

7th International Conference on Information Systems Security and Privacy (ICISSP 2021)

Online
11-13 February 2021

Editors:

**Paolo Mori
Gabriele Lenzini
Steven Furnell**

ISBN: 978-1-7138-4016-9

Printed from e-media with permission by:

Curran Associates, Inc.
57 Morehouse Lane
Red Hook, NY 12571



Some format issues inherent in the e-media version may also appear in this print version.

Copyright© (2021) by SCITEPRESS – Science and Technology Publications, Lda.
All rights reserved.

Printed with permission by Curran Associates, Inc. (2021)

For permission requests, please contact SCITEPRESS – Science and Technology Publications, Lda.
at the address below.

SCITEPRESS – Science and Technology Publications, Lda.
Avenida de S. Francisco Xavier, Lote 7 Cv. C,
2900-616 Setúbal, Portugal

Phone: +351 265 520 185
Fax: +351 265520 186

info@scitepress.org

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
Email: curran@proceedings.com
Web: www.proceedings.com

BRIEF CONTENTS

INVITED SPEAKERS	IV
WORKSHOP CHAIRS	IV
ORGANIZING COMMITTEES	V
PROGRAM COMMITTEE	VI
AUXILIARY REVIEWERS	VII
WORKSHOP PROGRAM COMMITTEE	VIII
SELECTED PAPERS BOOK	VIII
FOREWORD	IX
CONTENTS	XI

CONTENTS

INVITED SPEAKERS

KEYNOTE SPEAKERS

- New Directions for High-throughput and High-security Communication 5
Adrian Perrig
- Practical and Provably Sound Static Analysis of Ethereum Smart Contracts 7
Matteo Maffei
- Accessible Cyber Security: The Next Frontier? 9
Karen Renaud

PAPERS

FULL PAPERS

- Who Stores the Private Key? An Exploratory Study about User Preferences of Key Management for Blockchain-based Applications 23
Clemens Brunner, Günther Eibl, Peter Fröhlich, Andreas Sackl and Dominik Engel
- Utilizing Keystroke Dynamics as Additional Security Measure to Protect Account Recovery Mechanism 33
Ahmed Anu Wahab, Daqing Hou, Stephanie Schuckers and Abbie Barbir
- On Security Analysis of Periodic Systems: Expressiveness and Complexity 43
Musab A. Alturki, Tajana Ban Kirigin, Max Kanovich, Vivek Nigam, Andre Scedrov and Carolyn Talcott
- Predicting Security Program Effectiveness in Bring-Your-Own-Device Deployment in Organizations 55
Alexander O. Akande and Vu N. Tran
- Automatic Detection of Cyber Security Events from Turkish Twitter Stream and Newspaper Data 66
Özgür Ural and Cengiz Acartürk
- Improvement of Secure Multi-Party Multiplication of (k, n) Threshold Secret Sharing using Only $N = k$ Servers 77
Ahmad Akmal Aminuddin Mohd Kamal and Keiichi Iwamura
- An Analytic Attack against ARX Addition Exploiting Standard Side-channel Leakage 89
Yan Yan, Elisabeth Oswald and Srinivas Vivek
- Bridging Knowledge Gaps in Security Analytics 98
Fabian Böhm, Manfred Vielberth and Günther Pernul
- The Comparison of Word Embedding Techniques in RNNs for Vulnerability Detection 109
Hai Ngoc Nguyen, Songpon Teerakanok, Atsuo Inomata and Tetsutaro Uehara
- A Permissioned Blockchain-based System for Collaborative Drug Discovery 121
Christoffer Olsson and Mohsen Toorani
- Checking Contact Tracing App Implementations 133
Robert Flood, Sheung Shi Chan, Wei Chen and David Aspinall

