

PROGRAMME – ISSA 2010

Day 1 – Monday, 2 August 2010


07:00–08:20	Registration		
	<i>Session chair: Professor Hein Venter</i>		
08:20-08:30	Welcome address: Dr Marijke Coetzee		
08:30-09:20	Information Security in the 21st Century Keynote address: Professor Mark Pollitt Professor Mark Pollitt joined UCF as a full-time faculty member in 2006. He taught full time at UCF from 2006-2010 and am currently an Associate Professor, Engineering Technology, Daytona State College, Daytona Beach, Florida, USA.		
09:20-10:00	Lifting the cloud on security Guest speaker: Johann van der Merwe – Security Advisory Competency Leader, PricewaterhouseCoopers This talk will consider the security arms race looking at emerging technologies (such as cloud computing, virtualisation, Web 2.0) and how the security industry (locally and internationally) responds to the inherent security challenges. Based on observations, some interesting conclusions are drawn on why security is sometimes losing the competition and how one may (or will) overcome the security challenges posed by emerging technologies.		
10:00-10:40	Information Security – Key enabler of Information Governance Guest speaker: Elize van der Linde - Information Governance Specialist Chairperson for IBM South Africa Data Governance Council The King III Report requires the board to accept responsibility for IT Governance, where IT governance should focus on the governance of Information as well as the governance of Technology. This paper will focus on the “I” in IT Governance, with specific reference to Information Security and how Information security enables and informs an Information Governance Framework.		
10:40-11:10	Tea		
	<i>Session chair: Professor Mariki Eloff</i>		
11:10-11:50	Lessons from the Boer war trenches - aligning security (and multiple assurance functions) to business requirements Guest speaker: Craig Rosewarne - (MBA/CISM/CVE/ISO27001 LA/CobiT & ITIL instructor) Head: School of Risk Management within the Risk Advisory division of Deloitte & Touche and Founder & Chair, Information Security Group of Africa On 11 October 1899, the British service went to war with what was to prove antiquated tactics and in many cases, inappropriate equipment for the African terrain. Craig Rosewarne believes many organisations today may be making similar mistakes when it comes to mitigating risk.		
11:50-12:30	Hiding a giant – Analysis of Next Generation Botnets Guest speaker: Dino Covotsos - CEO, Telspace Systems This presentation will provide an insight into the inner workings of a next generation botnet. Why they exist and what kind of power they give to botmasters. What they are used for and what amounts of money these people are making. We will also cover how botnets have evolved and why they are so hard to take down. We will show how DNS is used to evade CNC control take down and analyze how mobile devices can be used in botnets including an analysis of the recent iPhone botnet and the more malicious worms that followed.		
12:30-13:30	Lunch		
	Stream 1 – (Reviewed Papers)	Stream 2 – (Reviewed Papers)	Stream 3 – (Research in Progress)
	Digital forensics <i>Session chair: Michael Kohn</i>	Web services security <i>Session chair: Kamil Reddy</i>	<i>Session chair: Stephen Flowerday</i>
13:30-14:00	A Digital Evidence Management Plan Cornelia Grobler and Buks Louwrens	Considering web services security policy compatibility Tristan Lavarack and Marijke Coetzee	Multi-channel, Multi-level Authentication for More Secure eBanking Mohamed Al Fairuz and Karen Renaud A Test Bed for Information Security Skill Development with Virtual Training Environment Alok Tripathi, Abhinav Mishra and G.V. Raghunathan
14:00-14:30	Adding digital forensic readiness to the email trace header Francois Ruan Van Staden and Hein Venter	Towards an Ethical Analysis of the W3C Web Services Architecture Model Valiya Gangadharan and Laurette Pretorius	Towards a Standardised Digital Forensic Process: E-mail Forensics Himal Lalla and Stephen Flowerday A Generalized model for understanding and education of Information and Computer Security Hendrik Visage and Martin Olivier

