

LNCS 13285

Jianying Zhou · Sridhar Adepu · Cristina Alcaraz ·  
Lejla Batina · Emiliano Casalicchio ·  
Sudipta Chattopadhyay · Chenglu Jin · Jingqiang Lin ·  
Eleonora Losiouk · Suryadipta Majumdar · Weizhi Meng ·  
Stjepan Picek · Jun Shao · Chunhua Su ·  
Cong Wang · Yury Zhauniarovich · Saman Zonouz (Eds.)

# Applied Cryptography and Network Security Workshops

ACNS 2022 Satellite Workshops  
AIBlock, AIHWS, AIoTS, CIMSS, Cloud S&P, SCI, SecMT, SiMLA  
Rome, Italy, June 20–23, 2022, Proceedings

## Founding Editors

Gerhard Goos

*Karlsruhe Institute of Technology, Karlsruhe, Germany*

Juris Hartmanis

*Cornell University, Ithaca, NY, USA*


## Editorial Board Members

Elisa Bertino

*Purdue University, West Lafayette, IN, USA*

Wen Gao

*Peking University, Beijing, China*

Bernhard Steffen 

*TU Dortmund University, Dortmund, Germany*

Moti Yung 

*Columbia University, New York, NY, USA*


More information about this series at <https://link.springer.com/bookseries/558>


Jianying Zhou · Sridhar Adepu ·  
Cristina Alcaraz · Lejla Batina ·  
Emiliano Casalicchio · Sudipta Chattopadhyay ·  
Chenglu Jin · Jingqiang Lin ·  
Eleonora Losiouk · Suryadipta Majumdar ·  
Weizhi Meng · Stjepan Picek ·  
Jun Shao · Chunhua Su ·  
Cong Wang · Yury Zhauniarovich ·  
Saman Zonouz (Eds.)


# Applied Cryptography and Network Security Workshops

ACNS 2022 Satellite Workshops  
AIBlock, AIHWS, AIoTS, CIMSS, Cloud S&P, SCI, SecMT, SiMLA  
Rome, Italy, June 20–23, 2022  
Proceedings


### *Editors*

Jiaying Zhou   
Singapore University of Technology  
and Design  
Singapore, Singapore

Cristina Alcaraz   
University of Malaga  
Malaga, Spain


Emiliano Casalicchio   
Sapienza University of Rome  
Rome, Roma, Italy

Chenglu Jin   
Centrum Wiskunde & Informatica  
Amsterdam, The Netherlands


Eleonora Losiouk   
University of Padua  
Padua, Italy

Weizhi Meng   
Technical University Denmark  
Kongens Lyngby, Denmark


Jun Shao  
Zhejiang Gongshang University  
Hangzhou, China


Cong Wang   
City University of Hong Kong  
Hong Kong, Hong Kong


Saman Zonouz  
Rutgers University  
Piscataway, NJ, USA

Sridhar Adepu   
University of Bristol  
Bristol, UK

Lejla Batina   
Radboud University Nijmegen  
Nijmegen, The Netherlands


Sudipta Chattopadhyay   
Singapore University of Technology  
and Design  
Singapore, Singapore

Jingqiang Lin   
University of Science and Technology  
of China  
Hefei, China

Suryadipta Majumdar   
Concordia University  
Montreal, QC, Canada

Stjepan Picsek   
Delft University of Technology  
Delft, The Netherlands

Chunhua Su   
University of Aizu  
Aizu-Wakamatsu, Japan

Yury Zhauniarovich   
Delft University of Technology  
Delft, The Netherlands

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-031-16814-7

ISBN 978-3-031-16815-4 (eBook)

<https://doi.org/10.1007/978-3-031-16815-4>

© The Editor(s) (if applicable) and The Author(s), under exclusive license  
to Springer Nature Switzerland AG 2022

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG  
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

# Preface

The proceedings contain the papers selected for presentation at the ACNS 2022 satellite workshops, which were held in parallel with the main conference (the 20th International Conference on Applied Cryptography and Network Security) during June 20–23, 2022. Due to the ongoing COVID-19 crisis, ACNS 2022 was held in Rome, Italy, in a hybrid mode while the workshops were organized as online events.

In response to this year’s call for workshop proposals, there were eight satellite workshops, the same as last year. Each workshop provided a forum to address a specific topic at the forefront of cybersecurity research.

