALIS in the framework of a thesis on the formalisation and establishment of an algebraic model for the cyber attack and critical infrastructure concepts.

Virginia Greiman is a Professor of Cyber Law and Cybersecurity at Boston University and holds academic appointments at Harvard University Law School and the Kennedy School of Government. She served as a diplomatic official to the U.S. Department of State in EasternEurope, Asia and Africa and has held several high level appointments with the U.S. Department of Justice.

Andreas Haggman is a researcher in the Centre for Doctoral Training in Cyber Security at Royal Holloway, University of London. He previously has BA (Hons) and MA degrees from the War Studies Department at King's College London. His academic interests are cyber security strategies, weaponised code proliferation, and cyber forces recruitment.

Mohamed Hassan received MSc in Computer Science and near completion of his PhD in Cyber-Security. Currently he is a lecturer (part-time) at the School of Computing, Staffordshire University, UK. His primary research areas are Bio-inspired computing, A Life, Cyber-Security, Fuzzy Logic, and Artificial Intelligence.

Roland Heickerö has a PhD from the Royal Institute of Technology (KTH) in Stockholm, Sweden and is Associated Professor at the Swedish National Defence College (FHS). His research examines different aspects of information warfare and

cyber threats and their effects at security policy level and technical systems levels. Between 2003 and 2012 he was Deputy Research Director at the Swedish Defence Research Agency (FOI) in charge of cyber defence research. Today he work part time as Adjunct Professor in information security at KTH combined with an appointment as senior management consultant at Knowit Secure.

Stefanie Hills is a first-year doctoral researcher in Information Management at Loughborough University. Holding an MSc in Forensic Speech Science and an MA (hons.) in Linguistics, Stefanie has worked as a Computational Linguist in Speech Technology prior to commencing her research at Loughborough and teaches part-time at Northampton Business School.

Stephen Hill is currently the InfoSec Project Manager for the Directorate of Academic Support, University of Wolverhampton, United Kingdom. He received his MSc in Technology Management from the Open University in 2014. He has worked on a number of UK governmental projects involving data aggregation and behaviour pattern identification and currently contributes to the MSc Digital Forensics course at the University of Wolverhampton as well as researching effective use of machine learning tools in enterprise network security.

Aki-Mauri Huhtinen, PhD, LTC (G.S.), Military Professor at the Finnish National Defence University, Department of Leadership and Military Pedagogy. Mr. Huhtinen is a military professor at the Finnish National Defence University. His areas of expertise are military leadership, the philosophy of science in military organizational research and the philosophy of war.

Margarita Jaitner is a researcher of Information Warfare in the cyber space at the Swedish Defence University. She currently focuses on the Russian concept of "information superiority". Margarita holds an MA degree in Societal Risk Management as well as a BA in Political Science.

Muhammer Karaman received his BS degree in Turkish Military Academy in 2005. He finished the Information System Management Course (ISM) in 2012 at Army School of Information Technologies in Georgia, USA. He currently continues his study at the Turkish Army War College. His research interests are cyber operations, cyber law and international relations.

Anthony Keane, MSc, PhD has a background in astrophysics research and computer science and is currently the Head of the Department of Informatics in the Institute of Technology Blanchardstown, Dublin, Ireland. He is also the principal

investigator of the Information Security & Digital Forensics (ISDF) research group in Cyber Bullying, Cyber Warfare and Cloud Forensics.

Victor Kebande is a PhD researcher at the University of Pretoria in the field of Cloud Forensic Readiness at the department of computer science, University of Pretoria. He is a member of institute of information technology professionals of South Africa (IIPTSA) and an active member of Information and Computer Security Architectures (ICSA) research group.

Timo Kiravuo is a postgraduate student in Aalto University. He received his MSc. (1999) from Helsinki University of Technology. After a career in private sector his work focuses on Internet security and related matters. Currently he is researching technical and societal aspects of cyber-security, especially in relation to critical infrastucture.

Tomas Klima is a PhD student, teacher and researcheratthe University ofEconomics in Prague focusing on penetrationtesting, ethicalhacking and IT forensics. Tomas also is an IT security analystat Czech national bank.

Fatih Koç is currently a fourth grade student in the Department of Aerospace Engineering at Turkish Air Force Academy. He graduated from Işıklar Military High School in 2011. His research interests lie in the areas of unmanned aerial vehicles and cyber security in the world. After graduating from Turkish Air Force Academy, he will begin to take pilotage training in Cigli, İzmir.

Michael Kouremetis is a Graduate student at Purdue University studying Computer Science and specializing in Information Security and Assurance. Michael is specifically interested in systems security of high consequence systems (critical infrastructure, utilities, and government systems) as well as malware analysis. Other significant fields of interest include Foreign Policy, Intelligence, Cyber Security Policy, Counter-terrorism, and Economics.

Jyrki Kronqvist holds a Master´s degree in mathematics and information technology from the Jyväskylä University, where he is currently working towards his dissertation in the area of information security. His research interests include information security, cyber espionage, cloud computing and data encryption. He has also worked in large global organizations in several information security related positions.

Stephen Kuhn is a Research Scientist at Dartmouth College. A recent graduate of the Ph.D program in 2014 with a thesis focused on virtualization and forensics. He

completed his Masters at Syracuse University in 2008 investigating large scale internet packet processing and attribution.

Professor Rauno Kuusisto works for the Finnish Defence Forces. He has contributed as an expert, consultant and manager particularly on the areas of information availability in strategic decision-making, strategy thinking, product development, research purchasing, project portfolio management, network enabled management and leadership in innovative environment, systems thinking, as well as modeling comprehensive challenges.

Tuija Kuusisto works for Ministry of Finance and National Defence University in Finland. Her area of expertise includes ICT strategies, information management for decision-making, cyber security management and program and project management. She has about 70 scientific publications in international and national journals, conference proceedings and books.

Martti Lehto Col (ret.) has over 30 years of experience as developer and leader of C4ISR Systems in Finnish Defence Forces. He is now a Cyber security and Cyber defence researcher and teacher in the University of Jyväskylä. He also coordinates the Cyber Security MSc. and Doctoral programmes.

Dr. Andrew Liaropoulos is Assistant Professor in University of Piraeus, Department of International and European Studies, Greece. His research interests include international security, intelligence reform, strategy, military transformation and cyber security.Dr. Liaropoulos is also the assistant editor of the Journal of Mediterranean and Balkan Intelligence (JMBI) and a member of the editorial board of the Journal of Information Warfare (JIW).

Áine MacDermott is a PhD research student studying at Liverpool John Moores University in the School of Computing and Mathematical Sciences. She achieved a 1st class BSc. in the field of Computer Forensics. Her research interests include critical infrastructure protection, computer network security and digital forensics.

Derek Masvosvere is currently working toward a Master's degree in the Department of Computer Science at the University of Pretoria, South Africa. He is under the supervision of Prof Hein S. Venter. His research interests are in digital forensics and Internet security with the main focus being forensic readiness in e-supply chains.

Jarkko Paavola received the Doctoral degree in technology in the field of wireless communications from University of Turku, Finland. He is currently a research

team leader and a principal lecturer with Turku University of Applied Sciences, Turku, Finland. His current research interests include information security and privacy, dynamic spectrum sharing, and information security architectures for systems utilizing spectrum sharing.

Christo Panchev is a Senior Lecturer in Computing at the University of Sunderland. His research interests are in the areas of Computer Security, Ethical Hacking, Big Data and Computer Forensics.

Jorge Proença is a PhD student in Informatics Engineering at the University of Coimbra. He received his M.Sc. degree from the same institution in 2012. Since then he has served as a junior researcher at the Centre for Informatics and Systems of the University of Coimbra (CISUC).

Nuno Santos has a Bachelor's degree in Bioengineering and a Master's degree in Computer Science from the University of Beira Interior, Covilhã, Portugal. He is a member of the RELEASE – RELiablE And SEcure Computation Group – at UBI, as well as a researcher at the Institute of Telecommunications. His research interests focus on new informatics solutions for the healthcare industry, with particular interest on e-health and security and privacy of data communication.

Miika Sartonen is a part-time doctoral student at the Finnish National Defence University.

Dr Keith Scott is the Programme Leader for English Language at De Montfort University in Leicester; where he is also a member of the Centre for Cybersecurity. His research deals with the intersection of communication and culture, with a particular interest in strategies of influence and persuasion.

Stephen Sheridan has been a lecturer in the Computer Science Department in the Institute of Technology Blanchardstown for the past fourteen years. In 2013 Stephen joined the Security & Digital Forensics research group at ITB in order to complete his Ph.D. Stephen's main research interests are in the area of Information security and Computational Intelligence.

Armin Simma is a senior lecturer at the Vorarlberg University of Applied Sciences, Austria. After graduating at the University Of Linz, Austria he worked 2 years at CERN, Switzerland. Since 2001 he is teaching and doing research in the areas of IT security, virtualization, cloud technology, operating systems and computer networks.

Professor Jill Slay is Professor and Director of the Australian Centre for Cyber Security at UNSW Canberra @ ADFA. She has established an international research reputation in cyber security and collaborates with many industrial partners. She was made a Member of the Order of Australia (AM) for service to the information technology industry.

Mikhail Styugin is a senior lecturer and a scientist at Siberian State Aerospace University (Krasnoyarsk, Russia). He holds a PhD degree in computer science. He conducts research in area of information security system and technologies of information warfare. He owns two companies that develop solutions in area of information security system in the Internet.

Tuğkan Sülün attended in computer engineering of the Turkish Air Force Academy, Istanbul, Turkey, in 2011.

Stephen Taylor is a Professor of Computer Engineering at Dartmouth College and a nationally recognized leader in cyber security. Among other awards, he has received Secretary of Defense and USAF Medals for Public Service and the DARPA Directors Award for Outstanding Portfolio of Technical Programs.

Neha Thethi is a Researcher at ITB, Ireland with the focus on 'Digital Forensic Investigations in the Cloud Environment'. She is also working as an Information Security Analyst with a reputed security consulting firm BH Consulting that provides services such as ISO 27001 alignment and Risk Management.

Jaromir Veber, Ph.D. is the academic staff at the Department of System Analysis at University of Economics in Prague. His main research and development work is specifically focused on the IS/ICT security management and cloud services.

Stephen Vemi is currently studying his final year of Network Computing at University of Sunderland. Prior to University has studied at New College Durham on a two year IT course. His interest lies broadly in the are of network security, software engineering and cyber security.

Prof Hein Venter is one of the founding members and current head of the Information and Computer Security Architectures (ICSA) Research Group in the University's Department of Computer Science. He is also the chair of the Information Security for South Africa (ISSA) national conference and the South African Institute of Computer Science.

Murdoch Watney is a professor in the Department of Public Law at the University of Johannesburg, South Africa where she teaches criminal law. She worked as a prosecutor and is an admitted advocate of the High Court of South Africa. She contributed to three textbooks and has published extensively nationally and internationally in law journals on the law of criminal procedure, criminal law, law of evidence and cyber law. She has delivered a number of papers at national and international conferences.

Ben Whitham has spent more than 20 years designing and protecting IT systems. He was a founder of M5 Network Security, and co-inventor of the Secure Communications System, finalist in SC Magazine Security Product of the Year, 2011. Ben is currently completing his doctorate in Cyber Deception and the University of New South Wales.

