9th International Conference on Information Systems Security and Privacy (ICISSP 2023)

Lisbon, Portugal
22-24 February 2023

Editors:

Paolo Mori
Gabriele Lenzini
Steven Furnell

ISBN: 978-1-7138-7659-5

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.

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

CONTENTS

INVITED SPEAKERS

KEYNOTE SPEAKERS

Usable Security: Security 'Warnings' 2.0 5
Melanie Volkamer

Cybersecurity, Nicolas Cage and Peppa Pig 7
Luca Viganò

INVITED LECTURE

Protecting IoT Ecosystems and AI Leveraging TCG Standards 11
Thorsten Stremlau

PAPERS

FULL PAPERS

IVNPROTECT: Isolable and Traceable Lightweight CAN-Bus Kernel-Level Protection for Securing in-Vehicle Communication 17
Shuji Ohira, Kibrom Desta Araya, Ismail Arai and Kazutoshi Fujikawa

Towards a Rust SDK for Keystone Enclave Application Development 29
Jukka Julku and Markku Kylänpää

Tracing Cryptographic Agility in Android and iOS Apps 38
Kris Heid, Jens Heider, Matthias Ritscher and Jan-Peter Stotz

Veto: Prohibit Outdated Edge System Software from Booting 46
Jonas Röckl, Adam Wagenhäuser and Tilo Müller

Clipaha: A Scheme to Perform Password Stretching on the Client 58
Francisco Blas Izquierdo Riera, Magnus Almgren, Pablo Picazo-Sanchez and Christian Rohner

Automating XSS Vulnerability Testing Using Reinforcement Learning 70
Kento Hasegawa, Seira Hidano and Kazuhide Fukushima

An Efficient Unified Architecture for Polynomial Multiplications in Lattice-Based Cryptoschemes 81
Francesco Antognazza, Alessandro Barenghi, Gerardo Pelosi and Ruggero Susella

Use-Case Denial of Service Attack on Actual Quantum Key Distribution Nodes 89
Patrik Burdiak, Emir Dervisevic, Amina Tankovic, Filip Lauterbach, Jan Rozhon, Lukas Kapicak, Libor Michalek, Dzana Pivac, Merima Fehric, Enio Kaljic, Mirza Hamza, Miralem Mehic and Miroslav Voznak

A Systematic Review of Secure IoT Data Sharing 95
Thanh Thao Thi Tran, Phu H. Nguyen and Gencer Erdogan

Dark Ending: What Happens when a Dark Web Market Closes down 106
Yichao Wang, Budi Arief and Julio Hernandez-Castro

Data Leakage in Isolated Virtualized Enterprise Computing Systems 118
Zechariah Wolf, Eric C. Larson and Mitchell A. Thornton

Exploring False Demand Attacks in Power Grids with High PV Penetration 124
Ashish Neupane and Weiqing Sun

SPA Attack on NTRU Protected Implementation with Sparse Representation of Private Key 135
Tomáš Rabas, Jiří Buček and Róbert Lórencz

XMeDNN: An Explainable Deep Neural Network System for Intrusion Detection in Internet of Medical Things 144
Mohammed M. Alani, Atefeh Mashatan and Ali Miri

A Stochastic Game Model for Cloud Platform Security 152
Lu Li, Lisheng Huang, Guanling Zhao, Kai Shi and Fengjun Zhang

Systematic Literature Review of Threat Modeling Concepts 163
Pedro Alfradique Lohmann, Carlos Albuquerque and Raphael Machado

On the Use of Multiple Approximations in the Linear Cryptanalysis of Baby Rijndael 174
Josef Kokeš and Róbert Lórencz

Automating Vehicle SOA Threat Analysis Using a Model-Based Methodology 180
Yuri Gil Dantas, Simon Barner, Pei Ke, Vivek Nigam and Ulrich Schöpp

