

# **2020 International Conference on Cyber Security and Protection of Digital Services (Cyber Security 2020)**

**Dublin, Ireland  
15 – 19 June 2020**



**IEEE Catalog Number: CFP20F48-POD  
ISBN: 978-1-7281-6429-8**

**Copyright © 2020 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:	CFP20F48-POD
ISBN (Print-On-Demand):	978-1-7281-6429-8
ISBN (Online):	978-1-7281-6428-1

**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

# Table of Contents

<b>Cyber Security 2020</b>	
<b>Sponsors and Partners</b>	ii
<b>Themes</b>	iii
<b>Preface</b>	iv
<b>Programme Committee</b> Cyber Security 2020 Programme Committee	vi
<b>Keynote and Industry Speakers</b> <i>Dr Ruoyi Zhou – Director of IBM Research, Ireland</i> <i>Dr Phillippa M. Spencer – Senior Principal Statistician, DSTL, UK</i> <i>Dr Jason R. C. Nurse – Assistant Professor, University of Kent, UK</i> <i>Paul C. Dwyer – CEO, Cyber Risk International, Ireland</i> <i>Professor Steven B. Lipner – Executive Director, SAFECode</i> <i>Wayne Burse – Industrial Cyber Security Lead, Siemen Ltd</i> <i>James Chappell – Founder &amp; Chief Innovation Officer, Digital Shadows</i> <i>Valerie Lyons – Chief Operating Officer, BH Consulting, Ireland</i> <i>Vincent Blake – Vice President, IT Security, GRCA, Pearson Plc</i> <i>Dr Si�n Lloyd – Lead Security, Stability &amp; Resiliency Specialist, ICANN</i>	viii
<b>Track 1: Critical National Infrastructures &amp; CERTs</b>	
<b>Chapter 1</b> An Empirical Study of CERT Capacity in the North Sea <i>Martin Gilje Jaatun, Lars Bodsberg, Tor Olav Gr�tan and Marie Elisabeth Gaup Moe</i>	1
<b>Chapter 2</b> Developing a security behavioural assessment approach for cyber rating U.K. MSBs <i>Andrew Rae and Asma Patel</i>	9
<b>Chapter 3</b> Vulnerability-Based Impact Criticality Estimation for Industrial Control Systems <i>Uchenna Daniel Ani, Hongmei He and Ashutosh Tiwari</i>	17
<b>Chapter 4</b> What Could Possibly Go Wrong? Smart Grid Misuse Case Scenarios <i>Inger Anne T�ndel, Ravishankar Borgaonkar, Martin Gilje Jaatun and Christian Fr�ystad</i>	25
<b>Chapter 5</b> Automated Artefact Relevancy Determination from Artefact Metadata and Associated Timeline Events <i>Xiaoyu Du, Quan Le and Mark Scanlon</i>	33
<b>Track 2: Cyber Attacks, SOCs &amp; Deception</b>	
<b>Chapter 6</b> Towards a Framework for Measuring the Performance of a Security Operations Center Analyst <i>Enoch Agyepong, Yulia Cherdantseva, Philipp Reinecke and Pete Burna</i>	41
<b>Chapter 7</b> Slave Clock Responses to Precision Time Protocol Attacks: A Case Study <i>Waleed Alghamdi and Michael Schukat</i>	49
<b>Chapter 8</b> Deep Down the Rabbit Hole: On References in Networks of Decoy Elements <i>Daniel Reti, Daniel Fraunholz, Janis Zemitis, Daniel Schneider and Hans Dieter Schotten</i>	53
<b>Chapter 9</b> Restricting Data Flows to Secure Against Remote Attack <i>John O’Raw and David Lavery</i>	64
<b>Chapter 10</b>	

