Lecture Notes in Computer Science 11735

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
Gerhard Woeginger
RWTH Aachen, Aachen, Germany
Moti Yung
Columbia University, New York, NY, USA

More information about this series at http://www.springer.com/series/7410

Kazue Sako · Steve Schneider ·
Peter Y. A. Ryan (Eds.)

Computer Security – ESORICS 2019

24th European Symposium
on Research in Computer Security
Luxembourg, September 23–27, 2019
Proceedings, Part I

Springer

Editors
Kazue Sako
NEC Corporation
Kawasaki, Japan

Steve Schneider
University of Surrey
Guildford, UK

Peter Y. A. Ryan
University of Luxembourg
Esch-sur-Alzette, Luxembourg

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-29958-3 ISBN 978-3-030-29959-0 (eBook)
https://doi.org/10.1007/978-3-030-29959-0

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer Nature Switzerland AG 2019
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

This book contains the papers that were selected for presentation and publication at the 24th European Symposium on Research in Computer Security (ESORICS 2019) which was held together with affiliated workshops in Luxembourg, September 23–27, 2019. The aim of ESORICS is to further the progress of research in computer, information, and cyber security, as well as in privacy, by establishing a European forum for bringing together researchers in these areas, by promoting the exchange of ideas with system developers, and by encouraging links with researchers in related fields.

In response to the call for papers, 344 papers were submitted to the conference. These papers were evaluated on the basis of their significance, novelty, and technical quality. Each paper was reviewed by at least three members of the Program Committee and external reviewers, and papers authored by Program Committee members had four reviewers. The reviewing process was single-blind. The Program Committee had intensive discussions which were held via EasyChair. Finally, 67 papers were selected for presentation at the conference, giving an acceptance rate of 19.5%. We were also delighted to welcome keynote talks from Adi Shamir, Véronique Cortier, and Bart Preneel.

Following the reviews, two papers were selected for joint Best Paper Award, to share the 1,000 EUR prize generously provided by Springer: "A Frame-work for Evaluating Security in the Presence of Signal Injection Attacks," by Ilias Giechaskiel, Youqian Zhang, and Kasper Rasmussen; and "Breakdown Resilience of Key Exchange Protocols: NewHope, TLS 1.3, and Hybrids," by Jacqueline Brendel, Marc Fischlin, and Felix Günther.

The Program Committee consisted of 95 members across 24 countries. There were submissions from a total of 1,071 authors across 46 countries, with 23 countries represented among the accepted papers.

ESORICS 2019 would not have been possible without the contributions of the many volunteers who freely gave their time and expertise. We would like to thank the members of the Program Committee and the external reviewers for their substantial work in evaluating the papers. We would also like to thank the organization chair, Peter B. Roenne, the workshop chair, Joaquin Garcia-Alfaro, and all workshop co-chairs, the posters chair, Alfredo Rial, the publicity chair, Cristina Alcaraz, and the ESORICS Steering Committee and its chair, Sokratis Katsikas.

Finally, we would like to express our thanks to the authors who submitted papers to ESORICS. They, more than anyone else, are what makes this conference possible.

We hope that you found the program to be stimulating and a source of inspiration for future research.

July 2019

Kazue Sako
Steve Schneider
Peter Y. A. Ryan

Organization

ESORICS Steering Committee

Sokratis Katsikas (Chair)	NTNU, Norway
Michael Backes	Saarland University, Germany
Joachim Biskup	TU Dortmund, Germany
Frederic Cuppens	IMT Atlantique, France
Sabrina De Capitani di Vimercati	Università degli Studi di Milano, Italy
Dieter Gollmann	Hamburg University of Technology, Germany
Mirek Kutylowski	Wroclaw University of Technology, Poland
Javier Lopez	University of Malaga, Spain
Jean-Jacques Quisquater	University of Louvain, Belgium
Peter Y. A. Ryan	University of Luxembourg, Luxembourg
Pierangela Samarati	Università degli Studi di Milano, Italy
Einar Snekkenes	NTNU, Norway
Michael Waidner	Fraunhofer, Germany

