Abstracts of Papers
Presented at the
10th International Conference on
Cyber Warfare and Security
ICCWS-2015

Co-hosted by the
University of Venda
and
The Council for Scientific and Industrial Research
Kruger National Park
South Africa

24-25 March 2015

Edited by
Dr Jannie Zaaiman
And
Dr Louise Leenen

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

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

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

Further copies of this book and previous year's proceedings can be purchased from http://academic-bookshop.com

E-Book ISBN: 978-1-910309-97-1
E-Book ISSN: 2048-9889
Book version ISBN: 978-1-910309-96-4
Book Version ISSN: 2048-9870
CD Version ISBN: 978-1-910309-98-8
CD Version ISSN: 2048-9897

The Electronic version of the Conference Proceedings is available to download from **DROPBOX**. (**http://tinyurl.com/ICCWS2015**) Select Download and then Direct Download to access the Pdf file.

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

Contents

Preface

These Proceedings are the work of researchers contributing to the 10th International Conference on Cyber Warfare and Security ICCWS-2015, co-hosted this year by the University of Venda and The Council for Scientific and Industrial Research. The conference is being held at the Kruger National Park, South Africa on the 24-25 March 2015.

The Conference Chair is Dr Jannie Zaaiman from the University of Venda, South Africa, and the Programme Chair is Dr Louise Leenen from the Council for Scientific and Industrial Research, South Africa.

The opening keynote address this year is given by Mr Laurens Cloete, Group Executive Operations at the Council for Scientific and Industrial Research (CSIR), Pretoria, South Africa and the second keynote will be given by Marius Hamman from the Digital Crimes Unit, Legal & Corporate Affairs, Middle East & Africa, Microsoft on the topic of "*Defending against modern threats*". The second day will be opened by General AJ Coetzee of the South African National Defence Force.

An important benefit of attending this conference is the ability to share ideas and meet the people who hold them. The range of papers will ensure an interesting and enlightened discussion over the full two day schedule. The topics covered by the papers this year illustrate the depth of the information Operations' research area, with the subject matter ranging from the highly technical to the more strategic visions of the use and influence of information in cyber war and information security.

With an initial submission of 134 abstracts, after the double blind, peer review process there are 47 research papers, 7 PhD research papers, 6 masters research papers, 1 Work in Progress papere and 2 Non-academic papers published in these Conference Proceedings. These includes contributions from Australia, Botswana, Czech Republic, Denmark, Germany, Lithuania, Namibia, The Netherlands, Portugal, South Africa, Sudan, Tunisia, UK, USA.

We wish you a most enjoyable conference.

Dr Jannie Zaaiman
And
Dr Louise Leenen
March 2015

Conference Committee

Conference Executive

Dr Jannie Zaaiman, University of Venda, South Africa
Dr Louise Leenen, Council for Scientific and Industrial Research, South Africa
Joey Jansen van Vuuren, Council for Scientific and Industrial Research
Suné von Solms, Council for Scientific and Industrial Research, South Africa
Brett van Niekerk, University of KwaZulu-Natal, South Africa

Mini track chairs:
Dr John S. Hurley, Defense University (NDU) iCollege, USA
Dr John McCarthy, Airport CyberSec division, ServiceTec, UK

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

Dr. Kareem Kamal A.Ghany (Faculty of Computers & Information, Egypt); Abukari Abdul Hanan (University For Development Studies, Ghana); Prof Azween Abdullah (Malaysian University if Science and Technology, Malaysia); Dr. Bulent Acma (Anadolu University, Eskisehir, Turkey); Dr. William Acosta (University of Toledo, USA); Gail-joon Ahn (University of North Carolina at Charlotte, USA); Dr. Todd Andel (University of South Alabama, USA); Dr. Leigh Armistead (Edith Cowan University, Australia); Johnnes Arreymbi (University of East London, UK); Prof. Richard Baskerville (Georgia State University, USA); Prof. Alexander Bligh (Ariel University Center, Ariel, Israel); Dr. Svet Braynov (University of Illinois, Springfield, USA); Dr. Raymond Buettner (Naval Postgraduate School, USA); Ivan Burke (CSIR, Pretoria, South Africa); Dr. Jonathan Butts (AFIT, USA); Ass Prof. Marco Carvalho (Florida Institute of Technology, USA); Dr. Joobin Choobineh (Texas A&M University, USA); Prof. Sam Chung (University of Washington, Tacoma, USA); Dr. Nathan Clarke (University of Plymouth, UK); Dr. Ronen Cohen (Ariel University Centre, Israel); Earl Crane (George Washington University, USA); Dr. Michael Dahan (Sapir College, Israel); Geoffrey Darnton (Requirements Analytics., UK); Dr. Dipankar Dasgupta (Intelligent Security Systems Research Lab, University of Memphis, USA); Evan Dembskey (UNISA, South Africa); Dorothy Denning (Naval Post Graduate School, USA); jayanthila Devi (Anna university, India); Dr. Glenn Dietrich (University of Texas, Antonio, USA); Prokopios Drogkaris (University of the Aegean, Greece); Barbara Endicott-Popovsky (Center for Information Assurance and Cybersecurity, University of Washington, Seattle,, USA); Prof. Dr. Alptekin Erkollar

(ETCOP, Austria); Dr. Cris Ewell (Seattle Children's, USA); Dr Christophe Feltus (Public Research Centre Henri Tudor, Luxembourg); Larry Fleurantin (Larry R. Fleurantin & Associates, P.A., USA); Kenneth Geers (Cooperative Cyber Defence Centre of Excellence, USA); Dr Ahmad Ghafarian (University of North Georgia, USA); Prof. Klaus-Gerd Giesen (Université d'Auvergne, France); Kevin Gleason (KMG Consulting, MA, USA); Dr. Samiksha Godara (Shamsher Bahadur Saxena College Of Law, India); Prof. Dr. Tim Grant (Retired But Active Researcher, Netherlands., The Netherlands); Mr. Murray Greg (Department of Navy , USA); Virginia Greiman (Boston University, USA); Dr. Michael Grimaila (Air Force Institute of Technology, USA); Daniel Grosu (Wayne State University, Detroit, USA, USA); Dr ALASADI HAMID (Basra University, Iraq); Dr. Drew Hamilton (Mississippi State University, USA); Joel Harding (IO Institute, Association of Old Crows, USA); Dr. Douglas Hart (Regis University, USA); Dr. Dwight Haworth (University of Nebraska at Omaha, USA); Michael Henson (Thayer School of Engineering at Dartmouth College, Hanover, USA); Dr. John Hurley (National Defense University, USA); Prof. Bill Hutchinson (Edith Cowan University, Australia); Dr. Berg Hyacinthe (State University of Haiti, Haiti); Dr. Cynthia Irvine (Naval Post Graduate School, USA); Prof. Barry Irwin (Rhodes University, South Africa); Ramkumar Jaganathan (VLB Janakiammal College of Arts and Science (affiliated to Bharathiar University), India); Russell James (Metropolitan Airports Commission, USA); Joey Jansen van Vuuren (CSIR, South Africa); Dr Chen Jim (U.S. National Defense University, USA); Dr. Andy Jones (BT, UK); James Joshi (University of Pittsburgh, USA); Prof Leonard Kabeya Mukeba Yakasham (ESURS/ISTA-KIN & ASEAD, Democratic Republic of Congo); Dr. Anthony Keane (Institute of Technology Blanchardstown, Ireland); Ayesha Khurram (National University of Sciences &Technology, Pakistan); Michael Kraft (CSC, USA); Prashant Krishnamurthy (University of Pittsburgh, USA); Mrs Marina Krotofil (Hamburg University of Technology, Germany); Dr. Dan Kuehl (National Defense University, USA); Takakazu Kurokawa (The National Defense Academy, Japan); Rauno Kuusisto (Finnish Defence Force, Finland); Dr. Tuija Kuusisto (National Defence University, Finland); Peter Kunz (Diamler, Germany); Arun Lakhotia (University of Louisiana Lafayertte, USA); Michael Lavine (John Hopkins University's Information Security Institute, USA); Louise Leenen (CSIR, Pretoria, South Africa); Tara Leweling (Naval Postgraduate School, Pacific Grove, USA); Dr. Andrew Liaropoulos (University of Piraeus, Greece); Dan Likarish (Regis University, Denver,, USA); Prof. Peter Likarish (Drew University, Madison, USA); Dr Sam Liles (Center for Education and Research in Information Assurance and Security (CERIAS), Purdue University, West Lafayette, Indiana, USA); Cherie Long (Georgia Gwinnett College. Lawrenceville, GA., USA); Juan Lopez Jr. (Air Force Institute of Technology, USA); Dr. Bin Lu (West Chester University of PA, USA); Volodymyr Lysenko (University of Washington, USA); Fredrick Magaya (Kampala Capital City Authority, Uganda); Dr. Bill Mahoney (University of Nebraska, Omaha, USA); Dr.

hossein malekinezhad (Islamic Azad University, Iran); Dr. John McCarthy (Cranfield University , UK); Dr. Todd McDonald (Air Force Institute of Technology, USA); Dr. Jeffrey McDonald (University of South Alabama, USA); Dr. Robert Mills (Air Force Institute of Technology, USA); Dr. Nighat Mir (Effat University, Saudi Arabia); Dr. Apurva Mohan (Honeywell ACS Labs, USA); Assoc Prof Dr Salwani Mohd Daud (Universiti Teknologi Malaysia, Malaysia); Evangelos Moustakos (Middlesex University, UK); Wilmuth Mueller (Fraunhofer Institute of Optronics, System Technologies and Image Exploitation - IOSB, Germany); Dr. Srinivas Mukkamala (New Mexico Tech, Socorro, USA); Dr. Barry Mullins (Air Force Institute of Technology, USA); Dr Lilian Nassif (Public Ministry of Minas Gerais, Brazil); Muhammad Naveed (University of Engineering and Technology, Peshawar, Pakistan); Professor Abdelnaser Omran (Universiti Sains Malaysia, Malaysia); Prof. Dr. Frank Ortmeier (Otto-von-Guericke Universität, Magdeburg, Germany); Rain Ottis (Cooperative Cyber Defence Centre of Excellence, Estonia); Prof. Evgeny Pashentsev (Lomonosov Moscow State University, Russia); Dr. Gilbert Peterson (Air Force Institute of Technology, USA); Pete Peterson (The George Washington University, USA); Andy Pettigrew (George Washington University, USA); Dr. Jackie Phahlamohlaka (Council for Scientific and Industrial Research, Petoria, South Africa); Engur Pisirici (govermental - independent, Turkey); Dr. Ajeet Poonia (Govt. College Of Engineering & Technology, India); Dr. ajeet poonia (Govt. College of Engineering & Technology, India); Dr Bernardi Pranggono (Glasgow Caledonian University, UK); Prof aunshul rege (temple university, USA); Dr. Ken Revett (British University in Egypt,, Egypt); Lieutenant Colonel Ernest Robinson (U.S. Marine Corps / Air War College, USA); Dr. Neil Rowe (US Naval Postgraduate School, Monterey, USA); Daniel Ryan (National Defence University, Washington DC, USA); Julie Ryan (George Washington University, USA); Prof Julie Ryan (George Washington University, USA); Prof. Lili Saghafi (Canadian International College, Montreal, Canada); Ramanamurthy Saripalli (Pragati Engineering College, India); Sameer Saxena (IAHS Academy, Mahindra Special Services Group , India); Mark Scanlon (University College Dublin, Ireland); Dr Mark Scanlon (University College Dublin, Ireland); Corey Schou (Idaho State University, USA); Dr. Yilun Shang (Singapore University of Technology and Design, Singapore); Dr. Dan Shoemaker (Singapore University of Technology and Design, Singapore, USA); Prof. Ma Shuangge (Yale University, USA); Dr Elena Sitnikova (University of South Australia, Australia); Ass.Prof.Dr. Risby Sohaimi (National Defence University of Malaysia, Malaysia); William Sousan (University Nebraska, Omaha, USA); Dr. William Spring (University of Hertfordshire, UK); Prof. Michael Stiber (University of Washington Bothell, USA); Dr. Kevin Streff (Dakota State University, USA); Dennis Strouble (Air Force Institute of Technology, USA); Dr. arwin sumari (indonesian defense university, Indonesia); Peter Thermos (Columbia Univeristy/Palindrome Technologies, USA); Dr. Bhavani Thuraisingham (University of Texas at Dallas, USA); Mr. Patrick Tobin (University College Dublin,

Ireland); Eric Trias (Air Force Institute of Technology, USA); Dr Chia-Wen Tsai (Department of Information Management, Ming Chuan University, Taiwan); Dr. Doug Twitchell (Illinois State University, USA); Dr. Shambhu Upadhyaya (University at Buffalo, USA); Renier van Heerden (CSIR, Pretoria, South Africa); Brett van Niekerk (University of KwaZulu-Natal, South Africa); Prof. Hendrik (Hein) Venter (University of Pretoria, South Africa); Prof Hendrik Venter (University of Pretoria, South Africa); Stylianos Vidalis (Newport Business School, Newport, UK); Prof. Kumar Vijaya (High Court of Andhra Pradesh, India); Dr. Natarajan Vijayarangan (Tata Consultancy Services Ltd, India); Sune Von Solms (Council for Scientific and Industrial Research, South Africa); Fahad Waseem (University of Northumbria, UK); Prof Murdoch Watney (University of Johannesburg, South Africa); Dr. Kenneth Webb (Edith Cowan University , Australia); Martha Woolson (Metropolitan Washington Airports Authority, USA); Mohamed Reda Yaich (École nationale supérieure des mines , France); Enes Yurtoglu (Turkish Air War College, Turkey); Dr Jannie Zaaiman (University of Venda, South Africa); Dr. Zehai Zhou (University of Houston-Downtown, USA); Tanya Zlateva (Boston University, USA)

Biographies

Conference Chair

Dr Jannie Zaaiman is the Deputy Vice Chancellor: Operations of the University of Venda in the Limpopo Province, South Africa. Before entering the academic world, he was inter alia Group Company Secretary of Sasol, Managing Executive: Outsourcing and Divestitures at Telkom and Group Manager at the Development Bank of Southern Africa. His area of research is cyber security awareness especially in rural areas of South Africa.

Programme Chair

Dr Louise Leenen is a Senior Researcher in the Cyber Defence research Group at PhD Computer Science (in Constraint Programming) from the University of Wollongong in Australia. Her research focus is on artificial intelligence applications in the defence environment, cyber defence and ontology development. She is the Chair of the IFIP Working Group 9.10 on ICT in War and Peace.

Mini Track Chairs

Dr. John S. Hurley is presently Professor of Information Strategies, at the National Defense University (NDU) iCollege. He worked as the Senior Manager, Distributed Computing in the Networked Systems Division, The Boeing Company, Bellevue, WA. Dr. Hurley was Director of Scalable and Embedded Applications Center and the Co-Director, Army Center of Excellence in Electronic Sensors and Combat at Clark Atlanta University, in Atlanta, GA. Hurley's research interests are focused in the area of Threat management in Distributed Computing environments.

Dr John McCarthy has worked with ServiceTec since 2003 and currently holds the position of Vice President of Cybersecurity for the Airport CyberSec division. His responsibilities include the development and management of a complete set of cybersecurity services created specifically for the airport industry, as well as the deployment of those services at some of the world's busiest airports. John's list of posts include seats on a number of prominent US and UK committees that offer

advice and policy guidance to the UK and US governments on cybersecurity matters.

Biographies of Presenting Authors

Gaseb Alotibi, is working with Saudi police Agency. Gaseb has a Master's degree from Glamorgan University in 2010 in the UK, and is now a PhD researcher in The Centre for Security, Communications and Network Research (CSCAN) at Plymouth University in cybersecurity area".

Tina AlSadhan is a doctoral student in the School of Information Studies at Syracuse University. Her research interests include security automation, Information Security Continuous Monitoring, and Risk Management. She is employed with the United States Department of Defense focused on Cyber Security.

Thomas Armistead is a Midshipman at the United States Naval Academy where he currently studies Information Technology. He will graduate in May of 2016 and commission as an officer into the United States Navy. Midshipmen Armistead hopes to select Naval Aviation as his service selection.

Lieutenant Colonel M.J. Aschmann is currently a senior officer class 1 within the SANDF , and is currently working within the Directorate Information Warfare. His current focus is the capability development within the Network Warfare environment. of which he has obtained numerous experience in this field and has been both internally and externally deployed within the African battle space.

