15th European Conference on Cyber Warfare and Security (ECCWS 2016)

Munich, Germany
7 – 8 July 2016

Editors:

Robert Koch
Gabi Rodosek

ISBN: 978-1-5108-2544-4

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, (2016). 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. (2016)

Published by Academic Conferences and Publishing International Ltd.
33 Wood Lane
Sonning Common RG4 9SJ UK

Phone: 441 189 724 148
Fax: 441 189 724 691

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
Web: www.proceedings.com

Contents

Paper Title	**Author(s)**	**Paper no**
Preface		iv
Committee		v
Biographies		vii
Research papers		
Failure or Denial of Service? A Rethink of the Cloud Recovery Model	Muhammed Bello Abdulazeez, Dariusz Kowalski, Alexei Lisista and Sultan Alshamrani	1
Balancing Mobility Algorithm for Monitoring Virtual Machines in Clouds	Sultan Alshamrani, Dariusz Kowalski, Leszek Gąsieniec and Muhammed Abdulazeez	9
Multi-Stage Analysis of Intrusion Detection Logs for Quick Impact Assessment	Henry Au, Mamadou Diallo and Krislin Lee	18
Compliance With Information Security Policies in the Slovene Insurance Sector	Igor Bernik	28
Detecting and Correlating Supranational Threats for Critical Infrastructures	Konstantin Böttinger, Gerhard Hansch and Bartol Filipovic	34
A Cross-Disciplinary Approach to Modelling and Expressing Adversity	Ian Bryant, Carsten Maple and Tim Watson	42
On Cyber Dominance in Modern Warfare	Jim Chen and Alan Dinerman	52
Military Strategy as a Guide for Cybersecurity	Allen Church	58
Applications of Identity Based Cryptography and Sticky Policies With Electronic Identity Cards	Paul Crocker and João Silveira	65
Security Implications of SCADA ICS Virtualization: Survey and Future Trends	Tiago Cruz, Rui Queiroz, Paulo Simões and Edmundo Monteiro	74
Heuristic and Proactive IAT/EAT-Based Detection Module of Unknown Malware	Baptiste David, Eric Filiol, Kevin Gallienne and Olivier Ferrand	84
Conceptualising Cyber Counterintelligence: Two Tentative Building Blocks	Petrus Duvenage, Victor Jaquire and Sebastian von Solms	93
A Semantic web Approach for the Organisation of Information in Security and Digital Forensics	Dagney Ellison and HS Venter	104
An Ontology for Threat Intelligence	Courtney Falk	111
An Analytical Approach to the Recovery of Data From 3rd Party Proprietary CCTV File Systems	Richard Gomm, Nhien-An Le-Khac, Mark Scanlon and M-Tahar Kechadi	117
Intrusion Detection in Cyber Physical Systems Based on Process Modelling	Tamás Holczer, András Gazdag and György Miru	127
Junk Information in Hybrid Warfare: The Rhizomatic Speed of Social Media in the Spamosphere	Aki-Mauri Huhtinen and Jari Rantapelkonen	136

