

16th European Conference on Cyber Warfare and Security (ECCWS 2017)

Dublin, Ireland
29 – 30 June 2017

Editors:

**Mark Scanlon
Nhien-An Le-Khac**

ISBN: 978-1-5108-4519-0

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, (2017). 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. (2017)

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: 845-758-2633
Email: curran@proceedings.com
Web: www.proceedings.com

Contents

| Paper Title | Author(s) | Page No |
|---|--|---------|
| Preface | | vii |
| Committee | | viii |
| Biographies | | ix |
| What Systems Theory and Evolution can tell us About Cyberwar? | Sakari Ahvenainen | 1 |
| United Nations Digital Blue Helmets as a Starting Point for Cyber Peacekeeping | Nikolay Akatyev and Joshua James | 8 |
| The Estonian-Russian Border Negotiations: A Prelude to the Cyber-Attacks of 2007 | Kari Alenius | 17 |
| Graph Database Technology and k-Means Clustering for Digital Forensics | Henry Au and Krislin Lee | 24 |
| Phishing Campaigns in Corporate Water | Nikolaos Benias, Vasileios Chantzaras, George Iakovakis and Dimitris Gritzalis | 34 |
| Professionalising the Science of Digital Forensics: Policy Logging and Auditable Record Keeping as a Life-Long Record | Bob Bird, Diana Hintea and Mandeep Pannu | 44 |
| Ant Colony Induced Decision Trees for Intrusion Detection | Frans Hendrik Botes, Louise Leenen and Retha De La Harpe | 53 |
| Global Data Breaches Responsible for the Disclosure of Personal Information: 2015 & 2016 | Johnny Botha, Marthie Grobler and Mariki Eloff | 63 |
| Development of an Educational Platform for Cyber Defence Training | Agnė Brilingaitė, Linas Bukauskas and Eduardas Kutka | 73 |
| Treating Personal Data Like Digital Pollution | Ivan Burke and Renier Pelsers van Heerden | 82 |
| Information Operations: The use of Information Weapons in the 2016 US Presidential Election | Emily Darraj, Char Sample and Jennifer Cowley | 92 |
| Strong Authentication for Internet Application | Libor Dostálek | 102 |
| A Conceptual Framework for Cyber Counterintelligence: Theory That Really Matters | Petrus Duvenage, Thenjiwe Sithole and Sebastian von Solms | 109 |
| Towards Basic Design Principles for High- and Medium-Interaction Honeypots | Daniel Fraunholz, Frederic Pohl and Hans Dieter Schotten | 120 |
| Practical Considerations on the Provisioning of Protection Strategies in Process Control Systems | Bela Genge, Flavius Graur, Bogdan Crainicu and Piroška Haller | 127 |
| IT-Security for Smart Grids in Germany: Threats, Countermeasures and Perspectives | Carl-Heinz Genzel, Olav Hoffmann and Richard Sethmann | 137 |
| Cyberwarfare and the Winds of Change in World Politics | Virginia Greiman | 146 |
| Artificial Intelligence Within the Military Domain and Cyber Warfare | Bil Hallaq, Tiia Somer, Anna-Maria Osula, Kim Ngo and Timothy Mitchener-Nissen | 153 |

| Paper Title | Author(s) | Page No |
|--|--|----------------|
| A High-Integrity Cybersecurity Framework for Combat Systems | John Hamilton | 157 |
| An Investigation into Identifying Password Recovery and Data Retrieval in the Android Operating System | Diana Hintea, Robert Bird and James Moss | 165 |
| Nostradamus Prophecy as a Russian Information Warfare Concept | Michael Bennett Hotchkiss | 172 |
| Cultivating a Cyber Counterintelligence Maturity Model | Victor Jaquire and Sebastiaan von Solms | 176 |
| Model-Driven Situational Awareness for Moving Target Defense | Ravi Jhavar and Sjouke Mauw | 184 |
| The 2016 Hard Disk Study on Information Available on the Second Hand Market in the UK | Andy Jones, Olga Angelopoulou, Stilianos Vidalis and Helge Janicke | 193 |
| Formal Characterization of Cyberspace for Cyber Lexicon Development | Anas Mu'azu Kademi and Ahmet Koltuksuz | 200 |
| Experiences From Development of Security Audit Criteria | Tomi Kelo and Juhani Eronen | 208 |
| Security Culture in Digital Inter-Organizational Ecosystems | Tuija Kuusisto and Rauno Kuusisto | 216 |
| Developing a Capability to Classify Technical Skill Levels Within a Cyber Range | William Aubrey Labuschagne and Marthie Grobler | 224 |
| Metrics for Smart Security Awareness | William Aubrey Labuschagne and Namosha Veerasamy | 235 |
| Health Information Privacy of Activity Trackers | Miikael Lehto and Martti Lehto | 243 |
| Towards a General Framework for Network Traffic Time Series Anomaly Detection | Mohamed Wasim Lorgat, Alireza Baghai-Wadji and Andre McDonald | 252 |
| X86 Root of Trust: Technical vs. Political Considerations | Ijlal Loutfi and Audun Jøsang | 261 |
| Ensuring Information Flow and the Situation Picture in Public Safety Organisations' Situation Centres | Teija Norri-Sederholm, Minna Joensuu and Aki-Mauri Huhtinen | 267 |
| An Authorization-Based Cryptographically Secure Mobile Voting System | Murat Odemis and Ahmet Koltuksuz | 274 |
| The Cardinality Estimation of Destructive Information Influence Types in Social Networks | Elena Okhapkina, Valentin Okhapkin, and Oleg Kazarin | 282 |
| A Framework for the Modelling and Simulation of Battlespace Integrated Cyber-Kinetic Effects | David Ormrod and Benjamin Turnbull | 288 |
| Towards a Unified Data Storage and Generic Visualizations in Cyber Ranges | Radek Ošlejšek, Dalibor Toth, Zdenek Eichler and Karolína Burská | 298 |
| Data Exploitation at Large: Your way to Adequate Cyber Common Operating Pictures | Timea Pahi, Maria Leitner and Florian Skopik | 307 |
| A Case Study of the 2016 Korean Cyber Command Compromise | Kyoung Jae Park, Sung Mi Park and Joshua James | 315 |