An Overview of Web Robots Detection Techniques <i>Hanlin Chen, Hongmei He and Andrew Star</i>	68
<b>Chapter 11</b> Towards Identifying Human Actions, Intent, and Severity of APT Attacks Applying Deception Techniques - An Experiment <i>Joel Chacon, Sean McKeown and Richard Macfarlan</i>	74
<b>Track 3: Exploiting Deep Learning for Cyber Security</b>	
<b>Chapter 12</b> "What did you say?": Extracting unintentional secrets from predictive text learning systems <i>Gwyn Wilkinson and Phil Legg</i>	82
<b>Track 4: Human Factors &amp; Visual Analytics</b>	
<b>Chapter 13</b> Privacy Policy – “I agree”?! – Do alternatives to text-based policies increase the awareness of the users? <i>Pascal Faurie, Arghir-Nicolae Moldovan and Irina Tal</i>	90
<b>Track 5: Cyber Threat Intelligence, OSINT &amp; Cyber Microbiome</b>	
<b>Chapter 14</b> Smarter Password Guessing Techniques Leveraging Contextual Information and OSINT <i>Aikaterini Kanta, Iwen Coisel and Mark Scanlon</i>	96
<b>Chapter 15</b> Cyber Threat Intelligence and the Cyber Meta-Reality and Cyber Microbiome <i>Joshua Sipper</i>	98
<b>Track 6: Digital Evidence &amp; Forensics</b>	
<b>Chapter 16</b> Shouting Through Letterboxes: A study on attack susceptibility to voice assistants <i>Andrew McCarthy, Benedict R. Gaster and Phil Legg</i>	103
<b>Chapter 17</b> Forensic Considerations for the High Efficiency Image File Format (HEIF) <i>Sean Mckeown and Gordon Russell</i>	111
<b>Chapter 18</b> Using Amazon Alexa APIs as a Source of Digital Evidence <i>Clemens Krueger and Sean McKeown</i>	119
<b>Chapter 19</b> Introducing a forensics data type taxonomy of acquirable artefacts from programmable logic controllers <i>Marco Cook, Ioannis Stavrou, Sarah Dimmock and Christopher Johnson</i>	127
<b>Track 7: Cyber Security Detection</b>	
<b>Chapter 20</b> A Security Perspective on Unikernels <i>Joshua Talbot, Przemek Pikula, Craig Sweetmore, Samuel Rowe, Hanan Hindy, Christos Tachtatzis, Robert Atkinson and Xavier Bellekens</i>	135
<b>Chapter 21</b> A Taxonomy of Approaches for Integrating Attack Awareness in Applications <i>Tolga Ünlü, Lynsay Shepherd, Natalie Coull and Colin McLean</i>	142
<b>Chapter 22</b> Cyber-security research by ISPs: A NetFlow and DNS Anonymization Policy <i>Martin Fejrskov, Jens Myrup Pedersen and Emmanouil Vasilomanolakis</i>	146
<b>Track 8: Mobile Security &amp; Ransomware</b>	
<b>Chapter 23</b> Moving Targets: Addressing Concept Drift in Supervised Models for Hacker Communication Detection <i>Andrei Lima Queiroz, Brian Keegan and Susan Mckeever</i>	154
<b>Chapter 24</b>	

