

2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security 2018)

**Scotland, United Kingdom
11 – 12 June 2018**



**IEEE Catalog Number: CFP18F48-POD
ISBN: 978-1-5386-4684-7**

**Copyright © 2018 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:	CFP18F48-POD
ISBN (Print-On-Demand):	978-1-5386-4684-7
ISBN (Online):	978-1-5386-4683-0

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
Web: www.proceedings.com

CURRAN ASSOCIATES INC.
proceedings
.com

Contents

Sponsor / Technical Co-Sponsor (TCS) / Partnership

Preface

Cyber Security 2018 Programme Committee

Invited Keynotes

Keynote Seminar 1

A Cyber Science Challenge: Evaluating Residual Risks and Propagating Harm

Professor Sadie Creese

Keynote Seminar 2

Describing a CyberSA Analysis Model

Dr Cyril Onwubiko

Keynote Seminar 3

Getting Real about the Reasons for Insecure Behaviours

Professor Karen Renaud

Keynote Seminar 4

The Challenge to Policing in Investigating Cybercrime

Detective Inspector Eamonn Keane

Keynote Seminar 5

Internet of Things – A Hacker Perspective

Associate Professor Jens Myrup Pedersen

Keynote Seminar 6

An Imposter's Journey into Infosec

Stu Hirst

Cyber Security 2018 – Track 1: Machine Learning for Cyber Security Operations

Chapter 1

Unsupervised Approach for Detecting Low Rate Attacks on Network Traffic with Autoencoder00008

Baskoro Adi Pratomo, Pete Burnap and George Theodorakopoulos

Chapter 2

Combined and Robust SNOW-ZUC Algorithm Based on Chaotic System0000

Mahdi Madani and Camel Tanougast

Chapter 3

Detection of malicious domains through lexical analysis00008

Egon Kidmose, Matija Stevanovic and Jens Myrup Pedersen

Chapter 4

A supervised energy monitoring-based machine learning approach for anomaly detection in a clean water supply system000043

Andres Robles-Durazno, Naghmeh Moradpoor, James McWhinnie and Gordon Russell

Cyber Security 2018 - Track 2: Ransomware Cryptanalysis and Crypto Systems

Chapter 5

Ensuring Message Freshness in A Multi-Channel SMS Steganographic Banking Protocol00004;

Omego Obinna, Eckhard Pfluegel, Martin J. Tunnicliffe and Charles A. Clarke

Chapter 6

Quantisation feasibility and performance of RSS-based secret key extraction in VANETs000058

Mirko Bottarelli, Gregory Epiphaniou, Dhouha Kbaier Ben Ismail, Petros Karadimas and Haider Al-Khateeb

Chapter 7

Dynamic Opcode Analysis of Ransomware000066

Domhnall Carlin, Philip O'Kaney and Sakir Sezer

Chapter 8

Infection, Self-reproduction and Overinfection in Ransomware: The Case of TeslaCrypt00006:

Yassine LEMMOU and El Mamoun SOUIDI

Cyber Science 2018 - Track 3: Cyber Defence Exercise, Planning and Recovery

Chapter 9

An Approach to Detect and Prevent Cybercrime in Large Complex Networks00078

Andr'e Sørensen, Maxime J'er'ome Remy, Nicolaj Kjettrup, Rasmi Vlad Mahmoud, Jens Myrup Pedersen

Chapter 10

The Concept of Cyber Defence Exercises (CDX): Planning, Execution, Evaluation00086

Ensar Seker and Hasan Huseyin Ozbenli

Chapter 11

Introducing Falcom: A Multifunctional High-Interaction Honeypot Framework for Industrial and Embedded Applications00095

Daniel Fraunholz, Daniel Krohmer, Hans Dieter Schotten and Carolina Nogueira

Chapter 12

Attackers Constantly Threaten the Survival of Organisations, but there is a New Shark in the Water: Carcharodon Carcharias Moderator Europa Universalis000 3

Bob Duncan

Chapter 13

Cyber Security Considerations for Self-healing Smart Grid Networks000 8

Martin Gilje Jaatun, Marie Elisabeth Gaup Moe, Per Erik Nordbø

Cyber Security 2018 - Track 4: Cyber Physical Systems, Deep Learning and Cloud Computing

Chapter 14

Cloud-based Real-time Network Intrusion Detection Using Deep Learning000 5

Santhosh Parampottupadam, and Arghir-Nicolae Moldovann

Chapter 15

Sub-file Hashing Strategies for Fast Contraband Detection000823

Sean McKeown, Gordon Russell and Petra Leimich

Chapter 16

A Systems Security Approach for Requirements Analysis of Complex Cyber-Physical Systems00082:

Martin "Trae" Span, Logan O. Mailloux, Michael R. Grimaila, and William "Bill" Young

Cyber Security 2018 - Track 5: Cyber Risk Assessment and Management

Chapter 17

An Adversarial Risk-based Approach for Network Architecture Security Modeling and Design000038

Paul A. Wortman, Fatemeh Tehranipoor and John A. Chandy

Chapter 18

Cyber-Risk Assessment for Autonomous Ships000046

Kimberly Tam and Kevin Jones

Cyber Security 2018 - Track 6: Blockchain, IoT, Emerging Cyber Techniques, Tools and Concepts

Chapter 19

Analytical Tools for Blockchain: Review, Taxonomy and Open Challenges000054

Anastasios Balaskas and Virginia N. L. Franqueira

Chapter 20

Reducing the Impact of Network Bottlenecks on Remote Contraband Detection000062

Sean McKeown, Gordon Russell and Petra Leimich

Chapter 21

A Bayesian Intrusion Detection Framework000069

Shuai Fu and Nizar Bouguila

Chapter 22

Lightweight Distributed Attack Detection and Prevention for the Safe Internet of Things000077

Vladimir Eliseev and Olga Eliseeva

Cyber Security 2018 - Track 7: Cyber Security, Legal and Ethics

Chapter 23

Observation Measures to Profile User Security Behaviour000083

Farhad Foroughi and Peter Luksch

Chapter 24

Searching for crime on the web: Legal and Ethical perspectives000089

Dimitrios Kavallieros, Christina Chalanouli, Georgios Kokkinis, Anastasios Papathanasiou, Efthimios Lissaris, Georgios Leventakis, Georgios Giataganas and Georgios Germanos

Chapter 25

OWASP Top 10 - Do Startups Care?000097

Halldis S hoel, Martin Gilje Jaatun and Colin Boyd