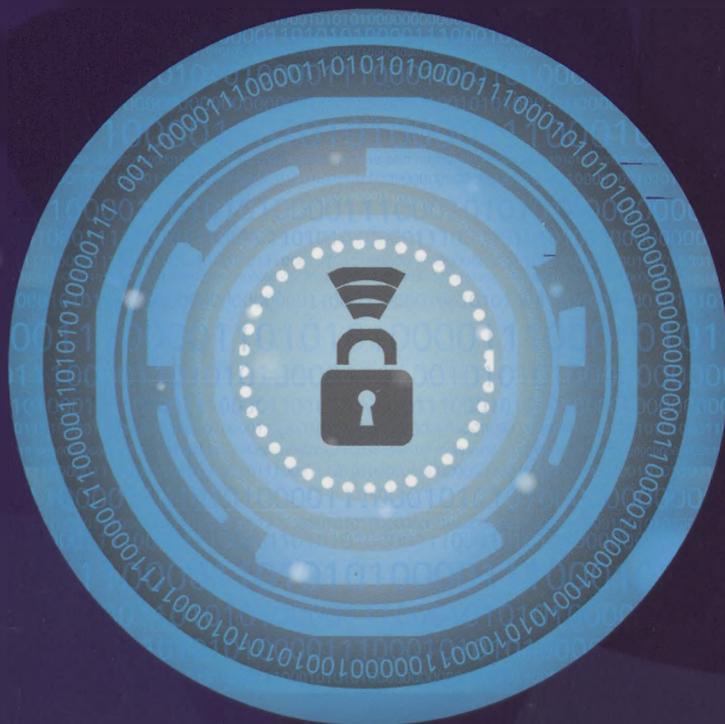


River Publishers Series in Security and Digital Forensics

**CHALLENGES IN
CYBERSECURITY AND PRIVACY –
THE EUROPEAN RESEARCH
LANDSCAPE**



Editors:
Jorge Bernal Bernabe
Antonio Skarmeta



River Publishers

Challenges in Cybersecurity and Privacy – the European Research Landscape

RIVER PUBLISHERS SERIES IN SECURITY AND DIGITAL FORENSICS

Series Editors:

WILLIAM J. BUCHANAN

Edinburgh Napier University, UK

ANAND R. PRASAD

NEC, Japan

Indexing: All books published in this series are submitted to the Web of Science Book Citation Index (BkCI), to SCOPUS, to CrossRef and to Google Scholar for evaluation and indexing.

The “River Publishers Series in Security and Digital Forensics” is a series of comprehensive academic and professional books which focus on the theory and applications of Cyber Security, including Data Security, Mobile and Network Security, Cryptography and Digital Forensics. Topics in Prevention and Threat Management are also included in the scope of the book series, as are general business Standards in this domain.

Books published in the series include research monographs, edited volumes, handbooks and textbooks. The books provide professionals, researchers, educators, and advanced students in the field with an invaluable insight into the latest research and developments.

Topics covered in the series include, but are by no means restricted to the following:

- Cyber Security
- Digital Forensics
- Cryptography
- Blockchain
- IoT Security
- Network Security
- Mobile Security
- Data and App Security
- Threat Management
- Standardization
- Privacy
- Software Security
- Hardware Security

For a list of other books in this series, visit www.riverpublishers.com

Challenges in Cybersecurity and Privacy – the European Research Landscape

Editors

Jorge Bernal Bernabe

Antonio Skarmeta

University of Murcia, Spain



River Publishers

Published, sold and distributed by:

River Publishers
Alsbjergvej 10
9260 Gistrup
Denmark

River Publishers
Lange Geer 44
2611 PW Delft
The Netherlands

Tel.: +45369953197
www.riverpublishers.com

ISBN: 978-87-7022-088-0 (Hardback)
978-87-7022-087-3 (Ebook)

©The Editor(s) (if applicable) and The Author(s) 2019. This book is published open access.