Mercy Bere is currently in Windhoek Namibia and works and study's at the Polytechnic of Namibia. Mercy is a PhD candidate in Computer Science and has obtained aMaster of Information Technology in 2013.

Johnny Botha is a Software developer & researcher at the Council for Scientific and Industrial Research(CSIR). He is studying his masters (MTech) degree in Information Technology, at University of South Africa(UNISA). Topic: "Personal Identifiable Information Disclosure since the Protection of Personal Information Act Adoption in South Africa". He has obtained NDip and BTech degree in Computer Systems Engineering at the Tswane University of Technology(TUT).

Pieter Botha received his B.Sc. (Hons) from the University of Pretoria in 1999. He worked on various business integration projects and was exposed to many enter-

prise systems with a focus on Microsoft platforms. He joined the CSIR in 2012 where he now specialises in Web and mobile technologies.

Christopher Brill is a Lieutenant in the Alaska Army National Guard. He holds a B.A. in History from Rutgers University and is currently completing his M.A. in Military Studies and Strategic Leadership from American Military University. He has served as a Signals Intelligence Analyst during OIF and Target Area Reporter at the National Security Agency.

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

Peter Chan is a researcher at the Council for Scientific and Industrial Research (CSIR).His research interests are in formal methods of computing, cybersecutiy awareness and network security.

Dr. Jim Chen is Professor of Systems Management / Cybersecurity in the iCollege at the U.S. National Defense University (NDU). His expertise is in cybersecurity technology and cybersecurity strategy. He is a recognized cybersecurity expert.

Ronald Chikati is a Computing lecturer at Botswana Accountancy College. He holds a BSc (Hons) (Computer Science), an MSc (Computer Science) and MSc (Strategic Management). He is an enthusiastic researcher in ICT4D. Ronald is currently pursuing a PhD (Computer Science) programme with UNISA focusing on developing new Swarm Intelligence techniques based on bacterial communication.

Prittish Dala received his Masters in Information Technology from the University of Pretoria, where he has now enrolled for his doctorate. Prittish has extensive industry experience in the audit and information security domains supported by internationally recognised certifications such as CISA, CISM, CRISC, CISSP, CEH, CHFI, COBIT 5, and ISO27001.

Dr. Tiny du Toit obtained his Ph.D. in Computer Science at the North-West University in 2006. Currently, he is a senior lecturer in Computer Science and part of the Telkom CoE programat the university's Potchefstroomcampus where he lectures and performs research in the field of Artificial Intelligence.

Dr. Royal Elmore recently completed his nuclear engineering PhD work at Texas A&M University. He received his M.Sc. in Nuclear Engineering and M.Sc. in Mechanical Engineering from the University of Wisconsin-Madison in 2011. Dr. Elmore has received graduate research support from several sources, including the National Science Foundation and Nuclear Nonproliferation International Safeguards fellowships.

Anne Gerdes is an Associate Professor at University of Southern Denmark, Department of Design and Communication. She lectures on ICT-ethics and value based design. She is a member of the steering committee of the ETHICOMP conference series and leader of the Danish ICT-ethics Network. Her research interests include ICT-ethics, AI, robot warfare and privacy.

Tim Grant is retired but an active researcher (Professor emeritus, Netherlands Defence Academy). Tim has a BSc in Aeronautical Engineering (Bristol University), a Masters-level Defence Fellowship (Brunel University), and a PhD in Artificial Intelligence (Maastricht University). Tim's research focuses on the operations-technology interplay in network-enabled Command & Control systems and in offensive cyber operations.

Virginia A. Greiman Professor of Cyber law and Cyber Security 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 Eastern Europe, Asia and Africa and has held several high level appointments with the U.S. Department of Justice.

Alan Herbert comes from East London. Alan has studied at Rhodes University. He has completed Master of Science at Rhodes University in 2014 in Computer Science. Major field of study: Networks, Security, Network Simulation and Electronics. Currently studying for PhD in Computer Science and Electronics at Rhodes University and supervised by Prof. Barry Irwin.

Steven Hersee is a PhD student at the Information Security Group at Royal Holloway, University of London. He has previously served in the Royal Air Force and his primary interests are in the geopolitics of cyber security and the different and

Barry Irwin is an Associate Professor in the Department of Computer Science at Rhodes University, South Africa. He established and has led the Security and Networks Research Group (SNRG) since its founding in 2003. He holds a PhD and a CISSP. His current areas of research include network traffic analysis, data visualization and webserver malware.

Suhaila Ismail is a PhD student in Information Assurance Group at the UniSA. She received her M.Sc. in Information Security and Computer Forensics from UEL, UK. Currently she is involved in research of Critical Infrastructures and SCADA Systems Security. She has published papers in Computer Forensics, Privacy, Education and SCADA Systems Security.

Victor Jaquire has been in ICT and Information security for 18 years within government and the private sector focussing on information security strategy, performance management, business management and development, and operations. His professional certifications include CISSP, CISM and CCISO. He is presently in the process of completing his Masters thesis in Cyber Security.

Roman Jasek is head of department of Informatics and Artificial Intelligence at the Faculty of Applied Informatics in Tomas Bata University in Zlin, Czech Republic. He deals with the security of business information systems and security applications on the mobile platform. The team, working under his direction, is deals with industrial applications using artificial intelligence.

Trishee Jobraj is currently an Information Security Liaison at Transnet SOC and has over 9 years' experience in the IT Support, Internal & External Audit and Information Security. She also manages the Membership and Marketing Portfolio for ISACA SA. Her qualifications include a BSC degree in Computer Science, ITIL Foundation, CISA and CRISC.

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. His research interest are in cloud forensics and internet security

Mohamed Khan is a senior analyst at Transnet. He is passionate about using statistics to help business deliver value through analysis of big data. Author of one book and a frequent speaker, his combination of actuarial science and information security give him a unique ability to find novel ways to analyse data.

Sam Lefophane is currently a Smart Card development engineer in the Information Security Unit of Modelling and Digital Science department at the CSIR. Sam's research focus is in RFID signal processing, hardware security, standardisation and intelligent systems.

Cynthia Mlambo is currently pursuing the Masters in Electrical Engineering at the University of Johannesburg. She holds an Honours Degree in Computer Engineering from the University of KwaZulu-Natal. Her areas of interest include image processing, pattern recognition and Smart ID Cards in biometrics.

Settana Mohammed Abdullah received second class B.Sc (honor) on computer science from faculty of Mathematical Sciences - University of Khartoum, Sudan, currently studying master of computer science in university of Khartoum,master thesis is network intrusion detection system, she was published a paper on ICCEEE (2013) on password strength measurements: password entropy and password quality .

Feroze Mohideen is a full-time employee of KPMG South Africa in the department of IT Advisory and a part time MSc Computer Science student at the University of Johannesburg. Dr Ian Ellefsen (PhD Computer Science) is a lecturer at the University of Johannesburg and is supervisor to Mr Feroze Mohideen.

Nkosinathi Mpofu is a lecturer in Computing at BAC, and has been active in Digital divide and Databases researches. With cloud computing having gained momentum, Nkosinathi enrolled for a PhD-Computer Science and shifted his research focus slightly to Identity management. His current research is motivated by the growth of the domain of Anything-as-a-Service (XaaS).

Rennie Naidoo lectures at the University of Pretoria. Prior to embarking on an academic career, he spent 15 years working in a number of commercial and consulting positions. He teaches IT project management, ERP and special topics in research methods. He researches key issues in IS use and IS decision making.

Andrew Nicholson is a PhD candidate at De Montfort University. His research looks at attack attribution, particularly with the use of deceptive systems. Andrew is also interested in industrial control system and security visualisation research and has published papers in these fields.

Stacey Omeleze obtained her B.sc Hon Computer Sci., from the Computer Science Department, University of Pretoria. She is currently working on a research degree towards a Masters in Computer Science, at the University of Pretoria in the field of Digital Forensics application to proactive crime reduction in South Africa. She is an active member of Information and Computer Security Architecture (ICSA) research group, IEEE South Africa and Institute of Information Technology Professionals of South Africa (IIPTSA). Her research interests are Digital forensics, Cloud

Computing, Mobile Forensics, Systems Security, Code Penetration and Testing and Digital Forensic Algorithmic.

Heloise Pieterse is currently employed as a researcher within the Command, Control and Information Warfare research group at the Council of Scientific and Industrial Research. She completed her MSc Computer Science degree in 2014 and her interests include information security and mobile devices.

Barend Pretorius Joined Transnet in April 2014 as a Senior Information Security Analyst at Transnet. He has more than eight years' experience at Ernst & Young in Information Technology, Security, Governance, Risk and Compliance where he was an IT audit manager. He holds a Bachelors of Science Honors in Statistics.

Mahlatse Sophia Ratsoma , studying towards a BSc Honours Degree in Computer Sciece at University of Pretoria and member of the Information and Computer Security Architecture (ICSA) research group. Obtained a BSc Degree Computer Science at University of Limpopo majoring in Computer Science and Statistics.

Neil Rowe is Professor of Computer Science at the U.S. Naval Postgraduate School where he has been since 1983. His main research interests are the modeling of deception, information security, surveillance systems, image processing, and data mining.

Vítor J. Sá holds a PhD in Technology and Information Systems from University of Minho, where he lectured for several years. He lived for four years in Germany as a guest researcher at the Fraunhofer IGD, in Darmstadt. Currently, he is an Assistant Professor at the Catholic University of Portugal, in Braga.

Meshack Shabalala is a Smart Cards development Engineer at the Council for Scientific and Industrial Research in Pretoria. He obtained his BSc.Eng in Electrical Engineering in 2010, and currently an MSc.Eng student in Pattern Recognition at the University of the Witwatersrand. His interests cover Biometric Identity Verification, Token Development and, more generally, Security related issues.

Zaheer Shaik is currently studying towards his MSc in computer science. He is currently a student research at the Council for Scientific and Industrial Research (CSIR), South Africa and studying at the University of KwaZulu-Natal (UKZN). His areas of interest include machine learning and its application within the cyber security domain.

Nobubele Angel Shozi is an employee at the Council for Scientific and Industrial Research (CSIR) in the Cyber Defence group. She completed her Mtech at the Nelson Mandela Metropolitan University in 2012. Her research interests are in Mobile health, Socio-technical systems, Big Data and Cybersecurity.

Paulo Simões is Assistant Professor at the Department of Informatics Engineering of the University of Coimbra, Portugal, from where he obtained his doctoral degree in 2002. He regularly collaborates with Instituto Pedro Nunes as senior consultant, leading technology transfer projects for industry partners such as telecommunications operators and energy utilities. His research interests include Future Internet, Network and Infrastructure Management, Security, Critical Infrastructure Protection and Virtualization of Networking and Computing Resources. He has over 150 publications in refereed journals and conferences and he is member of the IEEE Communications Society.

Dr. A. Skaržauskienė was the couch in the Self-managing team's project in European Parliament together with DEMOS Group Belgium (www.demosgroup.com). In her work dr. A. Skaržauskienė applies both knowledge of management and modern leadership-correlated disciplines such as Business dynamics, Systems thinking, Chaos and Complexity theories. Her current position is Director of Business and Media School together with Middlesex University, UK.

Ignus Swart joined the CSIR in 2010 and holds a Masters degree in computer science. A frequent speaker on radio and conferences and a active participant in a number of cyber security competitions, consistently placing in the top three nationally

Philip Trenwith is an MSc Computer Science student at the University of Pretoria studying Digital Forensics in the Cloud. The goal of his research is to find techniques to link digital space and physical space and ultimately produce a model for tracing data through the cloud using Data Provenance and Digital Forensic Readiness.

Shambhu Upadhyaya is a professor of computer science and engineering at the State University of New York at Buffalo where he also directs the Center of Excellence in Information Systems Assurance Research and Education (CEISARE), designated by the National Security Agency. His research interests are information assurance, computer security and fault tolerant computing.

Dr. Renier van Heerden is a senior researcher at Council for Scientific and Industrial Research (CSIR) in Pretoria, South Africa in the field of Information Warfare.

Prior to joining the CSIR he worked as a software engineer in advanced optics applications for South African based Denel Optronics and as a Lecturer at the University of Pretoria. Renier obtained a degree in Electronic Engineering, a Masters in Computer Engineering at the University of Pretoria and PhD at Rhodes University

Brett van Niekerk graduated with his PhD in 2012 from the University of KwaZulu-Natal, and has completed two years of postdoctoral research into information operations, information warfare, and critical infrastructure protection. He is currently a Senior Security Analyst at Transnet. He also holds a BSc and a MSc in electronic engineering.

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. His research interests are in computer and Internet security, which include network security, Intrusion detection, information privacy, and digital forensics and standardization.

Prof SH (Basie) von Solms is a Research Professor in the Academy for Computer Science and Software Engineering at the University of Johannesburg in Johannesburg, South Africa. He is also the Director of the newly established Centre for Cyber Security, jointly created by the UN's International Telecommunications Union (ITU) and the University of Johannesburg.

Dr. Suné von Solms obtained her PhD in Computer Engineering in 2012 from the North West University. She is a senior researcher at the Council for Scientific and Industrial Research in Pretoria, South Africa and an Extraordinary Senior Lecturer at the North West University in Potchefstroom, South Africa. Her interests lie in applied research in the field of Cyber Security, Communication and Education.

Behavioral-Based Feature Abstraction From Network Traffic

Gaseb Alotibi[1], Fudong Li[1], Nathan Clarke[1,2] and Steven Furnell[1,2]
[1]Centre for Security, Communications and Network Research (CSCAN), Plymouth University, Plymouth, UK
[2]Security Research Institute, Edith Cowan University, Western Australia

Abstract: Information security breaches cost organizations collectively billions in lost intellectual property and business. To mitigate this threat, a whole host of countermeasures have been devised to detect, monitor and respond to network-based attacks and compromise. These include: incident management teams operating 24/7, network forensic tools, Security Incident and Event Management (SIEM) systems, insider misuse detection, intrusion detection and intrusion prevention systems. A fundamental limitation of all these approaches however is the reliance upon analyzing network traffic based upon the computer node, which itself is derived from a dynamically allocated IP address, rather than being able to identify network traffic based upon the user. Identifying the user rather than IP provides a more complete and accurate set of data to be utilized within existing countermeasures. For example, in an organization, a user might have access to a desktop, laptop, tablet and mobile phone that all utilize and access the corporate network and who's IPs are different and vary against time. Currently understanding and identifying that user in such an environment is extremely challenging and time consuming. Whilst research has attempted to achieve this level of abstraction to the user, results are poor due to the volume and variability of data at the network-level. This paper describes a research study into the identification and extraction of high-level behavioural features from low-level network traffic. Having identified application-level services and derived sets of typical use cases, this research presents a set of experiments to demonstrate how user behaviours within internet-enabled applications can be determined through analysis of low-level network traffic metadata. The enhanced features that are derived not only inform us of which services a person is using but also how they use it. For example, from our social networking experiment it has been shown that it is possible to identify whether a person is reading, posting an image or using instant messenger. This feature-rich user-focused approach to metadata analysis of network traffic will provide the underlying information required for profiling and modelling user activity.

Keywords: behavioural profiling, authentication, identification, network traffic

A new Frontier in war: Cyber Warfare in Estonia

Thomas Armistead[1] and Leigh Armistead[2]
[1]United States Naval Academy, Annapolis, USA
[2]Edith Cowan University, Perth, Australia

Abstract: The last three decades have seen the explosion of a new technology unparalleled by any other in history with the rise of cyber capabilities. The mainstreaming of the computer and the advent of the Internet has drastically changed virtually all facets of today's society, including warfare. The undeniable advantages of utilising this new technology has driven a number of countries, corporations, groups and individuals, to adopt and embrace these modern innovations, but has also opened the door to new types of attacks. One of the most dramatic recent examples of this rapid development has occurred in Estonia, which is one of Europe's most wired nations" (Ashmore 2009). In 2007, Estonia fell victim to one of the world's first major cyber-attacks, where their government was forced to address several unforeseen shortcomings in both their technological and legal systems. From this attack, Estonia not only survived but eventually became a world leader in cyber defense. As a result, these attacks have become a case study to shape the progression of cyber propagation, as well as to educate the greater international community about the importance of cyber warfare and its potential ramifications.

