2nd Program Analysis and Verification on Trusted Platforms (PAVeTrust) Workshop

This workshop will be held in-person Tuesday, December 6, 2022, in conjunction with the Annual Computer Security Applications Conference (ACSAC), in Austin, Texas, USA.

Further information about the workshop can be found at the workshop website: https://www.acsac.org/2022/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 applications, that are not typically available in (untrusted) conventional platforms. Therefore, TEEs are being rapidly adopted by security-focused companies intending to harden their systems to provide such guarantees.

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 via Easychair.

Publication

Submissions will go through a peer-reviewing process aimed at selecting the papers to be presented at the workshop, but also at providing detailed constructive feedback to authors. The accepted papers will be made available in the workshop's online repository — no formal workshop proceedings will be published — and a selection of those will be invited to submit to the Cybersecurity Springer journal: https://cybersecurity.springeropen.com/. We welcome concurrent submissions provided that they are clearly marked as such - please, check whether the other venue also accepts such kinds of submission. Concurrent submissions will not be invited for Cybersecurity Springer journal, unless they are no longer concurrent by the time the invitations are being made.

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

Important dates

Paper submission deadline: 14 October 2022

Notification and feedback: 20 November 2022

Camera-ready deadline: 29 November 2022

Workshop date: 6 December 2022

Organisation Committee

Huafeng Zhang (TBTL Oxford, UK)

Muhammad Usama Sardar (TU Dresden, Germany)

Pedro Antonino (TBTL Oxford, UK)

PC Chair

TBD

Program committee

Ante Derek (University of Zagreb, Croatia)

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

Guido Salvaneschi (University of St.Gallen, Switzerland)

Ivan Martinovic (University of Oxford, UK)

Jo Van Bulck (KU Leuven, Belgium)

Huafeng Zhang (TBTL Oxford, UK)

Han Liu (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)

Srdjan Capkun (ETH Zurich, Switzerland)

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