Open Access

This book is distributed under the terms of the Creative Commons Attribution-Non-Commercial 4.0 International License, CC-BY-NC 4.0) (<http://creativecommons.org/licenses/by/4.0/>), which permits use, duplication, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, a link is provided to the Creative Commons license and any changes made are indicated. The images or other third party material in this book are included in the work's Creative Commons license, unless indicated otherwise in the credit line; if such material is not included in the work's Creative Commons license and the respective action is not permitted by statutory regulation, users will need to obtain permission from the license holder to duplicate, adapt, or reproduce the material.

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.

Printed on acid-free paper.

Contents

Preface	xv
List of Contributors	xix
List of Figures	xxxi
List of Tables	xxxv
List of Abbreviations	xxxvii
1 Introducing the Challenges in Cybersecurity and Privacy: The European Research Landscape	1
<i>Jorge Bernal Bernabe and Antonio Skarmeta</i>	
1.1 Introduction	1
1.2 Cybersecurity and Privacy Research Challenges	4
1.2.1 Main Cybersecurity Research Challenges	5
1.2.2 Privacy and Trust Related Research Challenges	11
1.3 H2020 Projects Facing the Challenges	13
1.3.1 Cybersecurity Related Projects Addressing the Challenges	13
1.3.2 H2020 Projects Addressing the Privacy and Trust Related Challenges	16
1.4 Conclusion	18
References	19

2	Key Innovations in ANASTACIA: Advanced Networked Agents for Security and Trust Assessment in CPS/IOT Architectures	23
	<i>Jorge Bernal Bernabe, Alejandro Molina, Antonio Skarmeta, Stefano Bianchi, Enrico Cambiaso, Ivan Vaccari, Silvia Scaglione, Maurizio Aiello, Rubén Trapero, Mathieu Bouet, Dallal Belabed, Miloud Bagaa, Rami Addad, Tarik Taleb, Diego Rivera, Alie El-Din Mady, Adrian Quesada Rodriguez, Cédric Crettaz, Sébastien Ziegler, Eunah Kim, Matteo Filipponi, Bojana Bajic, Dan Garcia-Carrillo and Rafael Marin-Perez</i>	
2.1	Introduction	24
2.2	The Anastacia Approach	26
2.2.1	Anastacia Architecture Overview	26
2.3	Anastacia Main Innovation Processes	28
2.3.1	Holistic Policy-based Security Management and Orchestration in IOT	28
2.3.2	Investigation on Innovative Cyber-threats	31
2.3.2.1	IoT 0-day attack	31
2.3.2.2	Slow DoS attacks	32
2.3.3	Trusted Security Orchestration in SDN/NFV-enabled IOT Scenarios	33
2.3.4	Dynamic Orchestration of Resources Planning in Security-oriented SDN and NFV Synergies	39
2.3.4.1	Resource planning module	39
2.3.4.2	The security enablers selection	40
2.3.4.3	Mobile edge computing resources optimization	40
2.3.4.4	Security enabler provider	41
2.3.5	Security Monitoring to Threat Detection in SDN/NFV-enabled IOT Deployments	41
2.3.5.1	Security monitoring and reaction infrastructure	41
2.3.5.2	Novel products for IoT- and cloud-based SDN/NFV systems	43

2.3.6	Cyber Threats Automated and Cognitive Reaction and Mitigation Components	44
2.3.7	Behaviour Analysis, Anomaly Detection and Automated Testing for the Detection of Known and Unknown Vulnerabilities in both Physical and Virtual Environments	46
2.3.8	Secured and Authenticated Dynamic Seal System as a Service	47
2.4	Conclusion	50
	References	51
3	Statistical Analysis and Economic Models for Enhancing Cyber-security in SAINT	55
	<i>Edgardo Montes de Oca, John M. A. Bothos and Stefan Schiffner</i>	
3.1	Introduction	56
3.2	SAINT Objectives and Results	57
3.2.1	Main SAINT Objectives	57
3.2.2	Main SAINT Results	58
3.2.2.1	Metrics for cyber-security economic analysis, cyber-security and cyber-crime market	58
3.2.2.2	Economic models for the reduction of cyber-crime as a cost-benefit operation	59
3.2.2.3	Benefits and costs of information sharing regarding cyber-attacks	61
3.2.2.4	Privacy and security level of internet applications, services and technologies	62
3.2.2.5	Benefits and costs of investing in cyber-security	63
3.2.2.6	Framework of automated analysis, for behavioural, social analysis, cyber-security risk and cost assessment	66
3.2.2.7	Recommendations to stakeholders	68
3.3	Conclusion	71
	References	73