Optimizing Leak Detection in Open-source Platforms with Machine Learning Techniques <i>Sofiane Lounici, Marco Rosa, Carlo Maria Negri, Slim Trabelsi and Melek Önen</i>	145
Adversarial Machine Learning: A Comparative Study on Contemporary Intrusion Detection Datasets <i>Yulexis Pacheco and Weiqing Sun</i>	160
Automatic Detection and Decryption of AES by Monitoring S-Box Access <i>Josef Kokeš, Jonatan Matějka and Róbert Lórencz</i>	172
Parallel Privacy-preserving Computation of Minimum Spanning Trees <i>Mohammad Anagreh, Eero Vainikko and Peeter Laud</i>	181
Hydra: Practical Metadata Security for Contact Discovery, Messaging, and Dialing <i>David Schatz, Michael Rossberg and Guenter Schaefer</i>	191
Automated Black Box Detection of HTTP GET Request-based Access Control Vulnerabilities in Web Applications <i>Malte Kushnir, Olivier Favre, Marc Rennhard, Damiano Esposito and Valentin Zahnd</i>	204
A State Saturation Attack against Massively Multiplayer Online Videogames <i>Blake Bryant and Hossein Saiedian</i>	217
CyExec*: Automatic Generation of Randomized Cyber Range Scenarios <i>Ryotaro Nakata and Akira Otsuka</i>	226
From Exposed to Exploited: Drawing the Picture of Industrial Control Systems Security Status in the Internet Age <i>Yixiong Wu, Jianwei Zhuge, Tingting Yin, Tianyi Li, Junmin Zhu, Guannan Guo, Yue Liu and Jianju Hu</i>	237
Towards Academic and Skills Credentialing Standards and Distributed Ledger Technologies <i>Morné Pretorius, Nelisiwe Dlamini and Sthembile Mthethwa</i>	249
A Protection against the Extraction of Neural Network Models <i>Hervé Chabanne, Vincent Despiegel and Linda Guiga</i>	258
SHORT PAPERS	
Admonita: A Recommendation-based Trust Model for Dynamic Data Integrity <i>Wassnaa Al-Mawee, Steve Carr and Jean Mayo</i>	273
Experiences and Recommendations from Operating a Tor Exit Node at a University <i>Michael Sonntag and René Mayrhofer</i>	283
Mobile Robots: An Overview of Data and Security <i>Esmeralda Kadena, Huu Phuoc Dai Nguyen and Lourdes Ruiz</i>	291
Automatically Extracting Business Level Access Control Requirements from BPMN Models to Align RBAC Policies <i>Roman Pilipchuk, Robert Heinrich and Ralf Reussner</i>	300
Protecting Privacy during a Pandemic Outbreak <i>Karsten Martiny, Linda Briesemeister, Grit Denker, Mark St. John and Ron Moore</i>	308
Enhanced Information Management in Inter-organisational Planning for Critical Infrastructure Protection: Case and Framework <i>Christine Große</i>	319

Model-based Threat and Risk Assessment for Systems Design <i>Avi Shaked and Yoram Reich</i>	331
Towards Collaborative Cyber Threat Intelligence for Security Management <i>Oleksii Oслиak, Andrea Saracino, Fabio Martinelli and Theo Dimitrakos</i>	339
A Secure Network Scanner Architecture for Asset Management in Strongly Segmented ICS Networks <i>Matthias Niedermaier, Thomas Hanka, Florian Fischer and Dominik Merli</i>	347
Canopy: A Learning-based Approach for Automatic Low-and-Slow DDoS Mitigation <i>Lucas Cadalzo, Christopher H. Todd, Banjo Obayomi, W. Brad Moore and Anthony C. Wong</i>	356
Remote WebAuthn: FIDO2 Authentication for Less Accessible Devices <i>Paul Wagner, Kris Heid and Jens Heider</i>	368
Active Directory Kerberoasting Attack: Detection using Machine Learning Techniques <i>Lukáš Kotlaba, Simona Buchovecká and Róbert Lórencz</i>	376
Field Studies on the Impact of Cryptographic Signatures and Encryption on Phishing Emails <i>Stefanie Pham, Matthias Schopp, Lars Stiemert, Sebastian Seeber, Daniela Pöhn and Wolfgang Hommel</i>	384
Towards a Formalisation of Expert's Knowledge for an Automatic Construction of a Vulnerability Model of a Cyberphysical System <i>Witold Klaudel and Artur Rataj</i>	391
A Novel Simplified Framework to Secure IoT Communications <i>Sairath Bhattacharjya and Hossein Saiedian</i>	399
Linking Biometric Voice Identity with Self-monitoring Health Data as a Temporal-spatial Event Stored in a Mobile Device <i>Bon Sy</i>	407
DLP-Visor: A Hypervisor-based Data Leakage Prevention System <i>Guy Amit, Amir Yeshooroon, Michael Kiperberg and Nezer J. Zaidenberg</i>	416
Continuous Authentication based on Hand Micro-movement during Smartphone Form Filling by Seated Human Subjects <i>Aratrika Ray, Daqing Hou, Stephanie Schuckers and Abbie Barbir</i>	424
Blockchain based Secured Virtual Machine Image Monitor <i>Srijita Basu, Sandip Karmakar and Debasish Bera</i>	432
The Proposal of Double Agent Architecture using Actor-critic Algorithm for Penetration Testing <i>Hoang Viet Nguyen, Songpon Teerakanok, Atsuo Inomata and Tetsutaro Uehara</i>	440
Two Stage Anomaly Detection for Network Intrusion Detection <i>Helmut Neuschmied, Martin Winter, Katharina Hofer-Schmitz, Branka Stojanovic and Ulrike Kleb</i>	450
Ontology-based Cybersecurity and Resilience Framework <i>Helmar Hutschenreuter, Salva Daneshgاده Çakmakçı, Christian Maeder and Thomas Kemmerich</i>	458
Study of Intra- and Inter-user Variance in Password Keystroke Dynamics <i>Blaine Ayotte, Mahesh K. Banavar, Daqing Hou and Stephanie Schuckers</i>	467

