

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/7410>

Eric Bodden · Mathias Payer
Elias Athanasopoulos (Eds.)

Engineering Secure Software and Systems

9th International Symposium, ESSoS 2017
Bonn, Germany, July 3–5, 2017
Proceedings

Editors

Eric Bodden
University of Paderborn
Paderborn
Germany

Elias Athanasopoulos
University of Cyprus
Nicosia
Cyprus

Mathias Payer
Purdue University
West Lafayette
USA

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-62104-3 ISBN 978-3-319-62105-0 (eBook)
DOI 10.1007/978-3-319-62105-0

Library of Congress Control Number: 2017944218

LNCS Sublibrary: SL4 – Security and Cryptology

© 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

It is our pleasure to welcome you to the proceedings of the 9th International Symposium on Engineering Secure Software and Systems (ESSoS 2017), co-located with the conference on Detection of Intrusions and Malware and Vulnerability Assessment (DIMVA 2017). ESSoS is part of a maturing series of symposia that attempts to bridge the gap between the software engineering and security communities with the goal of supporting secure software development. The parallel technical sponsorship from ACM SIGSAC (the ACM interest group in security) and ACM SIGSOFT (the ACM interest group in software engineering) demonstrates the support from both communities and the need for providing such a bridge.

Security mechanisms and the act of software development usually go hand in hand. It is generally not enough to ensure correct functioning of the security mechanisms used. They cannot be blindly inserted into a security-critical system, but the overall system development must take security aspects into account in a coherent way. Building trustworthy components does not suffice, since the interconnections and interactions of components play a significant role in trustworthiness. Lastly, while functional requirements are generally analyzed carefully in systems development, security considerations often arise after the fact. Adding security as an afterthought, however, often leads to problems. Ad hoc development can lead to the deployment of systems that do not satisfy important security requirements. Thus, a sound methodology supporting secure systems development is needed. The presentations and associated publications at ESSoS 2017 contributed to this goal in several directions: first, by improving methodologies for secure software engineering (such as flow analysis and policy compliance). Second, with results for the detection and analysis of software vulnerabilities and the attacks they enable. Finally, for securing software for specific application domains (such as mobile devices and access control).

The conference program featured two keynotes by Konrad Rieck (TU Braunschweig) and Cristiano Giuffrida (VU Amsterdam), as well as research and idea papers. In response to the call for papers, 32 papers were submitted. The Program Committee selected 12 full-paper contributions, presenting new research results on engineering secure software and systems. In addition, three idea papers were selected, giving a concise account of new ideas in the early stages of research. Many individuals and organizations contributed to the success of this event. First of all, we would like to express our appreciation to the authors of the submitted papers and to the Program Committee members and external reviewers, who provided timely and relevant reviews. Many thanks go to the Steering Committee for supporting this series of symposia, and to all the members of the Organizing Committee for their tremendous work and for excelling in their respective tasks. We owe gratitude to ACM SIGSAC/SIGSOFT and LNCS for continuing to support us in this series of symposia.

Finally, we thank the sponsors ERNW, genua, Huawei, Rohde & Schwarz Cybersecurity, and VMRay for generously supporting the ESSoS and DIMVA conferences this year.

May 2017

Eric Bodden
Mathias Payer
Elias Athanasopoulos

Organization

Program Committee

| | |
|----------------------|---|
| David Aspinall | University of Edinburgh, UK |
| Domagoj Babic | Google Inc., USA |
| Alexandre Bartel | University of Luxembourg, Luxembourg |
| Amel Bennaceur | The Open University, UK |
| Stefan Brunthaler | Paderborn University, Germany |
| Will Enck | NC State University, USA |
| Michael Franz | University of California, Irvine, USA |
| Christian Hammer | University of Potsdam, Germany |
| Michael Hicks | University of Maryland, USA |
| Trent Jaeger | The Pennsylvania State University, USA |
| Vassilis P. Kemerlis | Brown University, USA |
| Johannes Kinder | University of London, UK |
| Byoungyoung Lee | Purdue University, USA |
| Yang Liu | University of Oxford, UK |
| Ben Livshits | Imperial College London, UK |
| Clémentine Maurice | Technical University Graz, Austria |
| Andy Meneely | Rochester Institute of Technology, USA |
| Mira Mezini | Technical University Darmstadt, Germany |
| Alessandro Orso | Georgia Tech, USA |
| Christina Pöpper | New York University Abu Dhabi, UAE |
| Awais Rashid | Lancaster University, UK |
| Kaveh Razavi | Vrije Universiteit Amsterdam, The Netherlands |
| Tamara Rezk | Inria, France |
| Angela Sasse | University College London, UK |
| Zhendong Su | University of California, Davis, USA |
| Melanie Volkamer | Karlstad University, Sweden |
| Xiangyu Zhang | Purdue University, USA |