- 4 The FORTIKA Accelerated Edge Solution for Automating SMEs Security 77**
Evangelos K. Markakis, Yannis Nikoloudakis, Evangelos Pallis, Ales Černivec, Panayotis Fouliras, Ioannis Mavridis, Georgios Sakellariou, Stavros Salonikias, Nikolaos Tsinganos, Anargyros Sideris, Nikolaos Zotos, Anastasios Drosou, Konstantinos M. Giannoutakis and Dimitrios Tzovaras
 - 4.1 Introduction 77
 - 4.2 Related Work and Background 81
 - 4.3 Technical Approach 83
 - 4.3.1 FORTIKA Accelerator 84
 - 4.3.2 Fortika Marketplace 89
 - 4.4 Indicative FORTIKA Bundles 91
 - 4.4.1 Attribute-based Access Control (ABAC) 91
 - 4.5 Social Engineering Attack Recognition Service (SEARS) 94
 - 4.6 Conclusion 98
 - References 99

- 5 CYBECO: Supporting Cyber-Insurance from a Behavioural Choice Perspective 103**
Nikos Vassileiadis, Aitor Couce Vieira, David Ríos Insua, Vassilis Chatzigiannakis, Sofia Tsekeridou, Yolanda Gómez, José Vila, Deepak Subramanian, Caroline Baylon, Katsiaryna Labunets, Wolter Pieters, Pamela Briggs and Dawn Branley-Bell
 - 5.1 Introduction 104
 - 5.2 An Ecosystem for Cybersecurity and Cyber-Insurance 105
 - 5.3 The Basic Cybeco Model: Choosing the Optimal Cybersecurity and Cyber-Insurance Portfolio 107
 - 5.4 Validating CYBECO 109
 - 5.5 The CYBECO Decision Support Tool 111
 - 5.6 Conclusion 113
 - References 114

- 6 Cyber-Threat Intelligence from European-wide Sensor Network in SISSDEN 117**
Edgardo Montes de Oca, Jart Armin and Angelo Consoli
 - 6.1 Introduction 118
 - 6.2 SISSDEN Objectives and Results 119
 - 6.2.1 Main SISSDEN Objectives 119

6.2.2	Technical Architecture	121
6.2.2.1	Remote endpoint sensors (VPS)	121
6.2.2.2	Frontend servers	121
6.2.2.3	External partner and third-party systems	122
6.2.2.4	Backend servers	122
6.2.2.5	External reporting system	123
6.2.2.6	Utility server	123
6.2.3	Concrete Examples	124
6.2.3.1	Use Case 1: Targeted Cowrie attack that can be anticipated by the analysis of the traffic before it occurs	124
6.2.3.2	Use Case 2: Understanding the numbers – metrics	125
6.3	Conclusion	127
	References	128

7 CIPSEC-Enhancing Critical Infrastructure Protection with Innovative Security Framework 129

Antonio Álvarez, Rubén Trapero, Denis Guilhot, Ignasi García-Mila, Francisco Hernandez, Eva Marín-Tordera, Jordi Forne, Xavi Masip-Bruin, Neeraj Suri, Markus Heinrich, Stefan Katzenbeisser, Manos Athanatos, Sotiris Ioannidis, Leonidas Kallipolitis, Ilias Spais, Apostolos Fournaris and Konstantinos Lampropoulos