Keywords: cyber warfare, Estonia, Russia, Tallinn

Perception Shaping and Cyber Macht: Russia and Ukraine

Edwin 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 have conducted a case study that will focus on Perception Shaping with the thesis that truth and the internet have long been uncomfortable partners. Public opinion can often be easily shaped by tailoring information for specific groups and by not presenting or suppressing information not supportive of the desired public impression. The authors will use the conflict between the Ukraine and Russia in Eastern Europe in a case study to analyze how each side is attempting to use the media to their advantage in this conflict. While a war has not been officially declared (yet), sovereign territory has been invaded, personnel have been killed and is these researchers opinion that information operations (IO) is playing a huge role how this conflict is being conducted. This paper will analyze

the efforts of various IO initiatives by both sides and attempt to determine the key factors of success.

Keywords: cyber, power, theory, strategy, academic, comprehensive

Cyber Armies: The Unseen Military in the Grid

Michael Aschmann [1], Joey Jansen van Vuuren[2, 3] and Louise Leenen[2]
[1]Directorate Information Warfare, South African National Defence Force, Pretoria, South Africa
[2]Defence Peace Safety and Security: CSIR, Pretoria, South Africa
[3]University of Venda, South Africa

Abstract: Information in the Global Digital Industrial Economic Age is viewed as a strategic resource. This article focus on the establishment of cyber armies within the World Wide Web, commonly known as the Grid, with the emphases on an unseen military cyber power and/or civilian force within the cyber domain that has the ability to launch cyber-attacks and collect information in order to gain strategic military advantage on a national level. Selected cyber armies are compared to portray the impact of such armies on the citizen. The article also gives a view of a proposed generic structure for cyber in the military to defend and protect the cyber sovereignty and presents a proposed view on how a cyber army can be integrated within a military force. In addition, the article highlights the strategic benefits and strategic advantage to the military and will give a military perspective on the implementation of a cyber army as a proposed model.

Keywords: cyber army, cyber warfare, cyber offensive and defensive capability, cyber defence

Mobile Forensics for PPDR Communications: How and why

Konstantia Barbatsalou[1], Bruno Sousa[2], Edmundo Monteiro1and Paulo Simoes[1]
[1]CISUC-DEI, University of Coimbra, Coimbra, Portugal
[2]OneSource, Portugal

Abstract: Public Protection and Disaster Relief (PPDR) agencies increasingly depend on specialized communications systems for supporting critical activities such as law enforcement operations, fire fighting, response to traffic accidents and medical emergencies, crowd control in large events, anti-terrorism, disaster relief and public protection in general. Addressing this dependency, PPDR communications systems are rapidly evolving. While many countries still rely on old legacy technologies like TETRA and TETRAPOL (which are in practice limited to voice ser-

vices, due to the very low data rates they can carry), we currently witness a trend towards replacing them with more advanced technologies, such as 4G/LTE and beyond, able to integrate voice, video and data communications (thus providing more advanced situational awareness to PPDR teams) and to support more flexible communications management (for instance making it easier to dynamically create, on-demand, groups for inter-agency and cross border communications). However, this brave new world of modern PPDR communications also brings its own risks, related to various types of malicious activity against the participating devices and the networks themselves. In order to handle such risks, new generation PPDR systems require adequate security solutions, addressing the communications infrastructure, mobile terminals, voice and data applications and the PPDR command center. Mobile forensics may play an important role among those security solutions, assisting on the detection and profiling of malicious attacks against PPDR communications systems and on the gathering of legal evidence. However, current PPDR systems typically lack support for mobile forensics or, at most, provide very rudimentary tools. Thus, this paper discusses how and why mobile forensics should be integrated into new-generation PPDR communications.

Keywords: PPDR communications, mobile forensics

Evaluation of Online Resources on the Implementation of the Protection of Personal Information Act in South Africa

Johnny Botha[1, 3], M.M. Eloff[2, 3] and Ignus Swart[1]
[1]CSIR, Pretoria, South Africa
[2]Institute for Corporate Citizenship, University of South Africa (UNISA), Pretoria, South Africa
[3]University of South Africa (UNISA), Pretoria, South Africa

Abstract: The recent adoption of the privacy law, Protection of Personal Information (PoPI) Act in South Africa, mandates notable changes from both government departments and the public sector when dealing with personal identifiable information (PII). Recent research has shown that the level of change still required to comply with the new Act is significant. Surveys indicated that approximately only forty percent of organisations in South Africa have started with the compliance process. Private empirical research has found widespread leakage of PII within South African cyber infrastructures. The leaked information affected well over two million South African citizens in some or other manner and with penalties instituted by the PoPI of up to R10 million, it is crucial for organisations to clean up these incidents of non-compliance. Even without the monetary incentive, leaked PII holds a significant threat, not only for individuals but also for companies and governmental organisations alike. Several documented instances exist

where targeted phishing attacks, that has a 70% success rate once PII is included, has been successfully used against organisations. While technical controls may limit the leakage of PII, significant security vulnerabilities exist that allows for the circumvention of these controls. Cyber security awareness is still the primary defence against these technical control failures, but the notable challenge remains in educating users and responsible personnel. As with any cyber activity, there is a human factor that requires a significantly diverse skill set to understand the infrastructure that comprises an organisation. With cyber security education a continuous developing field, there is a dire need for additional research to supplement this knowledge base. This paper examines online resources available for individuals, organisations and governmental departments to comply with the PoPI Act. The approach used will be to examine content made available through popular social media platforms such as YouTube (YouTube, N.D.), Facebook (Facebook, N.D.), Twitter (Twitter, N.D.) and search engines. These data sources were chosen since it may be the most likely common route individuals will take to gain fundamental understanding of the requirements the PoPI Act places on them. Identified resources will be evaluated for the audience they serve (e.g. business owners, privacy officers, managers and employees), technical content (e.g. informative, guidelines or step by step instructions) and finally the cost involved to access or download resources (e.g. free or commercial).

Keywords: cyber security awareness, education, online resources, PII disclosure, PoPI

Securing Military Information Systems on Public Infrastructure

Pieter Botha, Shazia Vawda, Priaash Ramadeen and Alex Terlunen
Council for Scientific and Industrial Research (CSIR), Pretoria, South Africa

Abstract: Military information systems require high levels of security to protect sensitive information within these systems. Encrypted private networks are a common method of securing such systems. However these networks are not always available or practical to set up in time for scenarios which require real time information. This may force communications to utilise public infrastructure. Securing communications for military mobile and Web based systems over public networks poses a greater challenge compared to private encrypted networks. Several security mechanisms from commercial enterprise and social networking systems were adopted and customised in order to secure Cmore, a Web based real time distributed command and control system developed by the Council for Scientific and Industrial Research (CSIR). This paper highlights the security architecture of Cmore and discusses some of the successes and challenges encountered during the design and development of the Cmore architecture. Cmore has

been successfully utilised and tested in several field experiments and operations. The resulting security architecture can be applied to other Web and mobile systems.

Keywords: internet, mobile, information security

How to Tame Your Android Malware

Ivan Burke and Heloise Pieterse
Cyber Defence Research Group, DPSS, CSIR, Pretoria, South Africa

Abstract: The Android mobile market has expanded greatly in recent years, but with its increased market share Android became a popular target for malware developers. The latest Anti-Virus reports suggest that Android account for the majority of malware detected on mobile devices. This is largely due to the open nature of Android development and the level of system utilities Android software developers are given access to. This paper reviews the currently available open source solutions available, for analysing mobile malware. In this paper the authors, provide an overview of the anatomy of an Android applications. Several malware analysis tools and reverse engineering tools have been developed to analyse and deconstruct APK files. The paper presents a method by which common open source tools can be used to dissect the APK file to uncover its intent. To conclude the authors identify the current shortcomings, with regards to currently available open source software, when it comes to the classification of malicious Android applications.

Keywords: android, malware, reverse engineering, analysis, open source

Enrollment Time as a Requirement for Biometric Hand Recognition Systems

João Carvalho[1,4], Vítor Sá[1,3], Sérgio Tenreiro de Magalhães[1,3] and Henrique Santos[2,3]
[1]Faculty of Social Sciences, Catholic University of Portugal, Braga, Portugal
[2]Department of Information Systems, University of Minho, Guimarães, Portugal
[3]ALGORITMI Research Center, University of Minho, Braga/Guimarães, Portugal
[4]BSB, Braga, Portugal

Abstract: Biometric systems are increasingly being used as a means for authentication to provide system security in modern technologies. The performance of a biometric system depends on the accuracy, the processing speed, the template size, and the time necessary for enrollment. While much research has focused on the first three factors, enrollment time has not received as much attention. In

this work, we present the findings of our research focused upon studying user's behavior when enrolling in a biometric system. Specifically, we collected information about the user's availability for enrollment in respect to the hand recognition systems (e.g., hand geometry, palm geometry or any other requiring positioning the hand on an optical scanner). A sample of 19 participants, chosen randomly apart their age, gender, profession and nationality, were used as test subjects in an experiment to study the patience of users enrolling in a biometric hand recognition system.

Keywords: biometric systems requirements, security systems, hand geometry, biometric enrolment

An Ontological Knowledge Base for Cyber Network Attack Planning

Peter Chan[2], Jacques Theron[1], Renier van Heerden[2,3] and Louise Leenen[2]
[1]South African National Defence Force (SANDF), South Africa
[2]DPSS, CSIR, South Africa
[3]Dept of Computer Science, Rhodes University, South Africa

Abstract: In modern warfare it is no longer sufficient to only focus on physical attacks and counter-measures; the threat against cyber networks is becoming increasingly significant. Modern military forces have to provide counter measures against these growing threats in the cyberspace. These forces thus find themselves in the position where they need the capability to perform cyber operations. This paper presents a Network Attack Planning ontology which is aimed at providing support for military cyber operations. The cyber network operation domain is growing at a rapid rate and involves an ever increasing volume of associated information. Semantic technologies can contribute towards the intelligent processing of information in this complex problem area. An ontology enables the representation of semantic information and automated reasoning that can support the complexity of planning cyber operations. It also contributes towards the sharing of information and the creation and maintenance of a common vocabulary. The inferences that can be made with the automated reasoning capabilities of ontologies provide a unique insight into the relationships between network targets and attacks that could be launched against them.

Keywords: ontology, network attack planning, command and control, cyber warfare

Detecting Deception in Cyber Conflict: A Strategic Approach

Jim Chen and Gilliam Duvall
DoD National Defense University, Fort McNair, Washington, USA

Abstract: Deception is a strategy that has been widely used in cyber conflict. How to detect deception in a timely manner is always a challenge, especially for a cyber commander who is at the point of making decisions with respect to the actual target to go after, the exact location of the target, the starting and ending time of a cyber operation, the type of cyber operation, the way of launching the cyber operation, and the amount of resources and support needed. It is absolutely important for the cyber commander to know for sure that he/she is not deceived by the adversary so he/she will be able to make right decisions. Varied solutions do exist. However, they are either too narrow or too broad. The solutions represented by signature technology are narrow in scope, so that they are not capable of dealing with the deception that they have not handled before. The solutions represented by behavioral analysis are relatively broad, so that they require extra time to re-adjust their focuses, incorporate contextual information, and combine heterogeneous data resources in order to get to what is exactly needed. In addition, the use of contexts in analysis is at random and not in a systematic way in most cases. Even when contexts are included in analysis, their relations with the relevant events are not well explored in all these solutions. To address these issues, this paper proposes a new strategic and systematic solution applying the Operational-Level Cybersecurity Strategy Formation Framework. This new solution employs dynamic contexts analysis, baseline analysis, impact analysis, and benefit-cost analysis. A case study is provided to test the effectiveness of this solution in detecting deception in a timely manner. The benefits and limitations of this solution are discussed. The areas for further research are also suggested.

Keywords: deception, conflict, detection, strategy, contexts, relationship

Examination of the United States Nuclear Industry Approach to Critical Infrastructure Protection: Applicability to Improved Industry-Wide Network Cyber Security

Royal Elmore[1, 2] and Bryan Fearey[2]
[1]Texas A&M University, College Station, USA
[2]Los Alamos National Laboratory, Los Alamos, USA

Abstract: Since its foundation the nuclear field straddled the public and private spheres. The United States Nuclear Regulatory Commission (NRC) was created in 1975 to regulate civilian nuclear power and technology. After the 1979 Three Mile Island accident the nuclear industry recognized safety culture improvement necessities. In 1979 the Institute of Nuclear Power Operations (INPO) was founded to curtail severe reputational risks from underperforming nuclear operators. The combination of mandatory NRC regulations and voluntary industry standards recognized by INPO created a competitive environment for implementing best safety practices. Through INPO the nuclear industry demonstrates it is proactively meeting NRC expectations, but in a business conducive manner. The strong cyber defense orientation of the nuclear industry is a contemporary example of this arrangement. In mid-February 2014 the National Institute of Standards and Technology released its Executive Order 13636 mandated Framework for Improving Critical Infrastructure Cybersecurity. Yet, in 2002 INPO was already taking cyber defense assessment and training measures. In Washington, DC the February 2014 Bipartisan Policy Center cited the nuclear industry forward thinking on cyber security. One of the Bipartisan Policy Center Electric Grid Cybersecurity Initiative co-chairs is Michael Hayden, former Central Intelligence Agency and National Security Agency director. The unique nuclear industry aspects of insurance, regulation, information sharing, and other areas provides policy suggestions for strengthening American critical infrastructure cyber security. The paper breaks down several distinctive technical and programmatic features of the nuclear industry for critical infrastructure cyber security and their associated economic, social, and trust issues.

Keywords: nuclear, nuclear industry, critical infrastructure, cybersecurity, information sharing

Cyber Coercion: Cyber Operations Short of Cyberwar

Daniel Flemming and Neil Rowe
U.S. Naval Postgraduate School, Monterey, California, USA

Abstract: Countries should find ways to exert strong influence without resorting to excessive violence and warfare. Cyber coercion is a new option, the use of computer networks and software to influence other countries with cyber attacks short of full warfare. It could involve demonstrations of capabilities as a sample of what warfare could entail. An example would be when country A is threatening invasion of another country B, and B disables the computer networking on a single ship of A by using emplaced Trojan horses, to demonstrate that A's entire navy could be similarly disabled. Cyber coercion could enable phased aggression to compel adversaries to the bargaining table and avoid unnecessary escalation while expending fewer resources than alternative methods. Cyber coercion could permit flexible tailoring of an operation with varying levels of force, and could include features of attributability and reversibility. This paper surveys the potential for cyber coercion. It considers the possible goals, the possible targets, and the possible methods from a strategic point of view. Additional issues discussed are actors involved, possible ineffectiveness, reversibility, and attribution. Risks discussed are that of the attacker ignoring the coercion, the attacker escalating the conflict, stalemates, and spread of the conflict to civilian targets. Despite these risks, we argue there is a role for cyber coercion in the strategic arsenal of militaries.

Keywords: coercion, cyber, operations, attacks, nonlethal, compellence

ePOOLICE Security Technology - Fighting Organized Crime Whilst Balancing Privacy and National Security

Anne Gerdes
Department of Design and Communication, University of Southern Denmark, Kolding, Denmark

Abstract: This paper deals with the challenge of balancing privacy and national security in connection with environmental scanning systems, such as the ePOOLICE system (www.ePOOLICE.eu), which is currently under development. ePOOLICE aims at developing an environmental scanning system for fighting organized crime by improving law enforcement agencies opportunities for strategic proactive planning in response to emerging organized crime threats. Section 1 presents the overall aims of the ePOOLICE project, as an example of security technology within the field of environmental scanning systems for early warning, followed by a discussion of national security versus citizens' right to privacy (section 2). Here, it is

argued that core issues should not be addressed as a strict dichotomy of realms, formulated in a clash between citizens right to privacy as opposed to national security; rather we have to strike a balance between two dimensions of security at a national and individual level. Hence, security can be defined as nonattendance of danger at a state level, as well as at a societal level with reference to the citizens forming the society. Moreover - as discussed in section 3 - it is generally acknowledged that trust is essential for a flourishing society and that relations of trust are easily maintained and better preserved in moral communities with relatively low crime rates. Yet, at the same time - and especially important to be aware of in the context of security technology - societal trust basically rests on the ability of citizens to rely on that in interacting with others and governmental authorities, their integrity and autonomy will be respected; and to provide for this, privacy is a highly held value, which has to be properly protected. Accordingly, in the specific context of this paper, democratic societies are faced with the challenge of striking a balance between two sides of security; formulated as absence of organized crime threats and preservation of the freedom and integrity of the individual as important presumptions for democracy. Consequently, security technologies, such as the ePOOLICE system, have to find ways to balance data utility and data privacy.