A Survey of Continuous and Transparent Multibiometric Authentication Systems

Abdulwahid Al Abdulwahid[1,2], Nathan Clarke[1,3], Ingo Stengel[1], Steven Furnell[1,3] and Christoph Reich[4]

[1]Centre for Security, Communications and Network Research, Plymouth University, Plymouth, UK

[2]Computer Science and Engineering Department, Jubail University College, Jubail Industrial City, KSA

[3]Security Research Institute, Edith Cowan University, Perth, Western Australia, Australia

[4]Cloud Research Lab, Furtwangen University, Furtwangen, Germany

Abstract: The advancement of technologies and the increasing number of users utilizing them has given rise to a significant concern over protecting them from misuse. The integral aim of any IT system is to safeguard resources against any illegitimate access and authentication is the cornerstone to enabling this. Arguably, existing user authentication approaches have not adequately advanced proportionally with the advancement of digital devices technologies. The majority of implementations also operate merely at point-of-entry, providing little consideration to on-going identity confidence, leaving the system susceptible to misuse. Research has proposed continuous authentication as an alternative that can provide additional security, albeit introducing an additional burden upon the user if not implemented considerately. A range of studies have been proposed to overcome these downsides without compromising the user convenience by continuously and transparently authenticating the user throughout. This paper performs a survey and critical analysis of the domain, in particular focusing upon the role that multibiometrics has and its viability in practice. Studies have found that a variety of biometrics techniques have been investigated including physiological only, behavioral only and both, with the addition of soft biometrics or even passwords, rendering them not to be completely transparent thereby suffering from intrusive authentication drawbacks. The operational context also varies, including PC, mobile, wearable, various devices, and the Internet/cloud. Therefore, it is evident that there is a lack of an empirical solution that can be accomplished seamlessly in a location, technology and service independent fashion. With respect to performance, many studies never undertook an evaluation; others declared heterogeneous metrics, making a comparison implausible. Despite the fact that most of the studies deployed an identity confidence/trust adaptation, a small proportion of them associated it to the differing risk level of a particular data, action, or service. It is perceived that the success of a particular mechanism has the merit of ensuring an effective authentication method together with user acceptance. However, it is paramount to have a high level of performance, scalability, and

interoperability amongst existing and future systems, services and devices. Furthermore, all these requirements should be implemented and evaluated extensively on real data in order to prove that such a system is viable, including its acceptability and usability.

Keywords: authentication, transparent authentication, TAS, continuous authentication, biometrics

Cyber Terrorism Taxonomies: Definition, Targets, Patterns and Mitigation Strategies

Ali Al Mazari, Ahmed Anjariny, Shakeel Habib and Emmanuel Nyakwende
ALFAISAL University, PSCJ Campus, Jeddah, Saudi Arabia

Abstract: The aim of this paper is to identify common features in: the definition of cyber terrorism, cyber terrorism targets, cyber terrorism crimes and then develop effective mitigation strategies and countermeasures to tackle this phenomenon. Through rigorous analysis of literature covering academic articles and official reports, we develop cyber terrorism definition taxonomy which includes five elements: target, motive, means, effect and intention; cyber terrorism targets taxonomy identified from the following target areas: military forces, government cyber and physical infrastructures, critical national infrastructures, social and national identity, and private industry and entities. The following identified patterns constituted the cyber terrorism targets taxonomy: incursion, destruction, service interruption, disinformation and web sites defacement. We categorized effective strategic approaches to tackle cyber terrorism as: administrative, technological, national and local alliances, international alliances, and education, training and psychological approach. We developed cyber terrorism taxonomies which represent a systematic organization and classification of knowledge that improves scientific awareness of cyber terrorism definition, boundaries, potential targets, crime patterns and effective mitigation strategies.

Keywords: cyber terrorism, cyber warfare, critical infrastructure, mitigation strategies, taxonomy

What are the Metrics of Cyber Warfare? How Does one Measure Success?

Leigh Armistead[1] and Scott Starsman[2]
[1]Edith Cowan University, Perth, Australia
[2]Avineon, Inc., McLean, USA

Abstract: This paper continues the process of laying the groundwork for a new comprehensive academic theory on Cyber Macht (Cyber Power). In this particular paper, the authors will focus on trying to determine the metrics of cyber operations, ie how does one measure success? The ability to measure and validate success is always a crucial metric in the performance of a task, and in this case the conduct of IO campaigns is no different. The researchers for this paper will analyse two approaches for the development of metrics in a Cyber environment: A top-down approach with a strong feedback mechanism, one that allows actors to learn lessons from their actions and to apply changes to the system as deemed appropriate. A more decentralised methodology, which embraced any and all IO standards. This bottom-up view utilises a more liberal process for collecting metrics that attempts to bring together disparate activities into a collective force. This paper will analyse the efforts of various IO initiatives by both sides, and attempt to determine the key factors of success.

Keywords: IO standards, metrics, warfare, cyber power

Design of a Case-Based Reasoner for Information Security in Military Organizations

José Borges[1], José Martins[1], Jorge Andrade[1] and Henrique dos Santos[2]
[1]Academia Militar – CINAMIL, Lisboa, Portugal
[2]Universidade do Minho – DSI, Guimarães, Portugal

Abstract: Information security is concerned with the protection of information, which can be stored, processed or transmitted within the critical information systems from organizations, against loss of confidentiality, integrity or availability. Protection measures to prevent these problems result through the implementation of controls at several dimensions: technical, administrative or physical. A vital objective for military organizations is to ensure superiority in contexts of information warfare and competitive intelligence. Therefore, the problem of information security in military organizations has been a topic of intensive work at both national and transnational levels, and extensive conceptual and standardization work is being produced. A current effort is to develop automated decision support systems to assist military decision makers, at different levels in the com-

mand chain, to provide suitable control measures that can effectively deal with potential attacks and, at the same time, prevent, detect and contain vulnerabilities targeted at their information systems. The concept and processes of the Case-Based Reasoning (CBR) methodology outstandingly resembles classical military processes and doctrine, in particular the analysis of "lessons learned" and definition of "modes of action". Therefore, the present paper addresses the modeling and design of a CBR system with two key objectives: to support an effective response in context of information security for military organizations; to allow for scenario planning and analysis for training and auditing processes.

Keywords: conceptual model for information security, case-based reasoning, decision support system, method of attack, information security controls

Quantitative Analysis of PIN Choices: A Contribution to the Establishment of Authentication Requirements

José Carlos Carvalho[1], Vítor Sá[1,2], Maria José Magalhães[1] and Sérgio Tenreiro deMagalhães[1,2]
[1]Faculty of Social Sciences, Catholic University of Portugal, Braga, Portugal
[2]ALGORITMI Research Center, Universityof Minho, Braga/Guimarães, Portugal

Abstract: The authentication using a PIN number remains one of the most used ways to enter a system (mobile phone, ATM, etc.). Many people seem to dislike this form of authentication because they simply despise their use, placing unsafe PINs just because they have to put some. Some relevant results are the combination 1234, the combinations using only one digit (example: 1111), or the central line of the numerical keypad. On the other hand there is some understanding because it is proven that remember strong passwords is a difficult task for humans, and the tendency is to choose the simplest ones. This research had a sample of 497 participants and aimed to understand the preferred choice of the participants in relation to the number of digits used for a PIN number (a choice between four and/or six digits) and realized the amount of times that each of the available digits was used. To this end it was developed a web-based tool for entering the data. This application was intended only to the data collection process, being the information processed further. Through this application, the user was asked to enter four and/or six-digit PINs. The method does not raise any doubt on the participants, which were informed about the anonymity and confidentiality of the data, and never were they asked to identify themselves. Participants were asked to use the PINs that they normally use in other contexts. With the analysis of the data it was possible to understand the distribution of digits per position in a PIN, check which digits is more/less used in each position, and check which digit is more/less

used regardless of its position. Among the conclusions it appears that the layout of the numeric keypad of the system influence the PIN choice.

Keywords: PIN, digits, security, authentication, system, keypad

The Cyber Counterintelligence Process: A Conceptual Overview and Theoretical Proposition

Petrus Duvenage[1], Sebastian von Solms[1] and Manuel Corregedor[2]
[1]Centre for Cyber Security, University of Johannesburg, South Africa
[2]Academy of Computer Science and Software Engineering, University of Johannesburg, South Africa

Abstract: With the ineffectiveness of the defensive cyber security toolkit against advanced threats now commonly accepted, the quest is intensifying for viable and practical alternatives. While Cyber Counterintelligence (CCI) is gaining traction as such an approach, it is still in its infancy as a field of academic enquiry. This paper aims to contribute to an area largely underexplored, namely the conceptual structuring of the CCI process. The paper argues a proposition on the CCI process to be of critical academic and practical importance. On an academic level, such a proposition serves as a notional concept for directing and delineating further research into CCI. On a practical level, the conceptual outline of the process provides an organising template for performing CCI work in practice. On both accounts the proposition is an idealisation - where the CCI process appears to be optimally effective and where everything goes as planned. The paper is based on the premise that CCI can only be performed effectively as part of a multi-disciplinary Counterintelligence (CI) process. Moving from this premise, a contextual overview is provided of some existing postulations on the Intelligence, CI and CCI processes. Since existing propositions do not sufficiently explain CCI, an alternative process model is presented in the form of a diagram and a narrative conceptual outline. The aim is not to describe the process in detail, but to rather present a high-level theoretical framework.

Keywords: cyber counterintelligence, cyber-counterintelligence process, offensive cybersecurity, cyber security

Security in the Irish Information Technology Sector

Courtney Falk
Purdue University, West Lafayette, USA

Abstract: This paper analyzes the mechanisms that the Irish governments uses to protect the information security sector of its economy. The goal of the analysis is to determine if the Irish government is adequately defending its information security resources, and if not, what measures might improve the situation. These conclusions have applications beyond Ireland to other countries that look to develop a native information security industry. Nations, especially small nation states, looking to develop an indigenous information technology component to their economy can take note of the policies and actions of the Irish government and make better informed decisions about how they themselves might go about incentivizing and maintaining an information technology sector.

Keywords: Ireland, information technology, information security, policy, governance

New Techniques of IEEE 802.11 Family Hotspots Attacks, Principles and Defense

Jan Fesl[1,2], Marie Dolezalova[1], Frantisek Drdak[1] and Jan Janecek[2]
[1]Institute of Applied Informatics, University of South Bohemia in Ceske Budejovice, Czech Repulic
[2]Department of Computer Science and Engineering, Czech Technical University in Prague, Praha

Abstract: Today many places in the world allow paid internet connection via wireless hotspots. These solutions are available in places such as hotels, airports and conference halls. Because a wireless hotspot is accessible for any new potential user, common security techniques based on WPA/WPA2 encryption cannot be used. In the last few years a new type of an attack, based on DNS tunneling has been described. We will focus on detail analysis of this attack and we will propose a possible defense strategy. DNS tunneling attack has been implemented in several applications and inspired us to look at another type of a wireless hotspot attack. We will describe in detail all parts of the solution necessary to understand the defense against this type of an attack. At this time, there is no way to prevent this attack, except switching off all unencrypted common wireless hotspots infrastructures.

Keywords: hotspot, attack, DNS tunnel, wireless security, IEEE 802.11

Cyber Security and Global Governance

Virginia Greiman
Boston University, Boston, USA

Abstract: To understand better the challenges of developing a unified system of global cyber governance, a comparative analysis of national cybersecurity strategy and frameworks in 10 countries and the European Union from diverse regions in both the developed and developing world was conducted. In addition, in the course of the research, the author has interviewed various government and private sector experts on national intelligence and cybersecurity and has analyzed relevant documents, data, case studies and government and private industry reports concerning the present and future challenges they face in developing a global governance structure for cybersecurity. Recommendations are proposed based on the commonalities between national laws and policies in an effort to find common ground for the development of bilateral and multilateral cybersecurity agreements and global public private partnerships. Based on empirical research and an analysis of national and international cybersecurity strategies and policies, this paper explores the challenges and benefits of establishing a global legal and policy framework for cyber activity that advances the goals of national intelligence and technological innovation, while enhancing confidence and improving legal certainty in the global electronic marketplace.

Keywords: national cyber security strategy, cybersecurity, privacy, governance

Cell Based Intrusion Prevention System

Mohamed Hassan, Stilianos Vidalis and Alexios Mylonas
School of Computing, Staffordshire University, Stafford, UK

Abstract: In today's socially-driven knowledge-based computing era, digital devices have become household appliances. Ubiquitous computing and social networks are life style technologies which coupled with the political drive for e-inclusion strategies have exponentially increased the rate of new 0-day exploits. We hypothesise that building an adaptive, polymorphous, distributed system that can learn from its environment and dynamically change according to external stimuli, which can provide a cost-effective proactive solution to the problem. In this research we developed a novel and simple approach to defend common network threats and anomaly attacks. The design comprises of polymorphous elementary blocks called digital cells, these simple blocks are extremely rich, much like living cells. Cells are the fundamental structural unit of life, all living organisms are made of one or more cells. The cell characteristics including, the ability of self-division to a specific limit (e.g. human cells), capability of independent existence,

and the ability to communicate using signalling are going to be the fundamental elements for this research.