7.1	Introduction	130
7.1.1	Motivation and Background	130
7.1.2	CIPSEC Challenges	131
7.2	Project Innovations	133
7.3	CIPSEC Framework	135
7.3.1	CIPSEC Architecture	135
7.3.1.1	CIPSEC core components	139
7.3.1.2	CIPSEC collectors	140
7.4	CIPSEC Integration	141
7.5	CIPSEC Pilots	142
7.5.1	Integration of the Solution in the Pilots	143
7.5.2	Testing the Proposed Solution in the Pilots	145
7.6	Dissemination and Exploitation	146
7.6.1	Dissemination	146
7.6.2	Exploitation	146
7.7	Conclusions	147
	References	148

8	A Cybersecurity Situational Awareness and Information-Sharing Solution for Local Public Administrations Based on Advanced Big Data Analysis: The CS-AWARE Project	149
	<i>Thomas Schaberreiter, Juha Rönning, Gerald Quirchmayr, Veronika Kupfersberger, Chris Wills, Matteo Bregonzio, Adamantios Koumpis, Juliano Efson Sales, Laurentiu Vasiliu, Kim Gammelgaard, Alexandros Papanikolaou, Konstantinos Rantos and Arnolt Spyros</i>	
8.1	Introduction	150
8.2	Related Work	152
8.3	The CS-AWARE Concept and Framework	156
8.4	Framework Implementation	160
	8.4.1 System and Dependency Analysis	160
	8.4.2 Data Collection and Pre-Processing	163
	8.4.3 Multi-language Support	164
	8.4.4 Data Analysis	165
	8.4.5 Visualization	168
	8.4.6 Cybersecurity Information Exchange	170
	8.4.7 System Self-Healing	172
8.5	Discussion	175
8.6	Conclusion	176
	References	178
9	Complex Project to Develop Real Tools for Identifying and Countering Terrorism: Real-time Early Detection and Alert System for Online Terrorist Content Based on Natural Language Processing, Social Network Analysis, Artificial Intelligence and Complex Event Processing	181
	<i>Monica Florea, Cristi Potlog, Peter Pollner, Daniel Abel, Oscar Garcia, Shmuel Bar, Syed Naqvi and Waqar Asif</i>	
9.1	Introduction	182
9.2	Research Challenges Addressed	183
9.3	Architecture Overview	185
9.4	Results	187
	9.4.1 Natural Language Processing Module (NLP)	187
	9.4.2 Complex Event Processing Module (CEP)	192
	9.4.3 Semantic Multimedia Analysis Tool (SMA)	194
	9.4.3.1 Speech recognition	195
	9.4.3.2 Face detection	195
	9.4.3.3 Object detection	195

9.4.3.4	Audio event detection	196
9.4.4	Social Network Analysis Module (SNA)	196
9.5	Data Anonymization Tool	199
9.6	Data Networked Privacy Tool	201
9.7	Integration Component	202
9.8	Future Research Challenges	204
	References	205
10	TRUESSEC Trustworthiness Label Recommendations	207
	<i>Danny S. Guamán, Manel Medina, Pablo López-Aguilar, Hristina Veljanova, José M. del Álamo, Valentin Gibello, Martin Griesbacher and Ali Anjomshoaa</i>	
10.1	Introduction	208
10.2	Interdisciplinary Requirements	209
10.3	Criteria Catalogue and Indicators	212
10.4	Operationalization of the TRUESSEC.eu Core Areas of Trustworthiness	217
10.5	Recommendations	221
10.5.1	Questionnaire	222
10.5.2	Labelling Portal	224
10.5.3	Transparency Report and Visual Label	226
10.5.4	Governance and Authority	227
10.6	Conclusions	228
	References	230
11	An Overview on ARIES: Reliable European Identity Ecosystem	231
	<i>Jorge Bernal Bernabe, Rafael Torres, David Martin, Alberto Crespo, Antonio Skarmeta, Dave Fortune, Juliet Lodge, Tiago Oliveira, Marlos Silva, Stuart Martin, Julian Valero and Ignacio Alamillo</i>	
11.1	Introduction	232
11.2	The Aries Ecosystem	233
11.3	Main Innovative Processes in Aries	236
11.3.1	Fraud Prevention and Cyber-crime Investigation	236
11.3.2	Biometric Enrolment and Authentication	237
11.3.3	Privacy-by-Design Features (Anonymous Credential Systems)	238
11.4	The ARIES Ethical and Legal Approach	239
11.4.1	Ethical Impact Assessment	239