| Paper Title | Author(s) | Page No |
|--|--|----------------|
| Assisting Digital Forensics Investigations by Identifying Social Communication Irregularities | Heloise Pieterse | 322 |
| Cyber Security Creation as Part of the Management of an Energy Company | Jouni Pöyhönen and Martti Lehto | 332 |
| Forensic Analysis of Epic Privacy Browser on Windows Operating Systems | Alan Reed, Mark Scanlon and Nhien-An Le-Khac | 341 |
| Using Cyber-Security Exercises to Study Adversarial Intrusion Chains, Decision-Making and Group Dynamics | Aunshul Rege, Joe Adams, Edward Parker, Brian Singer, Nicholas Masceri and Rohan Pandit | 351 |
| Flow-Based Benchmark Data Sets for Intrusion Detection | Markus Ring, Sarah Wunderlich, Dominik Grödl, Dieter Landes and Andreas Hotho | 361 |
| Should 'RuNet 2020' be Taken Seriously? Contradictory Views About Cybersecurity Between Russia and the West | Mari Ristolainen | 370 |
| An Evolved Security Architecture for Distributed Industrial Automation and Control Systems | L. Rosa, J. Proença, J. Henriques, V. Graveto, Tiago Cruz, Paulo Simões, F. Caldeira and E. Monteiro | 380 |
| Cultural Observations on Social Engineering Victims | Char Sample, Steve Hutchinson, Andre Karamanian and Carsten Maple | 391 |
| The Information Blitzkrieg: Hybrid Operations Azov Style | Teemu Saressalo and Aki-Mauri Huhtinen | 402 |
| Cyber Personalities as a Target Audience | Miika Sartonen, Petteri Simola, Jussi Timonen and Lauri Lovén | 411 |
| Integration of Ether Unpacker into Ragpicker for Plugin-Based Malware Analysis and Identification | Erik Schaefer, Nhien-An Le-Khac and Mark Scanlon | 419 |
| Phobic Cartography: A Human-Centred, Communicative Analysis of the Cyber Threat Landscape | Keith Scott | 426 |
| Improving the Stealthiness of DNS-Based Covert Communication | Stephen Sheridan and Anthony Keane | 433 |
| Hybrid Emergency Response Model: Improving Cyber Situational Awareness | Jussi Simola and Jyri Rajamäki | 442 |
| Potential Privacy Ramifications of Modern Vehicle Software and Firmware | Paul Simon and Scott Graham | 452 |
| Energy Conscious Adaptive Security Scheme: A Reliability-Based Stochastic Approach | Chrysanthi Taramonli, Mark Leeson and Roger Green | 459 |
| An Approach to Mitigate Multiple Malicious Node Black Hole Attacks on VANETs | John Tobin, Christina Thorpe, Damien Magoni and Liam Murphy | 470 |
| A Hardware One-Time pad Prototype Generator for Localising Cloud Security | Paul Tobin, Lee Tobin, Michael McKeever and Jonathan Blackledge | 480 |
| PSYOP, Deception, and Cyberspace in the Open: Analysing Fake News in a Cyber new Normal Communications Environment | Terry Traylor, Chad Freese and William Wong | 488 |