PDIFT: A Practical Dynamic Information-Flow Tracker 192
Michael Kiperberg, Aleksei Rozman, Aleksei Kuraev and Nezer Zaidenberg

t.ex-Graph: Automated Web Tracker Detection Using Centrality Metrics and Data Flow Characteristics 199
Philip Raschke, Patrick Herbke and Henry Schwerdtner

Secure Joint Querying Over Federated Graph Databases Utilising SMPC Protocols 210
Nouf Al-Juaid, Alexei Lisitsa and Sven Schewe

Automata-Based Study of Dynamic Access Control Policies 218
Ahmed Khoumsi

A Framework for Assessing Decompiler Inference Accuracy of Source-Level Program Constructs 228
Jace Kline and Prasad Kulkarni

Fast-Flux Malicious Domain Name Detection Method Based on Domain Resolution Spatial Features 240
Shaojie Chen, Bo Lang and Chong Xie

Group Privacy for Personalized Federated Learning 252
Filippo Galli, Sayan Biswas, Kangsoo Jung, Tommaso Cucinotta and Catuscia Palamidessi

SeCloud: Computer-Aided Support for Selecting Security Measures for Cloud Architectures 264
Yuri Gil Dantas and Ulrich Schöpp

SHORT PAPERS

Efficient Aggregation of Face Embeddings for Decentralized Face Recognition Deployments 279
Philipp Hofer, Michael Roland, Philipp Schwarz and René Mayrhofer

Evaluation of DoS/DDoS Attack Detection with ML Techniques on CIC-IDS2017 Dataset 287
Saida Farhat, Manel Abdelkader, Amel Meddeb-Makhlouf and Faouzi Zarai

Cybersecurity Awareness and Capacities of SMEs 296
Gencer Erdogan, Ragnhild Halvorsrud, Costas Boletsis, Simeon Tverdal and John Brian Pickering

An Explainable Convolutional Neural Network for Dynamic Android Malware Detection 305
Francesco Mercaldo, Fabio Martinelli and Antonella Santone

Machine Learning Based Prediction of Vulnerability Information Subject to a Security Alert 313
Ryu Watanabe, Takashi Matsunaka, Ayumu Kubota and Jumpei Urakawa

An End-to-End Encrypted Cache System with Time-Dependent Access Control 321
Keita Emura and Masato Yoshimi

Concrete Quantum Circuits to Prepare Generalized Dicke States on a Quantum Machine 329
Shintaro Narisada, Shohei Beppu, Kazuhide Fukushima and Shinsaku Kiyomoto

Towards Audit Requirements for AI-Based Systems in Mobility Applications 339
Devi Padmavathi Alagarswamy, Christian Berghoff, Vasilios Danos, Fabian Langer, Thora Markert, Georg Schneider, Arndt von Twickel and Fabian Woitschek

CHARRA-PM: An Attestation Approach Relying on the Passport Model 349
Antonio Marques and Bruno Sousa

Evaluation Scheme to Analyze Keystroke Dynamics Methods 357
Anastasia Dimaratos and Daniela Pöhn

Revisiting the DFT Test in the NIST SP 800-22 Randomness Test Suite 366
Hiroki Okada and Kazuhide Fukushima

SHOID: A Secure Herd of IoT Devices Firmware Update Protocol 373
Frédéric Ruellé, Quentin Guellaën and Arnaud Rosay

An Analysis of Cybersecurity Awareness Efforts for Swiss SMEs 381
Ciarán Bryce

Using Infrastructure-Based Agents to Enhance Forensic Logging of Third-Party Applications 389
Jennifer Bellizzi, Mark Vella, Christian Colombo and Julio Hernandez-Castro

Systematically Searching for Identity-Related Information in the Internet with OSINT Tools 402
Marcus Walkow and Daniela Pöhn

Security Analysis of a Color Image Encryption Scheme Based on Dynamic Substitution and Diffusion Operations 410
George Teşeleanu

