14th European Conference on Cyber Warfare and Security 2015

Hatfield, United Kingdom
2-3 July 2015

Editors:

Nasser Abouzakhar

ISBN: 978-1-5108-0724-2

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

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)	Page No
Preface		iv
Committee		v
Biographies		vii
Research papers		
A Survey of Continuous and Transparent Multibiometric Authentication Systems	Abdulwahid Al Abdulwahid, Nathan Clarke, Ingo Stengel, Steven Furnell and Christoph Reich	1
Cyber Terrorism Taxonomies: Definition, Targets, Patterns and Mitigation Strategies	Ali Al Mazari, Ahmed Anjariny, Shakeel Habib and Emmanuel Nyakwende	11
What are the Metrics of Cyber Warfare? How Does one Measure Success?	Leigh Armistead and Scott Starsman	19
Design of a Case-Based Reasoner for Information Security in Military Organizations	José Borges, José Martins, Jorge Andrade and Henrique dos Santos	26
Quantitative Analysis of PIN Choices: A Contribution to the Establishment of Authentication Requirements	José Carlos Carvalho, Vítor Sá, Maria José Magalhães and Sérgio Tenreiro deMagalhães	3p
The Cyber Counterintelligence Process: A Conceptual Overview and Theoretical Proposition	Petrus Duvenage' Sebastian von Solms and Manuel Corregedor	42
Security in the Irish Information Technology Sector	Courtney Falk	52
New Techniques of IEEE 802.11 Family Hotspots Attacks, Principles and Defense	Jan Fesl, Marie Dolezalova, Frantisek Drdak and Jan Janecek	61
Cyber Security and Global Governance	Virginia Greiman	71
Cell Based Intrusion Prevention System	Mohamed Hassan, Stilianos Vidalis and Alexios Mylonas	79
Industrial Espionage and Theft of Information	Roland Heickerö	86
Culturing Defensive Immunity: Hardening Psychological Targets Against Cyber Attack	Mils Hills and Guy Batchelor	95
The Double Edge of the Information Sword	Aki-Mauri Huhtinen	104
Using Security Logs to Identify and Manage User Behaviour to Enhance Information Security	Rose Hunt and Stephen Hill	111
Cyber Education? Branches of Science Contributing to the Cyber Domain	Margarita Jaitner and Aine MacDermott	120
It's not a bug, it's a Feature: 25 Years of Mobile Network Insecurity	Audun Jøsang, Laurent Miralabé and Léonard Dallot	129
Peeking Under the Skirts of a Nation: Finding ICS Vulnerabilities in the Critical Digital Infrastructure	Timo Kiravuo, Seppo Tiilikainen, Mikko Särelä and Jukka Manner	137
The Weak Side of Unmanned Aerial Vehicles Against Cyber Attacks: How can we Solve These Security Problems?	Fatih Koc	145

