PLAS'16 – ACM SIGPLAN 11th Workshop on Programming Languages and Analysis for Security

Toby Murray
University of Melbourne and Data61
toby.murray@unimelb.edu.au

Deian Stefan
UC San Diego and Intrinsic
deian@cs.ucsd.edu

This year, 2016, marks the 11th *ACM SIGPLAN Workshop on Programming Languages and Analysis for Security* (PLAS). For the first time since PLAS began in 2006, PLAS is co-located with the *ACM Conference on Computer and Communications Security* (CCS). Over its now ten-year history, PLAS has provided a forum for researchers and practitioners to exchange ideas about programming language and program analysis techniques that improve the security of software systems.

PLAS started as a workshop co-located with the *ACM SIGPLAN Conference on Programming Language Design and Implementation* (PLDI) and remained co-located with PLDI for the following seven years. In its ninth and tenth installment PLAS was co-located with *European Conference on Object-Oriented Programming* (ECOOP). This year therefore marks a new phase in the growth of PLAS as it takes place—for the first time—not with a Programming Languages (PL) conference but instead with the ACM's premier conference on Security.

PLAS naturally sits at the intersection of these two diverse and vibrant fields. In the decade since PLAS's inception, the line between PL and Security has continued to blur as each field has further matured. Greenberg et al. [3] empirically documented the increasing presence of Security work in top PL conferences, as part of their recent study on the diffusion of ideas in PL literature. Likewise, many high-profile PL achievements in the Security literature over the past decade have highlighted how essential PL research is for the construction of secure systems. As but one example consider the formally verified TLS implementation miTLS [2], developed and verified in the dependently typed programming language F*, which led to the discovery of a range of flaws in mainstream TLS implementations [1].

The need for secure system development to be underpinned by solid PL foundations has not diminished, but is growing evermore. The recent attack [4] on the Ethereum smart contracts of The DAO aptly highlights this. As do the almost-weekly large-scale website breaches.

CCS'16 October 24-28, 2016, Vienna, Austria

ACM ISBN 978-1-4503-4139-4/16/10…$15.00

DOI: http://dx.doi.org/10.1145/2976749.2990484

Thus, it is perhaps no surprise that, this year, PLAS received its third-highest number of submissions in its ten-year history. PLAS has always welcomed the submission of both long research papers as well as short papers presenting preliminary or exploratory work. But, in a slight departure from previous years, the 2016 Call for Papers explicitly solicited short position papers likely to generate lively discussion, presenting radical, open-ended and forward-looking ideas. The Call for Papers attracted 21 submissions, of which 10 where short papers, from 13 countries (Australia, Belgium, Canada, Czech Republic, Denmark, Estonia, France, Germany, India, Italy, Romania, Sweden, USA), spanning academia and industry.

This year's program is composed of exciting papers that (1) employ foundational PL techniques to address security issues in a number of application domains—from web applications to smart contracts and smart homes—and (2) advance and question the state of the art in language-based security mechanisms (e.g., information flow control). Complementing these are two invited talks on the intersection of PL and Security coming from both industry and academia.

Besides the excellent program that promises lively discussion and debate across the day, PLAS 2016 will benefit from increased participation from students and those from under-represented groups, thanks to the generous support of Oracle, Data61 and Intrinsic that has enabled us to offer travel grants in 2016.

We are looking forward to hosting one of the most lively installments of PLAS to date.

References

[1] B. Beurdouche, K. Bhargavan, A. Delignat-Lavaud, C. Fournet, M. Kohlweiss, A. Pironti, P.-Y. Strub, and J. K. Zinzindohoue. A messy state of the union: Taming the composite state machines of TLS. In *IEEE Symposium on Security and Privacy*, pages 535–552, May 2015.

[2] K. Bhargavan, C. Fournet, M. Kohlweiss, A. Pironti, and P.-Y. Strub. Implementing TLS with verified cryptographic security. In *IEEE Symposium on Security and Privacy*, pages 445–459, May 2013.

[3] M. Greenberg, K. Fisher, and D. Walker. Tracking the flow of ideas through the programming languages literature. In *1st Summit on Advances in Programming Languages (SNAPL 2015)*, pages 140–155, May 2015.

[4] E. G. Sirer. Thoughts on The DAO hack, June 2016. Accessed August 24, 2016. Available at: http://hackingdistributed.com/2016/06/17/thoughts-on-the-dao-hack/.