PLAS 2017 – ACM SIGSAC Workshop on Programming Languages and Analysis for Security

Nataliia Bielova
INRIA
nataliia.bielova@inria.fr

Marco Gaboardi
University at Buffalo, The State University of New York
gaboardi@buffalo.edu

ABSTRACT

The 12^{th} ACM SIGSAC Workshop on Programming Languages and Analysis for Security (PLAS 2017) is co-located with the ACM Conference on Computer and Communications Security (CCS). Over its now more than ten-year history, PLAS has provided a unique forum for researchers and practitioners to exchange ideas about programming language and program analysis techniques with the goal of improving the security of software systems.

PLAS aims to provide a forum for exploring and evaluating ideas on using programming language and program analysis techniques to improve the security of software systems. Strongly encouraged are proposals of new, speculative ideas, evaluations of new or known techniques in practical settings, and discussions of emerging threats and important problems.

CCS CONCEPTS

• **Security and privacy → Software and application security**;

KEYWORDS

programming languages; security

1 INTRODUCTION

PLAS aims to provide a forum for exploring and evaluating ideas on the use of programming language and program analysis techniques to improve the security of software systems. Strongly encouraged are proposals of new, speculative ideas, evaluations of new or known techniques in practical settings, and discussions of emerging threats and important problems. We are especially interested in position papers that are radical, forward-looking, and likely to lead to lively and insightful discussions that will influence future research that lies at the intersection of programming languages and security.

2 SCOPE

The scope of PLAS includes, but is not limited to:

- Compiler-based security mechanisms (e.g. security type systems) or runtime-based security mechanisms (e.g. inline reference monitors)
- Program analysis techniques for discovering security vulnerabilities
- Automated introduction and/or verification of security enforcement mechanisms
- Language-based verification of security properties in software, including verification of cryptographic protocols
- Specifying and enforcing security policies for information flow and access control
- Model-driven approaches to security
- Security concerns for Web programming languages
- Language design for security in new domains such as cloud computing and IoT
- Applications, case studies, and implementations of these techniques

3 WORKSHOP FORMAT

This year, PLAS received a good number of submissions attesting the continued vitality of the community whose work sits at the intersection of programming languages and security.

PLAS 2017 welcomed the submission of both long research papers as well as short papers presenting preliminary or exploratory work aiming at generating lively discussions at the workshop. PLAS 2017 attracted 16 submissions—of which, 6 were short papers—from 9 countries (Australia, France, Germany, India, Singapore, Sweden, Taiwan, UK, USA), with authors spanning both academia and industry.

PLAS 2017 is delighted to have two excellent invited talks:

- Authorization Contracts, Stephen Chong (Harvard University)
- Languages for Oblivious Computation, Michael Hicks (University of Maryland)

4 PROGRAM COMMITTEE MEMBERS

- Mario Alvim, Universidade Federal de Minas Gerais, Brazil
- Aslan Askarov, Aarhus University, Denmark
- Lujo Bauer, Carnegie Mellon University, USA
- Nataliia Bielova, INRIA, France, Co-chair
- Marco Gaboardi, University at Buffalo, SUNY, USA, Co-chair
- Deepak Garg, MPI Software Systems, Germany
- Kevin Hamlen, University of Texas at Dallas, USA
- Boris Koepf, IMDEA Software Institute, Spain
- Steve Kremer, Loria & Inria, France
- Scott Moore Galois Inc, USA
- Frank Piessens, DistriNet, Katholieke Universiteit Leuven, Belgium
- Omer Tripp, Google, USA
- Danfeng Zhang, Penn State University, USA

CCS'17, , October 30–November 3, 2017, Dallas, TX, USA

ACM ISBN ISBN 978-1-4503-4946-8/17/10.
https://doi.org/http://dx.doi.org/10.1145/3133956.3137045

5 WORKSHOP ORGANISERS

Nataliia Bielova (PC co-chair) is a Research Scientist in the Secure Diffuse Programming group at Inria (French Institute for Research in Computer Science and Automation). Nataliia's research examines how to apply programming language analysis to security and privacy of web applications. In her latest work, Nataliia has been focusing on merging language-based information flow control with runtime monitoring to detect web tracking scripts. Nataliia is organising a Dagstuhl seminar on Online Privacy and Web Transparency and participated multiple times in the program committees of the major conferences and journals in formal methods and security (ACM TISSEC, IEEE CSF, POST), where she herself has a number of publications.

Marco Gaboardi (PC co-chair) is an Assistant Professor in the Department of Computer Science and Engineering at the University at Buffalo, SUNY. Previously, he was a faculty at the University of Dundee, Scotland. Marco's research is in programming language design and implementation, and in differential privacy. In particular, he has been developing different language-based techniques for the verification of differential privacy. Marco has been involved in the organization of two Dagstuhl seminars, a NII Shonan meeting, a NII Shonan school. He has been the PC chair of four international workshops and has been on the program committees of major conferences in programming languages and security.

6 ACKNOWLEDGMENTS

We would like to thank all the authors who has submitted contributions to PLAS and the program committee members who have helped in reviewing. Thanks also to the invited speakers Stephen Chong and Michael Hicks who have kindly accepted our invitation. Finally, we would like to thank INRIA for financial support.