Program Committee

Mitsuaki Akiyama	NTT, Japan
Cristina Alcaraz	University of Malaga, Spain
Elli Androulaki	IBM Research - Zurich, Switzerland
Frederik Armknecht	Universität Mannheim, Germany
Vijay Atluri	Rutgers University, USA
Marina Blanton	University at Buffalo, USA
Carlo Blundo	Università degli Studi di Salerno, Italy
Christian Cachin	University of Bern, Switzerland
Alvaro Cardenas	The University of Texas at Dallas, USA
Aldar C-F. Chan	University of Hong Kong, Hong Kong, China
Yan Chen	Northwestern University, USA
Sherman S. M. Chow	The Chinese University of Hong Kong, Hong Kong, China
Mauro Conti	University of Padua, Italy
Jorge Cuellar	Siemens AG, Germany
Frédéric Cuppens	Telecom Bretagne, France
Nora Cuppens-Boulahia	IMT Atlantique, France
Marc Dacier	EURECOM, France
Sabrina De Capitani di Vimercati	Università degli Studi di Milano, Italy
Hervé Debar	Telecom SudParis, France
Stéphanie Delaune	CNRS, France

Roberto Di Pietro	Hamad Bin Khalifa University, Qatar
Josep Domingo-Ferrer	Universitat Rovira i Virgili, Spain
Haixin Duan	Tsinghua University, China
François Dupressoir	University of Surrey, UK
José M. Fernandez	Ecole Polytechnique de Montreal, Canada
Jose-Luis Ferrer-Gomila	University of the Balearic Islands, Spain
Simone Fischer-Hübner	Karlstad University, Sweden
Simon Foley	Norwegian NTNU, Norway
Sara Foresti	Università degli Studi di Milano, Italy
David Galindo	University of Birmingham, UK
Debin Gao	Singapore Management University, Singapore
Joaquin Garcia-Alfaro	Telecom SudParis, France
Dieter Gollmann	Hamburg University of Technology, Germany
Stefanos Gritzalis	University of the Aegean, Greece
Guofei Gu	Texas A&M University, USA
Juan Hernández-Serrano	Universitat Politècnica de Catalunya, Spain
Xinyi Huang	Fujian Normal University, China
Ghassan Karame	NEC Laboratories Europe, Germany
Vasilios Katos	Bournemouth University, UK
Sokratis Katsikas	NTNU, Norway
Stefan Katzenbeisser	University of Passau, Germany
Steve Kremer	Inria, France
Marina Krotofil	FireEye, USA
Costas Lambrinoudakis	University of Piraeus, Greece
Yingjiu Li	Singapore Management University, Singapore
Kaitai Liang	University of Surrey, UK
Hoon Wei Lim	Royal Holloway, University of London, UK
Joseph Liu	Monash University, Australia
Peng Liu	The Pennsylvania State University, USA
Xiapu Luo	The Hong Kong Polytechnic, Hong Kong, China
Konstantinos Markantonakis	Royal Holloway, University of London, UK
Fabio Martinelli	IIT-CNR, Italy
Ivan Martinovic	University of Oxford, UK
Sjouke Mauw	University of Luxembourg, Luxembourg
Catherine Meadows	NRL, USA
Weizhi Meng	Technical University of Denmark, Denmark
Chris Mitchell	Royal Holloway, University of London, UK
John Mitchell	Stanford University, USA
Tatsuya Mori	Waseda University, Japan
Haralambos Mouratidis	University of Brighton, UK
David Naccache	DIENS, ENS, CNRS, PSL University, Paris, France
Satoshi Obana	Hosei University, Japan
Martín Ochoa	Cyxtera Technologies, Colombia
Rolf Oppliger	eSECURITY Technologies, Switzerland
Andrew Paverd	Microsoft Research, UK

