2016 Cybersecurity and Cyberforensics Conference (CCC 2016)

Amman, Jordan
2-4 August 2016

IEEE Catalog Number: CFP16H37-POD
ISBN: 978-1-5090-2658-6

IEEE Catalog Number: CFP16H37-POD
ISBN (Print-On-Demand): 978-1-5090-2658-6
ISBN (Online): 978-1-5090-2657-9

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

2016 Cybersecurity and Cyberforensics Conference

CCC 2016

Table of Contents

Message from the Conference General Chairs vii

Committees ix

Technical Program Committee x

List of Reviewers xii

Session 1

Multilevel Fuzzy Inference System for Risk Adaptive Hybrid RFID Access Control System 1
Malek Al-Zewairi, Dima Suleiman, and Adnan Shaout

Towards Cloud Security Monitoring: A Case Study 8
Umar Mukhtar Ismail, Syed Islam, and Shareeful Islam

Analysis of Strong Password Using Keystroke Dynamics Authentication in Touch Screen Devices 15
Asma Salem, Dema Zaidan, Andraws Swidan, and Ramzi Saifan

Covert Communication Using Port Knocking 22
Mariam Khader, Ali Hadi, and Amjad Hudaib

Authentication Techniques for the Internet of Things: A Survey 28
Maha Saadeh, Azzam Sleit, Mohammed Qatawneh, and Wesam Almobaideen

Session 2

IWNetFAF: An Integrated Wireless Network Forensic Analysis Framework 35
Nadia Benchikha, Mohamed Krim, Khaled Zeraoulia, and Chafika Benzaid

Windows Forensic Investigations Using PowerForensics Tool 41
Akram Barakat and Ali Hadi

Android Forensics: Investigating Social Networking Cybercrimes against Man-in-the-Middle Attacks 48
Khulood Ali Al Zaabi

Reviewing and Evaluating Existing File Carving Techniques for JPEG Files 55
Esra'a Alshammary and Ali Hadi

Session 3

A Proposed Model for Malicious Spam Detection in Email Systems of Educational Institutes 60
Aisha Zaid, Ja'far Alqatawna, and Ammar Huneiti

A Preliminary Analysis of Drive-by Email Attacks in Educational Institutes 65
Ja'far Alqatawna, Ali Hadi, Malek Al-Zwairi, and Mariam Khader

Boosting Usability for Protecting Online Banking Applications Against APTs 70
Mohannad Alhanahnah and David Chadwick

Detecting Ransomware with Honeypot Techniques 77
Chris Moore

Session 4

Analyzing CyberCrimes Strategies: The Case of Phishing Attack 82
Rola Al Halaseh and Ja'far Alqatawna

Fraud Prevention Framework for Electronic Business Environments: Automatic Segregation of Online Phishing Attempts 89
Nazeeh Ghatasheh

Users Profiling Using Clickstream Data Analysis and Classification 96
Wedyan Alswiti, Ja'far Alqatawna, Bashar Al-Shboul, Hossam Faris, and Heba Hakh

Where are All the Cyber Terrorists? From Waiting for Cyber Attack to Understanding Audiences 100
Julian Droogan and Lise Waldek

Session 5

Management Attitudes toward Information Security in Omani Public Sector Organisations 107
Fathiya Al-Izki and George R. S. Weir

Websites' Input Validation and Input-Misuse-Based Attacks 113
Izzat Alsmadi and Iyad Alazzam

Exploiting Vulnerability Disclosures: Statistical Framework and Case Study 117
MingJian Tang, Mamoun Alazab, and Yuxiu Luo

Detecting and Preventing SQL Injection Attacks: A Formal Approach 123
Mohammad Qbea'h, Mohammad Alshraideh, and Khair Eddin Sabri

Experimental and Analytical Evaluation of the Impact of Security Compliance on System Performance of Web Applications 130
John O. Babatunde

Cybersecurity and the Unbearability of Uncertainty 137
Karen Renaud and George R. S. Weir

Improving Resilience by Deploying Permuted Code onto Physically Unclonable Unique Processors 144
Andreas Aßmuth, Paul Cockshott, Jana Kipke, Karen Renaud, Lewis Mackenzie, Wim Vanderbauwhede, Matthias Söllner, Tilo Fischer, and George Weir

Author Index 151