- 4th Workshop on Application Intelligence and Blockchain Security (AIBlock 2022), chaired by Weizhi Meng and Chunhua Su
- 3rd Workshop on Artificial Intelligence in Hardware Security (AIHWS 2022), chaired by Lejla Batina and Stjepan Picek
- 4th Workshop on Artificial Intelligence and Industrial IoT Security (AIoTS 2022), chaired by Sridhar Adepu and Cristina Alcaraz
- 2nd Workshop on Critical Infrastructure and Manufacturing System Security (CIMSS 2022), chaired by Chenglu Jin and Saman Zonouz
- 4th Workshop on Cloud Security and Privacy (Cloud S&P 2022), chaired by Suryadipta Majumdar and Cong Wang
- 3rd Workshop on Secure Cryptographic Implementation (SCI 2022), chaired by Jingqiang Lin and Jun Shao
- 3rd Workshop on Security in Mobile Technologies (SecMT 2022), chaired by Eleonora Losiouk and Yury Zhauniarovich
- 4th Workshop on Security in Machine Learning and its Applications (SiMLA 2022), chaired by Sudipta Chattopadhyay

This year, we received a total of 52 submissions. Each workshop had its own Program Committee (PC) in charge of the review process. These papers were evaluated on the basis of their significance, novelty, and technical quality. The review process was double-blind. In the end, 31 papers were selected for presentation at the eight workshops, with an acceptance rate of 60%.

ACNS also gave the best workshop paper award. The winning papers were selected among the nominated candidate papers from each workshop. The following two papers shared the ACNS 2022 Best Workshop Paper Award. They will also receive the monetary prize sponsored by Frontiers.

- Yuanyuan Zhou and Francois-Xavier Standaert. “S-box Pooling: Towards More Efficient Side-Channel Security Evaluations” from the AIHWS workshop
- Thijs Heijligenberg, Oualid Lkhaoui, and Katharina Kohls. “Leaky Blinders: Information Leakage in Mobile VPNs” from the SecMT workshop

This year Frontiers specifically sponsored a best AIoTS workshop paper award. The program chairs of the AIoTS workshop selected the following paper for the award.

- Alessandro Visintin, Flavio Toffalini, Eleonora Losiouk, Mauro Conti, and Jianying Zhou. “HolA: Holistic and Autonomous Attestation for IoT Networks”

Besides the regular papers presented at the workshops, there were 14 invited talks.

- “Towards Decentralized Privacy-Preserving Application Intelligence” by S. M. Chow (Chinese University of Hong Kong, Hong Kong SAR, China) at the AIBlock workshop
- “Homomorphic Computing: Achieving the Pinnacle of Data Privacy” by Rosario Cammarota (Intel, USA) and “A Fault Can Do Wonders: On Advanced Fault Attacks on Protection Mechanisms, Post-Quantum Cryptography and Deep Learning” by Shivam Bhasin (NTU, Singapore) at the AIHWS workshop
- “Fusing AI and Design to Protect Critical Infrastructure” by Aditya P. Mathur (SUTD, Singapore) and “Trustworthy AI for Securing CPS” by Tingting Li (Cardiff University, UK) at the AIoTS workshop
- “Oh What a Tangled Web We Weave - Securing ICS Networks” by Nils Ole Tippenhauer (CISPA, Germany) and “Urban Water Infrastructure: Challenges and Smart Solutions” by Zoran Kapelan (TU Delft, The Netherlands) at the CIMSS workshop
- “Notions of Security and Trust in Virtualized Infrastructures” by Vijay Varadharajan (University of Newcastle, Australia) and “Vulnerability Detection for Emerging Technologies” by Paria Shirani (Toronto Metropolitan University, Canada) at the Cloud S&P workshop
- “Hey... it’s a PDF. What can go wrong?” by Christian Mainka and Vladislav Mladenov (Ruhr University Bochum, Germany) at the SCI workshop
- “Trust, But Verify: A Longitudinal Analysis of Android OEM Compliance and Customization” by Simone Aonzo (EURECOM, France) and “From the Analysis of Mobile Apps to the Analysis of the Mobile Ecosystem” by Antonio Bianchi (Purdue University, USA) at the SecMT workshop
- “Towards Trustworthy AI” by Jun Sun (SMU, Singapore) at the SiMLA workshop

There was also a poster session chaired by Emiliano Casalicchio. Five posters were included in the proceedings in the form of extended abstracts.