Olivier Pereira	UCLouvain, Belgium
Günther Pernul	Universität Regensburg, Germany
Joachim Posegga	University of Passau, Germany
Bart Preneel	Katholieke Universiteit Leuven, Belgium
Christina Pöpper	New York University, USA
Indrajit Ray	Colorado State University, USA
Giovanni Russello	The University of Auckland, New Zealand
Mark Ryan	University of Birmingham, UK
Reyhaneh Safavi-Naini	University of Calgary, Canada
Kazue Sako	NEC, Japan
Pierangela Samarati	Università degli Studi di Milano, Italy
Damien Sauveron	XLIM – University of Limoges, UMR CNRS 7252, France
Steve Schneider	University of Surrey, UK
Einar Snekkenes	NTNU, Norway
Willy Susilo	University of Wollongong, Australia
Pawel Szalachowski	SUTD, Singapore
Qiang Tang	Luxembourg Institute of Science and Technology, Luxembourg
Qiang Tang	New Jersey Institute of Technology, USA
Juan Tapiador	Universidad Carlos III de Madrid, Spain
Nils Ole Tippenhauer	CISPA, Germany
Helen Treharne	University of Surrey, UK
Aggeliki Tsohou	Ionian University, Greece
Jaideep Vaidya	Rutgers University, USA
Luca Viganö	King's College London, UK
Michael Waidner	Fraunhofer, Germany
Cong Wang	City University of Hong Kong, Hong Kong, China
Lingyu Wang	Concordia University, Canada
Edgar Weippl	SBA Research, Austria
Christos Xenakis	University of Piraeus, Greece
Zhe Xia	Wuhan University of Technology, China
Kehuan Zhang	The Chinese University of Hong Kong, Hong Kong, China
Sencun Zhu	The Pennsylvania State University, USA

Additional Reviewers

Abidin, Aysajan	Al-Mallah, Ranwa	Bamiloshin, Michael
Abusalah, Hamza	Andriotis, Panagiotis	Bampatsikos, Michail
Aggelogianni, Anna	Anglès-Tafalla, Carles	Batra, Gunjan
Ahmed, Chuadhry Mujeeb	Anikeev, Maxim	Belgacem, Boutheyna
Akand, Mamunur	Asif, Hafiz	Belles, Marta
Al Maqbali Fatma	Avizheh, Sepideh	Berger, Christian

Bezawada, Bruhadeshwar
Bkakria, Anis
Blanco-Justicia, Alberto
Blazy, Olivier
Bolgouras, Vaios
Bountakas, Panagiotis
Boureanu, Ioana
Brandt, Markus
Böhm, Fabian
Cao, Chen
Catuogno, Luigi
Cetinkaya, Orhan
Chadha, Rohit
Chan, Mun Choon
Chawla, Gagandeep
Chen, Haixia
Chen, Jianjun
Chen, Liqun
Chen, Long
Chen, Xihui
Chen, Yueqi
Chothia, Tom
Ciampi, Michele
Cook, Andrew
Cortier, Véronique
Costa, Nüria
Cui, Shujie
Dang, Hung
Dargahi, Tooska
Dashevskyi, Stanislav
de Miceli, Jean-Yves
De Salve, Andrea
Debant, Alexandre
Deo, Amit
Diamantopoulou, Vasiliki
Dietz, Marietheres
Divakaran, Dinil Mon
Dominguez Trujillo, Antonio
Dryja, Tadge
Du, Minxin
Du, Xuechao
Dufour Sans, Edouard
Duman, Onur
Duong, Dung
Elkhiyaoui, Kaoutar
Englbrecht, Ludwig
Espes, David
Fan, Xiong
Farao, Aristeidis
Farhang, Sadegh
Fdhila, Walid
Fenghao, Xu
Ferreira Torres, Christof
Gangwal, Ankit
Ge, Chunpeng
Geneiatakis, Dimitris
Georgiopoulou, Zafeiroula
Giorgi, Giacomo
Groll, Sebastian
Gupta, Maanak
Gusenbauer, Matthias
Han, Jinguang
Hassan, Fadi
Hermans, Jens
Hicks, Christopher
Hirschi, Lucca
Hlavacek, Tomas
Homoliak, Ivan
Horne, Ross
Hu, Kexin
Iliou, Christos
Jacomme, Charlie
Jeitner, Philipp
Jiongyi, Chen
Jonker, Hugo
Judmayer, Aljosha
Kalloniatis, Christos
Kambourakis, Georgios
Karamchandani, Neeraj
Kasinathan, Prabhakaran
Kavousi, Mohammad
Kern, Sascha
Khan, Muhammad Hassan
Kim, Jongkil
Klaedtke, Felix
Kohls, Katharina
Kostoulas, Theodoros
Koutroumpouxos, Nikolaos
Kuchta, Veronika
Köstler, Johannes
La Marra, Antonio
Labani, Hasan
Lakshmanan, Sudershan
Lal, Chhagan
Lazzeretti, Riccardo
Lee, Jehyun
Leng, Xue
León, Olga
Li, Li
Li, Shujun
Li, Wanpeng
Li, Wenjuan
Li, Xing
Li, Xusheng
Li, Yanan
Li, Zengpeng
Li, Zhenyuan
Libert, Benoît
Lin, Chengjun
Lin, Yan
Liu, Ximing
Lobe Kome, Ivan Marco
Losiouk, Eleonora
Loukas, George
Lu, Yang
Lu, Yuan
Lyvas, Christos
Ma, Haoyu
Ma, Jack P. K.
Maene, Pieter
Majumdar, Suryadipta
Malliaros, Stefanos
Mardziel, Piotr
Marin, Eduard
Marson, Giorgia
Martinez, Sergio
Matyunin, Nikolay
Menges, Florian
Menghan, Sun
Michailidou, Christina
Milani, Simone
Minaud, Brice
Minematsu, Kazuhiko
Mizera, Andrzej
Moch, Alexander

