6th International Conference on Information Systems Security and Privacy (ICISSP 2020)

Valletta, Malta
25 – 27 February 2020

Editors:

Steven Furnell	**Edgar Weippl**
Paolo Mori	**Olivier Camp**

ISBN: 978-1-7138-4034-3

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© (2020) 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

Contents

INVITED SPEAKERS

Keynote Speakers

Leveraging Blockchain Technology to Enhance Security and Privacy in the Internet of Things 5
Sokratis K. Katsikas

Toward Active and Passive Confidentiality Attacks on Cryptocurrency Off-chain Networks 7
Utz Nisslmueller, Klaus-Tycho Foerster, Stefan Schmid and Christian Decker

Backdooring Deep Learning Architectures: Threats and (some) Opportunities 15
Mauro Barni

PAPERS

Full Papers

AMNESIA: A Technical Solution towards GDPR-compliant Machine Learning 21
Christoph Stach, Corinna Giebler, Manuela Wagner, Christian Weber and Bernhard Mitschang

Secure Ownership Transfer for the Internet of Things 33
Martin Gunnarsson and Christian Gehrmann

Host Fingerprinting for Web Servers Authentication 45
Ezio Lefons, Sebastiano Pizzutilo and Filippo Tangorra

A Formal Approach for the Analysis of the XRP Ledger Consensus Protocol 52
Lara Mauri, Stelvio Cimato and Ernesto Damiani

Email Spoofing Attack Detection through an End to End Authorship Attribution System 64
Giacomo Giorgi, Andrea Saracino and Fabio Martinelli

Lightweight Authentication and Secure Communication Suitable for IoT Devices 75
Simona Buchovecká, Róbert Lórencz, Jiří Buček and Filip Kodýtek

CoRA: A Scalable Collective Remote Attestation Protocol for Sensor Networks 84
Aída Diop, Maryline Laurent, Jean Leneutre and Jacques Traoré

Track Down Identity Leaks using Threat Intelligence 96
Timo Malderle, Sven Knauer, Martin Lang, Matthias Wbbeling and Michael Meier

Assessing Testing Strategies for Access Control Systems: A Controlled Experiment 107
Said Daoudagh, Francesca Lonetti and Eda Marchetti

Secrecy and Authenticity Properties of the Lightning Network Protocol 119
Hans Hüttel and Vilim Staroveski

Privacy with Health Information Technologies: What Story Do Data Breaches in US Tell Us? 131
Sylvestre Uwizeyemungu and Placide Poba-Nzaou

Evaluating the Effect of Justification and Confidence Information on User Perception of a Privacy Policy Summarization Tool 142
Vanessa Bracamonte, Seira Hidano, Welderufael B. Tesfay and Shinsaku Kiyomoto

Harmonized Group Mix for ITS
Mirja Nitschke, Christian Roth, Christian Hoyer and Doğan Kesdoğan 152

A Quantitative Study of Vulnerabilities in the Internet of Medical Things
Hervé Debar, Razvan Beuran and Yasuo Tan 164

Speeding Up the Computation of Elliptic Curve Scalar Multiplication based on CRT and DRM
Mohammad Anagreh, Eero Vainikko and Peeter Laud 176

External Contextual Factors in Information Security Behaviour
D. P. Snyman and H. A. Kruger 185

A Homomorphic Proxy Re-authenticators based Efficient Multi-client Non-interactive Verifiable Computation Scheme
Shuaijianni Xu and Liang Feng Zhang 195

MedBIoT: Generation of an IoT Botnet Dataset in a Medium-sized IoT Network
Alejandro Guerra-Manzanares, Jorge Medina-Galindo, Hayretdin Bahsi and Sven Nõmm 207

SHORT PAPERS

Security of Digital Banking Systems in Poland: Users Study 2019
Wojciech Wodo and Damian Stygar 221

Comparison of the Paillier and ElGamal Cryptosystems for Smart Grid Aggregation Protocols
Fabian Knirsch, Andreas Unterweger, Maximilian Unterrainer and Dominik Engel 232

Privacy-preserving Surveillance Methods using Homomorphic Encryption
William Bowditch, Will Abramson, William J. Buchanan, Nikolaos Pitropakis and Adam J. Hall 240

Maturity Modelling to Prepare for Cyber Crisis Escalation and Management
Grethe Østby and Basel Katt 249

Translating Data Protection into Software Requirements
Ralf Kneuper 257

Revisiting Higher-order Computational Attacks against White-box Implementations
Houssem Maghrebi and Davide Alessio 265

Modeling Cyber Threat Intelligence
Siri Bromander, Morton Swimmer, Martin Eian, Geir Skjotskift and Fredrik Borg 273

Integration of Data Envelopment Analysis in Business Process Models: A Novel Approach to Measure Information Security
Agnes Åkerlund and Christine Große 281

Phishing URL Detection Through Top-level Domain Analysis: A Descriptive Approach
Orestis Christou, Nikolaos Pitropakis, Pavlos Papadopoulos, Sean McKeown and William J. Buchanan 289

An Approach to Secure Legacy Software Systems
Stefanie Jasser and Jonas Kelbert 299