| Paper Title | Author(s) | Page No |
|--|---|----------------|
| Uncertain Security Community: Building Western Cybersecurity Order | Agnija Tumkevič | 497 |
| Vulnerability Testing in the Development Cycle | Alice van Rensburg, and Sebastiaan von Solms | 505 |
| Cyber Threat Intelligence Exchange: A Growing Requirement | Namosha Veerasamy | 513 |
| Evaluating Internet Intermediary Responsibility and Liability for Criminal Law and National Security Enforcement | Murdoch Watney | 519 |
| Automated Protocol for the Establishment of Encrypted e-Mail Communication (APEEEC) | Nadja Mercedes Wernig and Armin Simmaa | 527 |
| A Parallel Cyber Universe: Botnet Implementations Over TOR-Like Networks | Hüseyin Yağcı, Çağatay Yücel, and Ahmet Koltuksuz | 537 |
| Risks of China's Rapidly Developing Internet Finance | Richard Yam and Xiaoya Xu | 544 |
| Understanding Cyber Terrorism From Motivational Perspectives: A Qualitative Data Analysis | Zahri Yunus, Nurul Mohd, Aswami Ariffin, and Rabiah Ahmad | 550 |
| PhD Research Papers | | 559 |
| Real-Time Malware Uniform Resource Locator Detection System Based on Multi-Layer Perceptron Neural Networks | Mohd Taufik Abdullah, Morufu Olalere, Ramlan Mahmud and Azizol Abdullah | 561 |
| Analysing the Characteristics of Middle Power Cyber Capability | Lisa Davidson | 566 |
| Evaluation of Digital Forensic Process Models With Respect to Digital Forensics as a Service | Xiaoyu Du, Nhien-An Le-Khac and Mark Scanlon | 573 |
| Towards a National Cybersecurity Capability Development Model | Pierre Jacobs, Basie von Solms and Marthie Grobler | 582 |
| Russia: A Cyber Fortress Besieged | Martti Kari and Rauno Kuusisto | 593 |
| Obstacles to the Development of a Universal Lexicon for Cyberwarfare | Mary Manjikian | 602 |
| Evolution of Military Information Security | Juha Mattila and Simon Parkinson | 610 |
| Inference of Endianness and Wordsize From Memory Dumps | Paulo Nunes de Souza and Pavel Gladyshev | 619 |
| Predicting Software Vulnerability Using Security Discussion in Social Media | Andrei Queiroz, Brian Keegan and Fredrick Mtenzi | 628 |
| Political Corporate Governance of ICT: Essential for National Service Delivery and Security | Tersia van der Walt and Sebastiaan von Solms | 635 |
| Masters Research Papers | | 645 |
| Application of Artificial Intelligence for Detecting Derived Viruses | Omotayo Asiru, Moses Dlamini and Jonathan Blackledge | 647 |
| Jigsaw: An Investigation and Countermeasure for Ransomware Attacks | Dermot Byrne and Christina Thorpe | 656 |

| Paper Title | Author(s) | Page No |
|---|--|----------------|
| An Analysis of how Information Security e-Learning can be Improved Through Gamification of Real Software Issues | Seán Duggan and Christina Thorpe | 666 |
| On Entropy-Based Detection of DDoS Attacks | Marios Gyftos, Vasilis Asthenopoulos and Ioanna Roussaki | 673 |
| Digital Forensics and the GDPR: Examining Corporate Readiness | Judith Mackie, Chrysanthi Taramonli and Robert Bird | 683 |
| Analysis of Spam: Honeypot Experiment | Cristobal Martinez and Christina Thorpe | 692 |
| Voice Recognition as a User-Authentication Method | Ebenhaeser Otto Janse van Rensburg and Rossouw Von Solms | 702 |
| Non Academic Papers | | 711 |
| The Cyber-Energy Nexus: The Military Operational Perspective | Daniel Nussbaum and Arnold Dupuy | 713 |
| Work In Progress Papers | | 719 |
| Securing Electronic Workflows With Digital Signatures | Paul Crocker, Tiago Carvalho and Vasco Nicolau | 721 |
| An Improved Ontology for Knowledge Management in Security and Digital Forensics | Dagney Ellison, Hein Venter and Ikuesan Adeyemi | 725 |
| May I Introduce you to a Troll? Defining and Categorizing Internet Behaviour Commonly Referred to as Trolling | Jarkko Paavola, Tuomo Helo, Harri Jalonen Miika Sartonen and Aki-Mauri Huhtinen | 734 |
| Collecting Metadata on an Instant Messaging Server | Alexandre Pujol, Christina Thorpe and Liam Murphy | 741 |
| Surveying the Hackers: The Challenges of Data Collection From a Secluded Community | Helen Thackray, Chris Richardson, Huseyin Dogan, Jacqui Taylor and John McAlaney | 745 |
| Eradicating Terrorist Exploitation of Cyberspace Through the Principle of due Diligence | Claire Yau | 749 |