11.4.2	Technological Innovation Informed by Ethical Awareness	239
11.4.3	The Socio-ethical Challenge	239
11.4.4	ARIES Starting Point: What is Meant by Ethics?	240
11.4.5	Embedding the Dominant Ethical Principle: Do No Harm	240
11.4.6	Baked in Ethics for the ARIES Use Cases	241
11.4.7	Ethics in the ARIES Use Cases	242
11.4.8	Legal Challenges and Lessons Learned in ARIES	243
11.5	ARIES Ecosystem Validation	245
11.5.1	E-Commerce	245
11.5.2	Airport Scenario Pilot and Validation	246
11.6	Cyber-security and Privacy Research Challenges	249
11.7	Conclusion	251
	References	252

12 The LIGHTest Project: Overview, Reference Architecture and Trust Scheme Publication Authority 255

Heiko Roßnagel and Sven Wagner

12.1	Introduction	255
12.2	Related Work	257
12.3	Reference Architecture	258
12.3.1	Components of the Reference Architecture	258
12.3.2	Usage Scenarios	260
12.4	Trust Scheme Publication Authority	262
12.4.1	Trust Schemes and Trust Scheme Publications	262
12.4.2	Concept for Trust Scheme Publication Authority (TSPA)	263
12.4.3	DNS-based Trust Scheme Publication and Discovery	265
12.5	Trust Policy	266
12.6	Discussion and Outlook	267
12.7	Summary	268
	References	269

13 Secure and Privacy-Preserving Identity and Access Management in CREDENTIAL 271

Peter Hamm, Stephan Krenn and John Sören Pettersson

13.1	Introduction	271
13.1.1	CREDENTIAL Ambition	272

13.2	Cryptographic Background	273
13.2.1	Proxy Re-encryption	273
13.2.2	Redactable Signatures	274
13.3	Solution Overview	274
13.3.1	Added Value of the CREDENTIAL Wallet	276
13.4	Showcasing CREDENTIAL in Real-World Pilots	277
13.4.1	Pilot Domain 1: eGovernment	277
13.4.2	Pilot Domain 2: eHealth	278
13.4.3	Pilot Domain 3: eBusiness	279
13.5	Conclusion and Open Challenges	280
13.5.1	Recommendations on Usability and Accessibility	281
13.5.2	Open Challenges	281
	References	283

14 FutureTrust – Future Trust Services for Trustworthy Global Transactions **285**

*Detlef Hühnlein, Tilman Frosch, Jörg Schwenk,
 Carl-Markus Piswanger, Marc Sel, Tina Hühnlein, Tobias Wich,
 Daniel Nemmert, René Lottes, Stefan Baszanowski, Volker Zeuner,
 Michael Rauh, Juraj Somorovsky, Vladislav Mladenov,
 Cristina Condovici, Herbert Leitold, Sophie Stalla-Bourdillon,
 Niko Tsakalakis, Jan Eichholz, Frank-Michael Kamm,
 Jens Urmann, Andreas Kühne, Damian Wabisch, Roger Dean,
 Jon Shamah, Mikheil Kapanadze, Nuno Ponte, Jose Martins,
 Renato Portela, Çağatay Karabat, Snežana Stojičić,
 Slobodan Nedeljkovic, Vincent Bouckaert, Alexandre Defays,
 Bruce Anderson, Michael Jonas, Christina Hermanns,
 Thomas Schubert, Dirk Wegener and Alexander Sazonov*