Is Ethereum's ProgPoW ASIC Resistant?
Jason Orender, Ravi Mukkamala and Mohammad Zubair 310

Exploring Vulnerabilities in Solidity Smart Contract
Phitchayaphong Tantikul and Sudsanguan Ngamsuriyaroj 317

Quantifying the Significance of Cybersecurity Text through Semantic Similarity and Named Entity Recognition
Otgonpurev Mendsaikhan, Hirokazu Hasegawa, Yamaguchi Yukiko and Hajime Shimada 325

A Comparison of Blockchain-based PKI Implementations
Clemens Brunner, Fabian Knirsch, Andreas Unterweger and Dominik Engel 333

A Domain-specific Modeling Framework for Attack Surface Modeling
Tithnara Nicolas Sun, Bastien Drouot, Fahad R. Golra, Joël Champeau, Sylvain Guerin, Luka Le Roux, Raúl Mazo, Ciprian Teodorov, Lionel Van Aertryck and Bernard L'Hostis 341

Visualizing Syscalls using Self-organizing Maps for System Intrusion Detection
Max Landauer, Florian Skopik, Markus Wurzenberger, Wolfgang Hotwagner and Andreas Rauber 349

CoProtect: Collaborative Management of Cryptographic Keys for Data Security in Cloud Systems
Lorenzo Bracciale, Pierpaolo Loreti, Emanuele Raso, Maurizio Naldi and Giuseppe Bianchi 361

Threat Modeling and Attack Simulations of Smart Cities: A Literature Review and Explorative Study
Robert Lagerström, Wenjun Xiong and Mathias Ekstedt 369

Bident Structure for Neural Network Model Protection
Hsiao-Ying Lin, Chengfang Fang and Jie Shi 377

Risk Identification: From Requirements to Threat Models
Roman Wirtz and Maritta Heisel 385

A Systematic Approach toward Extracting Technically Enforceable Policies from Data Usage Control Requirements
Arghavan Hosseinzadeh, Andreas Eitel and Christian Jung 397

Computer Viruses: The Abstract Theory Revisited
Nikolai Gladychev 406

Revisiting Privacy-aware Blockchain Public Key Infrastructure
Paul Plessing and Olamide Omolola 415

Securing IoT Devices using Geographic and Continuous Login Blocking: A Honeypot Study
Fredrik Heiding, Mohammad-Ali Omer, Andreas Wallström and Robert Lagerström 424

Active Directory Kerberoasting Attack: Monitoring and Detection Techniques
Lukáš Kotlaba, Simona Buchovecká and Róbert Lórencz 432

CCA Secure Unidirectional PRE with Key Pair in the Standard Model without Pairings
Anass Sbai, Cyril Drocourt and Gilles Dequen 440

Using Eyetracker to Find Ways to Mitigate Ransomware
Budi Arief, Andy Periam, Orcun Cetin and Julio Hernandez-Castro 448

Email Image Spam Classification based on ResNet Convolutional Neural Network
Vít Listík, Jan Šedivý and Václav Hlaváč 457

Evaluation to Classify Ransomware Variants based on Correlations between APIs
Jiaxing Zhou, Miyuki Hirose, Yoshio Kakizaki and Atsuo Inomata 465

A Practical Approach to Stakeholder-driven Determination of Security Requirements based on the GDPR and Common Criteria 473
Sandra Domenique Zinsmaier, Hanno Langweg and Marcel Waldvogel

Achieving Privacy, Security, and Interoperability among Biometric Networks using Symmetric Encryption 481
Eduardo M. Lacerda Filho and Vinicius P. Gonçalves

Improving Accuracy and Speed of Network-based Intrusion Detection using Gradient Boosting Trees 490
Ryosuke Terado and Morihiro Hayashida

Anomaly Detection in Communication Networks of Cyber-physical Systems using Cross-over Data Compression 498
Hubert Schölnast, Paul Tavolato and Philipp Kreimel

Privacy-preserving Measures in Smart City Video Surveillance Systems 506
Shizra Sultan and Christian D. Jensen

Homomorphic Encryption at Work for Private Analysis of Security Logs 515
Aymen Boudguiga, Oana Stan, Hichem Sedjelmaci and Sergiu Carpov

Radical Text Detection based on Stylometry 524
Álvaro de Pablo, Óscar Araque and Carlos A. Iglesias

On Analyzing Third-party Tracking via Machine Learning 532
Alfonso Guarino, Delfina Malandrino, Rocco Zaccagnino, Federico Cozza and Antonio Rapuano

The Root Causes of Compromised Accounts at the University 540
Philip Nyblom, Gaute Wangen, Mazaher Kianpour and Grethe Østby

Patients to Mobilize Their Data: Secure and Flexible mHealth Delegation 552
Rafael Almeida, Pedro Vieira-Marques and Ana Ferreira

Accountant: Protection of Data Integrity and Identification of Malicious Nodes in In-network Data Processing 561
David Jost and Mathias Fischer

Building Competitive Advantage from Ubuntu: An African Information Security Awareness Model 569
Tapiwa Gundu and Nthabiseng Modiba

