

# **10th International Conference on Cyber Warfare and Security**

**(ICCWS 2015)**

**Kruger National Park, South Africa  
24-25 March 2015**

**Editors:**

**Jannie Zaaiman  
Louise Leenen**

**ISBN: 978-1-5108-0097-7**

**Printed from e-media with permission by:**

Curran Associates, Inc.  
57 Morehouse Lane  
Red Hook, NY 12571



**Some format issues inherent in the e-media version may also appear in this print version.**

Copyright© The Authors, (2015). All Rights Reserved.

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

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

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

Printed by Curran Associates, Inc. (2015)

Published by Academic Conferences Ltd.  
Curtis Farm Kidmore End  
Reading RG4 9AY UK

Phone: 441 189 724 148

Fax: 441 189 724 691

[info@academic-conferences.org](mailto:info@academic-conferences.org)

**Additional copies of this publication are available from:**

Curran Associates, Inc.  
57 Morehouse Lane  
Red Hook, NY 12571 USA  
Phone: 845-758-0400  
Fax: 845-758-2634  
Email: [curran@proceedings.com](mailto:curran@proceedings.com)  
Web: [www.proceedings.com](http://www.proceedings.com)

## Contents

Paper Title	Author(s)	Page No
<b>Preface</b>		v
<b>Committee</b>		vi
<b>Biographies</b>		viii
<b>Research papers</b>		
Behavioral-Based Feature Abstraction From Network Traffic	Gaseb Alotibi, Fudong Li, Nathan Clarke and Steven Furnell	1
A new Frontier in war: Cyber Warfare in Estonia	Thomas Armistead and Leigh Armistead	10
Perception Shaping and Cyber Macht: Russia and Ukraine	Edwin Armistead and Scott Starsman	14
Cyber Armies: The Unseen Military in the Grid	Michael Aschmann, Joey Jansen van Vuuren and Louise Leenen	20
Mobile Forensics for PPDR Communications: How and why	Konstantia Barbatsalou, Bruno Sousa, Edmundo Monteiro and Paulo Simoes	30
Evaluation of Online Resources on the Implementation of the Protection of Personal Information Act in South Africa	Johnny Botha, Mariki Eloff and Ignus Swart	39
Securing Military Information Systems on Public Infrastructure	Pieter Botha, Shazia Vawda, Priaash Ramadeen and Alex Terlunen	49
How to Tame Your Android Malware	Ivan Burke and Heloise Pieterse	54
Enrollment Time as a Requirement for Biometric Hand Recognition Systems	João Carvalho, Vítor Sá, Sérgio Tenreiro de Magalhães and Henrique Santos	66
An Ontological Knowledge Base for Cyber Network Attack Planning	Peter Chan, Jacques Theron, Renier van Heerden and Louise Leenen	69
Detecting Deception in Cyber Conflict: A Strategic Approach	Jim Chen and Gilliam Duvall	78
Examination of the United States Nuclear Industry Approach to Critical Infrastructure Protection: Applicability to Improved Industry-Wide Network Cyber Security	Royal Elmore and Bryan Fearey	86
Cyber Coercion: Cyber Operations Short of Cyberwar	Daniel Flemming and Neil Rowe	95
ePOOLICE Security Technology - Fighting Organized Crime Whilst Balancing Privacy and National Security	Anne Gerdes	102
Specifying Functional Requirements for Simulating Professional Offensive Cyber Operations	Tim Grant	108
Public Private Partnerships in Cyberspace: Building a Sustainable Collaboration	Virginia Greiman	118
DDoS Attack Mitigation Through Control of Inherent Charge Decay of Memory Implementations	Alan Herbert and Barry Irwin	126

<b>Paper Title</b>	<b>Author(s)</b>	<b>Page No</b>
Observed Correlations of Unsolicited Network Traffic Over Five Distinct IPv4 Netblocks	Barry Irwin and Thizwilondi Nkhumaleni	135
Modelling the Cybersecurity Environment Using Morphological Ontology Design Engineering	Joey Jansen van Vuuren, Louise Leenen, Marthie Grobler, Peter Chan and ZC Khan	144
Security Deficiencies in the Architecture and Overview of Android and iOS Mobile Operating Systems	Roman Jasek	153
Snapchat Media Retrieval for Novice Device Users	Zubeida Casmod Khan, Thulani Mashiane and Nobubele Angel Shozi	162
The use of Semantic Technologies in Cyber Defence	Louise Leenen and Thomas Meyer	170
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	178
The ARM Based Network Sniffer and Bot Inside the Wide Computer Network	David Malanik	188
Information Sharing and Trust Between Sharing Parties: Sharing Sensitive Information With Regards to Critical Information Infrastructure Protection	Feroze Mohideen and Ian Ellefsen	197
Strategy Matrix for Containing Cyber-Attacks: A Generic Approach	Nkosinathi Mpfu and Ronald Chikati	207
Analysing Urgency and Trust Cues Exploited in Phishing Scam Designs	Rennie Naidoo	216
Rolling the Dice – Deceptive Authentication for Attack Attribution	Andrew Nicholson, Helge Janicke, Tim Watson and Richard Smith	223
Evolution Study of Android Botnets	Heloise Pieterse and Ivan Burke	232
Cyber-Security and Governance for ICS/SCADA in South Africa	Barend Pretorius and Brett van Niekerk	241
Strong Authentication: Closing the Front Door to Prevent Unauthorised Access to Cloud Resources	T.V. Raphiri, M.T. Dlamini and Hein Venter	252
The Ingredients of Cyber Weapons	Dusan Repel and Steven Hersee	261
An Adaptive Approach to Achieving Acceptable Functional Resilience and Identifying Functional Resonance	David Rohret	269
A Comparative Study of Correlation Engines for Security Event Management	Luís Rosa, Pedro Alves, Tiago Cruz, Paulo Simões and Edmundo Monteiro	277
Fingerprint Match-on-Card: Review and Outlook	Meshack Shabalala, Terrence Moabalobelo and Johannes van der Merwe	286
Persistent Technical Difficulties Preventing Effective Software Assurance	Zaheer Shaik, Ignus Swart and Nelishia Pillay	295
Social Engineering Attacks: An Augmentation of the Socio-Technical Systems Framework	Nobubele Angel Shozi and Mapule Modise	305
Modelling the Index of Collective Intelligence in Online Community Projects	Aelita Skaržauskienė and Monika Mačiulienė	313