14:30-15:00	A Digital Forensic Readiness Framework for South African SME's David Barske, Adrie Stander and Jason Jordaan	The Management of Cloud Computing Security Sumant Ramgovind, Mariki Eloff and Elme Smith	
15:00-15:30	Tea		
	Stream 4 – (Reviewed Papers)	Stream 5 – (Reviewed Papers)	Stream 6 – (Research in Progress)
	Compliance & soft issues <i>Session chair: Tristan Lavarack</i>	Privacy <i>Session chair: Prof Laurette Pretorius</i>	Session chair: <i>Joey Jansen van Vuuren</i>
15:30–16:00	Social Engineering Attack Detection Model: SEADM Monique Bezuidenhout, Francois Mouton and Hein Venter	Privacy: Aspects, Definitions and a Multi-Faceted Privacy Preservation Approach Karen Renaud and Dora Galvez-Cruz	Using Biometrics to Reduce Fraud in the Micro Lending Industry in South Africa Alain Craven and Mariki Eloff Inclusive Information Society - Challenges from a South African Rural Primary Healthcare Perspective Moses Dlamini, Elmarie Venter, Jan Eloff and Danie Smit
16:00-16:30	Phishing within E-Commerce: A Trust and Confidence Game Greg Megaw and Stephen Flowerday	Secure Publish-Subscribe Mediated Virtual Organizations Richard Ssekibuule	Phishing for Fortune Marthie Grobler Motivation for Cyberterrorism Namosha Veerasamy
16:30-17:00	Measuring Compliance with IS security policies and legislations in a University: Key considerations Michael Kyobe	On Monitoring Information Flow of Outsourced Data Anne Kayem	
17:00–19:00	Cocktail reception at Sandton Convention Centre		

Day 2 – Tuesday, 3 August 2010

07:30–08:10	Registration	
	<i>Session chair: Professor Jan Eloff</i>	
08:10-08:20	Welcome address: Professor Hein Venter	
08:20-09:10	<p>Observations on security in large-scale industrial landscapes Keynote address: Dr Andreas Schaad Dr Andreas Schaad's research interests include workflow- and application-level security as well as distributed systems security in general. He is a member of several ACM and IEEE conference committees in these subject areas. As a Certified Information Systems Security Professional (CISSP) he (co)authored over 40 international security related publications. He used work for Ernst&Young, London as a systems auditor. Currently Dr Schaad is the Research Program Manager of the SAP Research Security & Trust Group, Germany.</p>	
09:10-09:50	<p>Online privacy, the next battleground Guest speaker: Dominic White - security consultant working for SensePost This talk will highlight the often-nefarious methods used to gain personal data and the richness of the resulting picture provided. Examples of privacy attacks will be demonstrated, with a focus on arguing a case for online privacy. Finally, recommended business, technical and legislative practices will be discussed to assist end-users, organisations and potential legislators in this field.</p>	
09:50-10:30	<p>Trust in the Information Society - Trends, Challenges, Foresight, Research Topics Guest speaker: Dr Barend Taute - CSIR Meraka Institute This talk about trust will focus on South Africa, with reference to international development.</p>	
10:30-11:00	Tea	
	<i>Session chair: Professor Les Labuschagne</i>	
11:00-11:40	<p>Policy, process and mandate for a successful eCrime/eDiscovery unit in large corporate Guest speaker: Jock Forrester- Information Security Analyst, Standard Bank Large corporate networks are filled with sources of information that may be required to successfully defend or promote the organisations' position in legal dispute. eCrime can affect an organisation in terms of internal threat to external attackers attempting to breach the perimeter. In these cases, the organisation needs to be able to extract all the information available to it to successfully prosecute offenders. In the case of eDiscovery, the organisation needs to locate information that is relevant to the issue at hand and not, as in the case of eCrime, of finding as much as possible. What are the policies and processes that need to be in place for an organisation to successfully be able to gather eCrime evidence and to process eDiscovery requests in a legally sound manner and cost effectively? Where the unit should be placed in the organisation, what are the benefits of having such a unit and what skills are required to successfully process the large amounts of incidents generated in a large corporate community?</p>	
11:40-12:30	<p>Principles of Inference Control Applied to Controlled Query and Update Execution Keynote address: Professor Dr Joachim Biskup Joachim Biskup received his Diploma degree in mathematics from Technical University of Hannover in 1972, and his Ph.D. in computer science from RWTH Aachen in 1975. He has performed research in recursion and complexity theory, information systems with an emphasis on database schema design, query optimization and mediation, and various aspects of security, in particular access control and inference control. He has joined the program committees of many international conferences, including ICDT, FoIKS, ER, ESORICS and DBSEC. He has been Professor of Computer Science since 1981, and is now at Technische Universität Dortmund, Germany.</p>	
12:30-13:30	Lunch	
	Stream 7 – (Reviewed Papers)	Stream 8 – (Reviewed Papers)
	Organizational security <i>Session chair: Professor Hennie Kruger</i>	Network security <i>Session chair: Dr Marthie Grobler</i>
13:30-14:00	<p>A Conceptual Operational Risk Model for SMEs: Impact on Organisational Information Technology Anass Bayaga and Stephen Flowerday</p>	<p>A Novel Protocol to Allow Revocation of Votes in a Hybrid Voting System Oliver Spycher and Rolf Haenni</p>
14:00-14:30	<p>A framework for evaluating IT security investments in a banking environment Eugene Smith and Hennie Kruger</p>	<p>Agent-Based Host Enumeration and Vulnerability Scanning Using Dynamic Topology Information Ziyad Al-Salloum and Stephen Wolthusen</p>
14:30-15:00	<p>Towards Security Effectiveness Measurement utilizing Risk-Based Security Assurance Reijo Savola, Heimo Pentikäinen and Moussa Ouedraogo</p>	<p>Towards an Information Security Framework for Service-oriented Architecture Jacqui Chetty and Marijke Coetzee</p>
15:00-15:30	Tea	