Keywords: cell computing, unstructured, polymorphous, fuzzy logic, membrane computing

Industrial Espionage and Theft of Information

Roland Heickerö
Swedish National Defence College (FHS), Sweden

Abstract: One of the most serious threats to a modern country's trade, industry and long-term economic development is industrial espionage and insiders. The activities are directed against high-technological industries and companies with advanced basic research. The defence and telecoms sectors are of particular interest, just as biotechnics, medical and material technology. Behind this kind of espionage there may be individual states and security services as well as competing companies. One trend is that criminal players are getting involved both as thieves and fences of information. Computerisation and the development of the Internet drastically increase the possibility of procuring sensitive information through illegal means. This can be done in different ways. In the paper a number of examples are provided of how industrial espionage has been revealed and of the methods used during collection of information over the Internet – such as signals intelligence, monitoring of traffic, penetration and overtaking of computers with the aid of trojans. Examples are given on succesful cybertheft operations such as the operation Buckshot Yankee and the Chinese Ghostnet. The paper ends with a discussion on how to improve information security in organisations in order to reduce the risks for illegitimate information drainage.

Keywords: cyber espionage, information theft, Echelon, PRISM, SORM, Ghostnet

Culturing Defensive Immunity: Hardening Psychological Targets Against Cyber Attack

Mils Hills and Guy Batchelor
Northampton Business School, UK

Abstract: Academics in business science and elsewhere have begun to look at what Vaughan (1999) called the "dark side of organisations" and started to engage with the fact that people connected to cyber systems can be the source of great opportunity for exploitation. MacGillivray (2014) notes that organisations should be seen as socio-technical: where infrastructure and systems shape and are shaped by the people that work with them. The current paper puts these so-

cio-technical systems at the heart of cyber-attack and defence - where we see 'cyber' as being shorthand for any computer-dependent technologies used to achieve dark effects on the human mind and subsequent behaviour (e.g. SMS received on a mobile phone).There is no logic to restrictively focussing on user behaviour around laptops and desktops. This paper provides some unconventional examples of cyber-attack. Our concern is with enabling decision-makers (or those supporting them) to challenge their assumptions about information received, adjust behaviours accordingly and thereby render them and their organisations increasingly resilient to the efforts of creative adversaries, no matter whether those adversaries motivation is commercial, political or personal. From such target-hardening arises organisational competitive advantage.

Keywords: psychological, target, immunity, trap, culture

The Double Edge of the Information Sword

Aki-Mauri Huhtinen
Finnish National Defence University, Helsinki, Finland

Abstract: In 1990, after the collapse of the Soviet Union and its clandestine propaganda machine, the West became increasingly confident that globalization supported by an information technology network, the Internet, would increase openness, liberalism, and democracy; the core values of the 'free world'. Western leaders knew then, just as they know now, a quarter of a century later that the power of the Internet would grow as the technology that controls its use develops. And developed it has. However, no development is all good and the Internet is no exception. It seems that the technology that has enabled us to create a "global village" where people are able to communicate in a way that is open, free and that bypasses the encumbrances of class and ethnicity has also brought with it a very dark underworld, an uncontrolled rhizome or meshwork, where propaganda, trolling and hate speeches are rife (see Coyne 2014). However, this concern about negativity goes far beyond a few questionable messages posted online. According to Munro (2005), media, business, politics and military organizations are increasingly reliant upon information technology, which means that technology has become a valuable resource and a deadly weapon in its own right. This naturally means that all information, whether political or economic, has become militarized and weaponized (Chong 2013, 604). Cyber warfare, and everything it entails, from corrupting adversaries' networks to spreading false information, is thus slowly becoming the most dangerous form of warfare. For example, the Kremlin's weaponization of information, culture, and money is an integral part of its vision for the 21st-century "hybrid" or "non-linear" war: "In the 21st

century, we have seen a tendency toward blurring the lines between the states of war and peace" (Gerasimov 2013). This paper aims to describe this extremely modern and contemporary process of weaponizing information. First, I will familiarize the reader with the theoretical concept of the rhizome (Deleuze & Guattari 1983). Then, I aim to describe the weaponizing process of information by using Iain Munro's (2005) description of information warfare. I will also integrate some quotes that aptly reflect the Kremlin's new strategic communication policy. These quotes will facilitate the reader's understanding of the rhizome process. Lastly, I will discuss the possible consequences of the phenomenon of a hybrid information environment.

Keywords cyber, hybrid, information, rhizome, trolling, war, weaponizing

Using Security Logs to Identify and Manage User Behaviour to Enhance Information Security

Rose Hunt and Stephen Hill
University of Wolverhampton, UK

Abstract: This paper describes a study which seeks to evaluate the relationship between user behavior, including the use of social technologies within the workplace, and the prevalence of malware infections routinely detected on devices. The study's initial focus is the extent to which security breaches are linked to the use by staff of social technologies, namely Social Media, at work. It is a study which affirms previous research showing that Social Media use at work does present significant security risks. It provides a possible basis for research into the management and change of user behaviour with reference to security management, and would be of interest to Cyber and Information Security professionals and researchers in the field. The context is a large university where network security is achieved through the separation into two separate domains of the staff and student networks. The scope of this study focusses solely on staff behaviour, for reasons which include the very high numbers of students, and the fact that the student population is much more short-term and transient and is therefore not so appropriate for a longitudinal study. Daily automated logs were collected from a number of data sources including anti-virus data from F-Secure security software and web activity data from Palo Alto firewall logs.These logs were examined and a suitable data collection method was implemented which provided a successful combination of volume, manageability and processing, and delivered satisfactory performance whilst retaining data accuracy. Once collected, processed and stored, the user characteristic data derived from the logs was then analysed. Data mining and pattern recognition techniques were used, with the Kohonen Self-Organising map used as a model for this analysis. Neural network data analysis

tools within Matlab were used to process the inputs, and data clustering became evident within the presented data. Findings showed that social Media use increases users' susceptibility to the introduction of malware infections. The most frequently introduced malware types found in our study were trojans, but using Social Media also heightened the risk of introducing a variety of other malware. Other information was gathered which provided insight into the behaviour of different user types, grouped by age, and sex, and this will provide an underpinning to planned further research which seeks to find ways of managing user behaviour in relation to security breaches.

Keywords: information security, cyber security, user behaviour, social media, malware, threat vectors

Cyber Education? Branches of Science Contributing to the Cyber Domain

Margarita Jaitner[1] and Aine MacDermott[2]
[1]Swedish Defense University, Stockholm, Sweden
[2]School of Computing and Mathematical Sciences, Liverpool John Moores University, UK

Abstract: It is increasingly acknowledged, that academia plays an important role in a country's cyber readiness. Nations have started investing in new cyber-related programs at colleges and universities, promoting academic exchange with friendly countries, as well as putting effort into improved cooperation between industries and scholars in the area of cyber. In many cases the efforts focus largely on computer science and closely related branches of science. However, the very nature of the cyberspace as both a continuation and a reflection of the physical world requires a broader perspective on academic assets required to create and sustain sound cyber defense capabilities. Acknowledging this premise, this paper sets out to map branches of science that significantly contribute to the domain known as cyber. The first main aspect of the paper outlines the major branches that in the past have significantly contributed to generation of knowledge as well as development of skills that are necessary for a nation to maintain sustainable cyber readiness. Thereafter interdependencies between branches of science are identified in order to map out points of necessary collaboration, arguing that a nation's cyber defense draws great advantage from broad interdisciplinary efforts. In many cases, such collaboration is already being carried out and/or actively encouraged by policy makers, the academic establishment or both. However, it is argued that not all necessary collaborations are yet being carried out. Such desirable cooperation is mapped out and argued for in the final part of the paper. This paper acknowledges scholarly contributions produced and published in Eng-

lish and Russian languages, which also allows the identification of a focal point that is set in the respective academic environment. The results of the presented research can be of broad use for policy makers whenever it is necessary to assess to what extent cyber-related issues are covered academically within a nation. Further, personnel tasked with creation and improvement of cyber-related academic programs will find use in these findings when developing comprehensive curricula.

Keywords: cyber security, academia, cyber readiness, information security

It's not a bug, it's a Feature: 25 Years of Mobile Network Insecurity

Audun Jøsang[1], Laurent Miralabé[2] and Léonard Dallot[2]
[1]University of Oslo, Norway
[2]TazTag, France

Abstract: The global mobile networks are built with a set of core technologies developed during the 1980s, combined with subsequent generations of networking technologies for improved performance. Due to political pressure by European governments during the 1980 the initial GSM network, commonly called 2G, was purposely designed and built with weak security to allow easy interception of phone traffic by law enforcement agencies. Despite strengthened security in the more recent networking technologies of 3G and 4G, the weak security of 2G represents the 'weakest link' which thereby limits the security level of mobile networks in general. While this cybersecurity vulnerability is currently exploited by domestic law enforcement agencies for legal interception and surveillance, as well as by criminal and foreign powers for cybercrime and espionage, it is interesting to notice that it was created on purpose. This paper describes the background and the evolution of mobile network security, analyses the nature and consequences of security vulnerabilities in mobile networks, and proposes political and technical solutions to mitigate the threats posed by these vulnerabilities.

Keywords: cyber security, surveillance, security politics, GSM, mobile network, SIM, IMSI, 2G, 3G, 4G

Peeking Under the Skirts of a Nation: Finding ICS Vulnerabilities in the Critical Digital Infrastructure

Timo Kiravuo, Seppo Tiilikainen, Mikko Särelä and Jukka Manner
Aalto University, Helsinki, Finland

Abstract: The developed society depends on many critical infrastructure processes, such as power generation, water treatment, many types of manufacturing, or smart building control. These processes need control and today the connecting medium for control is often the Internet. However, the control systems thus opened to the world do not always have safeguards to withstand malicious users. Many systems have default passwords or known and unknown backdoors, or are not maintained and updated to close security weaknesses found after original installation. Several years ago the Shodan search engine showed how easy it is to find these control devices on the Internet. We followed this research line further by targeting one nation's IP address space with Shodan and finding thousands of control systems, many of which represent models and versions with known vulnerabilities. Presenting these findings and analyzing their significance is our first contribution. To gain further knowledge, we have built a prototype scanner capable of finding industrial control systems. This lets us evaluate the possibility of performing routine scans to gauge the vulnerability of a nation. Our second contribution is to present a template for a national Internet scanning program. We discuss the technology, performance, and legality of such a program. Based on our findings and analysis we argue that nations should continuously monitor their own Internet address space for vulnerabilities. Our findings indicate that the current level of vulnerabilities is significant and unacceptable. The cyber-space has become a playing field for criminals, terrorists and nation states, all of which may have a motive to disrupt the daily life of a nation.

Keywords: critical infrastructure, industrial automation, ICS, SCADA security, Shodan, search engine, cyber security, networked automation systems

---

The Weak Side of Unmanned Aerial Vehicles Against Cyber Attacks: How can we Solve These Security Problems?

Fatih Koc
Turkish Air Force Academy, Yesilyurt, Istanbul

Abstract: Unmanned aerial vehicles(UAVs) are ,generally, defined as vehicles which having no pilot on board, flying with aerodynamic forces, having ability to take off and land automatically, moving autonomously or controlled by pilot.

UAVs are fulfilling critical roles in terms of intelligence-surveillance and reconnaissance. The results are satisfying. Unmanned aerial vehicles (UAVs) are dependent on communication links to do its duty. There are two main types of communication links which are used to transfer datas. They are Blos (Beyond line of sight) and Los (line of sight) communication links. Blos communication link use communication satellites. Data transfer is carried out by wireless networks and satellites. These communication links can be interfered by outside. Unmanned aerial vehicles can be captured and important videos or images can be obtained. These can cause dangerous actions or failure in operations. In that scientific study, weak sides of data transfer links will be examined over some samples and some solutions will be presented at the end.