14.1	Background and Motivation	287
14.2	The FutureTrust Project	290
14.2.1	FutureTrust Partners	290
14.2.2	FutureTrust System Architecture	291
14.2.3	Global Trust List (gTSL)	292
14.2.4	Comprehensive Validation Service (Vals)	293
14.2.5	Scalable Preservation Service (PresS)	293
14.2.6	Identity Management Service (IdMS)	294
14.2.7	Signing and Sealing Service (SigS)	295

14.2.8 FutureTrust Pilot Applications	297
14.2.9 The go.eIDAS Initiative	297
14.3 Summary and Invitation for Further Collaboration	298
References	298
15 LEPS – Leveraging eID in the Private Sector	303
<i>Jose Crespo Martín, Nuria Ituarte Aranda, Raquel Cortés Carreras, Aljosa Pasic, Juan Carlos Pérez Baún, Katerina Ksystra, Nikos Triantafyllou, Harris Papadakis, Elena Torroglosa and Jordi Ortiz</i>	
15.1 Introduction	304
15.2 Solution Design	305
15.2.1 LEPS Mobile App	309
15.3 Implementation	309
15.4 Validation	312
15.5 Related Work	314
15.6 Market Analysis	316
15.7 Conclusion	319
References	319
Index	323
About the Editors	327

CHALLENGES IN CYBERSECURITY AND PRIVACY THE EUROPEAN RESEARCH LANDSCAPE

Biblioteka Główna
Akademii Sztuki Wojennej

26770/III (CB)



03-026770-000-0

**Jorge Bernal Bernabe and
Antonio Skarmeta (Editors)**

Cybersecurity and Privacy issues are becoming an important barrier for a trusted and dependable global digital society development. Cyber-criminals are continuously shifting their cyber-attacks specially against cyber-physical systems and IoT, since they present additional vulnerabilities due to their constrained capabilities, their unattended nature and the usage of potential untrustworthiness components. Likewise, identity-theft, fraud, personal data leakages, and other related cyber-crimes are continuously evolving, causing important damages and privacy problems for European citizens in both virtual and physical scenarios.

In this context, new holistic approaches, methodologies, techniques and tools are needed to cope with those issues, and mitigate cyberattacks, by employing novel cyber-situational awareness frameworks, risk analysis and modeling, threat intelligent systems, cyber-threat information sharing methods, advanced big-data analysis techniques as well as exploiting the benefits from latest technologies such as SDN/NFV and Cloud systems. In addition, novel privacy-preserving techniques, and crypto-privacy mechanisms, identity and eID management systems, trust services, and recommendations are needed to protect citizens' privacy while keeping usability levels.

The European Commission is addressing the challenge through different means, including the Horizon 2020 Research and Innovation program, thereby financing innovative projects that can cope with the increasing cyberthreat landscape. This book introduces several cybersecurity and privacy research challenges and how they are being addressed in the scope of 14 European research projects.

Each chapter is dedicated to a different funded European Research project, which aims to cope with digital security and privacy aspects, risks, threats and cybersecurity issues from a different perspective. Each chapter includes the project's overviews and objectives, the particular challenges they are covering, research achievements on security and privacy, as well as the techniques, outcomes, and evaluations accomplished in the scope of the EU project.

The book is the result of a collaborative effort among relative ongoing European Research projects in the field of privacy and security as well as related cybersecurity fields, and it is intended to explain how these projects meet the main cybersecurity and privacy challenges faced in Europe. Namely, the EU projects analyzed in the book are: ANASTACIA, SAINT, FORTIKA, CYBECO, SISSDEN, CIPSEC, CS-AWARE, RED-Alert, Truessec.eu, ARIES, LIGHTest, CREDENTIAL, FutureTrust, LEPS.

Challenges in Cybersecurity and Privacy – the European Research Landscape is ideal for personnel in computer/communication industries as well as academic staff and master/research students in computer science and communications networks interested in learning about cyber-security and privacy aspects.

ISBN 978-87-7022-088-0



9 788770 220880



River Publishers