The ACNS 2022 workshops were made possible by the joint efforts of many individuals and organizations. We sincerely thank the authors of all submissions. We are grateful to the program chairs and PC members of each workshop for their great effort in providing professional reviews and interesting feedback to authors in a tight time schedule. We thank all the external reviewers for assisting the PC in their particular areas of expertise. We are grateful to Frontiers for sponsoring the workshops. We also thank General Chairs Mauro Conti and Angelo Spognardi and the organizing team members of the main conference as well as each workshop for their help in various aspects.

Last but not least, we thank everyone else, speakers, session chairs, and attendees for their contribution to the success of the ACNS 2022 workshops. We are glad to see the workshops have become an important part of ACNS and provide a stimulating

platform to discuss open problems at the forefront of cybersecurity research. We would expect that in-person workshops will return in 2023.

June 2022

Jiaying Zhou  
ACNS 2022 Workshop Chair





# AIHWS 2022

## Third Workshop on Artificial Intelligence in Hardware Security

21 June 2022

### Program Chairs

Lejla Batina  
Stjepan Picek

Radboud University, The Netherlands  
Radboud University, The Netherlands

### Program Committee

Aydin Aysu  
Ileana Buhan  
Lukasz Chmielewski  
Chitchanok

North Carolina State University, USA  
Radboud University, The Netherlands  
Radboud University, The Netherlands  
University of Adelaide, Australia

Chuengsatiansup

Elena Dubrova

KTH Royal Institute of Technology, Sweden

Baris Ege

Riscure B.V., The Netherlands

Fatemeh Ganji

Worcester Polytechnic Institute, USA

Naofumi Homma

Tohoku University, Japan

Xiaolu Hou

Slovak University of Technology, Slovakia

Dirmanto Jap

Nanyang Technological University, Singapore

Luca Mariot

Radboud University, The Netherlands

Tsunato Nakai

Mitsubishi Electric Corp., Japan

Kostas Papagiannopoulos

University of Amsterdam, The Netherlands

Guilherme Perin

TU Delft, The Netherlands

Kazuo Sakiyama

University of Electro-Communications, Japan

Shahin Tajik

Worcester Polytechnic Institute, USA

Vincent Verneuil

NXP Semiconductors, Germany

Lichao Wu

TU Delft, The Netherlands

Zhengyu Zhao

CISPA Helmholtz Center for Information Security,  
Germany

### Publicity Chair

Marina Krcek

Delft University of Technology, The Netherlands

# AIoTS 2022

## Fourth Workshop on Artificial Intelligence and Industrial IoT Security

23 June 2022

### Program Chairs

Sridhar Adepu                      University of Bristol, UK  
Cristina Alcaraz                    University of Malaga, Spain

### Web Chair

Chuahdhy Mujeeb Ahmed        University of Strathclyde, UK

### Publicity Chair

Sergio Gonzalez                    University of Malaga, Spain

### Program Committee

Magnus Almgren                    Chalmers University, Sweden  
John Castellanos                    CISPA, Germany  
Luca Davoli                          University of Parma, Italy  
Sriharsha Etigowni                 Purdue University, USA  
Luis Garcia                          University of Southern California, USA  
Joseph Gardiner                    University of Bristol, UK  
Amrita Ghosal                        University of Limerick, Ireland  
Jairo Giraldo                        University of Utah, USA  
Shiyan Hu                            University of Southampton, UK  
Nandha Kumar Kandasamy        Singapore Institute of Technology, Singapore  
Marina Krotofil                      Maersk, UK  
Subhash Lakshminarayana        University of Warwick, UK  
Qin Lin                                Carnegie Mellon University, USA  
Rajib Ranjan Maiti                    Birla Institute of Technology, India  
Daisuke Mashima                    Advanced Digital Sciences Center, Singapore  
Weizhi Meng                        Technical Universtiy of Denmark, Denmark  
Alma Oracevic                        University of Bristol, UK  
Federica Pascucci                    Università degli Studi Roma Tre, Italy  
Christopher M. Poskitt              Singapore Management University, Singapore  
Neetesh Saxena                        Cardiff University, UK  
Zheng Yang                          Southwest University, China  
Urko Zurutuza                        Mondragon University, Spain

# CIMSS 2022

## Second Workshop on Critical Infrastructure and Manufacturing System Security

20 June 2022

### Program Chairs

Chenglu Jin  
Saman Zonouz

CWI Amsterdam, The Netherlands  
Georgia Institute of Technology, USA

### Publicity Chair

Zheng Yang

Southwest University, China

### Program Committee

Irfan Ahmed  
Cristina Alcaraz  
Binbin Chen

Virginia Commonwealth University, USA  
University of Malaga, Spain  
Singapore University of Technology and Design,  
Singapore