Contents

| | |
|---|-----|
| SEQUOIA: Scalable Policy-Based Access Control for Search Operations in Data-Driven Applications | 1 |
| <i>Jasper Bogaerts, Bert Lagaisse, and Wouter Joosen</i> | |
| A Voucher-Based Security Middleware for Secure Business Process Outsourcing | 19 |
| <i>Emad Heydari Beni, Bert Lagaisse, Ren Zhang, Danny De Cock, Filipe Beato, and Wouter Joosen</i> | |
| LASARUS: Lightweight Attack Surface Reduction for Legacy Industrial Control Systems | 36 |
| <i>Anhtuan Le, Utz Roedig, and Awais Rashid</i> | |
| Exploring the Relationship Between Architecture Coupling and Software Vulnerabilities | 53 |
| <i>Robert Lagerström, Carliss Baldwin, Alan MacCormack, Dan Sturtevant, and Lee Doolan</i> | |
| Natural Language Insights from Code Reviews that Missed a Vulnerability: A Large Scale Study of Chromium | 70 |
| <i>Nuthan Munaiah, Benjamin S. Meyers, Cecilia O. Alm, Andrew Meneely, Pradeep K. Murukannaiah, Emily Prud'hommeaux, Josephine Wolff, and Yang Yu</i> | |
| Idea: Optimized Automatic Sanitizer Placement | 87 |
| <i>Gebrehiwet Biyane Welearegai and Christian Hammer</i> | |
| FPRandom: Randomizing Core Browser Objects to Break Advanced Device Fingerprinting Techniques | 97 |
| <i>Pierre Laperdrix, Benoit Baudry, and Vikas Mishra</i> | |
| Control What You Include!: Server-Side Protection Against Third Party Web Tracking | 115 |
| <i>Dolière Francis Somé, Nataliia Bielova, and Tamara Rezk</i> | |
| Idea-Caution Before Exploitation: The Use of Cybersecurity Domain Knowledge to Educate Software Engineers Against Software Vulnerabilities | 133 |
| <i>Tayyaba Nafees, Natalie Coull, Robert Ian Ferguson, and Adam Sampson</i> | |

| | |
|---|-----|
| Defeating Zombie Gadgets by Re-randomizing Code upon Disclosure | 143 |
| <i>Micah Morton, Hyungjoon Koo, Forrest Li, Kevin Z. Snow, Michalis Polychronakis, and Fabian Monroe</i> | |
| KASLR is Dead: Long Live KASLR. | 161 |
| <i>Daniel Gruss, Moritz Lipp, Michael Schwarz, Richard Fellner, Clémentine Maurice, and Stefan Mangard</i> | |
| JTR: A Binary Solution for Switch-Case Recovery | 177 |
| <i>Lucian Cojocar, Taddeus Kroes, and Herbert Bos</i> | |
| A Formal Approach to Exploiting Multi-stage Attacks Based on File-System Vulnerabilities of Web Applications | 196 |
| <i>Federico De Meo and Luca Viganò</i> | |
| A Systematic Study of Cache Side Channels Across AES Implementations | 213 |
| <i>Heiko Mantel, Alexandra Weber, and Boris Köpf</i> | |
| Idea: A Unifying Theory for Evaluation Systems | 231 |
| <i>Giampaolo Bella and Rosario Giustolisi</i> | |
| Author Index | 241 |