Keywords: unmanned aerial vehicles (UAV), Blos, Los, data link

Adopting Encryption to Protect Confidential data in Public Clouds: A Review of Solutions, Implementation Challenges and Alternatives

Jyrki Kronqvist and Martti Lehto
Faculty of Information Technology, University of Jyväskylä, Finland

Abstract: A shift towards use of public cloud services is ongoing and more and more enterprises will start to use them in the near future. As public cloud services certainly promise to deliver many benefits, this new way of delivering services also introduces new types of risks. Due to the National Security Agency's (NSA)surveillance programs, non-US enterprises need to reassess the risks of public cloud services provided by US companies and look for available solutions to protect their confidential data transferred and stored in the cloud. Encryption is seen as a solution to help enterprises full-fill the requirements related to security and privacy, but is often challenging to implement. Encryption has its own security problems, like key management. Some cloud service providers have also announced that they are improving their security by encrypting all communications and other information flowing into their data centers. This paper will explore the common encryption solutions available on the market for enterprises to protect their confidential data transferred and stored in the cloud. In this paper we will review possible challenges enterprises may face while implementing these solutions and if these challenges play a role in the decision to use a public service. We will review also alternatives for data encryption.

Keywords: cyber espionage, cloud services, data encryption, confidentiality, trustworthy

Locating Zero-day Exploits With Course-Grained Forensics

Stephen Kuhn and Stephen Taylor
Dartmouth College, Hanover, USA

Abstract*:* This paper describes a novel coarse-grained forensics capability for locating zero-day exploits by recording and correlating on-host actions with network packets, with no discernible impact on user experience. The capability provides an alternative to fine-grained techniques, such as memory taint tracking, that are intractable approaches for typical high volume internet facing servers. Two associated network attack scenarios are described, based upon typical website designs, to illustrate how the technique can be used. These have been implemented and tested to verify the capability. Many government and businesses entities already record large volumes of network traffic for regulatory compliance and security analysis; specialized, high-performance hardware appliances are now available to support this activity. To augment this store, the course-grain forensics capability utilizes a small-footprint (i.e. attack surface) custom hypervisor with built in virtual machine introspection (VMI) mechanisms. These mechanisms allow forensic observation to extract exploits by observing the running micro-kernel's process creation, communications and network activities. This allows recorded network events to be directly correlated with on host actions. A custom micro-kernel has been developed to explore the core ideas which, in common with other designs such as Minix, uses a message passing for inter-process communication. This communication model enables strict enforcement of process interactions, which must pass through the kernel, creating a natural observation point for events of interest. Recording only process interactions minimizes the storage requirements to a manageable level -- sixteen bytes per event. This imparts minimal performance impact -- less than six micro seconds to record each event on host, enables recording of the process communication ontology in a computationally efficient manner. The process history allows an analyst to observe the past actions taken by a malicious or compromised process; supporting post-mortem analysis of on system events tracing back to the initial network packets containing the exploit. The results were experimental verified by non-deterministically injecting fake exploits into a vulnerable webserver running on top of the kernel. The LARIAT network traffic generator was used to simulate high-density, real world network loads over a period of 18 and 35 days respectively. The techniques were able to record all associations in real-time. Post-mortem, the forensics capability was able to isolate the packets containing the exploit and highlight the process interaction history in less than 5 minutes, reducing the numbers of packets subject to manual search by more than 99%. Two scenarios were constructed using a typical website with and without a connected database. These scenarios were chosen to exercise two specific cases: one in which there

was a direct path to the exploit via the process history, the other demonstrates the isolation of an exploit where there is no direct discernible trace in the process history. The forensics capability provides more than just isolation of zero-day exploits: this represents a jumping off point for further investigation into the process / network interaction history. These further investigations can then determine the impact of the attack, the processes affected, and the spread of tainted data to provide a basis for clean-up operations.

Keywords: security, virtualization, forensics, exploits

Situation Understanding for Operational art in Cyber Operations

Tuija Kuusisto[1], Rauno Kuusisto[2] and Wolfgang Roehrig[3]
[1]Ministry of Finance & National Defence University, Helsinki, Finland
[2]The Finnish Defence Research Agency, Riihimäki, Finland & National Defence University, Helsinki, Finland & University of Jyväskylä, Jyväskylä, Finland
[3]European Defence Agency, Brussel, Belgium

Abstract: Operational art is a major element of joint operations on land, sea, air, space and cyber. It is selecting steps on the path towards the realization of strategic objectives by creating such compositions and resources that enable success in military operations. It contains the creative application of knowledge, practice, cognition, imagination and intuition of a group of individuals in the operational planning process. Cyberspace provides opportunities for the creating of novel compositions and dynamic resources. The utilization of these opportunities demands, however, situation understanding beyond spatially and temporally imminent events and already known means. The advanced approaches on intelligence and information analysis for the refining of situation understanding typically rely on the processing of huge amounts of big data. This paper presents a theoretically motivated framework and methodology for finding out the major characteristics of a situation by the analysis of quite small information sets. The proposed approach is based on complexity thinking, system modeling, communication and cognition philosophy, social system theories and content analysis research technique. The paper demonstrates the proposed approach with a small case study about information aspect on operational art in joint operations. Operational art and operations are social interaction between people. This paper studies operational art and operations in complex social systems. The paper refers to a social system model and a human information model for finding out the emergent phenomena and information profiles of a situation of a social system. The paper applies the proposed approach to the analysis of an international cyber experiment of the Cyber Implications for Combined Operational Access (CICOA) program as

part of the Multinational Capability Development Campaign (MCDC) 2013-2014. The empirical data of the analysis consist of workshop findings and information requests placed in the experiment. The results of the analysis show that the planning process was proceeding well in the experiment and information about the situation was refined to situation awareness. It can be argued thus that the guidance and recommendations about cyber in operational planning developed during the CICOA program affect positively on the operational planning and increase the situation awareness of the planners.

Keywords: cyberspace, intelligence, operational art, situational understanding, system modelling, content analysis

Cyber Security Competencies – Cyber Security Education and Research in Finnish Universities

Martti Lehto,
Faculty of Information Technology, University of Jyväskylä, Finland

Abstract: The revolution in information technology that began in the 1990s has been transforming Finland into an information society. Imaginative data processing and utilization, arising from the needs of citizens and the business community, are some of the most important elements in a thriving society. Information and know-how have become key 'commodities' in society, and they can be utilized all the more efficiently through information technology. Individuals, public and private organizations alike depend on the cyber world. From the citizens using social media, to banks growing their business, to law enforcement supporting national security – every sector of the society is increasingly dependent upon technology and networked systems. While the public sector, the economy and the business community as well as citizens benefit from globally networked services, the digital IT society contains inherent vulnerabilities which may generate security risks to citizens, the business community or the vital functions of society. Without sufficient awareness of the risks in cyber world, however, behavioral decisions and unseen threats can negatively impact the security of the critical infrastructure and can cause physical damage in the real world. On an individual level, what is at stake is the vulnerability of each individual user in cyber world. As the world grows more connected through cyber world, a highly skilled cyber security workforce is required to secure, protect, and defend national critical information infrastructure. Across the private and public sector organizations are looking for well-trained professionals to assess, design, develop, and implement cyber security solutions and strategies. While the demand for cyber security professionals is high, the supply is low. Meeting the growing demand for cyber security professionals begins in the education system. The most efficient custom

to increase cyber security is the improvement of the know-how. The cyber security strategies and development plans require the improvement of the know-how of the citizens and actors of the economic life and public administration. Pursuant to Finland's Cyber Security Strategy (2013) "the implementation of cyber security R&D and education at different levels does not only strengthen national expertise, it also bolsters Finland as an information society". In this paper are analyzed the know-how demands and needs of the cyber security which the different actors of the cyber world present. The know-how demands and needs are compared with the cyber security research and education which is offered in Finland's universities. The paper is based on a survey conducted on Finnish universities in 2013 and 2014 and on the analysis of its results.

Keywords: cyber strategy, cyber education, cyber competence

Cyber-Security: A Human-Centric Approach

Andrew Liaropoulos
University of Piraeus, School of Economics, Business and International Studies Department of International and European Studies, Piraeus, Greece

Abstract: Cyber-security has been approached by various disciplines. Information technology experts, lawyers, strategists and state officials have enriched the debate about the nature of cyber-security. The dominant trend - regardless of its theoretical origin - is state-centric. This approach is to a large extent legitimate, but at the same time inadequate. Cyber-security relates directly to the threats posed to the nation's critical infrastructure, but should not be limited to the traditional concept of national security. The militarization of the cyber-security discourse has produced a security dilemma, which is not addressing sufficiently the needs of the people. The purpose of this paper is to highlight this shortcoming and view cyber-security, through a human-centric prism. The paper will address the way state and non-state practices violate human rights in cyberspace. Over the past years, the development of internet censorship techniques and Edward Snowden revelations about the global surveillance carried out by the United States National Security Agency (NSA), vividly demonstrate that Internet freedom, anonymity and data protection are constantly under attack. The challenge ahead is to establish a governance regime for cyberspace that successfully addresses human rights norms and standards.

Keywords: cyber-security, national security, security dilemma, human security, cyber governance

Collaborative Intrusion Detection in a Federated Cloud Environment Using the Dempster-Shafer Theory of Evidence

Áine MacDermott, Qi Shi and Kashif Kifayat
PROTECT: Research Centre for Critical Infrastructure Computer Technology and Protection
School of Computing and Mathematical Sciences, Liverpool John Moores University, UK

Abstract: Cloud Computing is being adopted in critical sectors such as energy, transport, and finance. This makes Cloud Computing services critical in themselves. Cloud Computing is a model in which vast quantities of computer resources are used to provide services to many concurrent users. The services may be offered directly or as part of a composite system. The greater scalability and larger size of Clouds compared to traditional service hosting infrastructure, involve more complex monitoring systems, which have to be scalable and robust. Therefore, monitoring systems and intrusion detection systems (IDSs) must be refined and adapted to different situations in Cloud environments. To embrace the above challenge, we propose a methodology that develops a robust collaborative IDS in a federated Cloud environment. Federated Clouds are a logical evolution of the centralised approach. A Cloud federation is an association among different Cloud Service Providers (CSPs) with the goal of sharing resources and data. Our approach offers a proactive collaborative model for Cloud intrusion detection based on the distribution of responsibilities. The responsibility for managing the elements of the Cloud is distributed among several monitoring nodes. Our architecture consists of four major entities: the CloudBroker, the Monitoring Nodes, the Local Coordinator (Super Nodes), and the Global Coordinator (Command and Control: C2). For collaborative intrusion detection, we use the Dempster-Shafer theory of evidence. Dempster-Shafer executes as a main fusion node, with the role to collect and fuse the beliefs provided by the monitoring entities, taking the final decision regarding a possible attack. This type of detection and prevention helps increase resilience to attacks in the Cloud. Collaboration among CSPs can ensure that they are up to date on different Cloud threats. Protecting the federated Cloud against cyber attacks is a key concern, since there are potential significant economic consequences. Our current work focuses on the deployment of such a solution for Cloud service provider collaboration: Security as a Service.