Long Cheng  
Jairo Giraldo  
Charalambos Konstantinou

Clemson University, USA  
University of Utah, USA  
King Abdullah University of Science and Technology,  
Saudi Arabia

Andres Murillo

Singapore University of Technology and Design,  
Singapore

Marco Rocchetto  
Carlos Rubio-Medrano  
Alexandru Stefanov  
Richard J. Thomas  
Mark Yampolskiy  
Zheng Yang

V-Research, Italy  
Texas A&M University - Corpus Christi, USA  
Delft University of Technology, The Netherlands  
University of Birmingham, UK  
Auburn University, USA  
Southwest University, China

# **CLOUD S&P 2022**

## **Fourth Workshop on Cloud Security and Privacy**

22 June 2022

### **Program Chairs**

Suryadipta Majumdar  
Cong Wang

Concordia University, Canada  
City University of Hong Kong, HK SAR, China

### **Program Committee**

Irfan Ahmed  
Prabir Bhattacharya  
Mauro Conti  
Helei Cui  
Nora Cuppens  
Sabrina De Capitani  
di Vimercati  
Carol Fung  
Yosr Jarraya  
Kallol Krishna Karmakar  
Rongxing Lu  
Taous Madi

Virginia Commonwealth University, USA  
Thomas Edison State University, USA  
University of Padua, Italy  
Northwestern Polytechnical University, China  
École Polytechnique de Montréal, Canada  
Università degli Studi di Milano, Italy  
  
Concordia University, Canada  
Ericsson Security, Sweden  
University of Newcastle, UK  
University of New Brunswick, Canada  
King Abdullah University of Science and Technology,  
Saudi Arabia

Makan Pourzandi  
Pierangela Samarati  
Paria Shirani  
Lingyu Wang  
Xingliang Yuan  
Mengyuan Zhang

Ericsson Security, Sweden  
Università degli Studi di Milano, Italy  
Ryerson University, Canada  
Concordia University, Canada  
Monash University, Australia  
Hong Kong Polytechnic University, HK SAR, China

### **Additional Reviewers**

Mohammad Ekramul Kabir  
Riccardo Lazzeretti

Concordia University, Canada  
Sapienza Università di Roma, Italy

# SCI 2022

## Third Workshop on Secure Cryptographic Implementation

23 June 2022

### Program Chairs

Jingqiang Lin  
Jun Shao

University of Science and Technology of China, China  
Zhejiang Gongshang University, China

### Publication Chair

Bo Luo

University of Kansas, USA

### Publicity Chairs

Hao Peng  
Fangyu Zheng

Zhejiang Normal University, China  
Chinese Academy of Sciences, China

### Program Committee

Florian Caullery  
Bo Chen  
Jiankuo Dong

HENSOLDT Cyber GmbH, Germany  
Michigan Technological University, USA  
Nanjing University of Posts and Telecommunications,  
China

Niall Emmart  
Johann Großschädl  
Miroslaw Kutylowski  
Bingyu Li  
Fengjun Li  
Ximeng Liu  
Rongxing Lu  
Chunli Lv  
Di Ma  
Yuan Ma  
Ziqiang Ma  
Zhiguo Wan  
Ding Wang  
Juan Wang  
Fan Zhang  
Fangyu Zheng  
Cong Zuo

NVIDIA Corporation, USA  
University of Luxembourg, Luxembourg  
Wroclaw University of Technology, Poland  
Beihang University, China  
University of Kansas, USA  
Fuzhou University, China  
University of New Brunswick, Canada  
China Agricultural University, China  
ZDNS, China  
Chinese Academy of Sciences, China  
Ningxia University, China  
Shandong University, China  
Nankai University, China  
Wuhan University, China  
Zhejiang University, China  
Chinese Academy of Sciences, China  
Nanyang Technological University, Singapore

# **SecMT 2022**

## **Third Workshop on Security in Mobile Technologies**

20 June 2022

### **Program Chairs**

Eleonora Losiouk  
Yury Zhauniarovich

University of Padua, Italy  
Delft University of Technology, The Netherlands

### **Program Committee**

Yazan Boshmaf  
Marco Casagrande  
Flavio Toffalini  
Giorgos Vasiliadis

Hamad Bin Khalifa University, Qatar  
EURECOM, France  
EPFL, Switzerland  
Hellenic Mediterranean University and FORTH-ICS,  
Greece

