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/

Workshop Program

8:30-9:00 Opening remarks by Bill Roscoe (University of Oxford & The Blockhouse Technology Limited, UK)

9:00-10:00 Invited talk 1: "Committable: OSS monetisation via trusted software analysis" by Liu Han (The Blockhouse Technology Limited, UK — Remote presentation)

Abstract: "Committable is a decentralised protocol aimed at establishing a sustainable open-source ecosystem. The core design of the protocol is to allow developers to permissionlessly monetise an open-source software with a sequence of commits they contributed. The monetisation is algorithmic and realised through trusted software analysis which runs software analysis algorithms in trusted environments (e.g., TEE) and generates verifiable proofs for the development contribution made by specific developers. This talk will introduce the Committable protocol in general with a specific focus on the software monetisation process enabled by trusted software analysis and further highlight the potential of Committable to achieve sustainability for the open-source ecosystem."

10:00-10:30 Break

10:30-11:00 Paper 1: “Towards SoK: Attestation in Confidential Computing” by Muhammad Usama Sardar (TU Dresden, Germany)

Abstract: “Attestation is arguably the most critical and most misunderstood mechanism in confidential computing. In this short paper, we present a structured approach for precise specification of attestation mechanism in confidential computing. We demonstrate the approach by presenting a detailed mapping of attestation architecture to an industrial TEE, namely Intel TDX. In the process, we highlight a number of shortcomings and ambiguities in IETF RATS architecture. We also highlight some of the missing specifications from Intel.”

11:00-12:00 Invited talk 2: "Towards Distributed and Virtualized Trusted Execution Environments" by Zhiqiang Lin (The Ohio State University, US)

Abstract: "Today, we are in the era of data economy, where a large volume of privacy sensitive data is collected and processed by various edges and clouds. However, these data-centric, edge-cloud innovations are under persistent threats of security breaches as well as growing regulatory pressure. While cryptographic solutions (e.g., homomorphic encryption) are promising, they are still far away from wide deployment, due to their performance predicaments. Recently, the progress in trusted execution environments (TEEs) such as Intel SGX and AMD SEV offers a new hope. However, current TEEs and their applications are tightly bound to the hardware implementation, hindering their

evolutions and compatibility. In this talk, I will present a vision towards distributed and virtualized TEEs, where data can be collected and processed in a distributed and faster evolvable TEEs across the edge and cloud. In particular, I will talk about a step we recently made with vSGX, which virtualizes the execution of an Intel SGX enclave on top of AMD SEV, with the goal of decoupling TEEs from the hardware and enabling faster evolutions. Next, I will talk about how to use distributed TEEs for important data protection applications such as those in connected and autonomous vehicles. Finally, I will talk about how verification can help to provide the confidence for the virtual and distributed TEEs."

12:00-13:30 Lunch

13:30-14:30 Invited talk 3: "Making Transparency Normal" by Razieh Behjati (Google, UK — Remote presentation)

Abstract: "Transparency is crucial for building trust in security-critical systems as it provides a mechanism for achieving accountability. Certificate transparency has famously introduced the idea of using a public, verifiable, and append-only log to detect compromised or fraudulent certificate issuance. Binary transparency uses the same idea to improve discoverability and verifiability of the legitimacy of software binaries.

With a focus on the security of open-source software, we extend binary transparency and integrate it with software supply chain security frameworks to verify not only the legitimacy of a binary, but also its origin, and eventually claims about its security and privacy properties.

In this presentation, I will talk about some of our recent ideas for using transparency. I will discuss the main challenges in the way ahead, and will explain how transparency contributes to verifiability and trust."

14:30-15:00 Paper 2: “Flexible remote attestation of pre-SNP SEV VMs using SGX enclaves” by Pedro Antonino (The Blockhouse Technology Limited, UK); work co-authored by Ante Derek (Faculty of Electrical Engineering and Computing, University of Zagreb) and Wojciech Woloszyn (The Blockhouse Technology Limited, UK)

Abstract: “We propose a protocol that explores a synergy between two TEE implementations: it brings SGX-like remote attestation to SEV VMs. We use the notion of a *trusted guest owner*, implemented as an SGX enclave, to deploy, attest, and provision a SEV VM. This machine can, in turn, rely on the trusted owner to generate SGX-like attestation proofs on its behalf. Our protocol combines the application portability of SEV with the flexible remote attestation of SGX. We formalise our protocol and prove that it achieves the intended guarantees using the Tamarin prover. Moreover, we develop an implementation for our trusted guest owner together with an example SEV machine, and put those together to demonstrate how our protocol can be used in practice. We also discuss how our protocol can be extended to provide a simple remote attestation mechanism for a heterogeneous infrastructure of trusted components.”

15:00-15:30 Break

15:30-16:30 Invited talk 4: "Verification of Realm Management Monitor (RMM)" by Shale Xiong (Arm, UK)

Abstract: "We present Arm's efforts in verifying the specification and prototype reference implementation of an essential firmware component of Arm Confidential Computing Architecture (Arm CCA), the recently-announced Confidential Computing technologies incorporated in the Armv9-A architecture. Arm CCA introduced the Realm Management Extension (RME), an architectural extension for Armv9-A architecture, and a technology that will eventually be deployed in hundreds of millions of devices. Given the security-critical nature of Arm CCA and its taxing threat model, we use a combination of interactive theorem proving, model checking, and concurrency-aware testing to validate and verify security and safety properties of both the specification and a prototype implementation of the firmware component of Arm CCA, namely Realm Management Monitor (RMM) [1]. Crucially, our verification efforts were---and are currently being---developed contemporaneously with active development of both specification and implementation and have been adopted by
Arm's product teams.
We describe our major achievements, (a) a HOL4 model of the RMM specification, (b) an auto-generated model checking harness for the RMM prototype and (c) a system-level testing and debugging tool with the focus on concurrency control. We believe that the work is the most thorough application of formal techniques to the design and implementation of any current commercially-viable Confidential Computing implementation, setting a new high-water mark for work in this area.

[1] https://developer.arm.com/documentation/den0137/latest"

16:30-17:00 Wrap-up discussion and concluding remarks by Bill Roscoe (University of Oxford & The Blockhouse Technology Limited, UK)

Sponsored by

The Blockhouse Technology Ltd

www.tbtl.com