Keywords: critical infrastructure; cloud federation; intrusion detection; cloud computing; collaboration; security; Dempster-Shafer; fusion algorithms

Creating Novel Features to Anomaly Network Detection Using DARPA-2009 Data set

Nour Moustafa and Jill Slay
School of Engineering and Information Technology, University of New South Wales at the Australian Defence Force Academy, Canberra, Australia

Abstract: The increased usage of Internet, E-business, and social network enables attack behaviour with diverse fashions. A Network Intrusion Detection System (NIDS) is software which can protect the network from both internal and external attacks/intrusions. NIDSs detect the known attacks by using signature-based systems and discover novel attacks by using anomaly based systems. In order to represent modern low foot print attack environments, there is a need to generate new data set. In evaluating IDSs, KDDCUP99 and NSLKDD data sets were generated a decade ago, however for current network threat environment these data sets are not comprehensive reflection. Developing IDSs with a comprehensive low foot print attack dataset, in this paper DARPA-2009 is utilised. A novel statistical based feature extraction strategy is applied to construct the new features from DARPA-2009 Data set that consists of different style of attacks. A TCP trace tool is used to construct the features from the Pcap files and describe the new attacks behaviours. Finally, this data set is labelled and applied multiple machine learning (ML) algorithms to empirically observe the performance. The ML algorithms utilised were Naive Bayes classifier (NB), Decision Tree learning (DT), Artificial Neural Network classifier (ANN), and EM Clustering algorithm. The decision tree proved the better performance for this data set with suggested feature extraction strategy. The results show that these classifiers are not able to detect zero-day attacks, because of the two issues. Firstly, no payload for packets of DDoS which cause biased learning classifiers. Secondly, there is an unbalancing between attack records as well as normal records which cause highly false alarm rates. Future work includes establishing new methods to tackle the problem of imbalance between attack vectors and normal information. These methods will be applied to online network traffic and non-linear data of inter-arrival time and inter-packet length of flow-based features.

Keywords: NIDS, DARPA-2009 data set, low foot print attacks, feature selection, pcap files

An Approach to Detect and Analyze the Impact of Biased Information Sources in the Social Media

Jarkko Paavola and Harri Jalonen
Turku University of Applied Sciences, Turku, Finland

Abstract: The paper presumes that social media is an environment where local and small events may escalate into bigger and even global ones in a very short period of time. This is because social media offers opportunities for discussion of shared interest in way which cannot be controlled: everything that can be exposed will be exposed – for all intents and purposes. This possibility has also changed the landscape of discussions of controversial issue, such as foreign and security policy. Compared to traditional mass media, social media enable disclosing opinions without censorship. Nowadays people have access to online discussions, blogs and even websites entirely devoted to sharing negative information. It has been seen that, during crisis situations social media has become a major way of affecting people's opinions. Consequently we are witnessing the rise of trolls – individual who shares inflammatory, extraneous or off-topic messages in social media, with the primary intent of provoking readers into an emotional response or of otherwise disrupting normal on-topic discussion. Based on the lack of censorship, on the one hand, and trolling behavior, on the other, the paper aims to understand the rise and diffusion of extreme opinions in Twitter. This is a case study paper, where the analysed case is Twitter messages on Ukrainian crisis during 2014 written in Finnish language. The aim is to utilize sentiment analysis for the automatic detection of trolling behavior. Sentiment analysis provides tools for strategic communications for the automatic analysis of social media discussions and to recognize opportunities for participating in the discussion at the most effective stage.

Keywords: opinion mining, social media, emotion, Twitter

How to use Software-Defined Networking to Improve Security – a Survey

Jorge Proença, Tiago Cruz, Edmundo Monteiro and Paulo Simões
Universidade de Coimbra, Portugal

Abstract: Despite being a relatively recent development, the SDN paradigm has already challenged the established network design, management and operation concepts. SDN is the result of a number of studies and ideas on network programming, oriented towards the improvement of the traditional network functionality and management, due to its unique levels of flexibility .One of the main characteristics of this paradigm is the breakout of the functionalities of traditional network elements (e.g., routers), moving part of them to a centralized controller.

Network elements such as routers become simpler forwarding devices, and the controller becomes responsible for routing decisions. This allows the controller to have complete perspective and control over the network. Moreover, network changes become seamless, as the controller can change the network behaviour online. In this paper we present an overview and survey on the usage of the Software Defined Networking (SDN) concept for security purposes, discussing how to use to increase network security awareness, as well as for reacting to ongoing attacks .This survey analyses research studies that are representative of a variety of security measures that can be improved by the use of SDN enabled technologies. We address network security in four distinct fields: SDN-enabled honeypots, Denial-of-Service (DoS) mitigation, source address spoofing countermeasures, and network scanning avoidance.

Keywords: software defined network, SDN, network security, IP spoofing mitigation, DoS spoofing mitigation, network scan avoidance, honeypot

The Security and the Credibility Challenges in e-Voting Systems

Ahmed Rana[1], Ibrahim Zincir[2] and Samsun Basarici[1]
[1]Computer Technologies Department, Yasar University, Izmir, Turkey
[2]Computer Engineering Department, Yasar University, Izmir, Turkey

Abstract: E-voting is one of the most emerging social innovations of the 21st century which is being adopted by many countries, since it represents the peak of e-government solutions and also enables an easier way to vote for their citizens and expatriates. In addition, e-voting systems will not only increase the amount of voters' participation but also will decrease the total cost of electoral process. The main concern with the e-voting system is security. Unlike any other offence, it is first difficult to observe ambiguities in voting and also it is much more difficult to locate the lost or to detect the rigged votes. Challenges such as how to authenticate the voter, how to securely cast his/her vote and then how to store and to count these votes without outside influence generate whole scrutiny over the e-voting systems. This paper first discusses these challenges and then proposes a unique approach to ensure public confidence and credibility over the electoral systems. This proposal inherits 2 independent modules; first module to verify authentication by implementing an e-government application and smartphone to identify a registered voter. After the completion of successful validation, the second module, that provides anonymity to the voter similar to TOR (The Onion Router), will be activated to cast the e-ballot.

Keywords: e-voting, security, cyber security

Culture and Cyber Behaviours: DNS Defending

Char Sample[1] and Andre Karamanian[2]
[1]Carnegie Mellon University/CERT, USA
[2]Cisco, USA

Abstract: The Domain Name System (DNS) provides the mapping information that allows software to associate names to IP addresses. The DNS software acts as an infrastructure service on the Internet and because so many applications rely on properly functioning DNS service, the DNS software is a popular and potent attack vector. Many of the DNS attacks can be prevented through the adoption of DNS security extensions (DNSSEC). DNSSEC provides assurance of data authenticity (Arends, Larson, Massey & Rose, 2005). The DNSSEC standard was introduced in 2005 (Ibid) yet adoption has remained uneven. The uneven adoption rate of DNSSEC may have several reasons; this paper focuses on potential cultural reasons. DNSSEC represents a defensive tool that provides protection against a range of DNS related attacks, and adoption of DNSSEC requires planning. This suggests both conscious and unconscious thought are is use, andculture influences both conscious and unconscious thought. Adoption of DNSSEC by countries opens up the analysis through culture. Culture offers a technology independent path for analysing computer network defence (CND) behaviours. These researchers seek to determine if a relationship exists between culture and DNSSEC adoption and rejection rates. Quantitative evaluation of culture relies on a framework that provides operationalized data. Geert Hofstede's cultural dimensions quantitatively define a framework for evaluating and understanding various behaviours, by nation. This framework has been used in academia and business for research in order to better understand other cultures. The quantitative nature of the Hofstede framework makes possible meaningful statistical processing on human behaviours. Hofstede avails his data for researchers in all disciplines. The preliminary findings support the hypothesis: culture influences CND behaviours. The data set was examined for DNSSEC adoption rates and rejection rates across all six dimensions. The analysed data displayed statistically significant findings across three dimensions: power distance, individualism versus collectivism, and long-term versus short-term orientation. The tests performed were quantitative and included the use of the Mann-Whitney u-test and the Spearman's correlation where adoption and rejection rates were evaluated using culture as the independent variable and adoption/rejection rates as the dependent variable. The findings revealed valuable data in both the adoption and rejection rates. These findings suggest that culture influences CND choices and behaviours. These choices and behaviours suggest that cyber defensive preferences may vary by culture. The results of this research study suggest the need for additional research targeted toward spe-

cific cultural dimension and their relationship with cyber war strategies and tactics.

Keywords: computer network defence (CND) choices and behaviours, DNS, DNSSEC, Hofstede, cultural dimensions

Security of SmartPhone Solutions for Implantable Cardioverter Defibrillator Communication

Nuno dos Santos and Paul Crocker
Instituto de Telecomunicações ,Universidade da Beira Interior, Covilhã, Portugal

Abstract: In a world where the number of people with heart diseases is continuously increasing, the need for people to implant auxiliary systems for the normal functioning of the human body's main organ is increasing. Implantable cardioverter defibrillators (ICDs) are currently the class of devices amongst implantable medical devices (IMDs) that facilitate the widest range of therapeutic features for the different existing cardiac anomalies, there is however a difficult balance between privacy and security with safety and utility. These devices are updated over wireless connections which can be the subject of active security attacks also data from these devices is transmitted to remote data centres raising privacy concerns from passive attacks. Current solutions use proprietary and expensive hardware and software. This work presents an architecture requiring the use of a smartphone application for improving security and privacy in mobile applications for ICDs. This architecture can be separated in two distinct parts. The first aims to improve and simplify the communications between the implanted device and the patient by the use of NFC and WISP technologies, while the second appears in order to extend those communications to a back office using MQTT.

Keywords: ICD, smartphones, privacy; security, NFC, MQTT

From Influencee to Influencer – the Rhizomatic Target Audience of the Cyber Domain

Miika Sartonen[1], Aki-Mauri Huhtinen[1] and Martti Lehto[2]
[1]Finnish National Defence University, Helsinki, Finland
[2]University of Jyväskylä, Jyväskylä, Finland

Abstract: The messages of an influence operation are interpreted in a variety of ways by their receivers. To increase the probability of success, these messages are typically tailored to affect a defined group, a target audience. Target audience analysis (TAA) is a process of finding suitable target audiences for influence opera-

tions. There are multiple ways of completing the task, ranging from fast and intuitive to complex multi-staged processes. These processes use the information available at the moment of making presumptions about the effectiveness of competing approaches in order to choose those with best end results. The internet presents a challenge to this type of sequential, linear process by resisting to stop changing while the process is being executed or to conform to direct causalities. The internet is more like a rhizome, as presented by Deleuze and Guattari in the Thousand Plateaus. Within the context of rhizome, we also suggest defining the target audience(TA) – not as a pre-defined, but as a time-sensitive group, temporarily advantageous to the intended influence effort. This temporal advantage may be due to different causes, such as the topic being promoted by a popular media figure (a blogger for instance) or real-life incidents capable of shifting opinions towards the intended end of opinion charts. Instead of carrying outa linear, effectively one-time process of TAA we argue that it is possible to use the powers granted by the digital domain to constantly be on the lookout for, not perhaps the rhizome itself, but the 'fruiting bodies' it produces. Whenever the rhizome produces a favourable TA, it can be found by software, analysed and either catalysed into growing or suffocated with a spiral of silence.

Keywords: cyber domain, psychological operations, rhizome, social media, target audience

Dissuasion, Disinformation, Dissonance: Complexity and Autocritique as Tools of Information Warfare

Keith Scott
De Montfort University, Leicester, UK

Abstract: "Yesterday's was a totalitarian war, in which the dominant elements were quantity, mass and the power of the atomic bomb. Tomorrow's war will be globalitarian, in which, by virtue of the information bomb, the qualitative will be of greater importance than geophysical scale or population size." (Virilio 2005: 144) Virilio's*The Information Bomb* presents a vision of future conflicts occurring as much on an informational and conceptual battlefield as a physical terrain. In a world where even the 24-hour news cycle of conventional broadcasting fails to keep up with the endlessly proliferating, instantly updated streams of data, and where the boundaries between sender and receiver are blurred to the point of non-existence, any concept of "full-spectrum dominance" in the informational realm is doomed to failure. Conventional models of influence, based on one to many, top-down delivery will be rejected out of hand by audiences who display an ever-growing disillusion with and distrust of official channels of information. In this paper, I suggest that the present terrain offers a number of opportunities for

developing strategies and tactics of information warfare which are based on the techniques already deployed by anti-establishment actors: détournement, satire, and the appropriation and subversion of pre-existing media artefacts. I will also argue that conflict in the "fifth domain" should view the inherent complexity, diversity and apparent anarchy of the online realm as aids, rather than threats to the effective exercise of influence. Norbert Wiener wrote in 1954 that "There is no Maginot Line of the brain". This is both a salutary reminder that a fortress mentality is fatal in cybersecurity, and a call to arms against any system of thought which is not multidisciplinary. The final section of this paper will build on Wiener's idea, by arguing that we can learn from certain current trends in computer gaming (most notably what has been termed "ludonarrative dissonance") how to devise strategies of influence which rely, not on the presentation of a simplistic message or counter-narrative, but on the cultivation of a mindset which sows doubt, uncertainty in a receiver's mind, and an awareness that their worldview is not the only one possible. Truly successful information warfare must rely less on the information itself than on the construction of the mental frameworks through and within which that information is processed; this paper seeks to present a number of ways in which this framework may be reshaped.