# **SiMLA 2022**

## **Fourth Workshop on Security in Machine Learning and its Applications**

22 June 2022

### **Program Chair**

Sudipta Chattopadhyay      Singapore University of Technology and Design,  
Singapore

### **Web Chair**

Sakshi Udeshi      Singapore University of Technology and Design,  
Singapore

### **Publicity Chair**

Ezekiel Soremekun      University of Luxembourg, Luxembourg

### **Program Committee**

Amir Aminifar	Lund University, Sweden
Shuang Liu	Tianjin University, China
Chris Poskitt	Singapore Management University, Singapore
Ahmed Rezine	Linköping University, Sweden
Ezekiel Soremekun	University of Luxembourg, Luxembourg
Jingyi Wang	Zhejiang University, China



# Contents

## **AIBlock – Application Intelligence and Blockchain Security**

Universal Physical Adversarial Attack via Background Image. . . . .	3
<i>Yidan Xu, Juan Wang, Yuanzhang Li, Yajie Wang, Zixuan Xu, and Dianxin Wang</i>	
Efficient Verifiable Boolean Range Query for Light Clients on Blockchain Database. . . . .	15
<i>Jianpeng Gong, Jiaojiao Wu, Jianfeng Wang, and Shichong Tan</i>	
SuppliedTrust: A Trusted Blockchain Architecture for Supply Chains . . . . .	36
<i>Yong Zhi Lim, Jianying Zhou, and Martin Saerbeck</i>	
Towards Interpreting Vulnerability of Object Detection Models via Adversarial Distillation. . . . .	53
<i>Yaoyuan Zhang, Yu-an Tan, Mingfeng Lu, Lu Liu, Quanxing Zhang, Yuanzhang Li, and Dianxin Wang</i>	
Vulnerability Detection for Smart Contract via Backward Bayesian Active Learning . . . . .	66
<i>Jiale Zhang, Liangqiong Tu, Jie Cai, Xiaobing Sun, Bin Li, Weitong Chen, and Yu Wang</i>	
A Multi-agent Deep Reinforcement Learning-Based Collaborative Willingness Network for Automobile Maintenance Service. . . . .	84
<i>Shengang Hao, Jun Zheng, Jie Yang, Ziwei Ni, Quanxin Zhang, and Li Zhang</i>	
Hybrid Isolation Model for Device Application Sandboxing Deployment in Zero Trust Architecture . . . . .	104
<i>Jingci Zhang, Jun Zheng, Zheng Zhang, Tian Chen, Kefan Qiu, Quanxin Zhang, and Yuanzhang Li</i>	

## **AIHWS – Artificial Intelligence in Hardware Security**

On the Effect of Clock Frequency on Voltage and Electromagnetic Fault Injection . . . . .	127
<i>Stefanos Koffas and Praveen Kumar Vadnala</i>	
S-box Pooling: Towards More Efficient Side-Channel Security Evaluations . . . . .	146
<i>Yuanyuan Zhou and François-Xavier Standaert</i>	

Deep Learning-Based Side-Channel Analysis Against AES Inner Rounds. . . . .	165
<i>Sudharshan Swaminathan, Łukasz Chmielewski, Guilherme Perin, and Stjepan Picek</i>	
A Side-Channel Based Disassembler for the ARM-Cortex M0 . . . . .	183
<i>Jurian van Geest and Ileana Buhan</i>	
Towards Isolated AI Accelerators with OP-TEE on SoC-FPGAs . . . . .	200
<i>Tsumato Nakai, Daisuke Suzuki, and Takeshi Fujino</i>	
Order vs. Chaos: Multi-trunk Classifier for Side-Channel Attack . . . . .	218
<i>Praveen Kulkarni and Vincent Verneuil</i>	
<b>AIoTS – Artificial Intelligence and Industrial IoT Security</b>	
Framework for Calculating Residual Cybersecurity Risk of Threats to Road Vehicles in Alignment with ISO/SAE 21434 . . . . .	235
<i>Ahmed Khan, Jeremy Bryans, and Giedre Sabaliauskaite</i>	
Output Prediction Attacks on Block Ciphers Using Deep Learning . . . . .	248
<i>Hayato Kimura, Keita Emura, Takanori Isobe, Ryoma Ito, Kazuto Ogawa, and Toshihiro Ohigashi</i>	
HOLA: Holistic and Autonomous Attestation for IoT Networks . . . . .	277
<i>Alessandro Visintin, Flavio Toffalini, Eleonora Losiouk, Mauro Conti, and Jianying Zhou</i>	
<b>CIMSS – Critical Infrastructure and Manufacturing System Security</b>	
The Etiology of Cybersecurity . . . . .	299
<i>Michele Ambrosi, Francesco Beltramini, Federico De Meo, Oliviero Nardi, Mattia Pacchin, and Marco Rocchetto</i>	
Outsider Key Compromise Impersonation Attack on a Multi-factor Authenticated Key Exchange Protocol . . . . .	320
<i>Zhiqiang Ma and Jun He</i>	
Toward Safe Integration of Legacy SCADA Systems in the Smart Grid. . . . .	338
<i>Aldar C.-F. Chan and Jianying Zhou</i>	
<b>Cloud S&amp;P – Cloud Security and Privacy</b>	
RATLS: Integrating Transport Layer Security with Remote Attestation . . . . .	361
<i>Robert Walther, Carsten Weinhold, and Michael Roitzsch</i>	
DLPFS: The Data Leakage Prevention FileSystem . . . . .	380
<i>Stefano Braghin, Marco Simioni, and Mathieu Sinn</i>	