Keywords: informational privacy, national security, crime fighting, trust, environmental scanning

Specifying Functional Requirements for Simulating Professional Offensive Cyber Operations

Tim Grant
R-BAR, Benschop, The Netherlands

Abstract: Several nations have acquired or are acquiring the capability for conducting professional offensive cyber operations to fight wars and to combat crime and terrorism. For the capability to be effective, they need to know how the attack process works, what resources are required, what doctrine should be followed, and how to command, control, and govern such integrated operations. Simulation is a powerful technology for gaining understanding about these issues. While the general principles and techniques for developing and employing simulations are well known, their application to professional offensive cyber operations is new. The purpose of this paper is to present a preliminary requirements specification for a new, agent-based simulator capable of modelling professional offensive cyber operations in a networked environment. Because attack may be the best means for defence, simulation encompasses the adversarial interaction between attacker(s) and defender(s). The requirements cover the applications-

independent simulation infrastructure, touching on time handling, stochastic behaviour, the modelling representation, interfacing, and simulation control, and the cyber operations application. Cyber-specific use cases are grouped by stakeholder and phase of operation.

Keywords: requirements engineering, simulation, wargaming, operations research, agent-based modelling, command & control, OODA, networks, attack process

Public Private Partnerships in Cyberspace: Building a Sustainable Collaboration

Virginia Greiman
Boston University, Boston, USA

Abstract: Much has been written about the legal rights and interests of government, private industry and individual users in the cyberspace. However, relatively little has been written about how codes of conduct, public private partnerships, standards and collaborative efforts can be used to structure advancement in technological knowledge for the benefits of all users and how these efforts can better prioritize the rights and responsibilities of each of the actors in cyberspace. This paper presents a conceptual framework for building sustainable partnerships between government and private industry and looks to models of successful partnerships both nationally and internationally. The paper provides an overview of the various collaborations and conflicts in these partnerships, and the governance and organizational issues involved in protecting American cybersecurity. Based on empirical research and an analysis of national and international cybersecurity partnership initiatives, legislation and policies, this paper explores the issues impacting a cohesive, integrated, unified strategy between the government and the private sector including the issues of governance, incentives, risk sharing and the transnational nature of cyberspace. Recent government frameworks are analyzed including the proposed Cyber Intelligence Sharing and Protection Act (CISPA), the President's Executive Order (EO) 13636, "Improving Critical Infrastructure Cybersecurity," and the National Institute of Standards and Technology Cybersecurity Framework launched in February 2014. 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 viable public private partnerships. The research thus far has resulted in a better understanding of the major issues in cybersecurity and national intelligence and the importance of part-

nerships and information sharing as a critical component of advancing the goals of both domains in advancing world peace and private sector interests.

Keywords: cybersecurity, cybercrime, national intelligence, privacy

DDoS Attack Mitigation Through Control of Inherent Charge Decay of Memory Implementations

Alan Herbert and Barry Irwin
Rhodes University, Grahamstown, South Africa

Abstract: DDoS (Distributed Denial of Service) attacks over recent years have shown to be devastating on the target systems and services made publicly available over the Internet. Furthermore, the backscatter caused by DDoS attacks also affects the available bandwidth and responsiveness of many other hosts within the Internet. The unfortunate reality of these attacks is that the targeted party cannot fight back due to the presence of botnets and malware-driven hosts. These hosts that carry out the attack on a target are usually controlled remotely and the owner of the device is unaware of it; for this reason one cannot attack back directly as this will serve little more than to disable an innocent party. A proposed solution to these DDoS attacks is to identify a potential attacking address and ignore communication from that address for a set period of time through time stamping. Implementations of this logic in firewalling rules usually lead to some form of time lookup and comparison of this value to the last time an address was witnessed, if it had been witnessed. This can be a costly process within software based implementation of such logic. This research leverages the inherent discharge rate of capacitors in memory in order to achieve time stamping with minimal CPU intervention. By charging a capacitor to a level regarded as a logical 1 and then leaving it to discharge, it would eventually reach a logic 0. Using this information, this research controls the discharge timing of the memory cell to 0 in order to achieve a known and configurable timing. Coupling this with the large amount of addressable memory made available by modern day DRAM, and the multiple cycles of logic available for use between packets of ICs (Integrated Circuit), one can charge an assigned logic cell according to its source address when a packet is received. When the packet is received again, a simple read of this logic cell will tell whether a packet has been received within the suspected DDoS time window. If the cell is a logic one, it has been seen within the set discharge window and should be considered as a potential DDoS attack; if it is not, then it is safe to assume that the packet is not part of a flooding attack. The research presented in this paper aims to address an icmp based flood attacks through prototyped hardware over USB. This hardware is used as a smartwire, usually in the form of a non-

intrusive packet relay, to monitor and mitigate attacks from a suspected physical connection.

Keywords: DDoS, cyber-defence, Smartwire, analogue timestamp

Observed Correlations of Unsolicited Network Traffic Over Five Distinct IPv4 Netblocks

Barry Irwin and Thizwilondi Nkhumaleni
Department of Computer Science, Rhodes University, Grahamstown, South Africa

Abstract: Using network telescopes to monitor unused IP address space provides a favorable environment for researchers to study and detect malware, denial of service and scanning activities within global IPv4 address space. This research focuses on comparative and correlation analysis of traffic activity across the network of telescope sensors. Analysis is done using data collected over a 12 month period on five network telescopes each with an aperture size of /24, operated in disjoint IPv4 address space. These were considered as two distinct groupings. Time series' representing time-based traffic activity observed on these sensors was constructed. Using the cross- and auto-correlation methods of time series analysis, moderate correlation of traffic activity was achieved between telescope sensors in each category. Weak to moderate correlation was calculated when comparing category A and category B network telescopes' datasets. Results were significantly improved by considering TCP traffic separately. Moderate to strong correlation coefficients in each category were calculated when using TCP traffic only. UDP traffic analysis showed weaker correlation between sensors, however the uniformity of ICMP traffic showed correlation of traffic activity across all sensors. The results confirmed the visual observation of traffic relativity in telescope sensors within the same category and quantitatively analyzed the correlation of network telescopes' traffic activity.

Keywords: network telescope, internet background radiation

Modelling the Cybersecurity Environment Using Morphological Ontology Design Engineering

Joey Jansen van Vuuren[1,2], Louise Leenen[1], Marthie Grobler[1], Peter Chan[1] and ZC Khan[1]
[1]Defence Peace Safety and Security: CSIR, Pretoria, South Africa
[2]University of Venda, Venda, South Africa

Abstract: Acquiring, representing, and managing knowledge effectively has a considerable impact on constructing accurate and intelligent systems. A challenge faced by domain experts is the manner in which information about the cybersecurity environment can be extracted and represented, seeing that it is messy problem with great uncertainty within the environment. To address this problem, this article presents a new methodology to model the cybersecurity environment: Morphological Ontology Design Engineering (MODE). This methodology is based on the combination of three different research methods, i.e. design science, general morphological analysis, and ontology based representation. General morphological analysis offers a solution for extracting meaningful information from domain experts, while ontology based representation is used to logically and accurately represent such information. On a high level, the design science methodology guides the entire process. When applied to the cybersecurity environment, the results reveal that the aggregation of the mixed methods is beneficial. The new hybrid methodology allows domain experts to solve a messy problem that has quantitative and qualitative information, long term and short term goals, as well as logical and empirical evidence. The main benefit of the general morphological analysis aspect of the methodology is the acquisition of meaningful information, and the main benefits of the ontological aspect of the methodology are the representation, understanding, and analysis of the information. This article demonstrates the new methodology by applying it to the cybersecurity domain, resulting in a cybersecurity ontology which can be used in support of implementing a South African cybersecurity policy.

Keywords: cybersecurity, design science, general morphological analysis, morphological ontology design engineering (mode), ontology, research methodologies

Security Deficiencies in the Architecture and Overview of Android and iOS Mobile Operating Systems

Roman Jasek
Faculty of Applied Informatics, Tomas Bata University in Zlín, Czech Republic

Abstract: Mobile operating systems provide a layer with which users exclusively interact. Despite the simplicity of the Graphical User Interface (GUI), the underlying architecture exhibits a high level of complexity, opening attack vectors for adversaries and necessitating security precautions comparable to desktop stations. Developers are aware of the extensive threat potential that small form-factor devices represent and safeguards are deployed to counter the emergence of malicious mobile software. This article details security architecture and proceeds and provides to an overview of the Android and iOS (IOUS) mobile operating systems from a security standpoint, selected on the basis of their opposing approaches to openness and any third-party customizations that users are allowed to perform. The first part provides a brief overview of both systems´ system architectures, while the second part presents notable security and reverse engineering milestones. The third part provides recommendations on the safer use of mobile devices, which are extensively discussed. We argue that by practicing proper security hygiene, both existing and novel threats can be mitigated at the user level.

Keywords: android, architecture, iOS/IOUS, operating system, security

Snapchat Media Retrieval for Novice Device Users

Zubeida Casmod Khan[1,2], Thulani Mashiane[1,3] and Nobubele Angel Shozi[1]
[1]Council for Scientific and Industrial Research, Pretoria, South Africa
[2]Department of Computer Science, University of Cape Town, South Africa
[3]School of Mathematics, Statistics, and Computer Science, University of KwaZulu-Natal, South Africa

Abstract: With roughly 30 million monthly users Snapchat is becoming an increasingly popular photo messaging application. Snapchat allows users to send time-limited photos and videos to other Snapchat users with the promise of it being deleted forever afterward. The use of Snapchat has become prevalent amongst mobile users, mainly because of the ephemeral nature of the Snapchat media; Snapchat's policy promises that a user's embarrassing media is deleted after a short viewing time. However, the promise that this media is deleted from a device after viewing time is short-lived. There is some evidence that Snapchat media has been retrieved using digital forensic software. Apart from the fact that researchers have successfully used digital forensic tools to extract this media from devices,

there are easier ways to access Snapchat media. This coupled with the fact that there is evidence that some use the application for sexting, makes it extremely dangerous for unaware users. This paper will present an experiment for image retrieval on Snapchat with various devices. The purpose of this study is to raise awareness on the possibility, and the ease of image retrieval from Snapchat. It was found that researchers were able to retrieve pictures from Snapchat, using simple procedures that are easily enough for novice smartphone users to employ: not necessarily hackers or information security specialists, but an average smartphone user. The results indicate that, it is indeed possible for novices to retrieve Snapchat data, and as such this is a cyber security threat. A user's Snapchat media could be easily saved by novice users, and there is, thus, a privacy vulnerability. This indicates that Snapchat does not protect its server using API protection techniques, and that such protection is required. Until such API protection techniques are employed, it is the responsibility of the user to ensure that the application is used carefully.

Keywords: Snapchat, privacy, cyber security, vulnerability, image retrieval

The use of Semantic Technologies in Cyber Defence

Louise Leenen[1] and Thomas Meyer[2]
[1]DPSS, CSIR, South Africa
[2]CAIR, CSIR Meraka, and School of Maths, Stats and CS, University of Kwazulu Natal University, South Africa

Abstract: Governments, military forces and other organisations responsible for cybersecurity deal with vast amounts of data that has to be understood in order to lead to intelligent decision making. Semantic technologies is a knowledge representation paradigm where the meaning of data is encoded separately from the data itself. The use of semantic technologies such as logic-based systems to support decision making is becoming increasingly popular. Due the vast amounts of information pertinent to cybersecurity, automation is required for processing and decision making. However, most automated systems are currently based on syntactic rules. These rules are generally not sophisticated enough to deal with the complexity of decisions required to be made. The incorporation of semantic information allows for increased understanding and sophistication in cyber defence systems. An example of an application area is systems that detect and respond to cyber attacks: semantic information enables increased understanding and sophistication in network attack detection systems. In this paper the authors give an overview of the use of semantic technologies in cyber defence, and identify and discuss emerging trends and the way forward for future research.

Keywords: cyber defence, semantic technologies, decision making, automated systems

Mobile Security Threats: A Survey of how Mobile Device Users are Protecting Themselves From new Forms of Cybercrimes

Kudakwashe Madzima, Moses Moyo, Gilbert Dzawo and Munienge Mbodila
University of Venda, Thohoyandou, South Africa

Abstract: There has been a rapid increase in the use of mobile devices to conduct online business transactions by ordinary people across the globe. Currently, commercial banks and retail stores are all encouraging their customers to do most of the transactions through online channels. The current types of mobile devices provide such easy access and convenience for consumers. However, there are risks associated with these new cyberspace tools. The ordinary customers who unwittingly utilize this cyberspace are prone to cyber-attacks conducted by the ever alert and ruthless cyber criminals. The 2013 Norton Report on cybercrime puts South Africa on number 3 (at 73%) behind China (at 77%) and Russia (at 85%) in terms of the number of cybercrime victims. The study was conducted in 24 countries involving about 13,022 online adults aged between 18 and 64. These figures indicate that cybercrime is a real problem in South Africa. Cyber criminals always have mechanisms of getting easy access to unprotected data that these ordinary people transmit or store on their mobile devices. The criminals use the data for unorthodox activities such unauthorized bank debits. SD cards can either be removed from these devices or accessed through Bluetooth without the users' knowledge and the data can be used for criminal activities. In these difficult financial times, mobile device users easily fall victims to cyber criminals through many ways such as phishing and spoofing. The unsuspecting mobile device users oblige by divulging their personal and banking details to cyber criminals. Cyber criminals are difficult to track and their network is so complicated to untangle and under these circumstances business organizations cannot guarantee their customers with complete security. Therefore, ordinary mobile device users frequently fall prey to the cyber criminals and lose a lot of data, information and money. Some users have, however, become aware of the dangers of the cyberspace in which they use their mobile devices and seem to be taking precautionary measures to protect themselves against such criminal activities. This paper reports on a case study which was carried out in Thohoyandou area with ordinary users of mobile devices. The paper examines the prevalence of cybercrimes in Thohoyandou and the mechanism that users put in place to counter such crimes. Lastly the paper proposes some strategies that users could use to protect themselves against these malicious activities.

Keywords: cybercrime, cyber criminals, mobile device, malicious activities, phishing, spoofing

The ARM Based Network Sniffer and Bot Inside the Wide Computer Network

David Malanik
Faculty of Applied Informatics, Tomas Bata University in Zlín, Zlín,Czech Republic

Abstract: The paper deals with techniques that allow stealing and manipulating data on the wide computer network. The manipulating device is represented by the ARM minicomputer with Ethernet port. This device includes functions for capturing live data on the network, spoofing DNS records and redirecting the secure https connection to the unsecure http. It is possible to control the device remotely and it is suitable for performing many types of attacks. The testing environment is represented by the Windows 7 user workstation and the ARM device as the attacker. The report of attack might show that the big security issue is coming from the wide network with one subnet only.

Keywords: security, LAN, ARM, sniffer, malware

Information Sharing and Trust Between Sharing Parties: Sharing Sensitive Information With Regards to Critical Information Infrastructure Protection

Feroze Mohideen and Ian Ellefsen
University of Johannesburg, Auckland Park, South Africa

Abstract: Sharing sensitive, mission critical information between organisations and individuals in a secure and anonymous way is very difficult and very few effective methods and techniques exist which accomplish this task. The field of critical information infrastructure (CII) and the protection thereof is very young and requires further study and development. Cyber-attacks have been on the rise and the need for sensitive, mission critical information to be shared is of vital importance in order to protect a nation's CII. There do however exist many problems and barriers to the sharing of this sensitive, mission critical information and the sharing and privacy of this information thereof. Sensitive information such as that of viruses/attack patterns and virus signatures should be shared among the cyber community in order to increase the knowledge of the wider audience and capture the attention of companies who could be victims to similar attacks thereby helping the owners of CII to protect their infrastructure better. A solution to this problem would consist of a trusted community where a trusted, sharing centre would be established where information could be sent, analysed and distributed. A mechanism such as a software program would be put in place at both the sender and receiver's organisations and would allow these participants to send

and receive this sensitive, mission critical information. This paper aims to discuss the current landscape of cyber-security information sharing, barriers to this information sharing, the current technical methods that exists in order to share sensitive information between private organizations or individuals, to create a new model and software tool for sharing sensitive information between private and public organizations in the field of CII protection, and to further the field of critical information infrastructure protection.