Keywords: information warfare, influence, gaming, confusion

Detection of DNS Based Covert Channels

Stephen Sheridan and Anthony Keane
Institute of Technology Blanchardstown, Dublin, Ireland

Abstract: Information theft or data exfiltration, whether personal or corporate, is now a lucrative mainstay of cybercrime activity. Recent security reports have suggested that while information, such as credit card data is still a prime target, other data such as corporate secrets, employee files and intellectual property are increasingly sought after on the black market. Malicious actors that are intent on exfiltrating valuable data, usually employ some form of Advanced Persistent Threat (APT) in order to exfiltrate large amounts of data over a long period of time with a high degree of covertness. Botnet's are prime examples of APTs that are usually established on targeted systems through malware or exploit kits that leverage system vulnerabilities. Once established, Botnet's rely on covert command and control (C&C) communications with a central server, this allows a malicious actor to keep track of compromised systems and to send out instructions for compromised systems to do their biding. Covert channels provide an ideal mechanism for data exfiltration and the exchange of command and control messages that are essential to a Botnet's effectiveness. Our work focuses on one particular form of covert channel that enables communication of hidden messages over

normal Domain Name Server (DNS) network traffic. Covert channels based on DNS traffic are of particular interest, as DNS requests are an essential part of most Internet traffic and as a result are rarely filtered or blocked by firewalls. As part of our work we have created a test bed system that uses a covert DNS channel to exfiltrate data from a compromised host. Using this system we have carried out network traffic analysis that uses baseline comparisons as a means to fingerprint covert DNS activity. Even though detection of covert DNS activity is relatively straightforward, there is anecdotal evidence to suggest that most organizations do not filter or pay enough attention to DNS traffic and are therefore susceptible to data exfiltration attacks once a host on their network has been compromised. Our work shows that freely available covert DNS tools have particular traffic signatures that can be detected in order to mitigate data exfiltration and C&C traffic.

Keywords: data exfiltration, covert channels, advanced persistent threat (APT), DNS, botnet, command & control (C&C)

Hands-on Learning of Computer Security: A Cost-effective Laboratory Infrastructure Based on Virtualization Software

Armin Simma, Jeremias Eppler and Bernhard Lang
Vorarlberg University of Applied Sciences (FHV), Dornbirn, Austria

Abstract: Hands-on exercises facilitate learning practical Information Technology (IT) and, in particular, IT security skills. To provide students with the necessary IT infrastructure, universities have implemented learning laboratories. Virtualization is a proven alternative for such laboratories since virtualized systems are flexible and easily restorable. Easy and fast restorability is necessary because of, first, limited change periods between classes and, second, denial of service or damage to systems that can occur or sometimes is the specified goal of security-related exercises. This paper describes a decentralized virtualization approach that allows higher education IT departments to reuse existing investments in personal computers. The personal computers (PC), which are physically located in laboratory rooms, are used as virtualization hosts. Each PC can host different Virtual Machines (VM) used for exercises. These VMs can be connected using a virtual network. Each virtual network on a PC is isolated from other networks. Therefore various lab scenarios can be setup and executed including security-related exercises that require strong isolation. The solution uses a central file server where lecturers prepare lab scenarios consisting of one or more VMs. Each VM contains the operating system (OS) and application software necessary for performing the lab exercise. The OSs and applications can differ from VM to VM. The deployment of VMs from the server to all PCs is a critical part of the solution because - without using broadcast technology or other optimizations - the amount of data to be

transferred is high; in certain scenarios too high to be able to transfer the data within the class change period using state-of-the art network bandwidth. The solution described in this paper is based on (1) dividing the VM image into a base image and one or more delta snapshots,(2) data deduplication and (3) peer-to-peer technology. The system is based on open source and free software. Experiments and practical application of the solution have shown a high throughput.

Keywords: virtualization; education technology, hands-on laboratory infrastructure, virtual laboratory, IT and IT security education, computer security

Absolutely Indiscernible Data Transfer Channel

Mikhail Styugin
Siberian State Aerospace University, Krasnoyarsk, Russia
Siberian Federal University, Krasnoyarsk, Russia

Abstract: The present paper reviews the technology for establishing absolutely indiscernible data transfer channels. The fact of message transfer is only known to the sender and the recipient. Unlike the classical concept of a data transfer channel, in steganography there is no specific container in which transferred information is embedded. The main condition for an absolutely indiscernible data transfer channel is that the volume of information transferred through it should not be greater than the number of hypotheses, which a potential adversary needs to enumerate in order to detect the channel. Hence, even the mere task to detect such channels appears infeasible. Some original solutions, which allow solving technical difficulties in establishing such channels, are reviewed in this paper. One of those solutions is aliasing one channel with another. Eventually even after disclosing the channel in some way we can find information, which is ultimately not the information that had been transferred through the channel. That solution reveals new opportunities for misinformation in cyber wars. Another technical solution is constant modification of the channel's structure and even modification of the rules for changing it. That is after some volume of data has been transferred the channel's structure changes so significantly that it can be regarded as a new channel. That changing process is continuous. In case an eavesdropper somehow acquired the channel's structure at a certain moment in time the next moment the channel will disappear from the eavesdropper as it shall change its structure. An absolutely indiscernible channel was implemented and tested in Facebook social network. It took around 8 hours to transmit the text of this paper. That channel in Facebook network was established by means of two chat bots. Information was transmitted using not the text messages but environment parameters. The parameters used were time delays between reading messages,

between replies to messages, appearance of "typing" indicators, etc. Transmission speed of 33 bytes per minute was reached. In case of using other (non-timing) environment parameters a significant increase of a channel's throughput capacity is possible.

Keywords: steganography, stereotyped patterns, protection from research, moving target defence

Standard ISO 27037:2012 and Collection of Digital Evidence: Experience in the Czech Republic

Jaromir Veber and Zdenek Smutny
Faculty of Informatics and Statistics, University of Economics, Prague, Czech Republic

Abstract: Collection of digital evidence in criminal investigation is gaining in importance. It is an outgrowth of the development and penetration of ICT into society (informatization). After a brief introduction of ISO/IEC 27037:2012, this paper compares the suggested practices with those that are currently used by investigators (criminal police) and analysts (forensic laboratory). This is followed by a discussion of general experience in collecting and analysing digital evidence in the Czech Republic. The contribution allows experts from other countries to compare their practices with the standard, and also with practical approaches that are applied by Czech departments.

Keywords: digital evidence, ISO 27037, expert opinion, acquisition, collection, Czech Republic

The Legal Conundrum Facing ISPs in Social Media Policing Against Extremism

Murdoch Watney
University of Johannesburg, Gauteng, South Africa

Abstract: The purpose of this discussion is to consider whether ISPs have a legal duty to police social media against extremism and if affirmative, the scope of the legal duty. The role of the ISP in social media policing must be seen against the background of a proliferation in extremism which in itself is a controversial topic as it may impact on sensitive topics relating to politics, religion and foreign policy to name but a few. The relevance of ISP policing was highlighted after the 2013

revelations by Snowden, a former US NSA contractor. The NSA allegedly obtained direct access through a program referred to as PRISM to servers of Internet US companies such as Google, Apple and Facebook to collect information which apparently allowed access to the content of information and not merely metadata. Against this background, the Snowden disclosures served as a catalyst for a long-overdue debate pertaining to state surveillance and the role of the ISP in assisting law enforcement and intelligence agencies with surveillance and/or conducting surveillance out of its' own accord. Early 2014 saw the European Court of Justice declaring the Data Retention Directive 2006/24/EC invalid. The Directive provided for ISPs in EU countries to collect metadata of all Internet users for a specified period of time. The Court recognized that although the retention of metadata for investigative purposes was compatible with the European framework, it was disproportionate and contrary to the protection of fundamental human rights. In this regard it should be noted that the Australian government is considering implementing compulsory blanket data retention laws. The legal position of how far ISP policing should go is also ambiguous following a 2014 UK Intelligence and Security Committee report. The report criticized ISPs and in this instance, Facebook, for failing to report to intelligence agencies a social media communication by one of the Islamic extremists who was involved in the 2013 murder of UK soldier, Rigby. The report suggests that ISPs and in this instance, social media providers, should identify potential perpetrators and report it to law enforcement and security agencies. Islamic extremism culminating in terrorist attacks has become a serious threat to the safety and security in several countries. Extremism is a globalized concern as has been illustrated by the killing of a Canadian soldier as well as the hostage taking of citizens in Sydney in 2014. Early 2015 saw the killing in Paris of 17 people by Islamic extremists. The question pertaining to the legal duty of ISPs in policing social media communications in order to identify extremism is an interesting, though problematic and controversial issue and applies to ISPs worldwide. It may be that the 2015 Paris events and prior incidents will constitute another 9/11 moment which will change ISP policing of social media against extremism and make the tightrope ISPs tread in ensuring a balance between human rights protection and security even more tenuous.

Keywords: ISP, social media, surveillance, law, ISP policing, extremism

Automated Processes for Evaluating the Realism of High-Interaction Honeyfiles

Ben Whitham, Tim Turner and Lawrie Brown
University of New South Wales, Canberra, Australia

Abstract: This paper presents an approach to measure high-interaction honeyfile realism by extracting *k* features from surrounding documents, mapping these to *k*-dimensional space, and then using Euclidean Distance to assess consistency and similarity with the honeyfile. This paper identified an initial set of seven realism features: average sentence length, number of paragraphs, average paragraph size, uncommon bigrams, topic consistency in paragraphs, sentence complexity and ratio of unidentified words. A scenario was established where honeyfiles were required to protect documents within a hierarchical document repository. This approach was demonstrated using two data sets: (1) an artificially constructed data set of Internet files, and (2) extracts from a real small business file system. Two honeyfile methods were used, a low-interaction method, which built files using random characters, and a high-interaction method that mimicked academic papers. The model was able to clearly distinguish between the realism of low-interaction honeyfiles constructed with random characters, and high-interaction honeyfiles that were purpose built to mimic the test data. The model was also able to detect a discernable drop in realism when these same high-interaction honeyfiles were matched with dissimilar data ,originating from the small business file system.
Keywords: honeyfiles, cyber deception, realism, high-interaction, data theft

PHD Research Papers

Hierarchical Model for Intrusion Detection Systems in the Cloud Environment

Muhammed Abdulazeez and Dariusz Kowalski
University of Liverpool, Liverpool, UK

Abstract: The recent emergence of cloud computing technology has drastically altered the way we perceive computing infrastructure, software delivery and development models. This massive leap from mainframe computers to highly scalable, dynamically configurable and heterogeneous cloud technology has turned computing and data centres to an innovative technology. This rapid transition towards the cloud has triggered security concerns on this delivery model. The two security challenges addressed in this paper are (i) Dynamic Large Scale System, where most cloud defence systems provide cloud-provider-oriented security in which the defence components are placed at the entrance of the cloud without considering scalability of the cloud and heterogeneity of the applications that run on the platform. (ii) Detection Rate vs. Performance, where we have an inverse relationship between detection rate and performance. However, as the underlying technology is changing, security experts are not amending their approach towards tackling the security challenges of cloud computing. This is because they do not consider the above challenges when building their cloud defence systems. They treat cloud computing security issues as if they were traditional network environments with homogeneous applications that are not easily scalable. To solve this problem, we introduced a lightweight, hierarchical, highly dynamic intrusion detection system architecture that is more suited for cloud computing environment. Our model uses application layer detection mechanisms to detect intrusions at different levels of the cloud computing hierarchy. We identified a number of rules that need to be checked in the application layer protocol to detect the possibility of attacks on the application server. The checking of the rules is not done at certain nodes in the cloud instead, our system decides where to check them based on the current load and the attacks detected at the node and the child nodes of the architecture. This solves the scalability issue of cloud computing architecture, because intrusion detection load will be distributed across the cloud eliminating single points of contention and failure. Our solution also addresses the heterogeneity challenge, because servers (virtual machines (VM)) running different applications can apply different detection approaches. We employed randomised approaches to improve the detection performance of our system, for instance, by selecting a subset of the rules to detect attacks; this is to improve the detection rate and performance challenge. To justify efficiency of our system, we present preliminary results comparing the detection rate vs. system performance. It is worthy to note that although in this paper, we concentrated on

Denial of Service and Distributed Denial of Service attacks, our model can be extended to other types of attacks as well.