Moessner, Klaus
Mohamady, Meisam
Mohammadi, Farnaz
Moisan, Frederic
Moreau, Solène
Moreira, Josè
Murayama, Yuko
Murmann, Patrick
Muñoz, Jose L.
Mykoniati, Maria
Ng, Lucien K. L.
Ngamboe, Mikaela
Nguyen, Quoc Phong
Ning, Jianting
Niu, Liang
Nomikos, Nikolaos
Ntantogian, Christoforos
Oqaily, Alaa
Oqaily, Momen
Ouattara, Jean-Yves
Oya, Simon
Panaousis, Manos
Papaioannou, Thanos
Parra Rodriguez, Juan D.
Parra-Arnau, Javier
Pasa, Luca
Paspatis, Ioannis
Peeters, Roel
Pelosi, Gerardo
Petrovic, Slobodan
Pfeffer, Katharina
Pitropakis, Nikolaos
Poh, Geong Sen
Polian, Ilia
Prestwich, Steve
Puchta, Alexander
Putz, Benedikt
Pöhls, Henrich C.
Qiu, Tian
Ramírez-Cruz, Yunior
Ray, Indrani
Reuben, Jenni
Rezk, Tamara
Rios, Ruben
Rizos, Athanasios
Román-García, Fernando
Rozic, Vladimir
Rupprecht, David
Sakuma, Jun
Saracino, Andrea
Schindler, Philipp
Schmidt, Carsten
Schnitzler, Theodor
Schumi, Richard
Sempreboni, Diego
Sengupta, Binanda
Sentanoe, Stewart
Sepideh Avizheh, Shuai Li
Shikfa, Abdullatif
Shioji, Eitaro
Shirani, Paria
Shrishak, Kris
Shuaike, Dong
Simo, Hervais
Singelée, Dave
Siniscalchi, Luisa
Situ, Lingyun
Smith, Zach
Smyth, Ben
Song, Yongcheng
Soriente, Claudio
Soumelidou, Aikaterini
Stifter, Nicholas
Sun, Yuanyi
Sundararajan, Vaishnavi
Tabiban, Azadeh
Tajan, Louis
Taubmann, Benjamin
Thomasset, Corentin
Tian, Yangguang
Tripathi, Nikhil
Tueno, Anselme
Ullrich, Johanna
Vanhoef, Mathy
Venugopalan, Sarad
Veroni, Eleni
Vielberth, Manfred
Viet Xuan Phuong, Tran
Walzer, Stefan
Wang, Daibin
Wang, Hongbing
Wang, Jiafan
Wang, Tielei
Wang, Xiaolei
Wang, Xiuhua
Wang, Zhi
Wattiau, Gaetan
Wesemeyer, Stephan
Wong, Harry W. H.
Wu, Daoyuan
Wu, Huangting
Xu, Jia
Xu, Jiayun
Xu, Ke
Xu, Shengmin
Xu, Yanhong
Yang, Kang
Yang, Shaojun
Yang, Wenjie
Yautsiukhin, Artsiom
Yuan, Chen
Zalonis, Jasmin
Zamyatin, Alexei
Zavatteri, Matteo
Zhang, Chao
Zhang, Liang Feng
Zhang, Yuexin
Zhao, Guannan
Zhao, Yongjun
Zheng, Yu
Zhou, Dehua
Zhou, Wei
Zhu, Tiantian
Zou, Qingtian
Zuo, Cong