<b>Paper Title</b>	<b>Author(s)</b>	<b>Page No</b>
Multi Sensor National Cyber Security Data Fusion	Ignus Swart, Barry Irwin and Marthie Grobler	320
Cache-Timing Attack Against AES Crypto-Systems Countermeasure Using Weighted Average Time Masking Algorithm	Yaseen Taha, Settana Abdulh, Naila Sadalla and Huwaida Elshoush	329
Secure Firmware Updates for Point of Sale Terminals	Hippolyte Djonon Tsague, Johannes Van Der Merwe and Terrence Moabalobelo	337
An Information Operations Roadmap for South Africa	Brett van Niekerk	347
The Consequences of Edward Snowden NSA Related Information Disclosures	Suné von Solms and Renier van Heerden	358
National Cyber Security in South Africa: A Letter to the Minister of Cyber Security	Rossouw von Solms and Basie von Solms	369
Graphical Passwords: A Qualitative Study of Password Patterns	Jo Vorster and Renier van Heerden	375
Cyber Maturity as Measured by Scientific Risk-Based Metrics	Lanier Watkins and John Hurley	384
Information Security: Machine Learning Experiments to Solve the File Fragment Classification Problem	Erich Wilgenbus, Hennie Kruger and Tiny du Toit	390
<b>PHD Research Papers</b>		399
Leveraging Information Security Continuous Monitoring for Cyber Defense	Tina AlSadhan and Joon Park	401
A Preliminary Review of ICS Security Frameworks and Standards Vs. Advanced Persistent Threats	Mercy Bere	409
A Framework of Security Safeguards for Confidentiality and Integrity of Electronic Personal Information	Prittish Dala and Hein Venter	415
SCADA Systems Cyber Security for Critical infrastructures: Case Studies in the Transport Sector	Suhaila Ismail, Elena Sitnikova and Jill Slay	425
Obfuscating a Cloud-Based Botnet Towards Digital Forensic Readiness	Victor KEBANDE and Hein Venter	434
Surviving Advanced Persistent Threats – a Framework and Analysis	Ruchika Mehresh and Shambhu Upadhyaya	445
A Trust Framework Model for Identity-Management-as-a-Service (IdMaaS)	Nkosinathi Mpofo and Wynand van Van Staden	455
<b>Masters Research Papers</b>		463
Air Power, Clausewitz, and the Cold War: A Strategy for Cyberspace	Christopher Brill	465
A Best Practice Strategy Framework for Developing Countries to Secure Cyberspace	Victor Jaquire and Basie von Solms	472
The Application of Hough Transform-Based Fingerprint Alignment on Match-on-Card	Cynthia Mlambo, Fulufhelo Nelwamondo and Mmamolatlato Mathekga	481

<b>Paper Title</b>	<b>Author(s)</b>	<b>Page No</b>
A Model for Access Management of Potential Digital Evidence	Stacey Omeleze and Hein Venter	491
A Conflict-Aware Placement of Client VMs in Public Cloud Computing	M.S. Ratsoma, M.T. Dlamini, J.H.P. Eloff and Hein Venter	502
A Model Aimed at Controlling the Flow of Information Across Jurisdictional Boundaries	Philip Trenwith and Hein Venter	510
<b>Non Academic Papers</b>		517
Protecting Sensitive Data in a Distributed and Mobile Environment	Florian Patzer, Andreas Jakoby, Thomas Kresken and Wilmuth Müller	519
Side Channel Analysis of SIM Cards Using Combined Higher Order Statistical Techniques	Paul Simon and Pranav Patel	525
<b>Work InProgress Papers</b>		535
A Security Review of Proximity Identification Based Smart Cards	Samuel Lefophane and Johan Van der Merwe	537