Paper Title	Author(s)	Page No
Adopting Encryption to Protect Confidential data in Public Clouds: A Review of Solutions, Implementation Challenges and Alternatives	Jyrki Kronqvist and Martti Lehto	151
Locating Zero-day Exploits With Course-Grained Forensics	Stephen Kuhn and Stephen Taylor	159
Situation Understanding for Operational art in Cyber Operations	Tuija Kuusisto, Rauno Kuusisto and Wolfgang Roehrig	169
Cyber Security Competencies – Cyber Security Education and Research in Finnish Universities	Martti Lehto	179
Cyber-Security: A Human-Centric Approach	Andrew Liaropoulos	189
Collaborative Intrusion Detection in a Federated Cloud Environment Using the Dempster-Shafer Theory of Evidence	Áine MacDermott, Qi Shi and Kashif Kifayat	195
Creating Novel Features to Anomaly Network Detection Using DARPA-2009 Data set	Nour Moustafa and Jill Slay	204
An Approach to Detect and Analyze the Impact of Biased Information Sources in the Social Media	Jarkko Paavola and Harri Jalonen	213
How to use Software-Defined Networking to Improve Security – a Survey	Jorge Proença, Tiago Cruz, Edmundo Monteiro and Paulo Simões	220
The Security and the Credibility Challenges in e-Voting Systems	Ahmed Rana, Ibrahim Zincir and Samsun Basarici	229
Culture and Cyber Behaviours: DNS Defending	Char Sample and Andre Karamanian	233
Security of SmartPhone Solutions for Implantable Cardioverter Defibrillator Communication	Nuno dos Santos and Paul Crocker	241
From Influencee to Influencer – the Rhizomatic Target Audience of the Cyber Domain	Miika Sartonen, Aki-Mauri Huhtinen and Martti Lehto	249
Dissuasion, Disinformation, Dissonance: Complexity and Autocritique as Tools of Information Warfare	Keith Scott	257
Detection of DNS Based Covert Channels	Stephen Sheridan and Anthony Keane	267
Hands-on Learning of Computer Security: A Cost-effective Laboratory Infrastructure Based on Virtualization Software	Armin Simma, Jeremias Eppler and Bernhard Lang	27c
Absolutely Indiscernible Data Transfer Channel	Mikhail Styugin	286
Standard ISO 27037:2012 and Collection of Digital Evidence: Experience in the Czech Republic	Jaromir Veber and Zdenek Smutny	294
The Legal Conundrum Facing ISPs in Social Media Policing Against Extremism	Murdoch Watney	300
Automated Processes for Evaluating the Realism of High-Interaction Honeyfiles	Ben Whitham, Tim Turner and Lawrie Brown	307
PHD Research Papers		317
Hierarchical Model for Intrusion Detection Systems in the Cloud Environment	Muhammed Abdulazeez and Dariusz Kowalski	319

Paper Title	Author(s)	Page No
The Semantic Approach to Cyber Security Towards Ontology Based Body of Knowledge	Adiel Aviad, Krzysztof Wecel and Witold Abramowicz	328
Resurrecting Anti-Malware Through Collaboration	Manuel Corregedor and Sebastiaan Von Solms	337
A Cloud Forensic Readiness Model for Service Level Agreements Management	Lucia De Marco, Filomena Ferrucci and Tahar Kechadi	346
Non-Interactive Privacy Preserving Protocol for Biometric Recognition Based on Somewhat Homomorphic Encryption	Giulia Droandi	355
How can Internal and External Dependencies Affect Infrastructures Security?	Eric Filiol and Cécilia Gallais	363
A Functional Architecture for Cloud Forensic Readiness Large-Scale Potential Digital Evidence Analysis	Victor Kebande and H.S.Venter	373
Project Management of Complex Penetration Tests	Tomáš Klíma and Martin Tománek	383
Analysis of the Implementation of an Interactive Kinetic Cyber Range Component	Brendan Lawless, Jason Flood and Anthony Keane	389
Masters Research Papers		395
Curb Your Enthusiasm: Why the Future is not Stuxnet	Andreas Haggman	397
An Analysis of Estonia's Cyber Security Strategy, Policy and Capabilities (Case Study)	Michael Kouremetis	404
A Conceptual Model for Digital Forensic Readiness in e-Supply Chains	Derek Masvosvere and Hein Venter	413
Work In Progress Papers		423
Vulnerability Testing of Wireless Access Points Using Unmanned Aerial Vehicles (UAV)	Stephen GergoVemi and Christo Panchev	425
Open-Source Intelligence Monitoring for the Detection of Domestic Terrorist Activity: Exploring Inexplicit Linguistic Cues to Threat and Persuasion for Natural Language Processing	Stefanie Hills, Tom Jackson and Martin Sykora	429
Late Submissions		433
Fighting the Last war to win the Next	Christopher Brill and James Tollefson	435
Social Process for Cyber-Threat Analysis (SPCTA)	Harry Brown III	441