Lecture Notes in Computer Science 8364

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

Jan Jürjens Frank Piessens
Nataliia Bielova (Eds.)

Engineering Secure Software and Systems

6th International Symposium, ESSoS 2014
Munich, Germany, February 26-28, 2014
Proceedings

Springer

Volume Editors

Jan Jürjens
Technical University Dortmund
Department of Computer Science
Dortmund, Germany
E-mail: jan.juerjens@isst.fraunhofer.de

Frank Piessens
KU Leuven
Department of Computer Science
Heverlee, Belgium
E-mail: frank.piessens@cs.kuleuven.be

Nataliia Bielova
Inria Sophia Antipolis – Mediterranee
Sophia Antipolis Cedex, France
E-mail: nataliia.bielova@inria.fr

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-319-04896-3 e-ISBN 978-3-319-04897-0
DOI 10.1007/978-3-319-04897-0
Springer Cham Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014930756

CR Subject Classification (1998): E.3, D.4.6, D.2.1, D.2.4, F.3.1, K.6.5

LNCS Sublibrary: SL 4 – Security and Cryptology

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

It is our pleasure to welcome you to the 6th International Symposium on Engineering Secure Software and Systems (ESSoS 2014). This event in a maturing series of symposia attempts to bridge the gap between the scientific communities from software engineering and security 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 2014 contribute to this goal in several directions: On the one hand, with secure software engineering results for specific application domains (such as Web and mobile security). On the other hand, improving specific methods in secure software engineering (such as model-based security or formal methods). A third set of presentations presents real-life applications of secure software engineering approaches.

The conference program featured three major keynotes from Ross Anderson (University of Cambridge) on the psychology of security, Adrian Perrig (ETH Zurich) on scalability, control, and isolation for next-generation networks, and Stephan Micklitz (Google Munich) on human factors and strong authentication, as well as a set of research and idea papers. In response to the call for papers, 55 papers were submitted. The Program Committee selected 11 full-paper contributions (20%), presenting new research results on engineering secure software and systems. In addition, there are four idea papers, giving a concise account of new ideas in the early stages of research.

Many individuals and organizations have 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 referees, 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. The DistriNet research group of the KU Leuven did an excellent job with the website and the advertising for the conference. Finally, we owe gratitude to ACM SIGSAC/SIGSOFT, IEEE TCSP, and LNCS for continuing to support us in this series of symposia.

December 2013

Jan Jürjens
Frank Piessens
Nataliia Bielova

Conference Organization

General Chair

Alexander Pretschner	Technische Universität München, Germany

Program Co-chairs

Jan Jürjens	TU Dortmund and Fraunhofer ISST, Germany
Frank Piessens	Katholieke Universiteit Leuven, Belgium

Publication Chair

Nataliia Bielova	Inria Sophia Antipolis, France

Publicity Chair

Pieter Philippaerts	Katholieke Universiteit Leuven, Belgium

Web Chair

Ghita Saevels	Katholieke Universiteit Leuven, Belgium

Local Arrangements Chair

Regina Jourdan	Technische Universität München, Germany

Steering Committee

Jorge Cuellar	Siemens AG, Germany
Wouter Joosen	Katholieke Universiteit Leuven, Belgium
Fabio Massacci	Universitá di Trento, Italy
Gary McGraw	Cigital, USA
Bashar Nuseibeh	The Open University, UK
Daniel Wallach	Rice University, USA

Program Committee

Ruth Breu	University of Innsbruck, Austria
Lorenzo Cavallaro	Royal Holloway, University of London, UK
Anupam Datta	Carnegie Mellon University, USA
Werner Dietl	University of Washington, USA
François Dupressoir	IMDEA, Spain
Eduardo Fernandez	Florida Atlantic University, USA
Eduardo Fernandez-Medina Paton	Universidad de Castilla-La Mancha, Spain
Cormac Flanagan	U.C. Santa Cruz, USA
Dieter Gollmann	TU Hamburg-Harburg, Germany
Arjun Guha	Cornell University, USA
Christian Hammer	Saarland University, Germany
Hannes Hartenstein	Karlsruher Institut für Technologie, Germany
Maritta Heisel	University of Duisburg Essen, Germany
Peter Herrmann	NTNU, Trondheim, Norway
Valerie Issarny	Inria, France
Limin Jia	Carnegie Mellon University, USA
Martin Johns	SAP Research, Germany
Jay Ligatti	University of South Florida, USA
Heiko Mantel	TU Darmstadt, Germany
Haris Mouratidis	University of East London, UK
Martín Ochoa	Siemens AG, Germany
Jae Park	University of Texas at San Antonio, USA
Erik Poll	RU Nijmegen, The Netherlands
Wolfgang Reif	University of Augsburg, Germany
Riccardo Scandariato	Katholieke Universiteit Leuven, Belgium
Ketil Stølen	SINTEF, Norway
Steve Zdancewic	University of Pennsylvania, USA
Mohammad Zulkernine	Queens University, Canada