Measurements of Cross-Border Quantum Key Distribution Link 418
Filip Lauterbach, Libor Michalek, Piotr Rydlichowski, Patrik Burdiak, Jaroslav Zdralek and Miroslav Voznak

Evaluating the Fork-Awareness of Coverage-Guided Fuzzers 424
Marcello Maugeri, Cristian Daniele, Giampaolo Bella and Erik Poll

SWaTEval: An Evaluation Framework for Stateful Web Application Testing 430
Anne Borcherding, Nikolay Penkov, Mark Giraud and Jürgen Beyerer

TTP-Aided Searchable Encryption of Documents Using Threshold Secret Sharing 442
Ahmad Akmal Aminuddin Mohd Kamal and Keiichi Iwamura

Privacy-Aware IoT: State-of-the-Art and Challenges 450
Shukun Tokas, Gencer Erdogan and Ketil Stølen

On the Feasibility of Fully Homomorphic Encryption of Minutiae-Based Fingerprint Representations 462
Pia Bauspieß, Lasse Vad, Håvard Myrekrok, Anamaria Costache, Jascha Kolberg, Christian Rathgeb and Christoph Busch

Query Log Analysis for SQL Injection Detection 471
Alexandra Rocha, Rui Alves and Tiago Pedrosa

How to Design a Blue Team Scenario for Beginners on the Example of Brute-Force Attacks on Authentications 477
Andreas Eipper and Daniela Pöhn

SCANTRAP: Protecting Content Management Systems from Vulnerability Scanners with Cyber Deception and Obfuscation 485
Daniel Reti, Karina Elzer and Hans Dieter Schotten

A k-Anonymization Method for Social Network Data with Link Prediction 493
Risa Sugai, Yuichi Sei, Yasuyuki Tahara and Akihiko Ohsuga

Bypassing Multiple Security Layers Using Malicious USB Human Interface Device 501
Mathew Nicho and Ibrahim Sabry

Evaluation of a Tool to Increase Cybersecurity Awareness Among Non-experts (SME Employees) 509
Kaiying Luan, Ragnhild Halvorsrud and Costas Boletsis

The Story of Safety Snail and Her e-Mail: A Digital Wellness and Cybersecurity Serious Game for Pre-School Children 519
Günther R. Drevin, Dirk P. Snyman, Lynette Drevin, Hennie A. Kruger and Johann Allers

Evading Detection During Network Reconnaissance 528
Ilias Belalis, Georgios Spathoulas and Ioannis Anagnostopoulos

Temporal Constraints in Online Dating Fraud Classification 535
Harrison Bullock and Matthew Edwards

Cloud Inspector: A Tool-Based Approach for Public Administrations to Establish Information Security Processes Towards Public Clouds 543
Michael Diener and Thomas Bolz

Evaluation of Persistence Methods Used by Malware on Microsoft Windows Systems 552
Amélie Dieterich, Matthias Schopp, Lars Stiemert, Christoph Steininger and Daniela Pöhn

Security Aspects of Digital Twins in IoT 560
Vitomir Pavlov, Florian Hahn and Mohammed El-Hajj

Identifying Personal Data Processing for Code Review 568
Feiyang Tang, Bjarte M. Østvold and Magiel Bruntink

Online Transition-Based Feature Generation for Anomaly Detection in Concurrent Data Streams 576
Yinzheng Zhong and Alexei Lisitsa

Design Rationale for Symbiotically Secure Key Management Systems in IoT and Beyond 583
Witali Bartsch, Prosanta Gope, Elif Bilge Kavun, Owen Millwood, Andriy Panchenko, Aryan M. Pasikhani and Ilia Polian

Assessing Security and Privacy Insights for Smart Home Users 592
Samiah Alghamdi and Steven Furnell

On the Design of GDPR Compliant Workflows for Responsible Neuroimage Data Sharing 600
Alexandros Karakasidis and Vassilios Vassalos

Human Factors for Cybersecurity Awareness in a Remote Work Environment 608
César Vásquez Flores, Jose Gonzales, Miranda Kajtazi, Joseph Bugeja and Bahtijar Vogel

