

# **2017 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA 2017)**

**London, United Kingdom  
19-20 June 2017**



**IEEE Catalog Number: CFP17C12-POD  
ISBN: 978-1-5090-5061-1**

**Copyright © 2017 by the Institute of Electrical and Electronics Engineers, Inc.  
All Rights Reserved**

*Copyright and Reprint Permissions:* Abstracting is permitted with credit to the source. Libraries are permitted to photocopy beyond the limit of U.S. copyright law for private use of patrons those articles in this volume that carry a code at the bottom of the first page, provided the per-copy fee indicated in the code is paid through Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923.

For other copying, reprint or republication permission, write to IEEE Copyrights Manager, IEEE Service Center, 445 Hoes Lane, Piscataway, NJ 08854. All rights reserved.

***\*\*\* This is a print representation of what appears in the IEEE Digital Library. Some format issues inherent in the e-media version may also appear in this print version.***

IEEE Catalog Number:	CFP17C12-POD
ISBN (Print-On-Demand):	978-1-5090-5061-1
ISBN (Online):	978-1-5090-5060-4

**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  
E-mail: [curran@proceedings.com](mailto:curran@proceedings.com)  
Web: [www.proceedings.com](http://www.proceedings.com)

CURRAN ASSOCIATES INC.  
**proceedings**  
.com

## **Cyber SA 2017 - Track 1: Situation Awareness Taxonomy, Cognition and Measurements**

### **Chapter 1**

A situation-aware user interface to assess users' ability to construct strong passwords: A conceptual architecture

*Eliana Stavrou*

### **Chapter 2**

Cybersecurity Situational Awareness Taxonomy

*Antti Evesti, Teemu Kanstrén, Tapio Frantti*

### **Chapter 3**

Security Awareness and Affective Feedback: Categorical Behaviour vs. Reported Behaviour

*Lynsay A. Shepherd and Jacqueline Archibald*

### **Chapter 4**

Development and validation of technique to measure cyber situation awareness

*Patrik Lif, Magdalena Granåsen and Teodor Sommestad*

## **Cyber SA 2017 - Track 2: Cyber Defense Operation, Cybercrime Analysis and Detection**

### **Chapter 5**

Automated Computer Network Defence using ARMOUR: Mission-oriented decision support and vulnerability mitigation

*Natalie Nakhla, Kathryn Perrett, Christopher McKenzie*

### **Chapter 6**

Multi-Dimensional Structural Data Integration for Proactive Cyber-Defense

*Ikwu Ruth*

### **Chapter 7**

Towards the normalization of cybercrime victimization; A routine activities analysis of cybercrime in Europe

*Marianne Junger, Lorena Montoya, Pieter Hartel and Maliheh Heydari*

### **Chapter 8**

Socio-economic factors in Cybercrime: Statistical study of the relation between socio-economic factors and cybercrime

*Pablo Casais Solano and Antonio José Reinoso Peinado*

### **Chapter 9**

Stock Market Reaction to Data Breaches: The Moderating Role of Corporate Social Responsibility

*Shuili Du, Kholekile Gwebu and Jing Wang*

## **Cyber SA 2017 - Track 3: Secure Cloud, Graph Theory and Advanced Crypto Systems**

### **Chapter 10**

For cloud services on a user's multiple devices, how do we measure the trusted zone defended by anti-malware?

*Anthony Arrott, Ivan Macalintal and Ian McMillan*

### **Chapter 11**

A Graphic-based Cryptographic Model for Authentication

*Boniface K. Alese, Abimbola Akindele, Folasade, M. Dahunsi, Aderonke F. Thompson and Tosin Adesuyi*

### **Chapter 12**

Performance Evaluation of a Fragmented Secret Share System

*Elochukwu Ukwandu, William J Buchanan and Gordon Russell*

### **Chapter 13**

A Methodology for Testing Virtualisation Security

*Scott Donaldson, Natalie Coull and David McLuskie*

## **Cyber SA 2017 - Track 4: Machine Learning and Visualisation for Cyber Situational Awareness**

### **Chapter 14**

A Temporal Assessment of Cyber Intrusion Chains Using Multidisciplinary Frameworks and Methodologies

*Aunshul Rege, Zoran Obradovic, Nima Asadi, Brian Singer and Nicholas Masceri*

### **Chapter 15**

RicherPicture: Semi-automated cyber defence using context-aware data analytics

*Arnau Erola, Ioannis Agrafiotis, Jassim Happa, Michael Goldsmith, Sadie Creese and Philip A. Legg*

## **Chapter 16**

Visualizing network events in a muggle friendly way

*Outi-Marja Latvala, Tommi Keränen, Sami Noponen, Niko Lehto, Mirko Sailio, Mikko Valta and Pia Olli*

## **Chapter 17**

Cr@ck3n: a cyber alerts visualization object

*David Brosset, Camille Cavelier, Benjamin Costé, Yvon Kermarrec, Joffrey Lartigaud and Pedro Merino Laso*

## **Chapter 18**

Visualisation of Device Datasets to Assist Digital Forensic Investigation

*Gavin Hales*

## **Chapter 19**

Random Forest Explorations for URL Classification

*Martyn Weedon, Dimitris Tsaptsinos and James Denholm-Price*

## **Cyber SA 2017 - Track 5: Game Theory, Social Engineering, Deception and Radicalisation**

### **Chapter 20**

A Location Privacy System in Mobile Network Using Game Theory

*Boniface K. Alese, Aderonke F. Thompson and Patricia Y. Oni*

### **Chapter 21**

Modeling the Effects of Amount and Timing of Deception in Simulated Network Scenarios

*Palvi Aggarwal, Cleotilde Gonzalez and Varun Dutt*

### **Chapter 22**

A Preliminary Radicalisation Framework Based on Social Engineering Techniques

*Sumaia Sabouni, Andrea Cullen and Lorna Armitage*

### **Chapter 23**

Measuring cloud-based anti-malware protection for Office 365 user accounts

*Ferenc Leitold, Anthony Arrott and William Kam*