Windows Malware Binaries in C/C++ GitHub Repositories: Prevalence and Lessons Learned <i>William La Cholter, Matthew Elder and Antonius Stalick</i>	475
Implementation of Secondary Available Digital Content Protection Schemes using Identity-based Signatures <i>Nozomi Nagashima, Masaki Inamura and Keiichi Iwamura</i>	485
Towards an Ontology for Enterprise Level Information Security Policy Analysis <i>Debashis Mandal and Chandan Mazumdar</i>	492
Enabling Monetization of Depreciating Data on Blockchains <i>Christian Dahdah, Coline Van Leeuwen, Ziad Kheil, Jérôme Lacan, Jonathan Detchart and Thibault Gateau</i>	500
Profiling and Discriminating of Containerized ML Applications in Digital Data Marketplaces (DDM) <i>Lu Zhang, Reginald Cushing, Ralph Koning, Cees de Laat and Paola Grosso</i>	508
Representation of PE Files using LSTM Networks <i>Martin Jureček and Matouš Kozák</i>	516
Understanding How People Weigh the Costs and Benefits of using Facebook <i>Jack McClary and Sid Stamm</i>	526
How to Improve the GDPR Compliance through Consent Management and Access Control <i>Said Daoudagh, Eda Marchetti, Vincenzo Savarino, Roberto Di Bernardo and Marco Alessi</i>	534
Sociocultural Influences for Password Definition: An AI-based Study <i>Carlos Ocanto Dávila, Rocío Cabrera Lozoya and Slim Trabelsi</i>	542
Efficient Semantic Representation of Network Access Control Configuration for Ontology-based Security Analysis <i>Florian Patzer and Jürgen Beyerer</i>	550
A Lemon by Any Other Label <i>Vaibhav Garg</i>	558
Implementing Secure Applications Thanks to an Integrated Secure Element <i>Sylvain Guilley, Michel Le Rolland and Damien Quenson</i>	566
An Asynchronous Federated Learning Approach for a Security Source Code Scanner <i>Sabrina Kall and Slim Trabelsi</i>	572
HyperPass: Secure Password Input Platform <i>Michael Kiperberg and Nezer J. Zaidenberg</i>	580
Detecting Cyber Security Attacks against a Microservices Application using Distributed Tracing <i>Stephen Jacob, Yuansong Qiao and Brian Lee</i>	588
Stopping DNS Rebinding Attacks in the Browser <i>Mohammadreza Hazhirpasand, Arash Ale Ebrahim and Oscar Nierstrasz</i>	596
Securing the Linux Boot Process: From Start to Finish <i>Jakob Hagl, Oliver Mann and Martin Pirker</i>	604
Leveraging Dynamic Information for Identity and Access Management: An Extension of Current Enterprise IAM Architecture <i>Alexander Puchta, Sebastian Groll and Günther Pernul</i>	611

