Lecture Notes in Computer Science **10744**

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

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

Peng Liu · Sjouke Mauw
Ketil Stølen (Eds.)

Graphical Models for Security

4th International Workshop, GraMSec 2017
Santa Barbara, CA, USA, August 21, 2017
Revised Selected Papers

Springer

Editors
Peng Liu
Pennsylvania State University
University Park, PA
USA

Ketil Stølen
SINTEF ICT Blindern
Oslo
Norway

Sjouke Mauw
University of Luxembourg
Esch-sur-Alzette
Luxembourg

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-74859-7 ISBN 978-3-319-74860-3 (eBook)
https://doi.org/10.1007/978-3-319-74860-3

Library of Congress Control Number: 2018930744

LNCS Sublibrary: SL4 – Security and Cryptology

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

Welcome to the proceedings of GraMSec 2017, the 4th International Workshop on Graphical Models for Security. This workshop seeks to bring together researchers from academia, government, and industry to report on the latest research and development results on graphical models for security, and to have productive discussion and constructive debate on this topic. The workshop was a single day event co-located with the 30th IEEE Computer Security Foundations Symposium (CSF 2017). Out of a total of 19 submissions from Europe and North America, we accepted five regular papers and four short papers.

These proceedings also contain the abstract of an invited talk by Anoop Singhal (U.S. National Institute of Standards and Technology) on "Security Metrics and Risk Analysis for Enterprise Systems." This valuable and insightful talk gave us a better understanding of the topic. In addition, these proceedings include an invited paper by members of the WISER project, entitled "Employing Graphical Risk Models to Facilitate Cyber-Risk Monitoring – the WISER Approach." We expect that the results and experiences from this project will help the reader to explore the WISER approach to graphical modeling for security.

Putting together GraMSec 2017 was a team effort. We thank all authors who submitted papers. We thank the Program Committee members and additional reviewers for their great effort toward a thought-provoking program. We are also very grateful to the invited speaker for his presentation and the financial support received from the Fonds National de la Recherche Luxembourg (FNR-CORE grant ADT2P). Finally, we thank the IEEE CSF organizers, particularly the general chair, Pedro Adão, for his support and help.

December 2017

Peng Liu
Sjouke Mauw
Ketil Stølen

Organization

Program Committee

Mathieu Acher	University Rennes 1/Inria, France
Massimiliano Albanese	George Mason University, USA
Ludovic Apvrille	Télécom ParisTech, CNRS LTCI, France
Thomas Bauereiß	University of Cambridge, UK
Kristian Beckers	Technical University of Munich, Germany
Giampaolo Bella	Università di Catania, Italy
Stefano Bistarelli	Università di Perugia, Italy
Marc Bouissou	EDF and Ecole Centrale Paris, France
Binbin Chen	Advanced Digital Sciences Center, Singapore
Frédéric Cuppens	Télécom Bretagne, France
Nora Cuppens-Boulahia	Télécom Bretagne, France
Hervé Debar	Télécom SudParis, France
Harley Eades Iii	Augusta University, USA
Mathias Ekstedt	KTH Royal Institute of Technology, Sweden
Ulrik Franke	Swedish Institute of Computer Science, Sweden
Frank Fransen	TNO, The Netherlands
Olga Gadyatskaya	University of Luxembourg, Luxembourg
Paolo Giorgini	University of Trento, Italy
Dieter Gollmann	Hamburg University of Technology, Germany
Joshua Guttman	Worcester Polytechnic Institute, USA
René Rydhof Hansen	Aalborg University, Denmark
Maritta Heisel	University of Duisburg-Essen, Germany
Hannes Holm	Swedish Defence Research Agency, Sweden
Siv Hilde Houmb	Secure-NOK AS, Norway
Sushil Jajodia	George Mason University, USA
Ravi Jhawar	University of Luxembourg, Luxembourg
Henk Jonkers	BiZZdesign, The Netherlands
Florian Kammueller	Middlesex University London, UK and TU Berlin, Germany
Nima Khakzad	Delft University of Technology, The Netherlands
Dong Seong Kim	University of Canterbury, New Zealand
Barbara Kordy	INSA Rennes, IRISA, France
Pascal Lafourcade	Université Clermont Auvergne, France
Jean-Louis Lanet	Inria, France
Peng Liu	Pennsylvania State University, USA
Sjouke Mauw	University of Luxembourg, Luxembourg

Per Håkon Meland	SINTEF, Norway
Jogesh Muppala	Hong Kong University of Science and Technology, SAR China
Simin Nadjm-Tehrani	Linköping university, Sweden
Andreas L. Opdahl	University of Bergen, Norway
Xinming Ou	University of South Florida, USA
Stéphane Paul	Thales Research and Technology, France
Wolter Pieters	Delft University of Technology, The Netherlands
Sophie Pinchinat	University Rennes 1, IRISA, France
Vincenzo Piuri	University of Milan, Italy
Ludovic Piètre-Cambacédès	EDF, France
Marc Pouly	Lucerne University of Applied Sciences and Arts, Switzerland
Nicolas Prigent	Supélec, France
Cristian Prisacariu	University of Oslo, Norway
Christian W. Probst	Technical University of Denmark, Denmark
David Pym	University College London
Saša Radomirović	University of Dundee, UK
Indrajit Ray	Colorado State University, USA
Arend Rensink	University of Twente, The Netherlands
Yves Roudier	Université Côte d'Azur, CNRS, I3S, UNS, France
Guttorm Sindre	Norwegian University of Science and Technology, Norway
Mariëlle Stoelinga	University of Twente, The Netherlands
Ketil Stølen	SINTEF, Norway
Xiaoyan Sun	California State University, USA
Axel Tanner	IBM Research - Zurich, Switzerland
Alexandre Vernotte	KTH Royal Institute of Technology, Sweden
Luca Viganò	King's College London, UK
Lingyu Wang	Concordia University, Canada
Jan Willemson	Cybernetica, Estonia

Additional Reviewers

Audinot, Maxime
Puys, Maxime
Venkatesan, Sridhar

Security Metrics and Risk Analysis for Enterprise Systems (Abstract of Invited Talk)

Anoop Singhal

Computer Security Division, National Institute of Standards and Technology (NIST), Gaithersburg, MD 20899, USA
psinghal@nist.gov

Abstract. Protection of enterprise systems from cyber attacks is a challenge. Vulnerabilities are regularly discovered in software systems that are exploited to launch cyber attacks. Security analysts need objective metrics to manage the security risk of an enterprise systems. In this talk, we give an overview of our research on *security metrics* and *challenges* for security risk analysis of enterprise systems. A standard model for security metrics will enable us to answer questions such as "are we more secure than yesterday" or "how does the security of one system compare with another?" We present a methodology for security risk analysis that is based on the model of attack graphs and the common vulnerability scoring system (CVSS).

Contents