Abstracts of Keynote Talks

The Insecurity of Machine Learning: Problems and Solutions

Adi Shamir

Computer Science Department, The Weizmann Institute of Science, Israel

Abstract. The development of deep neural networks in the last decade had revolutionized machine learning and led to major improvements in the precision with which we can perform many computational tasks. However, the discovery five years ago of adversarial examples in which tiny changes in the input can fool well trained neural networks makes it difficult to trust such results when the input can be manipulated by an adversary. This problem has many applications and implications in object recognition, autonomous driving, cyber security, etc, but it is still far from being understood. In particular, there had been no convincing explanations why such adversarial examples exist, and which parameters determine the number of input coordinates one has to change in order to mislead the network. In this talk I will describe a simple mathematical framework which enables us to think about this problem from a fresh perspective, turning the existence of adversarial examples in deep neural networks from a baffling phenomenon into an unavoidable consequence of the geometry of R^n under the Hamming distance, which can be quantitatively analyzed.

Electronic Voting: A Journey to Verifiability and Vote Privacy

Véronique Cortier

CNRS, LORIA, UMR 7503, 54506, Vandoeuvre-lès-Nancy, France

Abstract. Electronic voting aims to achieve the same properties as traditional paper based voting. Even when voters vote from their home, they should be given the same guarantees, without having to trust the election authorities, the voting infrastructure, and/or the Internet network. The two main security goals are vote privacy: no one should know how I voted; and verifiability: a voter should be able to check that the votes have been properly counted. In this talk, we will explore the subtle relationships between these properties and we will see how they can be realized and proved.

First, verifiability and privacy are often seen as antagonistic and some national agencies even impose a hierarchy between them: first privacy, and then verifiability as an additional feature. Verifiability typically includes individual verifiability (a voter can check that her ballot is counted); universal verifiability (anyone can check that the result corresponds to the published ballots); and eligibility verifiability (only legitimate voters may vote). Actually, we will see that privacy implies individual verifiability. In other words, systems without individual verifiability cannot achieve privacy (under the same trust assumptions).

Moreover, it has been recently realised that all existing definitions of vote privacy in a computational setting implicitly assume an honest voting server: an adversary cannot tamper with the bulletin board. As a consequence, voting schemes are proved secure only against an honest voting server while they are designed and claimed to resist a dishonest voting server. Not only are the security guarantees too weak, but attacks are missed. We propose a novel notion of ballot privacy against a malicious bulletin board. The notion is flexible in that it captures various capabilities of the attacker to tamper with the ballots, yielding different flavours of security.

Finally, once the security definitions are set, we need to carefully establish when a scheme satisfies verifiability and vote privacy. We have developed a framework in EasyCrypt for proving both verifiability and privacy, yielding machine-checked security proof. We have applied our framework to two existing schemes, namely Helios and Belenios, and many of their variants.

