2023 7th Cyber Security in Networking Conference (CSNet 2023)

Montreal, Quebec, Canada
16-18 October 2023

IEEE

IEEE Catalog Number:	**CFP23M97-POD**
ISBN:	**979-8-3503-4288-8**

Copyright © 2023 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:	CFP23M97-POD
ISBN (Print-On-Demand):	979-8-3503-4288-8
ISBN (Online):	979-8-3503-4287-1
ISSN:	2768-0010

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

Program

2023 7th Cyber Security in Networking Conference (CSNet)

Work-in-progress Session

IDS (Intrusion Detection System) Using Deep Learning Techniques
Meetsinh Vijaysinh Parihar (Concordia, Canada), Carol J Fung (Concordia University, Canada) 1

Mobile Networks and Cyber Security

Adversarial Security and Differential Privacy in mmWave Beam Prediction in 6G Networks
Ghanta Krishna (IIIT Naya Raipur, India), Kundrapu Supriya (IIIT Naya Raipur, India), Sanskar Singh (IIIT Naya Raipur, India), Sabur Baidya (University of Louisville, USA) 5

An Experimental Study of Denial of Service Attacks on a 5G COTS Hardware
Karim Baccar (INRIA, France), Abdelkader Lahmadi (University of Lorraine, France) 12

AI based Methods for Cyber Security

Security-Oriented Network Intent Placement Using Particle Swarm Optimization
Marios Avgeris (Carleton University, Canada), Gabriel Landeau (École de Technologie Supérieure - ÉTS, Canada), Aris Leivadeas (École de Technologie Supérieure, Canada), Ioannis Lambadaris (Carleton University, Canada) 19

A New Approach for Crypto Off-Loading Based on Personal HSM
Pascal Urien (Telecom Paris, France) 23

MCM-CASR: Novel Alert Correlation Framework for Cyber Attack Scenario Reconstruction Based on NLP, NER, and Semantic Similarity
Mouhamadou Lamine Diakhame (Gaston Berger University, Senegal), Cherif Diallo (Universite Gaston Berger & SAMOVAR Research Lab, Senegal), Mohamed Mejri (Laval University, Canada) 27

Privacy

Privacy-Preserving Attribute-Based Access Control with Non-Monotonic Access Structure
Maede Ashouri-Talouki (University of Isfahan, Iran), Nafiseh Kahani (Carleton University, Canada), Masoud Barati (Carleton University, Canada) 32

Employee Watcher: A Machine Learning-Based Hybrid Insider Threat Detection Framework
Usman Rauf (Mercy College, USA), Zhiyuan Wei (Mercy College, USA), Fadi Mohsen (University of Groningen & Information Systems Group, Bernoulli Institute for Mathematics, Computer Science and AI, The Netherlands) 39

Ariadne: A Privacy-Preserving Network Layer Protocol
Antoine Fressancourt (Huawei Technologies France S.A.S.U, France), Luigi Iannone (Huawei, France) 46

Deep Learning based Methods for Cyber Security

A Benchmark of Graph Augmentations for Contrastive Learning-Based Network Attack Detection with Graph Neural Networks
Tristan Bilot (Iriguard - Université Paris-Saclay - ISEP Engineering School, France), Nour El Madhoun (ISEP Engineering School & Sorbonne Université, LIP6, France), Khaldoun Al Agha (LRI, France), Anis Zouaoui (Iriguard, France) 53

A Generalizable Approach for Network Flow Image Representation for Deep Learning
Stefan Machmeier (Heidelberg University, Germany), Manuel Trageser (Heidelberg University, Germany), Marcus Buchwald (Heidelberg University, Germany), Vincent Heuveline (Interdisciplinary Center for Scientific Computing, Germany) 57

Vulnerability Assessment Based on Real World Exploitability for Prioritizing Patch Applications
SeongSu Yoon (Chonnam National University, Korea (South)), DoYeon Kim (Chonnam National University, Korea (South)), GaGyeong Kim (Chonnam National University, Korea (South)), IeckChae Euom (Chonnam National University, Korea (South)) 62

Authentication and Web

Collection and Statistical Analysis of a Fixed-Text Keystroke Dynamics Authentication Data Set
Halvor N Risto (University of South-Eastern Norway & Indra Navia, Norway), Olaf Hallan Graven (University of South-Eastern Norway, Norway) 67

Adaptive, Multi-Factor Authentication as a Service for Web Applications
David Morais (University of Aveiro & WIT SOFTWARE, Portugal), André Zúquete (University of Aveiro & IEETA, Portugal), António Mendes (WIT SOFTWARE, Portugal) 74

RanABD: Web Page Randomization for Advanced Web-Bot Detection
Natalija Vlajic (York University, Canada), Shadi Sadeghpour (York University, Canada) 81