Keywords: intrusion detection, cloud security, virtual machine, denial of service, application layer security

The Semantic Approach to Cyber Security Towards Ontology Based Body of Knowledge

Adiel Aviad, Krzysztof Wecel and Witold Abramowicz
Poznan University of Economics, Poznan, Poland

Abstract: Cyber defence must cope with a wide variety of possible attacks, appearing each day at increasing pace. In addition, an organization should master defence technologies and prioritize what defence should be taken, given that resources are limited. Evaluation of possible attacks and risks is therefore crucial. Since the relevant knowledge is complex and rapidly changing, ontology may be useful in integrating and sharing the knowledge required for evaluation of cyber security and for prioritizing defences.

Keywords: cyber security, semantic web technology, attacks, threats, ontology

Resurrecting Anti-Malware Through Collaboration

Manuel Corregedor and Sebastiaan Von Solms
Academy of Computer Science & Software Engineering, University of Johannesburg, Johannesburg, South Africa

Abstract: A number of reports indicate that malware infection rates continue to increase, additionally, the reports also indicate that malware is becoming increasingly advanced. The spread of malware has grown to such an extent that a number of security experts have declared that anti-virus is dead. We propose an architecture called Collab-AV that can be used to address the anti-malware product vulnerabilities. The Collab-AV architecture is based on the principle of collaboration between different sources of information and different existing anti-malware vendors thus following a “strength in numbers” philosophy. The Collab-AV architecture is essentially divided into three layers as follows: Collab-AV Remote Layer: Represents all the components of Collab-AV that exist outside of the users' environment i.e. external to the user's computer. This layer is responsible for providing Collab-AV with actionable threat intelligence by gathering and utilising information gathered from the following sources: malware hash registries, benign

software hash registries, threat information sources and trusted Collab-AV Peers. Collab-AV Local Layer: Contains the most important sub-systems of Collab-AV that execute on the user's computer. The sub-systems are collectively responsible for ensuring that the user is protected from malware infections by utilising the information gathered from the Collab-AV Remote layer and information gathered from the user's computer. Collab-AV Evaluation Layer: The purpose of this layer is to evaluate Collab-AV by continuously testing it for new vulnerabilities. The objectives of this layer can be achieved by using the evaluation framework we defined in our previous work or by integrating evaluations by third parties such as AV-Comparatives. The outputs of the evaluations will be used to guide future improvements on Collab-AV. The Collab-AV architecture has been designed to work with existing anti-malware products as opposed to replacing them while ensuring increased detection rates, trust, scalability and privacy.

Keywords: malware, anti-malware, virtualisation, collaboration, trust

A Cloud Forensic Readiness Model for Service Level Agreements Management

Lucia De Marco[1, 2], Filomena Ferrucci[2] and Tahar Kechadi[1]
[1]School of Computer Science and Informatics, University College Dublin, Ireland
[2]Department of Management and Information Technology DISTRA MIT University of Salerno, Fisciano, Italy

Abstract: Cloud computing is increasingly becoming a target of cyber-criminal attacks. Often the committed crimes violate the Service Level Agreement (SLA) contracts, which must be respected by all the involved parties. Cloud Forensics is a branch of Digital Forensic discipline dealing with crimes involving the Cloud. A manner for leveraging some of the attacks is the provisioning of a Forensic Readiness capability, by performing some activities before the crimes happen. In this paper we introduce a model aimed to represent the management of SLAs through a cloud system.

Keywords: cloud forensics readiness, service level agreements, cloud monitoring, SLA model, SLA management

Non-Interactive Privacy Preserving Protocol for Biometric Recognition Based on Somewhat Homomorphic Encryption

Giulia Droandi
Department of Information Engineering and Mathematics, University of Siena, Siena, Italy

Abstract: Biometric signals are often used in access control systems because of their immutable and highly discriminative characteristics. While the deployment of biometric access control systems allows user identification without the risk of password leakage or theft, at the same time it raises serious concerns about the leakage of individuals' privacy. A number of privacy preserving protocols have been proposed to guarantee users' privacy against a centralized database owner. Until now, mainly interactive protocols based on Garbled Circuits (GC) and additively Homomorphic Encryption (HE) have been presented. In this paper we describe a non-interactive protocol for privacy preserving biometric matching, whose complexity is totally moved to the server side. Only input encryption and output decryption are performed by the client. This is made possible by relying on a Somewhat Homomorphic Encryption (SHE) scheme, properly modified to handle integer values. Due to the characteristic of the chosen cryptosystem, it can be applied to many different biometrics, such as iris images and fingerprints. Comparison within vectors is done by using Hamming or Euclidean distance, depending on the biometric used. Since, in the encrypted domain, multiplication is expensive in terms of computation and time complexity, we have devised a solution that reduces the amount of multiplications. Moreover, several distances are evaluated in parallel to decrease the time complexity of the system. Furthermore, our solution has the advantage of moving all computation to the server side, eliminating the necessity for interaction with the private key owner. In identification scenarios, client biometric features must be compared with a whole database, owned by the server. This would lead to the necessity of storing the whole database encrypted with a user's public key. We also devise a solution to avoid this necessity. The new SHE-based protocol proposed has been implemented and tested. Results show that, even if the protocol is not as efficient as the interactive protocols based on GC or additively HE, a non-interactive solution based on SHE is feasible.

Keywords: biometric, iriscode, fingercode, somewhat homomorphic encryption, privacy preserving protocol

How can Internal and External Dependencies Affect Infrastructures Security?

Eric Filiol[1] and Cécilia Gallais[2]
[1]E.S.I.E.A, Laval, France
[2]TEVALIS, Rennes, France

Abstract: The main objective of the model of infrastructures presented in this paper is to identify the dependencies between the components of an infrastructure, be they internal or external, and regardless of whether they are strong or weak, in order to find more or less complex attack patterns that can be translated into attack scenarios against the modelled infrastructure. These scenarios enable the identification of security vulnerabilities and thanks to the real-life features they bring, it can be determined whether these vulnerabilities are operationally exploitable or not. The existing models of infrastructures tend to be extremely narrow as they are often reduced to the representation of its information technology (IT) components. This narrow-minded representation can lead to serious security breaches as it does not take into account all the components of an infrastructure, especially the human, organizational and informational ones, even if the IT components depend on them. Therefore the infrastructure model presented here takes into account all the possible components of an infrastructure. To illustrate the model, a realistic but fictional example of infrastructure is presented in the first part of this paper. This example is not real for obvious security reasons. As this infrastructure was previously studied and analyzed, attack scenarios against it already exist. So it is possible to use it to "validate" the model if the results obtained here correspond to the previous results. The infrastructure model is presented in the second part and is mainly based on graph theory. The example of the first part is modelled according to it. Then it is shown how this infrastructure model allows the determination of complex attack scenarios which do not only apply on the cyber domain.

Keywords: model, infrastructure, attack scenario, dependency, security, graph

A Functional Architecture for Cloud Forensic Readiness Large-Scale Potential Digital Evidence Analysis

Victor Kebande and H.S.Venter
Department of Computer Science, University of Pretoria, South Africa

Abstract: In this paper, the authors propose a novel concept of analysing large-scale potential digital evidence (DE) through reliable, efficient and timely compu-

tation across nodes in different clusters within the cloud environment. A concern to the digital forensic (DF) community is the increase in network traffic and big data in the cloud which has become exacerbated into security threats and new and emerging vulnerabilities, which have further compromised the security of the internet. This has happened due to acute distributed network attacks moving as raw traffic in the cloud environment. Because of this, there is a dire need to forensically process and analyse potential digital evidence (PDE) for purposes of digital forensic readiness (DFR) in the cloud environment. Through this, the effort required in performing a digital forensic investigation (DFI) in the cloud environment may be minimised. The problem that this paper addresses is a lack of an easy way of timeously and efficiently computing potential large-scale evidence in the cloud for DFR purposes. Finally, a functional architecture for a Cloud Forensic Readiness Evidence Analysis System (CFREAS) that forensically reduces PDE analysis time of big evidence using MapReduce is proposed. The results may significantly be deduced efficiently at a centralised security centre.

Keywords: cloud, forensic, readiness, large-scale, potential, digital, evidence, Hadoop, Mapreduce, functional, architecture

Project Management of Complex Penetration Tests

Tomáš Klíma and Martin Tománek
University of economics, Prague, Czech Republic

Abstract: In the last two decades the importance and sophistication of penetration tests of information systems (IS) have significantly increased. In cooperation with formal audit techniques they provide the thorough assessment of target systems security without excessive load or interruption of operations. Although majority of auditors use the proven (but often outdated) methodologies like ISSAF or OSSTMM, one of the biggest problems is the absence of structured approach to business justification, planning, executing and reporting. It results in problems in communication between client and supplier and also the management of extensive tests is based on ad hoc decisions and results in suboptimal outputs. In this article authors propose how to overcome the above mentioned issues by using the project management framework PRINCE2 as a framework for management of penetration tests of complex information systems. Emphasis is placed on utilizing the principles, themes and processes of PRINCE2 and their tailoring to specific needs of IS security audit requirements. Authors build on previous work focused on development of new IS penetration tests methodology with focus on implementing the COBIT as a framework for management of these tests, and on previ-

ous work focused on tailoring the project management framework PRINCE2 to other IT related frameworks. Also the experience from managing and conducting the penetration tests of (critical) IS (and other IT projects like IS development) will be used in order to deliver the concept useful for real world penetration tests that are properly and responsibly managed. Target audience is represented by the IS auditors as well as project managers of both client organization and supplier. All of them can benefit from the formalized concept that has the capability to help involved parties to responsibly manage and communicate the penetration tests in order to achieve expected results and benefits.

Keywords: penetration test, methodology, project management, PRINCE2, IS security

Analysis of the Implementation of an Interactive Kinetic Cyber Range Component

Brendan Lawless, Jason Flood and Anthony Keane
Institute of Technology Blanchardstown, Dublin, Ireland

Abstract: Securing the operational resilience of devices within the Internet of Everything (IOE) requires new and innovative approaches to cyber threats. One approach is to allow end-users to personally experience the impact of an attack on any IOE component using a scale model of a personal, corporate or national infrastructure using a Cyber Range. This paper looks at the implementation of individual Cyber Range components and analyses the methodologies and tools of the attacks on the components from Cyber Challenge CTF competitions.

Keywords: cyber-range, kinetic, analysis, cyber, attack

Master's Research Papers

Curb Your Enthusiasm: Why the Future is not Stuxnet

Andreas Haggman
Royal Holloway, University of London, London, UK

Abstract: This paper analyses and re-evaluates the significance of Stuxnet to warfare by placing it in the historical context of airships. At the beginning of the 20th century airships opened up the skies as a third domain in which to conduct war and were heralded as the future of warfare. Similarly at the dawn of the 21st century, Stuxnet has demonstrated the possibilities of using cyberspace as a fifth domain for warfare and there has been seemingly unreserved enthusiasm for the future of cyber weapons. This paper aims to provide a reality-check for such enthusiasm by looking at the parallels evident between airships and Stuxnet, as well as the future nature of war in which Stuxnet-like weapons might be deployed. Broadly speaking, the paper is divided into three sections. First, a brief overview and comparison of the bodies of literature surrounding both airships and Stuxnet is given. This reveals substantial similarities which may hold clues to the future prospects of Stuxnet and cyber weapons. Next, the paper delves into the particulars of airship warfare, concentrating on different types of effects airships had – physical, non-physical, and long-term. Overall it is found that the damage inflicted by airships, both material and non-material, was both insignificant and disappointing in comparison to the investment made in them. Where airships proved influential, however, was in introducing ideas of airpower which resonate in military strategies today. Having established this historical context, the paper then proceeds to analyse the applicability of cyber weapons given the particular characteristics of modern war. It is asserted that near-future wars are likely to retain the shift away from interstate industrial conflicts to war amongst the people as well as the enduring Clausewitzian nature of war as an imposition of will. Given these characteristics, the utility of cyber weapons is limited and Stuxnet's ultimate significance therefore diminished. Consequently, it shall be concluded that the enthusiasm surrounding Stuxnet deserves to be curbed.