Privacy-Preserving Record Linkage Using Local Sensitive Hash  
and Private Set Intersection . . . . . 398  
*Allon Adir, Ehud Aharoni, Nir Drucker, Eyal Kushnir, Ramy Masalha,  
Michael Mirkin, and Omri Soceanu*

**SCI – Secure Cryptographic Implementation**

UniqueChain: Achieving (Near) Optimal Transaction Settlement Time  
via Single Leader Election . . . . . 427  
*Peifang Ni and Jing Xu*

PEPEC: Precomputed ECC Points Embedded in Certificates and Verified  
by CT Log Servers . . . . . 447  
*Guangshen Cheng, Jiankuo Dong, Xinyi Ji, Bingyu Li, Haoling Fan,  
and Pinchang Zhang*

Efficient Software Implementation of GMT6-672 and GMT8-542 Pairing-  
Friendly Curves for a 128-Bit Security Level . . . . . 461  
*Zihao Song, Junichi Sakamoto, Shigeo Mitsunari, Naoki Yoshida,  
Riku Anzai, and Tsutomu Matsumoto*

**SecMT – Security in Mobile Technologies**

Leaky Blinders: Information Leakage in Mobile VPNs . . . . . 481  
*Thijs Heijligenberg, Oualid Lkhaoui, and Katharina Kohls*

Instrumentation Blueprints: Towards Combining Several Android  
Instrumentation Tools . . . . . 495  
*Arthur van der Staaij and Olga Gadyatskaya*

**SiMLA – Security in Machine Learning and its Applications**

A Siamese Neural Network for Scalable Behavioral Biometrics  
Authentication . . . . . 515  
*Jesús Solano, Esteban Rivera, Lizzy Tengana, Christian López,  
Johana Flórez, and Martín Ochoa*

A Methodology for Training Homomorphic Encryption Friendly  
Neural Networks. . . . . 536  
*Moran Baruch, Nir Drucker, Lev Greenberg, and Guy Moshkovich*

Scalable and Secure HTML5 Canvas-Based User Authentication. . . . . 554  
*Esteban Rivera, Lizzy Tengana, Jesús Solano, Christian López,  
Johana Flórez, and Martín Ochoa*

**Android Malware Detection Using BERT** . . . . . 575  
*Badr Souani, Ahmed Khanfir, Alexandre Bartel, Kevin Allix,  
and Yves Le Traon*

**POSTERS**

**POSTER: A Transparent Remote Quantum Random Number Generator  
over a Quantum-Safe Link** . . . . . 595  
*Sergejs Kozlovičs and Juris Vīksna*

**POSTER: Enabling User-Accountable Mechanisms in Decision Systems** . . . . 600  
*Rosario Giustolisi and Carsten Schürmann*

**Poster: Key Generation Scheme Based on Physical Layer** . . . . . 606  
*Hong Zhao and Chunhua Su*

**POSTER: ODABE: Outsourced Decentralized CP-ABE in Internet  
of Things** . . . . . 611  
*Mohammed B. M. Kamel, Peter Ligeti, and Christoph Reich*

**POSTER: Ransomware Detection Mechanism – Current State  
of the Project** . . . . . 616  
*Michał Glet and Kamil Kaczyński*

**Author Index** . . . . . 621