Memory Forensics Against Ransomware <i>Pranshu Bajpai and Richard Enbody</i>	161
<b>Chapter 25</b> An Empirical Study of Key Generation in Cryptographic Ransomware <i>Pranshu Bajpai and Richard Enbody</i>	169
<b>Chapter 26</b> Assessing the Influencing Factors on the Accuracy of Underage Facial Age Estimation <i>Felix Anda, Brett Becker, David Lillis, Nhien-An Le-Khac and Mark Scanlon</i>	177
<b>Track 9: Applications of Artificial Intelligence to Cyber Security</b>	
<b>Chapter 27</b> Acoustic Emanation of Haptics as a Side-Channel for Gesture-Typing Attacks <i>Jonathan Francis Roscoe and Max Smith-Creasey</i>	185
<b>Chapter 28</b> AI Crimes: A Classification <i>Fadi Sibai</i>	189
<b>Chapter 29</b> Cost-Effective OCR Implementation to Prevent Phishing on Mobile Platforms <i>Yunjia Wang, Yang Liu, Tiejun Wu and Ishbel Duncan</i>	197
<b>Chapter 30</b> Evaluation of Machine Learning Algorithms for Anomaly Detection <i>Nebrase Elmrabbit, Feixiang Zhou, Fengyin Li and Huiyu Zhou</i>	205
<b>Track 10: Emerging Nations &amp; Risk Management</b>	
<b>Chapter 31</b> Adapting STPA-sec for Socio-technical Cyber Security Challenges in Emerging Nations: A Case Study in Risk Management for Rwandan HealthCare <i>Joseph Kaberuka and Christopher Johnson</i>	213
<b>Chapter 32</b> Towards Security Attack and Risk Assessment during Early System Design <i>Lukas Gressl, Michael Krisper, Christian Steger and Ulrich Neffe</i>	222
<b>Track 11: Social Media Analytics, Communities &amp; Learning</b>	
<b>Chapter 33</b> Blurring lines between fiction and reality: Perspectives of experts on marketing effectiveness of virtual influencers <i>Evangelos Moustakas, Nishtha Lamba, Dina Mahmoud and C Ranganathan</i>	230
<b>Chapter 34</b> Social big data: A Twitter text mining approach to the communication of universities during the Lebanese protests <i>Katia Raya, Nicole D'almeida and Maroun Chamoun</i>	236
<b>Chapter 35</b> Introducing & Evaluating 'Nutrition Facts' for Online Content <i>Matthew Spradling, Jeremy Straub and Jay Strong</i>	244
<b>Track 12: Cyber Security Education</b>	
<b>Chapter 36</b> Think Smart, Play Dumb: Analyzing Deception in Hardware Trojan Detection Using Game Theory <i>Tapadhir Das, Abdelrahman Eldosouky and Shamik Sengupta</i>	252
<b>Chapter 37</b> Epistemological Questions for Cybersecurity <i>Timothy D. Williams</i>	260
<b>Track 13: Cyber Security, Privacy &amp; Ethics</b>	
<b>Chapter 38</b> Technical codes' potentialities in cyber security: A contextual approach on the ethics of small digital organizations in France <i>Theo Simon and Bertrand Venard</i>	264

<b>Chapter 39</b> Privacy Protection Behaviours: a diversity of individual strategies <i>Bertrand Venard</i>	272
<b>Chapter 40</b> Insider Threat Detection: A Solution in Search of a Problem <i>Jordan Schoenherr and Robert Thomson</i>	279
<b>Chapter 41</b> Platform for monitoring and clinical diagnosis of arboviruses using computational models <i>Sebastião Rogério da Silva Neto, Thomás Tabosa de Oliveira, Vanderson Sampaio, Theo Lynn and Patricia Endo</i>	286
<b>Track 14: Data Science &amp; Machine Learning for Cyber Security</b>	
<b>Chapter 42</b> Secure Framework for Anti-Money-Laundering using Machine Learning and Secret Sharing <i>Arman Zand, James Orwell and Eckhard Pfluegel</i>	289
<b>Track 15: Security Testing &amp; Continuous Vulnerability Assessment</b>	
<b>Chapter 43</b> Automated Vulnerability Testing via Executable Attack Graphs <i>Drew Malzahn, Zachary Birnbaum and Cimone Wright-Hamor</i>	296
<b>Track 16: Emerging Technologies, IoT &amp; Bots</b>	
<b>Chapter 44</b> Testing and Hardening IoT Devices Against the Mirai Botnet <i>Christopher Kelly, Nikolaos Pitropakis, Sean Mckeown and Costas Lambrinoudakis</i>	306
<b>Track 17: Blockchain &amp; Crypto</b>	
<b>Chapter 45</b> ethVote: Towards secure voting with distributed ledgers <i>Johannes Mols and Emmanouil Vasilomanolakis</i>	314
<b>Chapter 46</b> A DLT-based Trust Framework for IoT Ecosystems <i>Tharindu Ranathunga, Ramona Marfievici, Alan McGibney and Susan Rea</i>	322