Keywords: airships, Clausewitz, cyber warfare, Stuxnet

An Analysis of Estonia's Cyber Security Strategy, Policy and Capabilities (Case Study)

Michael Kouremetis
Purdue University, West Lafayette, Indiana, USA

Abstract: Estonia as a nation marks one of the most progressive adopters of information and communication technologies in all aspects of government, society

and culture. While the technological progress in all domains of Estonian society is astounding, it has also created an immense cyber threat for the nation. With the advent of information systems and infrastructure to support these numerous services has come the immense increase in the attack surface for any cyber adversary or attack. In response to this, this report is dedicated to analyzing Estonia's cyber security strategy, policy and capabilities in efforts to assess Estonia's ability to effectively mitigate and defend against cyber attacks and adversaries to their information services, systems and infrastructure as well as their realized digital way of life. It is initially hypothesized that Estonia does maintain significant technical and strategic capabilities to thwart possible threats via the cyber domain but does not possess the equivalent in operational resources in order to implement such capabilities. The analysis concludes that Estonian leadership is very aware of this and understands the threats and possible consequences in establishing such avocation of information and communication technologies. Additionally, there is substantial evidence to support that Estonia has the technical capabilities and strategic acumen to effectively defend against adversarial forces targeting their information services, systems and infrastructure; while there was not sufficient proof of resources required to implement and fully utilize these capabilities.

Keywords: Estonia, cyber security, cyber policy, critical infrastructure, National Defence

A Conceptual Model for Digital Forensic Readiness in e-Supply Chains

Derek Masvosvere and Hein Venter
Department of Computer Science, University of Pretoria, Pretoria, South Africa

Abstract: In recent years e-supply chains have received much research attention. Most of it has been towards improving supply chain management. Supply chain management involves looking at ways to improve the performance of trading partners within the supply chain. It is needless to say that little attention has been placed on improving the information security infrastructure across e-supply chains. The use of Information and Communications Technology, together with the Internet definitely have an impacton the supply chain in a positive way; providing benefits such as cost reduction and better service delivery to customers. However, this also leaves supply chains vulnerable to a number of security threats such as cyber terror, information theft and eavesdropping, amongst other threats. The problem this paper addresses is the lack of a well-formulated approach in e-supply chains to prepare trading partners for security incidents that might occur in the supply chain. Digital forensic readiness offers a data collection framework that has vast capabilities to obtain potentially useful information that

can be used for many purposes including Digital forensic investigations (DFIs). In this scenario the data collected can be used to detect vulnerabilities across the e-supply chain. It is therefore crucial to contribute different approaches to combat these threats and introduce processes that can prepare trading partners for security incidents. The authors propose an integration of some key security processes in the e-supply chain, which include monitoring the e-supply chain for incidents and collecting forensically sound data, which can be used to assess risk across the e-supply chain or in a court of law. The method proposed is a well-coordinated implementation of digital forensic readiness across the e-supply chain that involves adopting security policies and controls that help provide trading partners with useful information about the activities taking place in the e-supply chain.

Keywords: information and communication systems and technologies (ICT), digital forensic readiness (DFR), digital forensic investigation (DFI), trading partner (TP), e –supply chain digital forensic readiness model (E-SCDFRM)

Work In Progress Papers

Vulnerability Testing of Wireless Access Points Using Unmanned Aerial Vehicles (UAV)

Stephen GergoVemi and Christo Panchev
University of Sunderland, Sunderland, UK

Abstract: Wireless networks are essential part of our everyday life – we are using them at home, workplace, cafe shops and many other public places. Moreover, people trust such connections and readily use them to transfer sensitive information. With an explosive increase of their use we need expand the aspect of evaluating the security issues wireless networks. Majority of household are using the latest secured protocols the WPA2 with a government grade standard nowadays. These protocols are still vulnerable to dictionary attacks that are normally carried out by recording three-way handshakes between the wireless router and the connected client. This method is really common and widely used – its success depends on the strength of the password being used. The research presented here shows another efficient method of hijacking and breaking into home networks is by using a Man-in-the-Middle type attack. The proposed system is implemented on a Raspberry Pi carried by a drone. While until recently UAV's (Unmanned Aerial Vehicles) have been used mainly by militaries and some specialist organisations, nowadays they have become widely available, cheaper and user friendly. The use of a drone allows the system to cover a wide area of potential targets as well as relatively quickly move from one target and WiFi network to another. The system is based on war flying using commercially available drones (Wang, 2006). The main goal of this project is to be able to hijack a wireless connection session between a connected tablet PC and Access Point using WPA2 encryption. We will be able to automate a Man in the Middle attack just by flying the drone around a certain area, setting up a rogue access point and being able to harvest important credentials from the targeted wireless networks and connected devices. The system is based on a number of open source Wi-Fi penetration testing and configuration tools including iwconfig or airmon-ng and custom scripts. The drone payload (Raspberry Pi B+) is using two wireless dongles; one for monitoring the wireless networks and the other one for being the rogue access point. The Raspberry Pi is powered by a 1000 mAh battery and carried by a DJI Phantom Drone. The device is also capable of other types of attacks. Such as disconnecting devices from its currently connected networks or causing denial of service attack against wireless routers/hubs while remaining stealthy to the victim(s) and operating from a distance.

Keywords: drone, hijacking, wireless, raspberry pi, evil twin, rogue AP, war flying

Open-Source Intelligence Monitoring for the Detection of Domestic Terrorist Activity: Exploring Inexplicit Linguistic Cues to Threat and Persuasion for Natural Language Processing

Stefanie Hills, Tom Jackson and Martin Sykora
Loughborough University, Loughborough, UK

Abstract: This early stage work-in-progress doctoral research seeks to consolidate definitions of persuasive, powerful, and influential language to identify quantifiable key features and linguistic patterns described in the existing body of research across multiple disciplines for the purpose of expanding social media monitoring capability to the early detection of potential terrorist activity.

Keywords: social media monitoring, terrorism, cyberwarfare, cybersecurity, forensic linguistics, radicalisation

Late Submission Papers

Fighting the Last war to win the Next

Christopher Brill[1] and James Tollefson[2]
[1]American Military University, Alaska, USA
[2]Wayland Baptist University, Alaska, USA

Abstract: The potential for a cyber-attack on a nation's command and control system is a real threat, but does it equate to a neutralized force? This paper examines how critical national security functions may be supported using antiquated technologies to defeat such risks. The majority of the civilized world understands the crippling nature of cyber-attacks. These events can halt stock markets, commandeer traffic grids, redirect traffic, choke transportation, overload electrical grids, and send homes, businesses, and cities back a century. Exercises to counter these conceptual cyber-attacks may result in new technology, but without a watershed event, the size and scope of a blacked out network remains a mystery. While the total quantity and quality of equipment remaining operational in the aftermath of a sophisticated cyber-attack is beyond this document's scope, the general thesis will assume that some capabilities remain operational and available to reconsolidate. These facts will lead a reader to conclude that in the absence of total network assurance, good leadership becomes even more imperative. In other words, responsible commanders must improvise, adapt and consolidate remaining capabilities, requiring radical shifts in current methodology, training, equipment, etc. Based on the aforementioned, this paper theorizes how military services can exercise command and control in the short term using antiquated systems to overcome network interruptions, in effect bypassing cultural reliance on networked technologies. Using a qualitative approach and historical case studies of Operation JUST CAUSE, the authors articulate the importance of adaptable junior military leadership in adapting to such threats.

Keywords: cyberspace, history, leadership, command and control, operation JUST CAUSE

Social Process for Cyber-Threat Analysis (SPCTA)

Harry Brown III
Norwich University, USA

Abstract: Recently, we have experienced cases of how nation-states are confronted with cyber-threats, creating threats to state power through cyber-capabilities and cyber-interaction between actors in the international political system. Such cases are indicated in relations and incidents between the United States and Chi-

na, Russia and Georgia, Estonia and non-state actors, North Korea and South Korea, as well as between other states and non-state cyber-actors. This research proposes the Social Process for Cyber-Threat Analysis (SPCTA) framework for analyzing cyber-threats to a state. Cyber-threats and risks posed to the state have a foundation in the political, cultural, and economic domains where we may identify causative factors and enabling commonalities present in each state. SPCTA proposes methodology and an algorithm for assessing both qualitative and quantitative factors within these domains that relate to the cyber-disposition of nation-states. As state/non-state cyber-interaction is a means by which a cyber-actor poses a threat, examination was conducted to identify applicable International Relations theories that would both explain the subject matter and provide a basis for the framework. Neither the Realist nor Liberal schools provide a discrete methodology or framework. The Constructivist school offers an alternative perspective that accommodates a positivist approach to structuring analysis and assessment. It is here that SPCTA presents a cross-disciplinary notion—the convergence of IR theory, social process, and the phenomenon of interaction within the cyber domain. As such, SPCTA provides an applied methodology for identifying and assessing causative factors, capabilities, environment, vulnerabilities, and the utility of cyber-attack upon a state, as well as quantifying these components to derive the level of cyber-threat. SPCTA poses an applied theoretical framework for determining cyber-threats that may exist among states and non-state actors. SPCTA generates information and considerations that may be used to formulate effective policy for mitigating threats from cyber-actors. For the purposes of submission to the 14th European Conference on Cyber Warfare and Security ECCWS 2015 conference, this paper has been reduced to only present the core methodology used in the proposed framework.

Keywords: cyber-relations, cyber-threat, cyber-security, risk management, cyber-policy

The importance of paper citations and Google Scholar

As an academic researcher you will know the importance of having access to the work of other researchers in your field as well as making your own work available to others. In the area of academic publishing this is achieved through citation indexing. There are a number of bodies that undertake this task including Thompson ISI, Elsevier Scopus and Google Scholar – to name just a few.

At ACPI we do all we can to ensure that the conference proceedings and the journals that we publish are made available to the major citation bodies and you can see a list relevant to this conference on the home page of the conference website.

However, it is also important for you, the author, to make sure that you have made your work available for citation – particularly with organizations such as Google Scholar. We are providing you here with the simple steps you need to take to do this and we would ask you to take the time to upload your paper as soon as you can.

Step one: Extract your paper from the full proceedings that you have downloaded from the Dropbox link provided to you.

Step two: Upload your paper to your own website, e.g.,

www.university.edu/~professor/jpdr2009.pdf ; and add a link to it on your publications page, such as www.university.edu/~professor/publications.html.

Make sure that the full text of your paper is in a PDF file that ends with ".pdf",

The Google Scholar search robots should normally find your paper and include it in Google Scholar within several weeks. If this doesn't work, you could check if your local institutional repository is already configured for indexing in Google Scholar, and upload your papers there.

More information is available from
http://scholar.google.com.au/intl/en/scholar/inclusion.html

We will separately upload the proceedings to Google Books which is also searched – but evidence has shown that individual upload results in quicker indexing by Google Scholar.

Your own institution may also subscribe to an institutional repository such as
http://digitalcommons.bepress.com/ or
http://dspace.org/

Providing the original reference of your paper is included you have our permission as publishers to have your paper uploaded to these repositories.

Sue Nugus ACPIL

Research Jotter

Research ideas can happen at any time –
catch them in writing when they first occur