Dreaming of Keys: Introducing the Phantom Gradient Attack <i>Åvald Åslaugson Sommervoll</i>	619
Towards Exploring User Perception of a Privacy Sensitive Information Detection Tool <i>Vanessa Bracamonte, Welderufael B. Tesfay and Shinsaku Kiyomoto</i>	628
Evaluation of Vulnerability Reproducibility in Container-based Cyber Range <i>Ryotaro Nakata and Akira Otsuka</i>	635
Improving Classification of Malware Families using Learning a Distance Metric <i>Martin Jureček, Olha Jurečková and Róbert Lórencz</i>	643
A Dynamic Access Control System based on Situations of Users <i>Hirokazu Hasegawa and Hiroki Takakura</i>	653
An Overview of Cryptographic Accumulators <i>Ilker Ozelik, Sai Medury, Justin Broaddus and Anthony Skjellum</i>	661
MADLIRA: A Tool for Android Malware Detection <i>Khanh Huu The Dam and Tayssir Touili</i>	670
Securing Orchestrated Containers with BSI Module SYS.1.6 <i>Christoph Haar and Erik Buchmann</i>	676
Privacy Preserving Services for Intelligent Transportation Systems with Homomorphic Encryption <i>Ayemen Boudguiga, Oana Stan, Abdessamad Fazzat, Houda Labiod and Pierre-Emmanuel Clet</i>	684
Security Property Modeling <i>Hiba Hnaini, Luka Le Roux, Joel Champeau and Ciprian Teodorov</i>	694
Developing Cyber-risk Centric Courses and Training Material for Cyber Ranges: A Systematic Approach <i>Gencer Erdogan, Antonio Álvarez Romero, Niccolò Zazzeri, Anže Žitnik, Mariano Basile, Giorgio Aprile, Mafalda Osório, Claudia Pani and Ioannis Kechaoglou</i>	702
Release-aware In-out Encryption Adjustment in MongoDB Query Processing <i>Maryam Almarwani, Boris Konev and Alexei Lisitsa</i>	714
Learning from Smartphone Location Data as Anomaly Detection for Behavioral Authentication through Deep Neuroevolution <i>Mhd Irvan, Tran Phuong Thao, Ryosuke Kobayashi, Toshiyuki Nakata and Rie Shigetomi Yamaguchi</i>	723

**5TH INTERNATIONAL WORKSHOP ON FORMAL METHODS FOR SECURITY
ENGINEERING**

FULL PAPERS

Malware Classification with Word Embedding Features <i>Aparna Sunil Kale, Fabio Di Troia and Mark Stamp</i>	733
Malware Classification using Long Short-term Memory Models <i>Dennis Dang, Fabio Di Troia and Mark Stamp</i>	743
Malware Classification with GMM-HMM Models <i>Jing Zhao, Samanvitha Basole and Mark Stamp</i>	753
Unconventional Attack against Voting Machines Enlarging the Scope of Cybersecurity Risk Analysis <i>Eric Filiol</i>	763
A New Dataset for Smartphone Gesture-based Authentication <i>Elliu Huang, Fabio Di Troia, Mark Stamp and Preethi Sundaravaradhan</i>	771
On Formalising and Analysing the Tweekchain Protocol <i>Mariapia Raimondo, Simona Bernardi and Stefano Marrone</i>	781
Experimental Evaluation of Description Logic Concept Learning Algorithms for Static Malware Detection <i>Peter Švec, Štefan Balogh and Martin Homola</i>	792
Towards Formal Security Verification of Over-the-Air Update Protocol: Requirements, Survey and UpKit Case Study <i>Christophe Ponsard and Denis Darquennes</i>	800
SHORT PAPER	
Colluding Covert Channel for Malicious Information Exfiltration in Android Environment <i>Rosangela Casolare, Fabio Martinelli, Francesco Mercaldo and Antonella Santone</i>	811
AUTHOR INDEX	819