	Stream 9 - (Reviewed Papers)	Stream 10 - (Reviewed Papers)
	Cyber crime <i>Session chair: Namosha Veerasamy</i>	Network security <i>Session chair: Professor Reinhardt Botha</i>
15:30–16:00	Broadband broadens scope for cyber crime in Africa Marthie Grobler and Joey Jansen van Vuuren	Deep Packet Inspection – Fear of the Unknown Ryan Goss and Reinhardt Botha
16:00-16:30	Mobile Security from an Information Warfare Perspective Brett van Niekerk and Manoj Maharaj	The Cost of Observation for Intrusion Detection: Performance Impact of Concurrent Host Observation Mark M. Seeger, Stephen D. Wolthusen, Christoph Busch and Harald Baier
16:30-17:00	Common problems faced during the establishment of a CSIRT Marthie Grobler and Harri Bryk	An investigation and survey of response options for Intrusion Response Systems (IRSs) Nor Badrul Anuar, Maria Papadaki, Steve Furnell and Nathan Clarke
19:00-22:00	Gala Dinner: Lekgotla Restaurant, Sandton - Africa's dining room on Nelson Mandela Square. For more information, please see http://www.lekgotla.com/	

Day 3 – Wednesday, 4 August 2010 Venue: Academy for IT, University of Johannesburg, Kingsway avenue	
08:30–09:00	Registration
 IEEE Celebrating 125 Years <i>of Engineering the Future</i> South Africa Section	Workshop on hands-on ethical hacking and software security Brief description: The workshop deals with current issues in information security. During the workshop the participant will have hands-on experience doing software exploits, after which each software exploit will be explained with its associated countermeasure. After attending the workshop the participant should have a good understanding of the basic information security standards which should be adhered to in corporate environments. The entire session will be a hands-on and interactive session.
	Workshop facilitator: Francois Mouton , Information and Computer Security Architectures Research Group, Department of Computer Science, University of Pretoria
09:00-10:30	Workshop session 1: Password authoring and steganography
10:30-11:00	Tea
11:00-12:30	Workshop session 2: Intrusion detection systems and software exploits
12:30-13:30	Lunch
13:30-15:00	Workshop session 3: Corporate and personal firewalls
15:00-15:30	Tea
15:30-17:00	Workshop session 4: Social engineering and vulnerabilities in the South African context