Keywords: sensitive, mission-critical; critical information infrastructure; cyber-attacks; cyber-community

Strategy Matrix for Containing Cyber-Attacks: A Generic Approach

Nkosinathi Mpofu and Ronald Chikati
Botswana Accountancy College, Botswana

Abstract: Internet services are fast expanding, and continue to grow in response to customer needs and advances in technological development. The internet is widely regarded as a knowledge centre and its influence in service provision, and the manner in which transactions are carried out is beyond doubt. As more and more services are interconnected from logistics, power distribution, communication, to financial services, and education amongst others, vulnerability levels also rises (conservatively) at the same rate, since the internet can be exploited for both good and bad purposes. An increased activity in cyber-space has led to a new breed of attacks commonly referred to as *cyber-attacks*. Cyber-attacks cost organisation in a variety of ways including reputation and brand damage, lost productivity, lost revenue, forensic costs, technical support and compliance and regulatory costs. Attackers attack for a variety of reasons and their victims are variegated. This paper aims at highlighting the different kinds of cyber-attacks, the stages of the attack process and the mitigatory steps to curb cyber-attacks. The knowledge of the different classes of attacks and the stages of attack will help in the formulation of a matrix of strategies which can be applied pro-actively or reactively. The strategies, though not technical will go a long way in complementing other efforts in curtailing the impact of cyber-attacks.

Keywords: internet, cyber victim, cyber-attack, strategy matrix, security, vulnerability

Analysing Urgency and Trust Cues Exploited in Phishing Scam Designs

Rennie Naidoo
Department of Informatics, School of IT, University of Pretoria, RSA

Abstract: Fraudsters are constantly adapting their phishing scam designs by increasing the sophistication of urgency and trust cues used to deceive users. Drawing from the social engineering and social psychology literature, this paper uses deductive thematic analysis to examine how phishing scam designs employ urgency and trust cues. The complete anatomy of a sample of 51 distinctive email scams were analysed including the: *from, to, date, subject, content, links and attachment components,* using a major South African bank's archived records of phishing attacks from 2011-2013. The analysis suggests that urgency cues were almost always present to prime cognitive biases and lure users into compliance, while surprisingly important trust cues were less present. The study proposes that users can minimise their risk of being lured into compliance by assessing weaknesses in phishing designs attempting to mimic important trust cues. Technology based email text filtering countermeasures may be more effective if they apply the proposed critical trust and urgency attribute filtering detection approach.

Keywords: banking; filtering; phishing scams; psychology of compliance; social engineering; trust cues; urgency cues

Rolling the Dice – Deceptive Authentication for Attack Attribution

Andrew Nicholson, Helge Janicke, Tim Watson and Richard Smith
De Montfort University, Leicester, UK

Abstract: Technical attack attribution techniques aim to identify the details of the origin of a cyber attack, answering questions such as "who, what, when, where and why". This includes the actors involved, equipment and tools used, geographic data, motives and much more One frequently overlooked technique in the field of attack attribution is deception. In particular, the use of honeypots. Attribution techniques, such as traceback, are useful for detecting entry-points and defusing attacks at the network perimeter. However, whilst these techniques are effective, they face deployment issues such as scalability, cost and lack of incentives. Honeypots, on the other hand, have been used successfully in identifying the tools, techniques, motives and operational capability of adversaries, while being cheap to deploy and maintain. Deploying honeypots as attribution tools has its challenges, one of which is immersion. Immersion describes the experience of

an adversary when interacting with the honeypot. Adversaries should believe that they are interacting with high value targets. This requires honeypots to “test” adversaries in order to increase the quantity and quality of interaction, depending on whether the attack is automated, or perpetrated by a human. The resulting attribution data can be combined with data from other technical attribution techniques such as traceback and network traffic analysis. Combining technical results with data from non-technical attribution techniques, such as intelligence gathering and cui bono analysis, offers a wider spectrum of information for decision makers. In this article we present our technique, DICE (Deception Inside Credential Engine), that can be applied to any deception system, honeypot or not. The engine deceives the adversary using three techniques: non-determinism (dice probability), policy enforcement and honeytokens. Dice probability discards the traditional notion of comparing the username and password to a database entry. Instead, adversaries unknowingly roll a metaphorical dice for each authentication attempt. The honeypot operator controls the number of dice sides and therefore the likelihood of a successful login. Policy enforcement enables the operator to add policies which encourage complex credentials during the authentication procedure. Finally, the third technique ensures that once logged in, the successful credentials are used as a honeytoken, identifying when adversaries return from different points of origin. Using an experimental research methodology, a controlled experiment and a live experiment were devised to demonstrate the DICE approach. The second experiment was deployed as an Internet-facing honeypot. Using honeytokens, seemingly disparate sessions could be related yielding additional attribution information. This turns the tables on traditional honeypot authentication. The adversary now successfully authenticates on a semi-random basis which is controlled by the operator. Further, the adversary authenticates successfully only if their credentials meet an operator-enforced policy. The honeypot operator has a consistent real-time view of the activity using a situational awareness dashboard. The authentication process that was once a small barrier now presents a higher value target to the adversary. The main contribution is therefore improving the application of honeypots as attribution techniques. This is important as the presented deception approach, when compared with other attribution techniques, offer fewer risks to the operator and has the potential to gather a wide corpus of data that is useful for attribution.

Keywords: attribution, deceptive security, honeypots, authentication

Evolution Study of Android Botnets

Heloise Pieterse and Ivan Burke
Defence, Peace, Safety and Security, Council for Scientific and Industrial Research, Pretoria, South Africa

Abstract: Smartphones continue to excel in the 21st century due to the constant improvements of mobile technology. Advances in smartphones, such as increased computing power, improved device-to-device communication and the option of installing additional third-party applications, have led to a sharp rise in their popularity. This popularity, combined with the extensive adoption of smartphones by the general public, has now drawn the attention of mobile malware developers. On popular platforms, such as Android, malware have grown exponentially since the detection of the first mobile Trojan horse in 2010. Android malware families detected during 2013 displayed capabilities that revealed the transition from traditional computer-based botnets to the Android platform. To effectively mitigate or defend against Android botnets, an insightful understanding of them is required. This paper aims to characterise existing Android malware families that display botnet functionality, allowing for the development of proper mitigation and anti-botnet solutions. The contributions of this paper are two-fold. Firstly, the Android malware collection presented in this paper includes 20 families, which covers the majority of malware families displaying botnet behaviour, ranging from their debut in December 2010 to the recent ones discovered in December 2013. These families are thoroughly characterised based on their detailed behaviour breakdown, including propagation methods, command and control channels, and attack strategies. Secondly, an evolution-based study of representative Android botnet families is performed, revealing the rapid growth of Android botnets and the pressing need for anti-botnet solutions. The characterisation of the Android malware families and the subsequent evolution-based study reveal the sophistication of Android botnets. These identifiable characteristics can, however, be incorporated into new and existing mitigation solutions to defend and protect against Android botnet infections. The outcome of this study show that Android botnets are real and a current threat to smartphone users and that there is a need for proper anti-botnet solutions on mobile platforms.

Keywords: android, android botnets, mobile botnets, smartphones, mobile malware

Cyber-Security and Governance for ICS/SCADA in South Africa

Barend Pretorius[1, 2] and Brett van Niekerk[1,2]
[1]Transnet, Durban, South Africa
[2]University of KwaZulu-Natal, Durban, South Africa

Abstract: Industrial control systems (ICS) or supervisory, control, and data acquisition (SCADA) systems drive many key components of the national infrastructure. It makes these control systems targets for cyber-attacks by terrorists and nation-states who wish to damage their target economically and socially; and cyber-criminals who blackmail the companies operating the infrastructure. Despite the high risk of leaving these systems exposed, providing adequate cyber-security is often challenging. SCADA systems evolved in a relatively trusting environment, where operators could remotely access them over public networks. However, as the Internet rapidly grew, more untrusted and malicious parties could potentially gain access to the control systems, and security had to be implemented after the original design. Even with more modern systems, many have problems with patches and updates, making it difficult to provide the necessary controls for vulnerabilities discovered after implementation. The Stuxnet worm illustrated how vulnerable control systems potentially are when it bypassed a number of security mechanisms to cause physical damage to an Iranian nuclear facility. The paper focuses on ICS / SCADA in South Africa. An overview of historical incidents surrounding SCADA systems is provided. Vulnerabilities inherent in such systems and attack methodologies for targeting SCADA systems are discussed, as are the differences between ICS and traditional organisational networks. An overview of SCADA systems in South Africa is provided, and the unique challenges of securing control system in the South African environment are discussed. A governance and security framework for overcoming these challenges are proposed. The paper will be more theoretical in nature, discussing the attacks, vulnerabilities and characteristics unique to ICS / SCADA. The challenges surrounding the cyber-security will be reflective in nature, based on the experiences of those involved in the operating and security of the systems themselves. The main contribution will be the proposal of the governance and security framework for SCADA systems. The paper will be of interest to those who are involved in cyber-security strategies, or security officers in an organisation utilising ICS / SCADA systems.

Keywords: industrial control systems, cyber-security, cyber-attack, supervisory control and data acquisition, vulnerabilities

Strong Authentication: Closing the Front Door to Prevent Unauthorised Access to Cloud Resources

T.V. Raphiri[1], M.T. Dlamini[1,2] and Hein Venter[1]
[1]ICSA Research Group, Department of Computer Science, University of Pretoria, Pretoria, South Africa
[2]School of Computer Science, University of KwaZulu-Natal, Durban, South Africa

Abstract: Cloud computing is a computing paradigm where IT resources such as applications, software and hardware are made available over the Internet. However, inadequate authentication on the cloud is one of the major contributing factors to identity theft, leakage of sensitive data and security problems in general. Identity theft and leakage of sensitive data comes with a high risk for breached cloud customers. Such customers could suffer embarrassment, huge financial loss, bankruptcy or even lose their competitive edge. Hence, from the cloud customers' perspective, it is important that the cloud providers have the ability to protect their login credentials, prove their authenticity and prevent unauthorised access to their cloud-based IT resources through world class and proven authentication models, tools and architectures. Hence, this paper proposes strong authentication architecture to mitigate the leakage of sensitive information due to inadequate authentication on the cloud. The proposed architecture seamlessly authenticating end-users with a number of attributes such as device ID, geo-location, time of access etc. Our findings reflect that even though strong authentication has been around it is the better solution to prove identity and authenticity of cloud customers, its adoption has been slow. However, current trends indicate that the adoption of strong authentication is on the rise and will become the dominant and best practice authentication scheme in the future for cloud. With proper cost, risk and benefit analysis strong authentication can be applied to most cloud providers or any other organisations. The main objective is to ultimately prevent unauthorised access to customer data on the cloud through strong authentication.

Keywords: cloud computing, data leakage, identity theft, strong authentication

The Ingredients of Cyber Weapons

Dusan Repel and Steven Hersee
Royal Holloway, University of London, UK

Abstract: Cyberspace is increasingly embraced as the 5th domain of warfare, in addition to land, sea, air and space. Each of the four physical domains requires distinct weapons, which must be capable of infiltrating enemy territory and deploying a payload. Cyber weapons are, in principle, equivalent to physical weap-

onry, but the nature of weapons in cyberspace is often poorly defined and misunderstood. Despite several governments now stating that they are running cyber warfare programmes and actively developing cyber weapons, it is not clear what they mean by this. In this paper, we consider the nature of cyber weapons, as well as the differences and similarities to physical weaponry. In particular, we consider the differences in the intelligence requirement for the development, deployment and assessment of physical and cyber weapons and discuss how concepts such as assurance, proliferation, deterrence, Collateral Damage Modelling and Battle Damage Assessment apply to such weapons. We pay particular attention to the role that software exploits play in cyber weapons and contrast the properties of exploits, such as longevity and development costs, with those of physical weaponry. Exploits are considered to be important ingredients of cyber weapons, as they are instrumental in enabling the violation of fundamental security assumptions in target systems, which, in turn, facilitates the infiltration of a payload. Furthermore, we explore the nature of the supply chain for cyber weapons and consider the shift from the established leviathan of the defence industry, which traditionally provides physical weaponry, to the shadowy underground markets that are a rich source of cyber weapon ingredients. Finally, we elaborate on the challenges of acquiring exploits from diverse sources and discuss how the evolution of the vulnerability market may shape the future of cyber weapons, cyber warfare, and in turn, all future conflict.

Keywords: cyberspace, weapon, exploit, military

An Adaptive Approach to Achieving Acceptable Functional Resilience and Identifying Functional Resonance

David Rohret
FIERCE Laboratories, CSC Inc, San Antonio, Texas, USA

Abstract: The International Council on Systems Engineering's Resilient System's Working Group defines resiliency as, 'the capability of a system with specific characteristics before, during, and after a disruption to absorb the disruption, recover to an acceptable level of performance, and sustain that level for an acceptable period of time' [INCOSE, 2013]. An operational resiliency model describes a measurement process while demonstrating the scope of achieving resiliency through a dynamic process that includes anticipation of negative effects, withstanding the affects, recovery, and network evolution. In order to maintain the command and control (C^2) advantage during military operations and throughout cyberspace, the measure of functional resiliency must be quantified for integrated and operational systems to provide network defenders and military decision makers the level of capability (to recover) following a significant cyber incident or

a catastrophic natural event. To achieve functional resonance, and vet potential and future threats, technologies competing for network resources must be identified and stressed to determine their role in resiliency and the potential affect they will have on operational systems during an aggressive cyber attack. Through network analysis, based on actual adversarial research and case studies, adaptive analysis teams collect the necessary data to determine a systems' resonance characteristics, specifically, interdependent technologies and processes that can negatively affect a single system or an enterprise network. The traditional role of a vulnerability analysis team is to identify and exploit every vulnerable system or process in order to expose and mitigate weaknesses for the purpose of creating a more viable network. This scope is narrow and confined to a limited range of requirements or technologies based on a similarly narrow set of objectives and goals. To compound the problems associated with obtaining an acceptable resilient posture for a specific system or an enterprise network is the IT industry's misconception that resiliency is tantamount to bandwidth and not a measurement of capability. Network managers attempt to solve poor resiliency by installing more network appliances (redundancy) and adding additional bandwidth; both costly and often ineffective. It is paramount that network managers first identify their current resiliency and associated functional resonance issues prior to initiating corrective actions. The intent of this research is to identify current methods of measuring or achieving acceptable resilience for an enterprise network, identify shortfalls in acquiring accurate and actionable data, and the incorrect application of mitigations that result in no or little resiliency enhancement. The author outlines a process to accurately measure a networks resiliency posture, which will lead to effective mitigations and enhancements allowing for a rapid and cost-effective recovery of functionality.

Keywords: functional resiliency, functional resonance, cyber warfare

A Comparative Study of Correlation Engines for Security Event Management

Luís Rosa, Pedro Alves, Tiago Cruz, Paulo Simões and Edmundo Monteiro
CISUC-DEI, University of Coimbra, Coimbra, Portugal

Abstract: SIEM (Software Information and Event Management) systems are becoming increasingly commonplace in scenarios as diverse as ICT environments or Critical infrastructures, providing the means to process and analyse multiple distributed sources of information and events, for auditing or security purposes. The main component of its architecture is the correlation engine, which is used to normalize, reduce, filter and aggregate events from a set of heterogeneous inputs. Other modules of SIEM systems include agents for data acquisition, reporting modules for event notification, and storage components for log and auditing

purposes. From a cyber-security standpoint, correlators play a vital role in SIEM architectures, providing the means to infer security information from existing event sources such as security agents or services and device logs. In this perspective, correlator performance is a very relevant matter, as it needs to process large amounts of inputs, while having to provide fast results (i.e. security event notifications). Despite the existence of several correlation engines, there is a scarcity of published work comparing their characteristics and performance, a gap this paper addresses. This paper presents the concept of SIEM systems and correlation engines, providing a description of their architecture and functional characteristics, with a focus on some of the most popular open source rule-based correlation engines, such as the Simple Event Correlator (SEC), Esper, Nodebrain and Drools. It also provides a comparative performance evaluation of these correlation engines, based on experimental results.