Machine Learning for Cyber Security

A Study on the Privacy Concerns of the Internet of Things
Katie Zhang (Barnard College, USA), Yanjun Qian (Virginia Commonwealth University, USA), Vivian Motti (George Mason University, USA), Carol J Fung (Concordia University, Canada) 87

Real-Time Detection of Low-Rate DDoS Attacks in SDN-Based Networks Using Online Machine Learning Model
Abdussalam Alashhab Alashhab (Universiti Teknologi PETRONAS, Malaysia) 95

A Systematic Literature Review of Machine Learning Approaches for In-Browser Cryptojacking Detection
Otavio Kiyatake Nicesio (IPT - Institute for Technological Research of the State of São Paulo, Brazil), Adriano Galindo Leal (Institute for Technological Research of the São Paulo State, Brazil) 102

Anomaly Detection

Score-Based Unsupervised Anomaly Detection Using Graph Clustering and the Activity and Event Network Model
Amir Mohammadi Bagha (Toronto Metropolitan University, Canada), Isaac Woungang (Toronto Metropolitan University, Canada), Issa Traore (University of Victoria, Canada) 109

Towards Cluster-Based Split Federated Learning Approach for Continuous User Authentication
Mohamad Wazzeh (École de Technologie Supérieure, Canada), Mohamad Arafeh (Ecole de Technologie Superieure, Canada), Hakima Ould-Slimane (Université du Québec à Trois-Rivières, Canada), Chamseddine Talhi (Ecole de Technologie Superieure, Canada), Azzam Mourad (Lebanese American University, Lebanon), Hadi Otrok (Khalifa University, United Arab Emirates & Concordia University, Canada) 114

Feature Engineering for Injection Attack Detection: An Exploration from SQLI to XSS
Alexander Loginov (Dalhousie University, Canada), Nur Zincir-Heywood (Dalhousie University, Canada), M. I. Heywood (Dalhousie University, Canada) 119

Access Control

Incremental Threshold Scheme Enabled IoT Group Key Management
Mingyan Li (Oak Ridge National Laboratory, USA), Samuel C Hollifield (Oak Ridge National Laboratory, USA), Michael D Iannacone (Oak Ridge National Laboratory, USA) 123

Implementing the Principle of Least Privilege Using Linux Capabilities: Challenges and Perspectives
Eddie Billoir (Université Toulouse III Paul Sabatier, IRIT & Airbus Protect, France), Romain Laborde (Université Toulouse III, Paul Sabatier & IRIT, France), Ahmad Samer Wazan (Zayed University, United Arab Emirates), Yves Rütschlé (Airbus Protect, France), Abdelmalek Benzekri (Paul Sabatier University, France) 130

Protect the Gate - Not Only Once: Continuous Access Evaluation in Practice
Tobias Hilbig (Munich University of Applied Sciences, Germany), Vitali Serzantov (Munich University of Applied Sciences, Germany), Thomas Schreck (University of Applied Science Munich, Germany) 137

Privacy

Efficient Privacy-Preserving ML for IoT: Cluster-Based Split Federated Learning Scheme for Non-IID Data
Mohamad Arafeh (Ecole de Technologie Superieure, Canada), Mohamad Wazzeh (École de Technologie Supérieure, Canada), Hakima Ould-Slimane (Université du Québec à Trois-Rivières, Canada), Chamseddine Talhi (Ecole de Technologie Superieure, Canada), Azzam Mourad (Lebanese American University, Lebanon), Hadi Otrok (Khalifa University, United Arab Emirates & Concordia University, Canada) 143

Regulatory Compliance Verification: A Privacy Preserving Approach
Mohammed B. M. Kamel (Furtwangen University, Germany & Eotvos Lorand University, Hungary), Massimo Morello (European Central Bank, Germany), Petri Sainio (University of Turku, Finland) ..... N/A

Private Identity-Related Attribute Verification Protocol Using SoulBound Tokens and Zero-Knowledge Proofs
Miquel Àngel Cabot-Nadal (University of the Balearic Islands, Spain), Brendan Playford (Masa Finance, USA), María Magdalena Payeras-Capellà (Universidad de las Islas Baleares, Spain), Sebastian Gerske (Masa Finance, USA), Macià Mut-Puigserver (Universitat de les Illes Balears, Spain), Rosa Pericas Gornals (University of the Balearic Islands, Spain) 153

Inference and Deception for Cyber Security

Inferring the Confidence Level of BGP-Based Distributed Intrusion Detection Systems Alarms
Renato Souza Silva (Federal University of Rio de Janeiro (UFRJ), Brazil, Brazil), Felipe M. F. de Assis (Federal University of Rio de Janeiro (UFRJ), Brazil, Brazil), Evandro Luiz Cardoso Macedo (Federal University of Rio de Janeiro (UFRJ), Brazil), Luis Felipe M. de Moraes (Federal University of Rio de Janeiro (UFRJ), Brazil) 157

