

*Commenced Publication in 1973*

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

## Editorial Board

David Hutchison

*Lancaster University, Lancaster, UK*

Takeo Kanade

*Carnegie Mellon University, Pittsburgh, PA, USA*

Josef Kittler

*University of Surrey, Guildford, UK*

Jon M. Kleinberg

*Cornell University, Ithaca, NY, USA*

Friedemann Mattern

*ETH Zurich, Zurich, Switzerland*

John C. Mitchell

*Stanford University, Stanford, CA, USA*

Moni Naor

*Weizmann Institute of Science, Rehovot, Israel*

C. Pandu Rangan

*Indian Institute of Technology Madras, Chennai, India*

Bernhard Steffen

*TU Dortmund University, Dortmund, Germany*

Demetri Terzopoulos

*University of California, Los Angeles, CA, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

Gerhard Weikum

*Max Planck Institute for Informatics, Saarbrücken, Germany*

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

Andrea Saracino · Paolo Mori (Eds.)

# Emerging Technologies for Authorization and Authentication

First International Workshop, ETAA 2018  
Barcelona, Spain, September 7, 2018  
Proceedings

*Editors*  
Andrea Saracino  
IIT-CNR  
Pisa, Italy

Paolo Mori  
IIT-CNR  
Pisa, Italy

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-030-04371-1              ISBN 978-3-030-04372-8 (eBook)  
<https://doi.org/10.1007/978-3-030-04372-8>

Library of Congress Control Number: 2018962143

LNCS Sublibrary: SL4 – Security and Cryptology

© Springer Nature Switzerland AG 2018

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, express 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 selected for presentation at the First International Workshop on Emerging Technologies for Authorization and Authentication (ETAA 2018), which was held in Barcelona, Spain, on September 7, 2018, co-located with the 23rd European Symposium on Research in Computer Security (ESORICS 2018).

The workshop program included eight full papers and two short ones concerning the workshop topics, in particular: new techniques for biometric and behavioral-based authentication, authentication and authorization in the IoT and in distributed systems in general, techniques for strengthening password-based authentication and for dissuading malicious users from stolen password reuse, an approach for discovering authentication vulnerabilities in interconnected accounts, and strategies to optimize the access control decision process in the big data scenario.

We would like to express our thanks to the authors who submitted their papers to the first edition of this workshop, thus contributing to making it a successful event. We would like to thank the sponsors of the workshop: the EU Commission-funded projects: Collaborative and Confidential Information Sharing and Analysis for Cyber Protection (**C3ISP**), and European Network for Cyber Security (**NeCS**), Marie Skłodowska-Curie Actions (MSCA), and Innovative Training Networks (ITN). Last but not least, we would like to express our gratitude to the members of the Technical Program Committee for their valuable work in evaluating the submitted papers.

This workshop was supported by the EU Commission-funded projects:

**C3ISP:** Collaborative and Confidential Information Sharing and Analysis for Cyber Protection. Grant Agreement no. 700294

**NeCS:** European Network for Cyber Security, Grant Agreement no. 675320

September 2018

Paolo Mori  
Andrea Saracino

## **ETAA Workshop Introduction**

IT devices are rapidly becoming more pervasive in several application fields and in everyday life. The major driving factors are the ever-increasing coverage of Internet connectivity, the extreme popularity and capillarity of smartphones, tablets, and wearables, together with the consolidation of the Internet of Things (IoT) paradigm. Indeed, interconnected devices directly control and take decisions on industrial processes, regulate infrastructures and services in smart cities, and manage quality of life and safety in smart homes, taking decisions with user interactions or even autonomously. The involvement of these devices in so many applications unfortunately introduces a set of unavoidable security and safety implications, related to both the criticality of the aforementioned applications and to the privacy of sensitive information produced and exploited in the process. To address these and other related issues, there is an increasing need of instruments to control the access and the right to perform specific actions on devices or data. These instruments must be able to cope with the high complexity of the considered applications and environments, being flexible and adaptable to different contexts and architectures, from centralized to fully distributed ones, able to handle a high amount of information as well as taking into account non-conventional trust assumptions. The considered technologies should regulate the actions of both human users and autonomous devices, being effective in enforcing security policies, still without introducing noticeable overhead, both in terms of performance and user experience. Hence, the design of advanced, secure, and efficient mechanisms for continuous authentication and authorization, requiring limited-to-no active interaction is solicited.

The ETAA workshop aimed at being a forum for researchers and practitioners of security who are active in the field of new technologies for authenticating users and devices, and for enforcing security policies in new and emerging applications related to distributed systems, mobile/wearable devices, and IoT. It aimed to attract original research work covering both theoretical and practical aspects of authentication and authorization.

Paolo Mori  
Andrea Saracino



# Contents

## Authentication and Authorization Techniques

Authentication and Authorization for Interoperable IoT Architectures. . . . .	3
<i>Nikos Fotiou and George C. Polyzos</i>	
Bringing Access Control Tree to Big Data . . . . .	17
<i>Francesco Di Cerbo and Marco Rosa</i>	
SNAPAUTH: A Gesture-Based Unobtrusive Smartwatch User Authentication Scheme . . . . .	30
<i>Attaullah Buriro, Bruno Crispo, Mojtaba Eskandri, Sandeep Gupta, Athar Mahboob, and Rutger Van Acker</i>	
A Protocol to Strengthen Password-Based Authentication. . . . .	38
<i>Itzel Vazquez Sandoval, Borce Stojkovski, and Gabriele Lenzini</i>	
Managing Private Credentials by Privacy-Preserving Biometrics . . . . .	47
<i>Bian Yang and Guoqiang Li</i>	
Policy Support for Autonomous Swarms of Drones. . . . .	56
<i>Alan Cullen, Erisa Karafili, Alan Pilgrim, Chris Williams, and Emil Lupu</i>	

## Violation Detection and Countermeasures

A Logic-Based Reasoner for Discovering Authentication Vulnerabilities Between Interconnected Accounts . . . . .	73
<i>Erisa Karafili, Daniele Sgandurra, and Emil Lupu</i>	
Towards a Framework for Testing the Security of IoT Devices Consistently . . .	88
<i>Gurjan Lally and Daniele Sgandurra</i>	
Misuse Detection in a Simulated IaaS Environment. . . . .	103
<i>Burhan Al-Bayati, Nathan Clarke, Paul Dowland, and Fudong Li</i>	
Dissuading Stolen Password Reuse . . . . .	116
<i>Slim Trabelsi and Chedy Missaoui</i>	

<b>Author Index</b> . . . . .	129
-------------------------------	-----