Keywords: SIEM, event correlation, complex event processing

Fingerprint Match-on-Card: Review and Outlook

Meshack Shabalala, Terrence Moabalobelo and Johannes van der Merwe
Modelling and Digital Science (MDS), Information Security , Council for Scientific and Industrial Research (CSIR), Pretoria, South Africa

Abstract: As cybercrime is on the rise, individuals would like to rest assured that their authentication information cannot be stolen, and then used to gain access to their privileged information. Smart cards can and have played a pivotal role in lowering the statistics on identity theft. This has been achieved by predominantly implementing biometrics matching algorithms inside smart card technology. The biometric matching inside a smart card is known as Match-on-Card/On-Card comparison. However compared to traditional biometric systems implemented on PCs' and servers, smart cards are resource constrained. In addition smart cards do not implement mathematical functions such as trigonometry since they are mainly meant for secure data storage and simple processing. The current state of the On-Card biometric comparison technology is limited in that data for On-Card comparison either has to be pre-calculated outside the card at runtime or fetched from a look-up table. This is because of the limited mathematical operations available inside a smart card. The pre-calculation of data outside the smart card compromises the security offered by the card and the look-up table limits the accuracy of the biometric comparison. The paper reviews the techniques and challenges of implementing fingerprint On-Card comparison algorithms in a smart card environment. Approaches of overcoming the On-Card comparison challenges are also discussed.

Keywords: biometrics, smart cards, fingerprints, match-on-card, moc, on-card comparison

Persistent Technical Difficulties Preventing Effective Software Assurance

Zaheer Shaik[1, 2], Ignus Swart and Nelishia Pillay[2]
[1]Council for Scientific and Industrial Research (CSIR), Pretoria, South Africa
[2]University of KwaZulu-Natal (UKZN), Pietermaritzburg, South Africa

Abstract: Software is present in nearly every aspect of current human society affecting our daily lives. The assumption is thus almost natural that we possess the technology to verify and provide assurance that the software available in our environment is indeed only performing its intended purpose. Yet, numerous examples exist where software failures, infections or outright hidden malicious implementations negatively impacted on the security of individuals and organisations. To address these shortcomings the field of software assurance has been established. Software assurance is defined as the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its lifecycle and that the software functions in the intended manner. The goal of the established field of software assurance is thus clearly to ensure that software utilised performs its intended function and no more. Unfortunately the process of verifying software varies greatly depending on factors such as availability of source code or level of assurance required. This complicates software assurance to such a degree that irrespective of the verification level required, the task remains largely a manual process. Factors such as the complexity of underlying infrastructures used to build software, the variety of software languages and the lack of properly defined tools to decompile and analyse software all prevent efficient automation of these types of tasks. Automation of software is the end goal of security researchers due to the complexity and time consuming nature typical software verification services entail. Adjacent fields of research such as malware detection have similar goals and have contributed to the body of knowledge significantly to identify automation techniques for malware detection. There are however still a number of significant technical difficulties that prevent effective machine learning from occurring such as multiple opcode specifications, the 32-bit switch to 64-bit architecture and arguably the most critical, standardised tools to obtain reliable information regarding the internal workings of a binary. This paper examines common techniques used in software assurance and highlights how even simple variations in the examination process can produce radically different results that indicate the reliability of software. Examination of the main process variations required to perform 64-bit software assurance will be discussed as well as the upgrade in analysis tool chain required.

Keywords: software assurance, malware detection, computer security, automation, machine learning

Social Engineering Attacks: An Augmentation of the Socio-Technical Systems Framework

Nobubele Angel Shozi[1] and Mapule Modise[2]
[1]Council of Scientific and Industrial Research (CSIR), Defence Peace Safety Security, Pretoria, South Africa
[2]University of South Africa (UNISA), South Africa

Abstract: Social engineering attacks pose huge security threats to companies today. These attacks have succeeded mainly because they come from weaknesses that combine the social engineering practices that exploit the human vulnerabilities, with technical skills to bypass the defences of information systems. This paper is founded on the premise that social engineering attacks result from interdependent yet interrelating factors that combine to give an attacker the ability to compromise an individual or organisation's information. We analyse social engineering attacks as a Socio-technical System because it recognises the interaction between people and technology in a work environment. In the case of social engineering attacks, the social subsystem would encompass the people (both victim and attacker), the environmental subsystem would be the environment in which the social engineering attack occurs and the technical subsystem would be the technology used to perform the social engineering attack. The Socio-technical subsystems are further mapped against an existing framework known as the Socio-technical systems framework. This paper applies the currently existing Socio-technical systems framework along with the Socio-technical subsystems mappings to analyse a social engineering attack case study to help identify the underlying factors that made the attack successful. The case study is a popular attack known as 'The Francophone attack', which is an attack that was carried out on a French bank. Through the analysis of the case study, the researchers found that in order to analyse a social engineering attack using the framework, it is pivotal to augment the framework by adding an Information node in the environmental subsystem as one of the aims of any social engineering attacks is to trick you into handing over passwords or other sensitive financial and personal information. The outcome of this research is twofold – firstly, it aims to provide an in-depth perspective into the factors that can allow a social engineering attack to be successful and secondly, to augment the socio-technical systems framework to suit analysis of social engineering attacks when identifying socio-technical system factors.

Keywords: socio-technical systems, social engineering attack, socio-technical systems framework

Modelling the Index of Collective Intelligence in Online Community Projects

Aelita Skaržauskienė and Monika Mačiulienė
Mykolas Romeris University, Vilnius, Lithuania

Abstract: The recent successes of systems like Google, Wikipedia or InnoCentive suggest that individuals and groups can more effectively create valuable intellectual products by acting on the basis of a collective intelligence (CI) (Malone et al, 2012). The subject of our research paper is online community projects which include collective decision making tools and innovation mechanisms allowing and encouraging individual and team creativity, entrepreneurship, online collaboration, new forms of self-regulation and self-governance by considering these projects as being catalyst for emergence of CI. Our quantitative research explored the extent and major trends of the engagement and participation of Lithuanian society in online community projects and have proved the necessity to search for tools fostering civic engagement and collective decision making. The objective of our research project is the intention to propose managerial, social and legal measures for the stimulation of the process. The first step by implementing this ambitious task is to define a set of criteria for measuring Collective intelligence in networked platforms. In this paper we are introducing the theoretical model for CI Potential Index for a scientific discussion. The methodology will allow to identify and analyze conditions that lead online communities to become more collective intelligent: inclusive, reflective and safe. The CI Potential Index will show the state and dynamics of the CI according to changes of various internal and external parameters. The data necessary for the identification of the CI Potential Index dimensions were collected during the quantitative and qualitative research and will be revised during the scientific experiment. A longitudinal observation of a number of networked platforms will be undertaken to measure agreed representative parameters.

Keywords: collective intelligence, decision making, online communities

Multi Sensor National Cyber Security Data Fusion

Ignus Swart[2], Barry Irwin[1] and Marthie Grobler[2]
[1]Rhodes University, Grahamstown, South Africa
[2]CSIR, Pretoria, South Africa

Abstract: A proliferation of cyber security strategies have recently been published around the world with as many as thirty five strategies documented since 2009. These published strategies indicate the growing need to obtain a clear view of a country's information security posture and to improve on it. The potential attack

surface of a nation is extremely large however and no single source of cyber security data provides all the required information to accurately describe the cyber security readiness of a nation. There are however a variety of specialised data sources that are rich enough in relevant cyber security information to assess the state of a nation in at least key areas such as botnets, spam servers and incorrectly configured hosts present in a country. While informative both from an offensive and defensive point of view, the data sources range in a variety of factors such as accuracy, completeness, representation, cost and data availability. These factors add complexity when attempting to present a clear view of the combined intelligence of the data. By applying data fusion the potential exists to provide a comprehensive and representative view of all data sources fused together, regardless of their complexity. This method is not often used in cyber defence systems, since cyber sensor data is typically hard to classify in traditional data fusion techniques due to the diversity and ambiguity present in the sources. This research will examine a variety of currently available Internet data sources and apply it to an adapted Joint Directors of Laboratories (JDL) data fusion model. The model has been adapted to suit national level cyber sensor data fusion with the aim to formally define and reduce data ambiguity and enhance fusion capability in a real world system. The data examined will then be applied to a case study that will show the results of applying available open source security information against the model to relate to the current South African cyber landscape.

Keywords: attack surface, cyber security readiness, JDL model, open source, national security policy, personally identifiable information, sensor fusion

Cache-Timing Attack Against AES Crypto-Systems Countermeasure Using Weighted Average Time Masking Algorithm

Yaseen Taha, Settana Abdulh, Naila Sadalla and Huwaida Elshoush
Department of Computer Science, Faculty of Mathematical Sciences, University of Khartoum, Sudan

Abstract: Side channel attacks are based on side channel information, which is information leaked from encryption systems. Implementing side channel attacks is possible if and only if an attacker has access to a cryptosystem (victim) or can interact with it remotely. A cache timing attack is a special type of side channel attack. Here, an attacker collects and analyzes the variances in encryption timing caused by a cache miss/hit in order to extract sensitive information (encryption key or plaintext). The Advance Encryption Standard (AES) algorithm is a symmetric block cipher that is now used worldwide. Since it has immunity against many known attacks, this type of encryption algorithm is considered quite stable. Cache

timing attack against AES was defined only theoretically until Bernstein carried out a real implementation. Fortunately, this attack can succeed only by exploiting bad implementation in software or hardware rather than resulting from AES algorithm structure weaknesses, and that means it could be prevented if the proper implementation is used. For that reason, modification in software and hardware has been proposed as a countermeasure. This paper reviews some software techniques that have been applied to prevent the cache timing attack. In accordance with past research, the Weighted Average Masking Time (WAMT) algorithm is proposed as a countermeasure that reduces variances in encryption time. It forces each encryption process to take a predefined mask time that will be determined based on the server running the encryption software. Afterwards, the mask time is continually adjusted so that is not too large to lower the performance and too small to hide time variances. This is done using a modified version of the OpenSSL software, which deploys an implementation of the AES algorithm. After applying the cache timing attack on this implementation, the results show that the WAMT algorithm is able to hide the encryption timing required to make the attack feasible.

Keywords: aes algorithm, side channel attack, cache timing attack, cache timing countermeasures, weighted average masking time

Secure Firmware Updates for Point of Sale Terminals

Hippolyte Djonon Tsague, Johannes Van Der Merwe and Terrence Moabalobelo
Council for Scientific and Industrial Research (CSIR), Modeling and Digital Science (MDS), Johannesburg, South Africa

Abstract: A large number of electronic transactions are performed with credit or debit cards at point of sale terminals located at merchant stores. the success of this form of payment however, has an associated cost due to the management and maintenance of the equipment. In particular, there is an important cost related to the deployment of new software upgrades for the point of sale terminals, since in most cases human intervention is required. In this paper, we present a lightweight protocol for secure firmware updates for smart card based point of sale terminals. The protocol has especially been designed with respect to the limited hardware resources in such devices. also, the low bandwidth and the risk of packet loss in the wireless link have been taken into consideration. The protocol provides data integrity and authenticity protection, and thus prevents an attacker from modifying a firmware in transit and installing malicious firmware in the terminals. In addition, terminals can verify that, the received firmware originated from a trusted source. The protocol includes Confidentiality Protection, And Thus The Proprietary Firmware Is Kept Secret From Attackers.

Keywords: point of sale, firmware, upgrade, authenticity, confidentiality, security

An Information Operations Roadmap for South Africa

Brett van Niekerk[1,2]
[1]Transnet, Durban, South Africa
[2]University of KwaZulu-Natal, Durban, South Africa

Abstract: The latest arms race can be considered to be information-based, revolving around both cyber-attacks and the ability to influence mass audiences. Unlike previous arms races, any nation, non-state group or other organisation can participate. It can be attributed to the rise of the concepts of information warfare and information operations. As with any new concept, there are innovators, early adopters, and laggards. However, complexities in the constructs of both information warfare and information operations results in a number of potential adopters struggling to implement their own brand of information operations. A modified capability maturity model is proposed, and applied to the case of South Africa. Using guidance from previous studies, the 'ranking' of South Africa in the global community for information warfare capabilities are reviewed and publicly available documentation is analysed to illustrate the state of information warfare in South Africa. Current structures and capacities are discussed in both military and civilian contexts. The gaps identified by the model are highlighted in order to assess the challenges to evolving the current information warfare and information operations capability in South African. From this, a roadmap for developing an information operations capability is proposed, along with stakeholder responsibilities and accountabilities.

Keywords: capability maturity model, cyber-operations, information operations, information warfare, psychological operations, strategic communications

The Consequences of Edward Snowden NSA Related Information Disclosures

Suné von Solms [1, 2] and Renier van Heerden [1, 3]
[1]Council for Scientific and Industrial Research, Pretoria, South Africa
[2]School for Electronic, Electric and Computer Engineering, North West University, Potchefstroom, South Africa
[3]Department of Computer Science, Rhodes University, Grahamstown, South Africa

Abstract: In June 2013, the Guardian newspaper started to disclose thousands of classified documents, which uncovered the existence of several mass surveillance programmes run by the National Security Agency (NSA) in the USA in cooperation with several European countries. These disclosures exposed a massive NSA clandestine electronic surveillance data program called PRISM as well as evidence of

secret treaties amongst countries sharing surveillance data. The Guardian source was a NSA contractor, Edward Snowden, who was based in Hawaii. Edward Snowden is currently avoiding arrest after he initially fled to Hong Kong and then Russia. The leaks directly influenced US international relations in a negative manner, such as Brazil cancelling a state visit and Ecuador renouncing US trade benefits. The leaks had a financial impact on some of the massive US based IT companies; especially those who specialise in cloud based computing. Persons, companies and nations were affected by the leaks. Some secure email providers had to close down due to NSA and other government pressures to reveal their secret keys. The current estimation is that the US will lose between $25 billion to $35 billion in cloud computing based revenue due to Snowden's leaks. The trust in US based security professionals was also degraded after it was revealed that the NSA has pushed for flawed security standards. This will impact the status and US based security professionals in the future. In this paper we present a timeline of the Snowden related leaks, and discuss the reactions to these disclosures. We also explore the direct and indirect impact of these leaks. The consequences of these disclosures include strained foreign relationships, and the knowledge that mass surveillance programmes exists.

Keywords: Edward Snowden, information disclosures

National Cyber Security in South Africa: A Letter to the Minister of Cyber Security

Rossouw von Solms[1]and Basie von Solms[2]
[1]Nelson Mandela Metropolitan University, Port Elizabeth, South Africa
[2]University of Johannesburg, Johannesburg, South Africa

Abstract: South Africa, like the rest of the world, has become ever more reliant on cyberspace to govern and conduct business, but it is also increasingly exposed to cyber related threats. In 2010, the South African government released the Draft National Cyber Security Policy Framework. This draft policy acknowledged that "South Africa does not have a coordinated approach in dealing with cyber security" and that the "aim of this Policy is to establish an environment that will ensure confidence and trust in the secure use of ICTs". In March 2012 the South African cabinet approved the Policy, but to date absolutely no progress towards the implementation thereof is apparent to the public of South Africa. Meanwhile numerous other countries have published and implemented their National Cyber Security Strategies years ago. In fact, some countries, like the United Kingdom, have filed progress reports regarding the progress made in the implementation of their respective cyber security strategies. Thus, these countries are progressing towards securing cyberspace that is crucial to modern-day critical infrastructure

protection, economy and society. South Africa needs to urgently act in this regard. South Africa cannot continue to drag feet in securing cyberspace in South Africa. For this reason, the objective of this position paper is to motivate the criticality of the situation and, in the conclusion of the paper, to draft a letter addressed to the South African Minister for Cyber Security (whom we know does not exist, but hope that he/she will exist in the near future) to escalate and prioritize the agenda of a National Cyber Security Strategy as a matter of urgency.

Keywords: cyber security, cyber safety, cyber security policy, cyber security strategy

Graphical Passwords: A Qualitative Study of Password Patterns

Jo Vorster and Renier van Heerden
Liverpool University, Council for Scientific and Industrial Research, Rhodes University

Abstract: Graphical passwords schemas are becoming more main-stream. There are many different approaches to graphical passwords, each with its own drawbacks and advantages. There has been many studies to suggest that graphical passwords should be stronger in terms of security because people are better at remembering them. It is well known that the key-space for graphical passwords are at least equivalent to alpha-numeric passwords and can even be much stronger, depending on the schema. Similar to conventional passwords, graphical passwords may have patterns. A pattern that has been widely reported in the literature and studied in some detail are that of hotspots. That is, a high percentage of people will select the same spots on an image. This paper focus on a quantitative analysis of graphical passwords. During this study users from commercial companies were asked to enter graphical passwords. These passwords were then analysed and patterns identified. Users were also asked what there password selection strategies are. The combination of this information enable a qualitative analysis of graphical passwords. The results show that graphical passwords are less secure than expected, that there are a number of patterns that limit the key-space significantly and thus reduce the strength of such password schemas. Users were also asked about their perception of the security of graphical passwords. The survey suggest that users are divided in their opinion on how secure such technologies are. Lastly we also report on reasons that users gave for why they think such technology are not yet ready for use as a security mechanism in an organizational context.

