

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, 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/7411>

Jacek Rak · John Bay · Igor Kotenko
Leonard Popyack · Victor Skormin
Krzysztof Szczypiorski (Eds.)

Computer Network Security

7th International Conference
on Mathematical Methods, Models, and Architectures
for Computer Network Security, MMM-ACNS 2017
Warsaw, Poland, August 28–30, 2017
Proceedings

Editors

Jacek Rak
Gdansk University of Technology
Gdansk
Poland

John Bay
Binghamton University
Binghamton, NY
USA

Igor Kotenko
St. Petersburg Institute
for Informatics and Automation
St. Petersburg
Russia

Leonard Popyack
Utica College
Utica, NY
USA

Victor Skormin
Binghamton University
Binghamton, NY
USA

Krzysztof Szczypiorski
Warsaw University of Technology
Warsaw
Poland

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-319-65126-2

ISBN 978-3-319-65127-9 (eBook)

DOI 10.1007/978-3-319-65127-9

Library of Congress Control Number: 2017948184

LNCS Sublibrary: SL5 – Computer Communication Networks and Telecommunications

© Springer International Publishing AG 2017

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.

Printed on acid-free paper

This Springer imprint is published by Springer Nature

The registered company is Springer International Publishing AG

The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

This volume contains papers presented at the 7th International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security (MMM-ACNS 2017) held in Warsaw, Poland during August 28–30, 2017. The conference was organized by Gdansk University of Technology, in cooperation with Binghamton University (State University of New York), USA, and the Polish Association of Telecommunication Engineers (SIT), Poland.

MMM-ACNS 2017 followed six former editions of MMM-ACNS all hosted by St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS), RU. MMM-ACNS 2017 provided an international forum for sharing the original results referring to fundamental as well as applied problems in the context of computer network security. Special focus was put on mathematical aspects of information and computer network security.

In all, 40 regular papers submitted to the conference were subject to extensive reviews. Each paper received at least three reviews (and some of them as many as five reviews). Finally, 12 papers were accepted as full papers, and 13 papers as short papers. Approved regular papers were organized into seven technical sessions, namely:

- Critical Infrastructure Protection and Visualization
- Security and Resilience of Network Systems
- Adaptive Security
- Anti-malware Techniques: Detection, Analysis, Prevention
- Security of Emerging Technologies
- Applied Cryptography
- New Ideas and Paradigms for Security

The conference program was enhanced by three invited talks and two keynote speeches (by Dipankar Dasgupta from USA, and Antanas Cenys from Lithuania, accordingly).

The success of the conference was undoubtedly due to the team effort of the organizers, reviewers, and participants. In particular, we would like to acknowledge the individual contributions of the Technical Program Committee members and reviewers. Our sincere gratitude goes to all the participants of the conference as well as to Polish Association of Telecommunication Engineers, SIT, Poland (in particular to Ewa Woroszyło and Mirosław Stando), for their great help in solving the local arrangement issues.

August 2017

Jacek Rak
John Bay
Igor Kotenko
Leonard Popyack
Victor Skormin
Krzysztof Szczypiorski

Organization

General Co-chairs

Jacek Rak	Gdansk University of Technology, Poland
John Bay	Binghamton University (State University of New York), USA

Steering Committee

John Bay	Binghamton University (State University of New York), USA
Igor Kotenko	St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences, SPIRAS, Russia
Leonard Popyack	Utica College, USA
Jacek Rak	Gdansk University of Technology, Poland
Victor Skormin	Binghamton University (State University of New York), USA

Publication Chair

Krzysztof Szczypiorski	Warsaw University of Technology, Poland
------------------------	---

Local Organizing Committee

Andrzej Dulka	Polish Association of Telecommunication Engineers, Poland
Wojciech Halka	Polish Association of Telecommunication Engineers, Poland
Mirosław Stando	Polish Association of Telecommunication Engineers, Poland
Ewa Woroszyło	Polish Association of Telecommunication Engineers, Poland

Program Committee

Ryszard Antkiewicz	Military University of Technology, Poland
Cataldo Basile	Politecnico di Torino, Italy
Fabrizio Bayardi	University of Pisa, Italy
Nataliia Bielova	Inria, France
Elias Bou-Harb	Florida Atlantic University, USA
Julien Bourgeois	University of Franche-Comté/FEMTO-ST, France

