More information about this series at http://www.springer.com/series/7410
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
  Jasper Bogaerts, Bert Lagaisse, and Wouter Joosen

A Voucher-Based Security Middleware for Secure Business Process Outsourcing .......................................................................................... 19
  Emad Heydari Beni, Bert Lagaisse, Ren Zhang, Danny De Cock, Filipe Beato, and Wouter Joosen

LASARUS: Lightweight Attack Surface Reduction for Legacy Industrial Control Systems ............................................................... 36
  Anhtuan Le, Utz Roedig, and Awais Rashid

Exploring the Relationship Between Architecture Coupling and Software Vulnerabilities ............................................................. 53
  Robert Lagerström, Carliss Baldwin, Alan MacCormack, Dan Sturtevant, and Lee Doolan

Natural Language Insights from Code Reviews that Missed a Vulnerability: A Large Scale Study of Chromium ................................................. 70
  Nuthan Munaiah, Benjamin S. Meyers, Cecilia O. Alm, Andrew Meneely, Pradeep K. Murukannaiah, Emily Prud’hommeaux, Josephine Wolff, and Yang Yu

Idea: Optimized Automatic Sanitizer Placement ................................................................................................................................. 87
  Gebrehiwet Biyane Welearegai and Christian Hammer

FPRandom: Randomizing Core Browser Objects to Break Advanced Device Fingerprinting Techniques .................................................. 97
  Pierre Laperdrix, Benoit Baudry, and Vikas Mishra

Control What You Include!: Server-Side Protection Against Third Party Web Tracking ................................................................. 115
  Dolière Francis Somé, Nataliia Bielova, and Tamara Rezk

Idea-Caution Before Exploitation: The Use of Cybersecurity Domain Knowledge to Educate Software Engineers Against Software Vulnerabilities ......................................................... 133
  Tayyaba Nafees, Natalie Coull, Robert Ian Ferguson, and Adam Sampson
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defeating Zombie Gadgets by Re-randomizing Code upon Disclosure</td>
<td>143</td>
</tr>
<tr>
<td>Micah Morton, Hyungjoon Koo, Forrest Li, Kevin Z. Snow,</td>
<td></td>
</tr>
<tr>
<td>Michalis Polychronakis, and Fabian Monrose</td>
<td></td>
</tr>
<tr>
<td>KASLR is Dead: Long Live KASLR.</td>
<td>161</td>
</tr>
<tr>
<td>Daniel Gruss, Moritz Lipp, Michael Schwarz, Richard Fellner,</td>
<td></td>
</tr>
<tr>
<td>Clémentine Maurice, and Stefan Mangard</td>
<td></td>
</tr>
<tr>
<td>JTR: A Binary Solution for Switch-Case Recovery</td>
<td>177</td>
</tr>
<tr>
<td>Lucian Cojocar, Taddeus Kroes, and Herbert Bos</td>
<td></td>
</tr>
<tr>
<td>A Formal Approach to Exploiting Multi-stage Attacks Based</td>
<td>196</td>
</tr>
<tr>
<td>on File-System Vulnerabilities of Web Applications</td>
<td></td>
</tr>
<tr>
<td>Federico De Meo and Luca Viganò</td>
<td></td>
</tr>
<tr>
<td>A Systematic Study of Cache Side Channels Across AES</td>
<td>213</td>
</tr>
<tr>
<td>Implementations</td>
<td></td>
</tr>
<tr>
<td>Heiko Mantel, Alexandra Weber, and Boris Köpf</td>
<td></td>
</tr>
<tr>
<td>Idea: A Unifying Theory for Evaluation Systems</td>
<td>231</td>
</tr>
<tr>
<td>Giampaolo Bella and Rosario Giustolisi</td>
<td></td>
</tr>
<tr>
<td>Author Index</td>
<td>241</td>
</tr>
</tbody>
</table>