Program Analysis and Verification on Trusted Platforms (PAVeTrust) Workshop

This workshop will be held online Monday, December 6, 2021, in conjunction with the Annual Computer Security Applications Conference (ACSAC).

Statement on COVID-19. This workshop and ACSAC is being held *virtually* this year. More information is available at the conference site, https://www.acsac.org/

Further details about the workshop can be found at the workshop website: https://www.acsac.org/2021/workshops/pavetrust/

Call for Papers

Trusted Execution Environments (TEEs) are now commonplace with implementations like Intel SGX and AMD SEV widely available. This technology offers new guarantees, such as integrity and confidentiality for running programs, that are not typically available in (untrusted) conventional platforms. They are being rapidly adopted by security-focused companies intending to harden the systems they deliver and to offer properties such confidentiality for data in use which is difficult to achieve in practice without this technology.

This workshop intends to explore the interplay between TEE-based implementations of a Trusted Third Party (TTP) and program analysis and system verification. It should provide a venue where academics and practitioners interested in these topics come together to debate the connection between these two areas. We are especially interested in promoting:

> (A) the application of formal methods, and more specifically of program analysis and system verification, to the specification and/or analysis of the trusted stack executing these TEE-hardened applications - this stack might include CPU microcode, firmware code, Operating System (OS) code, protocols for provisioning and attestation, and the application itself - and
>
> (B) innovative applications of TEEs to execute formal methods technologies (such as program analysers/verifiers).

While the frameworks proposed in the context of (A) should help the adoption of TEE-based technologies by increasing the community's confidence on the security of TEE-based systems, the applications arising in the context of (B) should introduce analysis frameworks that enjoy non-conventional properties such as confidentiality of the analysed systems and trustworthiness of the analysis outcome. It should be possible to deliver object code to users who know that the corresponding sources have passed agreed verification procedures, without the users seeing the sources or having to have trust in other parties.

Paper format

We invite the submission of short papers presenting original work on topics (A) and (B) above. The accepted papers will have to be presented by one of the authors at the workshop. Papers should be submitted as a PDF file of a maximum of 8 2-column pages, excluding well-marked references and appendices limited to 3 pages. Submissions must be

generated using the 2-column ACM acmart template available at https://www.acm.org/publications/proceedings-template, using the [sigconf, anonymous] options. All submissions must be anonymous (i.e., papers should not contain author names or affiliations, or obvious citations). **Papers must be submitted to: submissions@tbtl.com and clearly mention the desired *category* as per below.**

Publication

Submissions must explicitly mention their category - either *formal* or *informal*. Submissions will go through the same peer-reviewing process regardless of their category. However, while papers submitted to the formal track will be formally published - we will publish them as workshop proceedings with the ACM - the informal submissions will be only made available in the workshop's repository. The informal category is intended to give authors the ability to resubmit their work to another venue if they wish to do so.

Any queries about the workshop should be addressed to workshop@tbtl.com.

Important dates

Paper submission deadline: ~~30 September 2021~~ 14 October 2021

Notification and feedback: 21 October 2021

Camera-ready deadline: 15 November 2021

Workshop date: 6 December, 2021

Organisation Committee

Huafeng Zhang (TBTL Oxford, UK)

Liu Han (TBTL Oxford, UK)

Pedro Antonino (TBTL Oxford, UK)

PC Chair

Bill Roscoe (University of Oxford and TBTL Oxford, UK)

Program committee

Aditya Oak (TU Darmstadt, Germany)

Ante Derek (University of Zagreb, Croatia)

Guido Salvaneschi (University of St.Gallen, Switzerland)

Ivan Martinovic (University of Oxford, UK)

Jo Van Bulck (KU Leuven, Belgium)

Liu Han (TBTL Oxford, UK)

Marcus Völp (University of Luxembourg, Luxembourg)

Muhammad Usama Sardar (TU Dresden, Germany)

Pedro Antonino (TBTL Oxford, UK)

Peter Ryan (University of Luxembourg, Luxembourg)

Shweta Shinde (ETH Zurich, Switzerland)

Srdjan Capkun (ETH Zurich, Switzerland)

Toby Murray (University of Melbourne, Australia)

Zhiqiang Lin (The Ohio State University, USA)

Workshop registration

If you are interested in attending the workshop, please check off the appropriate box on the conference registration form and add in the Program Analysis and Verification on Trusted Platforms (PAVeTrust) Workshop fee.

Sponsored by

The Blockhouse Technology Ltd

www.tbtl.com