Cryptocurrencies and Distributed Consensus: Hype and Science

Bart Preneel

COSIC, an imec lab at KU Leuven, Belgium

Abstract. This talk will offer a perspective on the fast rise of cryptocurrencies based on proof of work, with Bitcoin as most prominent example. In about a decade, a white paper of nine pages has resulted in massive capital investments, a global ecosystem with a market capitalization of several hundreds of billions of dollars and the redefinition of the term crypto (which now means cryptocurrencies). We will briefly describe the history of electronic currencies and clarify the main principles behind Nakamoto Consensus. Next, we explain how several variants attempt to improve the complex tradeoffs between public verifiability, robustness, privacy and performance. We describe how Markov Decision processes can be used to compare in an objective way the proposed improvements in terms of chain quality, censorship resistance and robustness against selfish mining and double spending attacks. We conclude with a discussion of open problems.

Contents – Part I

Machine Learning

Privacy-Enhanced Machine Learning with Functional Encryption 3
Tilen Marc, Miha Stopar, Jan Hartman, Manca Bizjak, and Jolanda Modic

Towards Secure and Efficient Outsourcing of Machine Learning Classification 22
Yifeng Zheng, Huayi Duan, and Cong Wang

Confidential Boosting with Random Linear Classifiers for Outsourced User-Generated Data 41
Sagar Sharma and Keke Chen

BDPL: A Boundary Differentially Private Layer Against Machine Learning Model Extraction Attacks 66
Huadi Zheng, Qingqing Ye, Haibo Hu, Chengfang Fang, and Jie Shi

Information Leakage

The Leakage-Resilience Dilemma 87
Bryan C. Ward, Richard Skowyra, Chad Spensky, Jason Martin, and Hamed Okhravi

A Taxonomy of Attacks Using BGP Blackholing 107
Loïc Miller and Cristel Pelsser

Local Obfuscation Mechanisms for Hiding Probability Distributions 128
Yusuke Kawamoto and Takao Murakami

A First Look into Privacy Leakage in 3D Mixed Reality Data 149
Jaybie A. de Guzman, Kanchana Thilakarathna, and Aruna Seneviratne

Signatures and Re-encryption

Flexible Signatures: Making Authentication Suitable for Real-Time Environments. 173
Duc V. Le, Mahimna Kelkar, and Aniket Kate

DGM: A Dynamic and Revocable Group Merkle Signature 194
Maxime Buser, Joseph K. Liu, Ron Steinfeld, Amin Sakzad, and Shi-Feng Sun

Puncturable Proxy Re-Encryption Supporting to Group Messaging Service . . . 215
Tran Viet Xuan Phuong, Willy Susilo, Jongkil Kim, Guomin Yang, and Dongxi Liu

Generic Traceable Proxy Re-encryption and Accountable Extension in Consensus Network . . . 234
Hui Guo, Zhenfeng Zhang, Jing Xu, and Mingyuan Xia

Side Channels

Side-Channel Aware Fuzzing . . . 259
Philip Sperl and Konstantin Böttinger

NetSpectre: Read Arbitrary Memory over Network . . . 279
Michael Schwarz, Martin Schwarzl, Moritz Lipp, Jon Masters, and Daniel Gruss

maskVerif: Automated Verification of Higher-Order Masking in Presence of Physical Defaults . . . 300
Gilles Barthe, Sonia Belaïd, Gaëtan Cassiers, Pierre-Alain Fouque, Benjamin Grégoire, and Francois-Xavier Standaert

Automated Formal Analysis of Side-Channel Attacks on Probabilistic Systems . . . 319
Chris Novakovic and David Parker

Formal Modelling and Verification

A Formal Model for Checking Cryptographic API Usage in JavaScript . . . 341
Duncan Mitchell and Johannes Kinder

Contingent Payments on a Public Ledger: Models and Reductions for Automated Verification . . . 361
Sergiu Bursuc and Steve Kremer

Symbolic Analysis of Terrorist Fraud Resistance . . . 383
Alexandre Debant, Stéphanie Delaune, and Cyrille Wiedling

Secure Communication Channel Establishment: TLS 1.3 (over TCP Fast Open) vs. QUIC . . . 404
Shan Chen, Samuel Jero, Matthew Jagielski, Alexandra Boldyreva, and Cristina Nita-Rotaru

Attacks

Where to Look for *What You See Is What You Sign*? User Confusion in Transaction Security 429
Vincent Haupert and Stephan Gabert

On the Security and Applicability of Fragile Camera Fingerprints 450
Erwin Quiring, Matthias Kirchner, and Konrad Rieck