Mariano Ceccato	Fondazione Bruno Kessler, Italy
Shiu-Kai Chin	Syracuse University, USA
Michal Choras	University of Technology and Life Sciences, Poland
Miguel Correia	INESC-ID, Portugal
Frédéric Cuppens	TELECOM Bretagne, France
Changyu Dong	Newcastle University, UK
Paolo Falcarin	University of East London, UK
Dennis Gamayunov	Lomonosov Moscow State University, Russia
Dieter Gollmann	Technical University of Hamburg-Harburg, Germany
Kartik Gopalan	Binghamton University (State University of New York), USA
Stefanos Gritzalis	University of the Aegean, Greece
Alexander Grusho	Institute of Informatics Problems FRC CSC RAS, Russia
Ming-Yuh Huang	Northwest Security Institute, USA
Andrew Hutchison	University of Cape Town, South Africa
Sushil Jajodia	George Mason University, USA
Bartosz Jasiul	Military Communication Institute, Poland
Alexey Kirichenko	F-Secure Corporation, Finland
Kevin Kwiat	Air Force Research Laboratory, USA
Jean-François Lalande	INSA Centre Val de Loire, France
Hanno Langweg	Norwegian Information Security Laboratory, Norway
Peeter Laud	University of Tartu, Estonia
Giovanni Livraga	Università degli Studi di Milano, Italy
Fabio Martinelli	CNR-IIT, Italy
Catherine Meadows	Naval Research Laboratory, USA
Stig Frode Mjolsnes	Norwegian University of Science and Technology, Norway
Nikolay Moldovyan	University of St. Petersburg, Russia
Wojciech Molisz	Gdansk University of Technology, Poland
Haris Mouratidis	University of Brighton, UK
Vladimir Oleshchuk	University of Agder, Norway
Piotr Pacyna	AGH University of Science and Technology, Poland
Josef Pieprzyk	Queensland University of Technology, Australia
Dmitry Ponomarev	Binghamton University (State University of New York), USA
Alfredo Rial	University of Luxembourg, Luxembourg
Roland Rieke	Fraunhofer, Germany
Andrzej Rucinski	University of New Hampshire, USA
Igor Saenko	Saint-Petersburg Institute for Informatics and Automation of Russian Academy of Sciences (SPIIRAS), Russia
Françoise Sailhan	CNAM, France
Victor Skormin	Binghamton University (State University of New York), USA

Douglas Summerville

Jerzy Surma

Nadia Tawabi

Bhavani Thuraisingham

Arnur Tokhtabayev

Shambhu Upadhyaya

Janusz Zalewski

Binghamton University

(State University of New York), USA

Warsaw School of Economics, Poland

Laval University, Canada

The University of Texas at Dallas, USA

T&T Security LLP, Kazakhstan

University at Buffalo, USA

Florida Gulf Coast University, USA

Additional Reviewers

Marios Anagnostopoulos

Spyros Kokolakis

Michał Misztal

Francesco Mercaldo

Christos Kalloniatis

Nael Abu-Ghazaleh

Singapore University of Technology and Design,
Singapore

University of the Aegean, Greece

Military University of Technology, Poland

Consiglio Nazionale delle Ricerche, Italy

University of the Aegean, Greece

University of California, Riverside, USA

Contents

Invited Papers

Meeting Requirements Imposed by Secure Software Development Standards and Still Remaining Agile	3
<i>Janusz Górski and Katarzyna Łukasiewicz</i>	
Adapting Enterprise Security Approaches for Evolving Cloud Processing and Networking Models.	16
<i>Andrew Hutchison</i>	
Data Mining and Information Security	28
<i>Alexander Grusho</i>	