Mirage: Cyber Deception Against Autonomous Cyber Attacks
Michael B Kouremetis (MITRE Corporation, USA), Ron Alford (MITRE Corporation, USA), Dean Lawrence (MITRE Corporation, USA) 163

Stealthy Attacks on Multi-Agent Reinforcement Learning in Mobile Cyber-Physical Systems
Sarra Alqahtani (Wake Forest University, USA), Talal Halabi (Laval University, Canada) 171

Graph based Methods for Cyber Security

Graph-Based Attack Path Discovery for Network Security
Qiaoran Meng (National University of Singapore, Singapore), Huilin Wang (National University of Singapore, Singapore), Nay Oo (NCS Cyber Special Ops-R&D, Singapore), Hoon Wei Lim (NCS Cyber Special Ops - R&D, Singapore), Benedikt J Schätz (National University of Singapore, Singapore), Biplab Sikdar (National University of Singapore, Singapore) 178

Towards Anomaly Detection Using Multiple Instances of Micro-Cluster Detection
Rafael N Copstein (Dalhousie University, Canada), Bradley Niblett (2Keys Corporation - An Interac Company, Canada), Andrew Johnston (2Keys Corporation - An Interac Company, Canada), Jeff Schwartzentruber (Dalhousie University, Canada), M. I. Heywood (Dalhousie University, Canada), Nur Zincir-Heywood (Dalhousie University, Canada) 185

Unveiling Stealth Attack Paths in Windows Environments Using AWARE
Manuel Poisson (CentraleSupélec Rennes & Amossys, France), Valérie Viet Triem Tong (Inria - CentraleSupelec, France), Gilles Guette (University of Rennes 1, France), Erwan Abgrall (Irisa, France), Frédéric Guihery (Amossys, France), Damien Cremilleux (Amossys, France) 192

IoT Cyber Security

A Blockchain-Enabled IoT Framework for NICU Infant Health Monitoring System
R Madhusudhan (National Institute of Technology Karnataka, India), Pravisha P (NITK, India) 199

DDoS Attack Detection in Edge-IIoT Using Ensemble Learning
Fariba Laiq (Institute of Management Sciences Peshawar, Pakistan), Feras Al-Obeidat (Zayed University, United Arab Emirates), Adnan Amin (Institute of Management Sciences, Peshawar, Hayatabad Pakistan, Pakistan), Fernando Moreira (REMIT IJP Universidade Portucalense Porto Portugal, Portugal) 204

Smart Home IoT Communication Protocols and Advances in Their Security and Interoperability
Ismael Holguin (University of Texas at El Paso, USA), Sai Mounika Errapotu (University of Texas at El Paso, USA) 208

Language Model based Methods for Cyber Security

Rejectable SoulBound Tokens for Credentials Assignment and Acceptance of Terms
Rosa Pericàs-Gornals (University of the Balearic Islands, Spain), Macià Mut-Puigserver (Universitat de les Illes Balears, Spain), María Magdalena Payeras-Capellà (Universidad de las Islas Baleares, Spain), Miquel Àngel Cabot-Nadal (University of the Balearic Islands, Spain), Jaume Ramis-Bibiloni (Universitat de les Illes Balears & Health Research Institute of the Balearic Islands (IdISBa), Spain) 212

Exploring Semantic vs. Syntactic Features for Unsupervised Learning on Application Log Files
Egil Alexander Thomas Karlsen (Dalhousie University, Canada), Rafael N Copstein (Dalhousie University, Canada), Xiao Luo (IUPUI, USA), Jeff Schwartzentruber (Dalhousie University, Canada), Bradley Niblett (2Keys Corporation - An Interac Company, Canada), Andrew Johnston (2Keys Corporation - An Interac Company, Canada), M. I. Heywood (Dalhousie University, Canada), Nur Zincir-Heywood (Dalhousie University, Canada) 219

NESec: A Modified-UI Honeyword Generation Strategy for Mitigating Targeted Guessing Attacks
Nilesh Chakraborty (Queen's University, Canada), Mohammad Shojafar (University of Surrey, United Kingdom (Great Britain)), Zhuangzhuang Chen (Shenzhen University, China), Victor C.M. Leung (Shenzhen University, China & The University of British Columbia, Canada), Jianqiang Li (Shenzhen University, China), Mohammad Zulkernine (Queen's University, Canada) 226

Cyber Security for Different Sectors

A Tree-Mapped Taxonomy of Blockchain Attacks
Emma Lubes (Rochester Institute of Technology, USA), Justin Pelletier (Rochester Institute of Technology, USA) 233

An Energy-Efficient Multiple-Factor Authentication Protocol for Critical Infrastructure IoT Systems
Mohammad Rasool Momeni (Concordia University, Canada), Abdollah Jabbari (Concordia University, Canada), Carol J Fung (Concordia University, Canada) 238