Keywords: graphical passwords, access management

Cyber Maturity as Measured by Scientific Risk-Based Metrics

Lanier Watkins[1] and John Hurley[2]
[1]Johns Hopkins University Information Security Institute, Baltimore, USA
[2]National Defense University, Washington, USA

Abstract: One of the major challenges to an organization achieving a certain level of preparedness to "effectively" combat existing and future cyber threats and vulnerabilities is its ability to ensure the security and reliability of its networks. Most of the existing efforts are quantitative, by nature, and limited solely to the networks and systems of the organization. It would be unfair to not acknowledge that for sure some progress has been achieved in the way that organizations, as a whole, are now positioning themselves to address the threats (GAO 2012). Unfortunately, so have the skill sets and resource levels improved for attackers--they are increasingly getting better at achieving the unwanted access to organizations' information assets. In large part we believe that some of this is due to the failure by methods to assess the overall vulnerability of the networks. In addition, significant levels of threats and vulnerabilities beyond organizations' networks and systems are not being given the level of attention that is warranted. In this paper, we propose a more comprehensive approach that enables an organization to more realistically assess its "cyber maturity" level in hope of better positioning itself to address existing and new cyber threats. We also propose the need to better understand another missing critical piece to the puzzle--the reliability and security of networks in terms of scientific risk-based metrics (e.g., the severity of individual vulnerabilities and overall vulnerability of the network). Our risk-based metrics are: (1) built on the CVSS Base Score which is modified by developing weights derived from the Analytic Hierarchy Process (AHP) to make the overall score more representative of the impact the vulnerability has on the global infrastructure, and (2) rooted in repeatable quantitative characteristics (i.e., vulnerabilities) such as the sum of the probabilities that devices will be compromised via client-side or server-side attacks stemming from software or hardware vulnerabilities. We will demonstrate the feasibility of our method by applying our approach to a case study and highlighting the benefits and impediments which result.

Keywords: cyber maturity, metrics, measures, threats, vulnerabilities

Information Security: Machine Learning Experiments to Solve the File Fragment Classification Problem

Erich Wilgenbus, Hennie Kruger and Tiny du Toit
School of Computer, Statistical and Mathematical Sciences, North-West University, Potchefstroom, South Africa

Abstract: The increased use of digital media to store legal as well as illegal data has increased the need for specialized tools to assist security and forensic specialists in the identification of file fragments. A file fragment classification problem involves the identification of the true file type to which a computer file fragment belongs without relying on traditional metadata. This is an important task because the file type associated with a file object may draw a connection between the file object and the application that can effectively use such a file object. Furthermore, it is also important to know the file type a file object belongs to in order to decide how to use, or not to use, this file object. In this paper the use of supervised learning techniques for content-based file object type identification is explored through the performance results of some empirical experiments to classify possible multi-class data fragments. The experiments include both the use of multilayer perceptron neural networks and linear programming-based discriminant classifiers as well as a combined ensemble of the techniques. To place the results in context, the well-known k-nearest neighbour classifier was also employed to provide a baseline for comparison purposes. Data used for training and testing was obtained from labelled byte frequency histograms and a "greedy" mutual information-based feature selection algorithm was used to rank features. The multi-class problem (as opposed to a binary problem where the classification result is either a confirmation or a rejection) was facilitated by considering ten different file types to which a file fragment may belong. Conclusions were based on classification accuracy as well as metrics such as precision and recall rates. Results have indicated that both the multilayer perceptron neural network and linear programming-based classifiers are individually able to predict file types with reasonable accuracy and proves to be a valid alternative to the k-nearest neighbour classifier. However, contrary to expectation, combined ensembles of these techniques do not significantly improve the prediction accuracy.

Keywords: classification, file fragment type identification, k-nearest neighbour, linear programming-based discriminant analysis, multilayer perceptron neural network

PHD Research Papers

Leveraging Information Security Continuous Monitoring for Cyber Defense

Tina AlSadhan and Joon Park
Syracuse University, Syracuse, New York, USA

Abstract: Cyber infrastructures are constantly under siege by attackers attempting to exploit vulnerabilities. Despite efforts and significant resources expended to protect cyber systems, attackers continue to launch attacks and compromise information systems. Attacks often go unnoticed or security professionals are unable to fully determine the extent of the compromise at the time of attack. Therefore, an earlier awareness and remediation of a security condition can narrow the window of opportunity for an adversary to attack. Considering the large scale of cyber infrastructure, the use of technology in security operations is a critical component for cyber defense. In this research, as part of technology enabled security operation, we analyze the information security continuous monitoring mechanisms and discuss how to leverage them more effectively with extension for cyber defense. In particular, we focus on security controls, security automation, security data, risk scoring, security measurement and situational awareness. Based on our analyses, we will compare the tradeoffs, discuss the challenges for improvements, and present the future strategies for information security continuous monitoring.

Keywords: information security continuous monitoring, cyber security, security automation, risk management

A Preliminary Review of ICS Security Frameworks and Standards Vs. Advanced Persistent Threats

Mercy Bere
Polytechnic of Namibia, Windhoek, Namibia

Abstract: Industrial Control Systems (ICS) control critical industrial processes. Just like any other computer system ICS are vulnerable to attacks which can compromise the infrastructure and or the system components of ICS. Consequently the process being controlled is affected by the attacks. ICS are secured by following best practices and recommendations from ICS security frameworks and standards. It would seem that after implementing and adhering to best practices ICS would be secure and difficult to gain access to, but this is not the case because ICS are being compromised by a new kind of threat christened “Advanced Persistent Threats” (APT). An APT is a multi-step attack designed to realise a particular objective. All the traditional methods of detecting attacks like firewalls, intrusion detection systems and antivirus scanners fail to detect APTs before they have

realised their objective. This implies that following ICS security best practices which recommend the use of firewalls, intrusion detection systems, and antivirus scanners is not enough to deter APTs. This paper will highlight why ICS security frameworks and standards are not sufficient for securing ICS from APTS and will propose possible methods of securing ICS from APTs.

Keywords industrial control systems, advanced persistent threat

A Framework of Security Safeguards for Confidentiality and Integrity of Electronic Personal Information

Prittish Dala and Hein Venter
Department of Computer Science, University of Pretoria, Pretoria, South Africa

Abstract: Privacy entails controlling the use and access to place, location and personal information. In South Africa, the first privacy legislation in the form of the Protection of Personal Information (POPI) Act was signed into law on 26 November 2013. The POPI Act promotes the protection of personal information by public and private institutions and specifies the minimum requirements in twelve chapters, which includes eight conditions for lawful processing of personal information. Condition Seven of the POPI Act makes specific provision for security safeguards to ensure confidentiality and integrity of personal information. However, one of the limitations of Condition Seven is that it is a requirement which is not supported by guidance relating to security safeguards to be considered to ensure confidentiality and integrity of electronic personal information. Hence, this paper aims to propose a framework based on a selection of security safeguards from several leading practices to be considered to prevent unauthorised disclosure and modification of electronic personal information stored, processed or transmitted. The authors believe that the proposed framework will facilitate the achievement and maintenance of compliance with Condition Seven of the POPI Act, with a specific focus on electronic personal information.

Keywords: protection of personal information, POPI Act, electronic personal information, security safeguards, confidentiality and integrity

SCADA Systems Cyber Security for Critical infrastructures: Case Studies in the Transport Sector

Suhaila Ismail[1], Elena Sitnikova[1] and Jill Slay[2]
[1]Information Assurance Group, School of Information Technology and Mathematical Sciences, University of South Australia, Adelaide, Australia
[2]Australian Centre for Cyber Security (ACCS), University of New South Wales at ADFA, Australia

Abstract: Past cyber-attacks on Supervisory Control and Data Acquisition (SCADA) Systems for Critical infrastructures have left these systems compromised and caused financial and economic problems for the relevant organisations. Deliberate attacks have resulted in delayed or denial of services, inconvenience to the public and physical injury to people in certain cases. This study will explore the past attacks on and vulnerabilities of SCADA Systems with specific reference to the transport sector by examining three case studies. The outcomes of these case studies will be further analysed according to the cyber-terrorist decision-making theories. These are strategic, organisational and psychological theories based on the study by McCormick (20003), who further categorized Nelson's (1999) cyber-terrorist capabilities that included: simple-unstructured, advance-structured and complex-coordinated capabilities categories that lead to an attack on a system, in particular SCADA Systems for Critical infrastructures. Based on existing theories, this paper outlines the level of capabilities and decision-making pattern that a cyberterrorist requires when attempting penetrating a SCADA systems environment. The results of this study will form the basis of a guideline that organisations can use so that they are better prepared in identifying potential future cybersecurity attacks on their SCADA systems.

Keywords: critical infrastructures, SCADA system, security best practices, security assessment, SCADA system vulnerabilities

---

Obfuscating a Cloud-Based Botnet Towards Digital Forensic Readiness

Victor Kebande and Hein Venter
Department of computer science, University of Pretoria, Pretoria, South Africa

Abstract: Cloud computing has evolved to be a very powerful distributed computing technology that has been preferred by many organizations due to its ability to run in a virtualized environment, provide service oriented architectures (SOA) and ability to support multi-tenancy architectures. This has, in turn, opened the environment for a subculture of hackers who have found ways of exploiting these

architectures and resources to the core. The problem that this paper is addressing is that, there is no easy way of performing Digital Forensic Readiness (DFR) in the cloud environment without modifying the existing cloud architecture. DFR is a proactive measure taken to counter pre-incident detection by gathering and preserving digital evidence in readiness for digital forensic investigations (DFI). A cloud-based botnet is a piece of non-malicious code deployed in stealth mode to infect virtual instances of computers for information harvesting. It is able to scan subnets, eavesdrop on activities over the network and communicate back to the master. The harvested information is digitally preserved for DFR purposes. In this paper, therefore, the authors report about the techniques of achieving DFR in the cloud using botnets, and how such a botnet can avoid being detected in the process.

Keywords: digital forensic readiness; cloud; botnet; obfuscating; artificial immune system; detectors

Surviving Advanced Persistent Threats – a Framework and Analysis

Ruchika Mehresh and Shambhu Upadhyaya
University at Buffalo, The State University of New York, USA

Abstract: Designing robust mission-critical systems demands bringing together fault tolerance and security. The emergence of advanced persistent threats (APT) has further added to the challenge of meeting mission assurance goals. Despite the advances in mission survivability, the existing solutions remain ineffective against APTs. In this paper, we propose a novel survivability framework against APTs in a distributed environment. It involves tamper-resistant and surreptitious detection and node-to-node verification of suspicious events. The solution aims to identify attacker intent, objectives and strategies (AIOS) and to design targeted recoveries that promote survivability. Its security strength has been theoretically analyzed, while the performance and scalability aspects are measured via simulation. Our simulations demonstrate high scalability with respect to network size and application runtime and the time overhead for long running applications can be easily kept under 1% of original runtime by carefully adjusting the security strength.

Keywords: intrusion detection, mission-critical systems, simulation, tamper-resistant monitoring

A Trust Framework Model for Identity-Management-as-a-Service (IdMaaS)

Nkosinathi Mpofu and Wynand van Van Staden
School of Computing, UNISA, Science Campus, South Africa

Abstract: Identity-Management-as-a-Service (IdMaaS) is a cloud service where a third party assumes the identity management role on behalf of identity owner (which is an organisation) leaving the organisations to devote almost their entire effort to their core business (Mpofu & Van Staden, 2014). IdMaaS increases staff augmentation, access to advanced security tools, access to contextual expertise, and requires least to no capital investment. It is subscription based as such; cost and growth of the system can be easily contained making it one of the attractive identity management paradigm. IdMaaS's reliance on third party management and the internet, diminishes owners' level of control over identities and raises risk exposure level which in turn triggers an array of questions related to identity confidentiality, integrity and availability, that can be loosely tied to lack of trust. IdMaaS's attractiveness leans on putting into place mechanisms to deal with threats to confidentiality, integrity and identity system availability. In recognition of the trust issues identified by(Mpofu & Van Staden, 2014),this research proposes a trust framework to enhance the chances of IdMaaS of becoming an identity management of choice. The framework will provide technical, legal and operational specifications necessary to preserve the confidentiality and integrity of the identities and ensuring business operations are not interrupted by guaranteeing identity system availability. Enabling IdMaaS will in turn provide an entrepreneurial avenue to cloud service providers at the same time adding to the domain of anything-as-a-service (XaaS).

Keywords: trust, trust issues, identity management, identity management-as-a-service, cloud computing, security

Masters Research Papers

Air Power, Clausewitz, and the Cold War: A Strategy for Cyberspace

Christopher Brill
American Military University, Alaska, USA

Abstract: From the first test flights at Kitty Hawk to the nuclear fission research that led to the Manhattan Project, US military planners have continuously sought technology as a means to an end. Cyber warfare cannot replace boots on the ground yet US digital networks - the backbone of US commerce, communications, and infrastructure - are vulnerable to attack by enemies of the state. Today, cyberspace represents the latest game changer in the conduct of warfare, and the paranoid minds of military planners are anxiously taking note. Cyber technology is evolving faster than strategy can keep pace, a problem reminiscent of the dilemma first encountered by air power leaders at the dawn of the Cold War. Aviation pioneers claimed that air power would reverse the body count of conventional war. Unfortunately, instead of using technology to win the fight at hand, the Air Force grew into an institution whose objective was better, newer technology. Without a foundational strategy, the Air Force quickly became a capabilities-obsessed, cost-prohibitive hydra. Military cyberspace strategy could encounter a similar fate. If cyber advocates commit to cyber technology too soon, they run the risk of repeating history, replacing strategic objectives with technology and marginalizing themselves in the process. This paper describes how US policy makers can craft an enduring cyber strategy, one that espouses a doctrine of deterrence and adaptability. If policy makers want to make cyber strategy relevant to current and future threats, then they must first characterize cyber war within the larger nature of war. For this we can turn to Carl von Clausewitz's epic treatise, *On War*. Cyber war is not an end-state in itself, just as war itself is not an end-state. Cyber war, like war, is an extension of politics, the objective of which is to compel one's enemy to bend to your will. Cyberspace is not the first technology to reshape the battlefield, but it could be a capability that dies on the vine unless cyber leaders and policy makers adopt a flexible and relevant cyber strategy. This paper contributes to the discussion of what a sensible cyber doctrine will require through a qualitative approach shaped by historical cases involving emergent air power technology, as well as a strategy of deterrence resurrected from the Cold War.

Keywords: cyber, Carl von Clausewitz, strategy, technology, air power, Cold War

A Best Practice Strategy Framework for Developing Countries to Secure Cyberspace

Victor Jaquire and Basie von Solms
University of Johannesburg, Johannesburg, South Africa

Abstract: The objective of this paper, flowing from an active post-graduates research program, is to provide a best practice strategy framework for developing countries to secure cyberspace, taking cognisance of the realities and constraints within a developing milieu. Cybersecurity policies and related strategies are required for developing countries in order to effectively safeguard against cyber related threats (the same as for developed countries). These policies and strategies for developing countries will differ from those of developed countries due to the unique realities within a developing world. Africa in specific is presently seen as a hotbed for cybercrime, and one of the reasons is that many African countries do not have a proper framework, policies and procedures to properly protect cyberspace.Experience has also shown that a pure adoption by developing countries of the cyber frameworks of developed nations will not always be effective, especially due to the unique requirements and realities within developing worlds, such as limited resources, infrastructure, technologies, skills and experience. The approach taken for the research program, and discussed in this paper, is based on a comprehensive literature study on several existing cybersecurity policies and strategies from both developed and developing countries. From this the drivers / elements for national cybersecurity policies and strategies were identified. These drivers were than adapted to specifically relate to the requirements of developing countries, and then, utilising the identified and adapted drivers, our best practice strategy framework for developing countries to secure their cyberspace was developed. This document will be very useful for those African countries venturing into defining relevant policies and procedures.