Attacking Speaker Recognition Systems with Phoneme Morphing 471
Henry Turner, Giulio Lovisotto, and Ivan Martinovic

Practical Bayesian Poisoning Attacks on Challenge-Based Collaborative Intrusion Detection Networks 493
Weizhi Meng, Wenjuan Li, Lijun Jiang, Kim-Kwang Raymond Choo, and Chunhua Su

A Framework for Evaluating Security in the Presence of Signal Injection Attacks 512
Ilias Giechaskiel, Youqian Zhang, and Kasper B. Rasmussen

Secure Protocols

Formalizing and Proving Privacy Properties of Voting Protocols Using Alpha-Beta Privacy 535
Sébastien Gondron and Sebastian Mödersheim

ProCSA: Protecting Privacy in Crowdsourced Spectrum Allocation 556
Max Curran, Xiao Liang, Himanshu Gupta, Omkant Pandey, and Samir R. Das

Breaking Unlinkability of the ICAO 9303 Standard for e-Passports Using Bisimilarity 577
Ihor Filimonov, Ross Horne, Sjouke Mauw, and Zach Smith

Symmetric-Key Corruption Detection: When XOR-MACs Meet Combinatorial Group Testing 595
Kazuhiko Minematsu and Norifumi Kamiya

Useful Tools

Finding Flaws from Password Authentication Code in Android Apps 619
Siqi Ma, Elisa Bertino, Surya Nepal, Juanru Li, Diethelm Ostry, Robert H. Deng, and Sanjay Jha

Identifying Privilege Separation Vulnerabilities in IoT Firmware with Symbolic Execution 638
Yao Yao, Wei Zhou, Yan Jia, Lipeng Zhu, Peng Liu, and Yuqing Zhang

iCAT: An Interactive Customizable Anonymization Tool 658
Momen Oqaily, Yosr Jarraya, Mengyuan Zhang, Lingyu Wang, Makan Pourzandi, and Mourad Debbabi

Monitoring the GDPR 681
Emma Arfelt, David Basin, and Søren Debois

Blockchain and Smart Contracts

Incentives for Harvesting Attack in Proof of Work Mining Pools 703
Yevhen Zolotavkin and Veronika Kuchta

A Lattice-Based Linkable Ring Signature Supporting Stealth Addresses 726
Zhen Liu, Khoa Nguyen, Guomin Yang, Huaxiong Wang, and Duncan S. Wong

Annotary: A Concolic Execution System for Developing Secure Smart Contracts 747
Konrad Weiss and Julian Schütte

PDFS: Practical Data Feed Service for Smart Contracts 767
Juan Guarnizo and Pawel Szalachowski

Towards a Marketplace for Secure Outsourced Computations 790
Hung Dang, Dat Le Tien, and Ee-Chien Chang

Author Index 809

Contents – Part II

Software Security

Automatically Identifying Security Checks for Detecting Kernel Semantic Bugs 3
Kangjie Lu, Aditya Pakki, and Qiushi Wu

Uncovering Information Flow Policy Violations in C Programs (Extended Abstract) 26
Darion Cassel, Yan Huang, and Limin Jia

`BinEye`: Towards Efficient Binary Authorship Characterization Using Deep Learning 47
Saed Alrabaee, ElMouatez Billah Karbab, Lingyu Wang, and Mourad Debbabi

Static Detection of Uninitialized Stack Variables in Binary Code 68
Behrad Garmany, Martin Stoffel, Robert Gawlik, and Thorsten Holz

Towards Automated Application-Specific Software Stacks 88
Nicolai Davidsson, Andre Pawlowski, and Thorsten Holz

Cryptographic Protocols

Identity-Based Encryption with Security Against the KGC: A Formal Model and Its Instantiation from Lattices 113
Keita Emura, Shuichi Katsumata, and Yohei Watanabe

Forward-Secure Puncturable Identity-Based Encryption for Securing Cloud Emails 134
Jianghong Wei, Xiaofeng Chen, Jianfeng Wang, Xuexian Hu, and Jianfeng Ma