Additional Reviewers

Azadeh Alebrahim	Kuzman Katkalov	David Pfaff
Kristian Beckers	Basel Katt	Fredrik Seehusen
Abhishek Bichhawat	Johannes Leupolz	Christian Sillaber
Marian Borek	Yan Li	Bjørnar Solhaug
Michael Brunner	Steffen Lortz	Barbara Sprick
Gencer Erdogan	Rene Meis	Kurt Stenzel
Stephan Faßbender	Jan Tobias Muehlberg	Lianshan Sun
Matthias Gander	Sebastian Pape	Marie Walter
Jinwei Hu	Davide Papini	Philipp Zech

Sponsoring Institutions

Technische Universität München, Germany

NESSoS FP7 Project, Network of Excellence on Engineering Secure Future Internet Software Services and Systems, www.nessos-project.eu

Keynote Abstracts

The Psychology of Security

Ross Anderson

University of Cambridge, UK

Abstract. A fascinating dialogue is developing between psychologists and security engineers. At the macro scale, societal overreactions to terrorism are founded on the misperception of risk and uncertainty, which has deep psychological roots. At the micro scale, more and more crimes involve deception; as security engineering gets better, it's easier to mislead people than to hack computers or hack through walls. Many frauds can be explained in terms of the heuristics and biases that we have retained from our ancestral evolutionary environment.

At an even deeper level, the psychology of security touches on fundamental scientific and philosophical problems. The 'Machiavellian Brain' hypothesis states that we evolved high intelligence not to make better tools, but to use other monkeys better as tools: primates who were better at deception, or at detecting deception in others, left more descendants. Yet the move online is changing the parameters of deception, and robbing us of many of the signals we use to make trust judgments in the "real" world; it's a lot easier to copy a bank website than it is to copy a bank. Many systems fail because the security usability has not been thought through: the designers have different mental models of threats and protection mechanisms from users. And misperceptions cause security markets to fail: many users buy snake oil, while others distrust quite serviceable mechanisms.

Security is both a feeling and a reality, and they're different. The gap gets ever wider, and ever more important. In this talk I will describe the rapidly-growing field of security psychology which is bringing together security engineers not just with psychologists but with behavioural economists, anthropologists and even philosophers to develop new approaches to risk, fraud and deception in the complex socio-technical systems on which we are all coming to rely.

SCION: Scalability, Control, and Isolation On Next-Generation Networks

Adrian Perrig

Swiss Federal Institute of Technology (ETH), Switherland

Abstract. We present an Internet architecture designed to provide route control, failure isolation, and explicit trust information for end-to-end communications. SCION separates ASes into groups of independent routing sub-planes, called isolation domains, which then interconnect to form complete routes. Isolation domains provide natural separation of routing failures and human misconfiguration, give endpoints strong control for both inbound and outbound traffic, provide meaningful and enforceable trust, and enable scalable routing updates with high path freshness. As a result, our architecture provides strong resilience and security properties as an intrinsic consequence of good design principles, avoiding piecemeal add-on protocols as security patches. Meanwhile, SCION only assumes that a few top-tier ISPs in the isolation domain are trusted for providing reliable end-to-end communications, thus achieving a small Trusted Computing Base. Both our security analysis and evaluation results show that SCION naturally prevents numerous attacks and provides a high level of resilience, scalability, control, and isolation.

Human Factors and Strong Authentication

Stephan Micklitz

Google Munich, Germany

Abstract. Google's login team began focusing on strong authentication in the spring of 2008, and in almost six years we have come a long way in protecting our users. In this presentation we will talk about the progress we have made since then, such as introducing strict 2-step verification, risk-based login challenges and OpenID-style login.

We will then identify the biggest challenges we are currently facing in establishing stronger authentication – both from a technological as well as a usability point of view. We will also talk important privacy considerations for such systems, and how we are addressing them. Next we will look into our plan to address these challenges in the next years ahead of us, making use of technological developments, e.g. the vastly increased adoption of smart mobile devices.

Table of Contents

Model-Based Security

Formal Methods

Web and Mobile Security

Applications