Keywords: cybersecurity, cyberspace, developing countries, best practice, strategy framework, policy

The Application of Hough Transform-Based Fingerprint Alignment on Match-on-Card

Cynthia Mlambo[1, 2], Fulufhelo Nelwamondo[1, 2] and Mmamolatelo Mathekga[2]
[1]Department of Electrical and Electronic Engineering Science, University of Johannesburg, Johannesburg, South Africa
[2]Council for Scientific and Industrial Research, Pretoria, South Africa

Abstract: Smart cards are one of the most commonly used technologies that are integrated with fingerprints to develop higher security. One of the important uses of smart cards is the development of authentication systems for an individual. The demand of these cards, has led to the need for further improvements on smart cards combined with fingerprint biometrics. Due to the insufficient memory space and few instruction sets in Java smart cards, developers and programmers are faced with implementing efficient applications with limited memory space. This paper presents the application of an improved Hough Transform-based fingerprint alignment on a Java match on card. Experiments conducted determine the performance of Hough Transform based fingerprint alignment algorithm on Java smart card in terms of accuracy of alignment, memory usage and computing time. The algorithm was tested on a public database FVC2004 DB4 because this database contains rotated and translated images that will show results of alignment from the algorithm. Minutiae points were extracted from mentioned databases and used to compute alignment between two fingerprint images of the same finger that are captured at different instances. In addition, the experiments were conducted on two types of smart cards, Java Card Platform for Government ID, contact (ISO/IEC 7816) and contactless (ISO/IEC 14443). The performance measures considered in this research are memory usage and computing time since smart cards have limited resources which affect the performance of its applications. The results show that if the memory required in the alignment process is reduced, the whole matching process will also be reduced. The required memory for the entire process of alignment varies with the number of minutiae points that need to be aligned. As a result, if few minutiae points i.e. less than 20 are used, the accuracy of alignment decreases. Conversely when the number minutiae points have increased, alignment results becomes more accurate but requires more memory for processing. The average computing time that were taken to compute alignment parameters from two sets of minutiae points were depended on the number of minutiae points and the implementation of instruction sets. With sufficient amount of minutiae points the accuracy becomes more correct, however it requires more time to compute alignment parameters and process all minutiae points.

Keywords: fingerprints, alignment, Hough transform, smart cards, memory usage, computing time

A Model for Access Management of Potential Digital Evidence

Stacey Omeleze and Hein Venter
ICSA Research Group, Computer Science Department, University of Pretoria, South Africa

Abstract: In digital forensic investigation, one of the challenges law enforcement agencies encounter is to corroborate the events of a crime with evidence recovered from the crime scene. However, in using mobile and portable devices as a tool for acquiring real-time potential digital evidence (PDE) in the form of photos, video and audio recordings, this challenge can be over-come. The existing online neighbourhood watch (ONW) model published by the authors enables members of a community in any country like South Africa to upload potential digital evidence of a crime scene onto the ONW repository. The acquired and stored PDE is then made available to authorised users, such as the law enforcement agents, digital forensic investigators and the judiciary to continue investigation or be employed as evidence during a trial. Potential digital evidence can only be validly employed during investigations or as evidence when adequate access control management is in place. Ensuring the integrity and confidentiality of the PDE and maintaining access control of the stored PDE while preserving privacy is an essential component of the ONW concept. The challenge, therefore, is to put in place adequate access management measures at the time of download of PDE from the ONW repository by the authorised users. To address this problem, a PDE access management model is proposed. This model employs the use of roles and attributes to allow access to only the required PDE by an authorised user. This model also confines legitimate users to view or download only the PDE that is required for a particular incident under investigation. In this way, privacy is incorporated into the dataset stored in the ONW repository. Finally, a case scenario is presented to illustrate the application of the PDE access management model.

Keywords: mobile devices; online neighborhood watch; RBAC; ABAC; digital evidence; law enforcement; crime and law

A Conflict-Aware Placement of Client VMs in Public Cloud Computing

M.S. Ratsoma[1], M.T. Dlamini[1, 2], J.H.P. Eloff[1, 3] and Hein Venter[1]
[1]ICSA Research Group, Department of Computer Science, University of Pretoria, Pretoria, South Africa
[2]School of Computer Science, University of KwaZulu-Natal, Durban, South Africa
[3]SAP Product and Innovation Center, Pretoria, South Africa

Abstract: The usage and adoption of cloud computing as a public deployment model is continuously improving, regardless of the security issues involved. This can be attributed to the huge benefits that the cloud provides such as pay-per-use model, quick deployment, turn-around times, huge cost saving, flexible and on-demand self-service provision to cloud users. Since public cloud makes use of virtualisation technology, VMs belonging to clients who are in competition may be placed within the same physical infrastructure. This raises the issue around hosting VMs from clients who might be in direct conflict on the same physical infrastructure. Malicious clients could exploit and launch inter-VM attacks to leak confidential information with a competitive advantage. A lot could happen once confidential data is illegally disclosed to unauthorized users. This work makes an attempt to eliminate the confidential data leakage threat posed by inter-VM attacks within the cloud. Hence, it sets itself up to investigate and determine an approach to physically separate potentially conflicting client VMs within the cloud in order to mitigate the confidential data leakage threat posed by inter-VM attacks. In this paper, we propose a conflict-aware VM allocation and placement architecture that is implemented with an algorithm modelled using a Chinese Wall Security Policy for physical separation of VMs. The solution is abstracted and applied to different levels of conflict and different levels of the cloud; the data centres, clusters and physical nodes, hence optimizing allocation in terms of conflict of interest. This solution focuses on optimally allocating compute space to client VMs depending on their conflict of interest which then determines the separation distances between conflicting clients' VM. This guarantees that clients who are in direct conflict will have their VMs placed very far from each other and VMs belonging to clients that are not in conflict may be placed within the same physical node.

Keywords: cloud computing, virtualisation, conflict of interest, inter-VM attack, Chinese wall policy

A Model Aimed at Controlling the Flow of Information Across Jurisdictional Boundaries

Philip Trenwith and Hein Venter
Department of Computer Science, University of Pretoria, Pretoria, South Africa

Abstract: The inability to gain physical access to devices in the cloud is seen as one of the biggest stumbling blocks digital forensic investigators has to overcome in cloud forensics. Access to devices in the cloud is difficult, if not impossible, because data in cloud computing environments is often spread over a wide range of hosts and data centres. In some cases these data centres may even be located in different jurisdictional domains, making the job of a digital forensic investigator even more challenging. This is not only a challenge for digital forensic investigators, but Cloud Service Providers are also faced with the challenge of jurisdiction. In the European Unions' Data Protection Directive it is referred that no sensitive data may leave the European Union. Hence CSP's need to take considerable care to ensure the sensitive data, such as medical status or political alliance, of its users, remains within the control and jurisdiction of the E.U. This provides sufficient cause to investigate whether a technique can be developed to anchor digital space to physical space in order to ensure that sensitive data remains within the jurisdiction of the CSP. In this paper the author investigate the techniques used to determine the jurisdictional domain in which data in the cloud is located. The author looks at research conducted in the area of Data Provenance, aimed at providing the history of digital objects. The author further looks at the possible techniques that can be used to limit the distribution of data in the cloud to a single jurisdictional domain or a subset of domains, and define a model for implementing such techniques. This model is aimed at enforcing the policy of the European Unions' Data Protection Directive in a practical manner, and provides Cloud Service Provider's with the ability to control the location from where its data is accessible from. The successful implementation of this model benefits cloud service providers and digital forensic investigators alike.

Keywords: digital forensics, cloud computing environments, cloud forensics, jurisdiction, cloud service providers, European unions' data protection directive, data provenance, encryption

Non Academic Papers

Protecting Sensitive Data in a Distributed and Mobile Environment

Florian Patzer[1], Andreas Jakoby[2], Thomas Kresken[1] and Wilmuth Müller[1]
[1]Fraunhofer Institute of Optronics, System Technologies and Image Exploitation – IOSB
Karlsruhe, Germany
[2]Bauhaus University, Weimar, Germany

Abstract: The Cloud and other publically available storage services enable a high potential for time and location independent access to information particularly combined with smart mobile devices. Especially law enforcement agencies, like the police, require such possibilities to access information related to an investigation at any time from any place. However, storing sensitive data on public servers isn't an option for law enforcement agencies due to the possibility of unauthorized access to these data by third parties. To allow the storage of sensitive data on public servers in the Cloud, it has to be encrypted so that the cloud providers and possible attackers do not gain access to that information. At the Fraunhofer IOSB a device called CyphWay® has been developed and presented at ICCWS 2014, which makes sure that sensitive publicly stored data are protected by encryption. This device guaranties that encryption and decryption keys are only available within a specific trusted and protected hardware module. The access to those keys is controlled by a specially designed key management system. The paper at hand describes a security concept using such a trusted environment to build a secure and distributed file system for encrypted data. For this purpose, each file or data set is encrypted independently. The resulting system provides a hierarchical key structure, which controls access to uploaded data and maps the data structure at the same time. The goals of this system are to protect every publicly stored data through encryption and to provide a hierarchical access control. By decoupling the data structure from the actual data and by encrypting the metadata, unauthorized observers will not be able to see meta-information like directory contents or directory structures. Therefore, the presented technique enables the creation of a deniable distributed file system. Unlike several encrypted container solutions the presented system allows to distribute encrypted data over a huge number of divergent publically available storage services, like cloud storages. In addition, it is possible to combine those storages with own private or corporal storage. The key management system implements naturally an access control system and, additionally, allows the allocation of temporary access rights to other users to share data.

Keywords: storage-as-a-service, secure distributed file system, cloud storage, crypto container, mobile security

Side Channel Analysis of SIM Cards Using Combined Higher Order Statistical Techniques

Paul Simon and Pranav Patel
Department of Electrical & Computer Engineering, Air Force Institute of Technology, Wright Patterson AFB, USA

Abstract: The complexity and ubiquity of computing systems is ever increasing in our modern age. From social networking to online banking, from mobile devices to home wireless media and data networks, we constantly communicate and operate through networked systems. At the same time, myriad technologies have been developed to protect the burgeoning amount of sensitive electronic information from unauthorized access. Vulnerabilities in these protection technologies still exist despite these efforts. This paper presents a statistical analysis technique for evaluating electromagnetic (EM) information leakage from Subscriber Identity Module (SIM) cards used in mobile computing devices, bank cards, and Smart Cards. The statistical and differential side channel analysis (SCA) techniques demonstrated here are used to create a spatial leakage map for the surface of the SIM card, as well as a temporal window of highest activity. This statistical SCA technique shows inherent resistance to frequency based noise generation, such as digital clock management circuits. The spatial leakage map and temporal window thus provide a useful basis for further focused, location-based SCA research which, as a proof of concept, aims to extract the PIN encryption algorithm and secret key from SIM cards.

Keywords: side channel analysis; encryption; information leakage; smart cards; statistical analysis

Work In Progress Paper

A Security Review of Proximity Identification Based Smart Cards

Samuel Lefophane and Johan Van der Merwe
Modelling and Digital Science: CSIR, Pretoria, South Africa

Abstract: The widely used ISO/IEC 14443 product standard of Radio Frequency Identification (RFID) technology is currently increasingly penetrating the government and public sector applications in South Africa (e.g. National e-ID and public transportation). The security of ISO/IEC 14443 proximity cards is covered widely in literature addressing different types of attacks, e.g. relay, skimming and eavesdropping attacks. These attacks are performed on certified compliant proximity smart cards illustrating vulnerable standardised parameters that the ISO/IEC 14443 standard left out for the user or designer security implementation. From literature it shows that most attacks (e.g. relay attacks) manage to overcome the implemented security measures. This paper sets out to review the current status quo for the security threats of contactless smart cards that may still prevail once applicable standards have been followed; highlighting that compliance to a standard does not make it secure. It then highlights that relay attacks are the only threat that contactless smart card systems fail to secure against. A countermeasure method is illustrated that will addresses the relay attack threat. The paper concludes by also suggesting where future efforts will be focussed by the authors regarding the security, test and compliance of proximity-based smart cards, especially considering the South African landscape.

Keywords: standards, compliance, security, smart cards

Abstracts Only

Information Security Awareness at a South African Parastatal: Challenges and Successes

Trishee Jobraj[1] and Brett van Niekerk[1, 2]
[1]Transnet, South Africa
[2]UKZN, South Africa

Abstract: Awareness education is an essential component for any information security or cyber-secure culture within an organisation. This aspect becomes even more crucial when the organisation is responsible for operating critical national infrastructures. Many international frameworks and best practices (such as COBIT, the NIST cyber security framework, and King III in South Africa) advocate awareness initiatives to improve organisational information security. However, security cultures and awareness education initiatives often experience challenges, not least the lack of financial and moral support from the organisation's leadership, and other hindrances due to internal politics. The paper focuses on information awareness initiatives within a large South African government-owned organisation mandated with the operation of physical transport infrastructure. The main vision of the awareness programme was to educate users to behave in a secure manner in their personal lives so it would translate into secure behaviour in the workplace. The paper is practitioner based, evolving out of experiences of those involved in running the awareness initiatives within the organisation. An overview of education theory and techniques are presented, along with literature illustrating the effectiveness of the initiatives. The activities in the awareness programme are described, and the alignment of the awareness programme to corporate governance and information security strategy is highlighted. In addition, the impact of the security team and how they generate security awareness indirectly through their project involvement will be described. The challenges experienced in implementing the awareness activities is discussed, and contrasted with the successes achieved by the awareness programme. Ongoing and future activities within the security awareness programme will be presented. Anyone involved in the information security strategy and awareness programmes will benefit from this presentation as the key take-a-ways from the presentation include the awareness techniques used and their successes. The discussion on challenges and successes will be facilitated through a qualitative analysis of evaluations and debriefings from conducted sessions, and other documentation of the various activities and interventions. Where relevant, example awareness education material will be demonstrated.

Keywords: awareness education, governance, information security, information security culture, information security strategy

Analysis of Attacks Against a South African Infrastructure Provider

Mohamed Khan, Justin Williams and Brett van Niekerk
Transnet, South Africa

Abstract: Data is everywhere, its volume is growing every year, and it's fast becoming one of the business's biggest resource. Every digital action we initiate, whether sending an email, logging on to a website or GPS tagging a photograph creates a dataset that can be collected and analyses. The growth of big data impacts and changes the way that an organisation can identify new opportunities to maximise profit or reduce risk. Mastering the collection and analysis of this data will provide an organisation with an insight to maximise opportunity or reduce risk. Specifically in the field of information security including, network monitoring, authentication and authorisation of users, identity management, fraud detection, and systems of governance, risk and compliance, big data and its analysis is being more carefully considered and managed. Next generation firewalls installed at a large South African infrastructure operator primarily as a tool to enhance network security, captured all the data traffic inclusive of applications, threats and content, that either passed through the firewall or was stopped by the firewall from breaching the network security. This presented a unique opportunity in that large volumes of data were being captured by the firewalls. This paper details the collection categorisation and the analysis of the firewall data and its role in identifying vulnerabilities within the organisation. The paper explains how data from existing technology can be leveraged to improve information security and situational awareness and how data analytics can be employed to analyse log files, and network traffic to identify anomalies and suspicious activities, and to correlate multiple sources of information into a coherent view. This paper, while focused more on the business case at the infrastructure provider also discusses the relevance and potential usage at various other organisations. The paper will be of interest to those who are interested in innovative uses of data and data analysis or those tasked with information security management.

Keywords: big data, data analytics, threat prediction, vulnerability management

Techniques that Allow Hidden Activity Based Malware on Android Mobile Devices

Milan Oulehla and David Malaník
Faculty of Applied Informatics, Tomas Bata University in Zlín, Zlín, Czech Republic

Abstract: Currently, number of Android based mobile devices has been constantly increasing. In 2014, Google had over 1 billion active Android users (Trout 2014). Android has become the most popular operating system in the world. However, the Android operating system is not only popular with its users but also with malware programmers. The main issue concerning such widespread operating system is not the GUI and reliability but security. This paper tries to open a different perspective on the Android security issue. While the majority of already published articles describes techniques allowing malware detection, this article is focused on malware from the attacker's perspective and tries to shed light on the techniques allowing functioning of hidden Activity based malware on Android mobile devices. Specifically, the text describes a technique based on camouflage of an Activity that allows running of BroadcastReceiver which has been waiting in background and responds to events such as receiving an SMS, pushing the home button, Wi-Fi connection etc. This technique is important for malware aimed at devices with Android version 3.1 or higher. For safety reasons, these Android versions do not allow running of BroadcastReceiver without an Activity. The article describes how to avoid this protection.

Keywords: android; activity; BroadcastReceiver; camouflage; malicious activity; malicious software; mobile devices; mobile malware; mobile virus; smart phones; tablet

Extra Pages

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