A Curious Exploration of Malicious PDF Documents 577
Julian Lindenhofer, Rene Offenthaler and Martin Pirker

Dual-use Research in Ransomware Attacks: A Discussion on Ransomware Defence Intelligence 585
Ziya Alper Genç and Gabriele Lenzini

Systematization of Threats and Requirements for Private Messaging with Untrusted Servers: The Case of e-Mailing and Instant Messaging 593
Iraklis Symeonidis and Gabriele Lenzini

An Analytical Scanning Technique to Detect and Prevent the Transformed SQL Injection and XSS Attacks 603
Mohammad Qbea'h, Saed Alrabaee and Djedjiga Mouheb

Neural Network Security: Hiding CNN Parameters with Guided Grad-CAM 611
Linda Guiga and A. W. Roscoe

Distributed Defence of Service (DiDoS): A Network-layer Reputation-based DDoS Mitigation Architecture 619
Andikan Otung and Andrew Martin

Presence Metadata in the Internet of Things: Challenges and Opportunities 631
Robert Hegarty and John Haggerty

A Study of Classification of Texts into Categories of Cybersecurity Incident and Attack with Topic Models 639
Masahiro Ishii, Satoshi Matsuura, Kento Mori, Masahiko Tomoishi, Yong Jin and Yoshiaki Kitaguchi

New General Secret Sharing Scheme using Hierarchical Threshold Scheme: Improvement of Information Rates for Specified Participants 647
Kouya Tochikubo

Greater Control and Transparency in Personal Data Processing 655
Giray Havur, Miel Vander Sande and Sabrina Kirrane

Securing Industrial Production from Sophisticated Cyberattacks 663
Andrew Sundstrom, Damas Limoge, Vadim Pinskiy and Matthew Putman

A Meta Model for a Comprehensive Description of Network Protocols Improving Security Tests 671
Steffen Pfrang, David Meier, Andreas Fleig and Jürgen Beyerer

Introducing a Verified Authenticated Key Exchange Protocol over Voice Channels for Secure Voice Communication 683
Piotr Krasnowski, Jerome Lebrun and Bruno Martin

Legislation and the Negative Impact on Cybersecurity in Healthcare 691
Jesse Daniels and Sajal Bhatia

Secure Comparison and Interval Test Protocols based on Three-party MPC 698
Wataru Fujii, Keiichi Iwamura and Masaki Inamura

Multi-level Distributed Intrusion Detection System for an IoT based Smart Home Environment 705
Simone Facchini, Giacomo Giorgi, Andrea Saracino and Gianluca Dini

Ontology-based Automation of Penetration Testing 713
Ge Chu and Alexei Lisitsa

Recommender Systems Robust to Data Poisoning using Trim Learning 721
Seira Hidano and Shinsaku Kiyomoto

Distance Metric Learning using Particle Swarm Optimization to Improve Static Malware Detection 725
Martin Jureček and Róbert Lórencz

Security and Privacy in Smart Grids: Challenges, Current Solutions and Future Opportunities 733
Ismail Butun, Alexios Lekidis and Daniel Ricardo dos Santos

Tool Support for Risk-driven Planning of Trustworthy Smart IoT Systems within DevOps 742
Andreas Thompson and Gencer Erdogan

Methodology and Feedback about Systematic Cybersecurity Experts Auditing in Belgium 754
Christophe Ponsard, Jeremy Grandclaudon and Nicolas Point

4TH INTERNATIONAL WORKSHOP ON FORMAL METHODS FOR SECURITY ENGINEERING

FULL PAPERS

Towards a Comprehensive Solution for Secure Cryptographic Protocol Execution based on Runtime Verification 765
Christian Colombo and Mark Vella

Detection of Crawler Traps: Formalization and Implementation Defeating Protection on Internet and on the TOR Network 775
Maxence Delong, Baptiste David and Eric Filiol

Verifying Sanitizer Correctness through Black-Box Learning: A Symbolic Finite Transducer Approach 784
Sophie Lathouwers, Maarten Everts and Marieke Huisman

The Blockchain Potential in Computer Virology 796
Joanna Moubarak, Eric Filiol and Maroun Chamoun

Android Run-time Permission Exploitation User Awareness by Means of Formal Methods 804
Fausto Fasano, Fabio Martinelli, Francesco Mercaldo and Antonella Santone

Analysis of Security Attacks in Wireless Sensor Networks: From UPPAAL to Castalia 815
Cinzia Bernardeschi, Gianluca Dini, Maurizio Palmieri and Francesco Racciatti

Accidental Sensitive Data Leaks Prevention via Formal Verification 825
Madalina G. Ciobanu, Fausto Fasano, Fabio Martinelli, Francesco Mercaldo and Antonella Santone

SHORT PAPERS

Bank Credit Risk Management based on Data Mining Techniques 837
Fabio Martinelli, Francesco Mercaldo, Domenico Raucci and Antonella Santone

Comparing Machine Learning Techniques for Malware Detection 844
Joanna Moubarak and Tony Feghali

AUTHOR INDEX 853