Towards Long-Term Continuous Tracing of Internet-Wide Scanning Campaigns Based on Darknet Analysis 617
Chansu Han, Akira Tanaka, Jun'ichi Takeuchi, Takeshi Takahashi, Tomohiro Morikawa and Tsung-Nan Lin

Vehicle Data Collection: A Privacy Policy Analysis and Comparison 626
Chiara Bodei, Gianpiero Costantino, Marco De Vincenzi, Ilaria Matteucci and Anna Monreale

A Scenario-Driven Cyber Security Awareness Exercise Utilizing Dynamic Polling: Methodology and Lessons Learned 634
Maria Leitner

Cyber Teaching Hospitals: Developing Cyber Workforce Competence 643
James R. Elste and David Croasdell

Correlating Intrusion Detection with Attack Graph on Virtual Computer Networkings 651
Hanwen Zhang, Wenyong Wang, Lisheng Huang, Junrui Wu, Fengjun Zhang and Kai Shi

Vulnerabilities in IoT Devices, Backends, Applications, and Components 659
Rauli Kaksonen, Kimmo Halunen and Juha Röning

Comparing the Effect of Privacy and Non-Privacy Social Media Photo Tools on Factors of Privacy Concern 669
Vanessa Bracamonte, Sebastian Pape and Sascha Loebner

Improving Unlinkability in C-ITS: A Methodology For Optimal Obfuscation 677
Yevhen Zolotavkin, Yurii Baryshev, Vitalii Lukichov, Jannik Mähn and Stefan Köpsell

P2BAC: Privacy Policy Based Access Control Using P-LPL 686
Jens Leicht and Maritta Heisel

Secure Software Updates for IoT Based on Industry Requirements 698
Ludwig Seitz, Marco Tiloca, Martin Gunnarsson and Rikard Höglund

A Game Theoretic Analysis of Cyber Threats 706
Paul Tavolato, Robert Luh and Sebastian Eresheim

RPCDroid: Runtime Identification of Permission Usage Contexts in Android Applications 714
Michele Guerra, Roberto Milanese, Rocco Oliveto and Fausto Fasano

Towards Security Attack Event Monitoring for Cyber Physical-Systems 722
Elias Seid, Oliver Popov and Fredrik Blix

Anomalous File System Activity Detection Through Temporal Association Rule Mining 733
M. Reza H. Iman, Pavel Chikul, Gert Jervan, Hayretdin Bahsi and Tara Ghasempouri

StegWare: A Novel Malware Model Exploiting Payload Steganography and Dynamic Compilation 741
Daniele Albanese, Rosangela Casolare, Giovanni Ciaramella, Giacomo Iadarola, Fabio Martinelli, Francesco Mercaldo, Marco Russodivito and Antonella Santone

A Biometric Self Authentication Scheme 749
Hervé Chabanne

Forecasting Cyber-Attacks to Destination Ports Using Machine Learning 757
Kostas Loumponias, Sotiris Raptis, Eleni Darra, Theodora Tsikrika, Stefanos Vrochidis and Ioannis Kompatsiaris

A Self-Configuration Controller To Detect, Identify, and Recover Misconfiguration at IoT Edge Devices and Containerized Cluster System 765
Areeg Samir and Håvard Dagenborg

Assessing the Impact of Attacks on Connected and Autonomous Vehicles in Vehicular Ad Hoc Networks 774
Kaushik Krishnan Balaji, Dimah Almani and Steven Furnell

Differential Privacy: Toward a Better Tuning of the Privacy Budget (ε) Based on Risk 783
Mahboobeh Dorafshanian and Mohamed Mejri

Assessing Risk in High Performance Computing Attacks 793
Erika Leal, Cimone Wright-Hamor, Joseph Manzano, Nicholas Multari, Kevin Barker, David Manz and Jiang Ming

AUTHOR INDEX 805