Critical Infrastructure Protection and Visualization

Extending FAST-CPS for the Analysis of Data Flows in Cyber-Physical Systems	37
<i>Laurens Lemaire, Jan Vossaert, Bart De Decker, and Vincent Naessens</i>	
Visualization-Driven Approach to Anomaly Detection in the Movement of Critical Infrastructure.	50
<i>Evgenia Novikova and Ivan Murenin</i>	
Detection and Mitigation of Time Delay Injection Attacks on Industrial Control Systems with PLCs	62
<i>Emrah Korkmaz, Matthew Davis, Andrey Dolgikh, and Victor Skormin</i>	
Choosing Models for Security Metrics Visualization	75
<i>Maxim Kolomeec, Gustavo Gonzalez-Granadillo, Elena Doynikova, Andrey Chechulin, Igor Kotenko, and Hervé Debar</i>	

Security and Resilience of Network Systems

iCrawl: A Visual High Interaction Web Crawler	91
<i>Deeraj Nagothu and Andrey Dolgikh</i>	
Race Condition Faults in Multi-core Systems	104
<i>Leonard Popyack and Jay Biernat</i>	
Security Requirements for the Deployment of Services Across Tactical SOA	115
<i>Vasileios Gkioulos and Stephen D. Wolthusen</i>	

Adaptive Security

Nodal Cooperation Equilibrium Analysis in Multi-hop Wireless Ad Hoc Networks with a Reputation System	131
<i>Jerzy Konorski and Karol Rydzewski</i>	
Network Anomaly Detection Based on an Ensemble of Adaptive Binary Classifiers	143
<i>Alexander Branitskiy and Igor Kotenko</i>	
Cardholder's Reputation System for Contextual Risk Management in Payment Transactions	158
<i>Albert Sitek and Zbigniew Kotulski</i>	
Towards Self-aware Approach for Mobile Devices Security	171
<i>Nanda Kumar Thanigaivelan, Ethiopia Nigussie, Seppo Virtanen, and Jouni Isoaho</i>	

Anti-malware Techniques: Detection, Analysis, Prevention

Resident Security System for Government/Industry Owned Computers	185
<i>Matthew Davis, Emrah Korkmaz, Andrey Dolgikh, and Victor Skormin</i>	
tLab: A System Enabling Malware Clustering Based on Suspicious Activity Trees.	195
<i>Anton Kopeikin, Arnur Tokhtabayev, Nurlan Tashatov, and Dina Satybaldina</i>	
Malware Analysis and Detection via Activity Trees in User-Dependent Environment	211
<i>Arnur Tokhtabayev, Anton Kopeikin, Nurlan Tashatov, and Dina Satybaldina</i>	
A Concept of Clustering-Based Method for Botnet Detection	223
<i>Hubert Ostap and Ryszard Antkiewicz</i>	

Security of Emerging Technologies

Easy 4G/LTE IMSI Catchers for Non-Programmers.	235
<i>Stig F. Mjølunes and Ruxandra F. Olimid</i>	
Anomaly Detection in Cognitive Radio Networks Exploiting Singular Spectrum Analysis	247
<i>Qi Dong, Zekun Yang, Yu Chen, Xiaohua Li, and Kai Zeng</i>	
HEPPA: Highly Efficient Privacy Preserving Authentication for ITS	260
<i>An Braeken, Sergey Bezzateev, Abdellah Touhafi, and Natalia Voloshina</i>	

Applied Cryptography

Automated Cryptographic Analysis of the Pedersen Commitment Scheme . . .	275
<i>Roberto Metere and Changyu Dong</i>	
Steganalysis Based on Statistical Properties of the Encrypted Messages	288
<i>Valery Korzhik, Ivan Fedyanin, Artur Godlewski, and Guillermo Morales-Luna</i>	
Security Assessment of Cryptographic Algorithms.	299
<i>Marcin Niemiec and Maciej Francikiewicz</i>	
Quick Response Code Secure: A Cryptographically Secure Anti-Phishing Tool for QR Code Attacks	313
<i>Vasileios Mavroeidis and Mathew Nicho</i>	

New Ideas and Paradigms for Security

A Novel and Unifying View of Trustworthiness in Cyberphysical Systems . . .	327
<i>Steven Drager and Janusz Zalewski</i>	
Information Security of SDN on the Basis of Meta Data	339
<i>Alexander Grusho, Nick Grusho, Michael Zabezhailo, Alexander Zatsarinny, and Elena Timonina</i>	
Toward Third-Party Immune Applications	348
<i>Omar Iraqi and Hanan El Bakkali</i>	
Author Index	361