Paper Title	**Author(s)**	**Paper no**
Modeling the Impact of Cyber Risk for Major Dutch Organizations	Vivian Jacobs, Jeroen Bulters and Maarten van Wieren	145
Reflexive Control in Cyber Space	Margarita Levin Jaitner and Harry Kantola	155
Automating Cyber Defence Responses Using Attack-Defence Trees and Game Theory	Ravi Jhawar, Sjouke Mauw and Irfan Zakiuddin	163
Leadership for Cyber Security in Public-Private Relations	Tuija Kuusisto and Rauno Kuusisto	173
Cyber Security Capability and the Case of Finland	Martti Lehto and Jarno Limnéll	182
The Sound a Rattling Cyber-Sabre Makes: Cases Studies in Cyber Power Projection	Antoine Lemay, Scott Knight, José Fernandez and Sylvain Leblanc	191
Exploring the Puzzle of Cyberspace Governance	Andrew Liaropoulos	198
Privacy Concerns of TPM 2.0	Ijlal Loutfi and Audun Jøsang	205
Future Digital Forensics in an Advanced Trusted Environment	Markus Maybaum and Jens Toelle	212
The Situation Picture in a Hybrid Environment: Case Study of two School Shootings in Finland	Teija Norri-Sederholm, Heikki Paakkonen and Aki-Mauri Huhtinen	221
The Nexus Between Cyber Security and Energy Security	Daniel Nussbaum, Stefan Pickl, Arnold Dupuy and Marian Sorin Nistor	228
The Automated Detection of Trolling Bots and Cyborgs and the Analysis of Their Impact in the Social Media	Jarkko Paavola, Tuomo Helo, Harri Jalonen, Miika Sartonen and Aki-Mauri Huhtinen	237
Responding to North Korean Cyberattacks	Ji Min Park, Neil Rowe and Maribel Cisneros	245
An Overview of Linux Container Based Network Emulation	Schalk Peach, Barry Irwin and Renier van Heerden	253
High Performance Intrusion Detection and Prevention Systems: A Survey	Sasanka Potluri and Christian Diedrich	260
Cultural Comparison Between and Attackers and Victims	Char Sample and Mardi John	269
Utilising Journey Mapping and Crime Scripting to Combat Cyber Crime	Tiia Somer, Bil Hallaq and Tim Watson	276
Extracting Intelligence From Digital Forensic Artefacts	Stilianos Vidalis, Olga Angelopoulou and Andy Jones	282
Law Enforcement Access to Evidence Stored Abroad in the Cloud	Murdoch Watney	288
Clandestine Cell Based Honeypot Networks	Cagatay Yucel, Ahmet Koltuksuz and Huseyin Yagci	295
PHD Research Papers		303
The Quincy Wright Model: Postmodern Warfare as a Fifth and Global Phase of Warfare	Sakari Ahvenainen	305

Paper Title	**Author(s)**	**Paper no**
Decision-Support by Aggregation and Flexible Visualization of Risk Situations	Alexander Beck and Stefan Rass	313
A Method to Generate SQL Queries Filtering Rules in SIEM Systems	Martin Dvorak	323
Designing Real-Time Anomaly Intrusion Detection Through Artificial Immune Systems	Adriana-Cristina Enache and Valentin Sgârciu	333
Continuous Supervision: A Novel Concept for Enhancing Data Leakage Prevention	Barbara Hauer	342
E-CMIRC: Towards a Model for the Integration of Services Between SOCs and CSIRTs	Pierre Jacobs, Sebastiaan von Solms and Marthie Grobler	350
A Generic Framework for Digital Evidence Traceability	Nickson Karie, Victor Kebande and Hein Venter	361
Towards a Prototype for Achieving Digital Forensic Readiness in the Cloud Using a Distributed NMB Solution	Victor Kebande, Hermann Stephane Ntsamo and H.S.Venter	369
Stability of Iris Patterns in Different Parts of the Visible Spectrum	Ľuboš Omelina, Bart Jansen, Alexandra Biľanská and Miloš Oravec	379
Grid Security Policy Monitoring System (GridSPMS): Towards Monitoring the Security Dimension of Grids	Abdulghani Suwan and Francois Siewe	384
Applied web Traffic Analysis for Numerical Encoding of SQL Injection Attack Features	Solomon Ogbomon Uwagbole, William Buchanan and Lu Fan	393
Masters Papers		403
Architectural Requirements Specifications for Designing Digital Forensic Applications	Stacey Omeleze and Hein Venter	405
Non Academic Papers		417
Protecting Real-time Transactional Applications With DDoS Resistant Objects	Hugh Harney and Robert Simon	419
Increased C-Suite Recognition of Insider Threats Through Modern Technological and Strategic Mechanisms	Amie Taal, Jenny Le and James Sherer	428
Work In Progress Papers		435
Creation of Specific Flow-Based Training Data Sets for Usage Behaviour Classification	Florian Otto, Markus Ring, Dieter Landes and Andreas Hotho	437
Patterns of Bureaucratic Politics Related to Commercial Military Service Providers	Mikko Räkköläinen	441