Feistel Structures for MPC, and More 151
Martin R. Albrecht, Lorenzo Grassi, Léo Perrin, Sebastian Ramacher, Christian Rechberger, Dragos Rotaru, Arnab Roy, and Markus Schofnegger

Arithmetic Garbling from Bilinear Maps 172
Nils Fleischhacker, Giulio Malavolta, and Dominique Schröder

Security Models

SEPD: An Access Control Model for Resource Sharing in an IoT Environment 195
Henrique G. G. Pereira and Philip W. L. Fong

Nighthawk: Transparent System Introspection from Ring -3 217
Lei Zhou, Jidong Xiao, Kevin Leach, Westley Weimer, Fengwei Zhang, and Guojun Wang

Proactivizer: Transforming Existing Verification Tools into Efficient Solutions for Runtime Security Enforcement 239
Suryadipta Majumdar, Azadeh Tabiban, Meisam Mohammady, Alaa Oqaily, Yosr Jarraya, Makan Pourzandi, Lingyu Wang, and Mourad Debbabi

Enhancing Security and Dependability of Industrial Networks with Opinion Dynamics 263
Juan E. Rubio, Mark Manulis, Cristina Alcaraz, and Javier Lopez

Searchable Encryption

Dynamic Searchable Symmetric Encryption with Forward and Stronger Backward Privacy 283
Cong Zuo, Shi-Feng Sun, Joseph K. Liu, Jun Shao, and Josef Pieprzyk

Towards Efficient Verifiable Forward Secure Searchable Symmetric Encryption 304
Zhongjun Zhang, Jianfeng Wang, Yunling Wang, Yaping Su, and Xiaofeng Chen

Generic Multi-keyword Ranked Search on Encrypted Cloud Data 322
Shabnam Kasra Kermanshahi, Joseph K. Liu, Ron Steinfeld, and Surya Nepal

An Efficiently Searchable Encrypted Data Structure for Range Queries 344
Florian Kerschbaum and Anselme Tueno

Privacy

GDPiRated – Stealing Personal Information On- and Offline 367
Matteo Cagnazzo, Thorsten Holz, and Norbert Pohlmann

Location Privacy-Preserving Mobile Crowd Sensing with Anonymous Reputation 387
Xun Yi, Kwok-Yan Lam, Elisa Bertino, and Fang-Yu Rao

OCRAM-Assisted Sensitive Data Protection on ARM-Based Platform 412
Dawei Chu, Yuewu Wang, Lingguang Lei, Yanchu Li, Jiwu Jing, and Kun Sun

Privacy-Preserving Collaborative Medical Time Series Analysis Based on Dynamic Time Warping 439
Xiaoning Liu and Xun Yi

Key Exchange Protocols

IoT-Friendly AKE: Forward Secrecy and Session Resumption Meet Symmetric-Key Cryptography 463
Gildas Avoine, Sébastien Canard, and Loïc Ferreira

Strongly Secure Identity-Based Key Exchange with Single Pairing Operation 484
Junichi Tomida, Atsushi Fujioka, Akira Nagai, and Koutarou Suzuki

A Complete and Optimized Key Mismatch Attack on NIST Candidate NewHope 504
Yue Qin, Chi Cheng, and Jintai Ding

Breakdown Resilience of Key Exchange Protocols: NewHope, TLS 1.3, and Hybrids 521
Jacqueline Brendel, Marc Fischlin, and Felix Günther

Web Security

The Risks of WebGL: Analysis, Evaluation and Detection 545
Alex Belkin, Nethanel Gelernter, and Israel Cidon

Mime Artist: Bypassing Whitelisting for the Web with JavaScript Mimicry Attacks 565
Stefanos Chaliasos, George Metaxopoulos, George Argyros, and Dimitris Mitropoulos

Fingerprint Surface-Based Detection of Web Bot Detectors 586
Hugo Jonker, Benjamin Krumnow, and Gabry Vlot

Testing for Integrity Flaws in Web Sessions 606
Stefano Calzavara, Alvise Rabitti, Alessio Ragazzo, and Michele Bugliesi

Author Index 625