November 25, 2024

HACS 2025 Overview

Gilles Barthe, Karthik Bhargavan, Sofía Celi, Deirdre Conolly,
Allen Gunn, Diane Hosfelt, Ben Laurie, Trevor Perrin, Peter Schwabe, Cathie Yun

Introduction

Since 2016, the workshop on High Assurance Cryptographic Software has been bringing together cryptographic developers, cryptographers, and formal verification experts to improve the quality of cryptographic software. HACS has helped forge connections between these communities, leading to many new research projects, collaborations, and tool deployments (see https://hacs-workshop.org).

To foster small-group dynamics and community feeling, HACS is a small workshop: we're aiming for <100 attendees. The organizers select new focus topics each year and adjust the attendee mix to match, trying to strike a balance between new attendees and continuity with ongoing projects.

HACS 2025 will have the following focus topics:

- **Zero-Knowledge Proofs**. We'll focus on correct and secure implementation of ZK circuits, compilers, and libraries; as well as security proofs for complex ZK systems. We will leverage the co-located ZKproof workshop to introduce more of the ZK community into HACS.

- **Proof Assistants** (Coq, EasyCrypt, F*, Isabelle, Lean, etc.). These are a dynamic and promising class of formal methods tools. We'll focus on proof assistants for program verification, as well as creating and checking security proofs.

- **Usability of formal tools by practitioners** (cryptographers, developers, protocol designers, etc.). We will approach this goal via a near-term focus on identifying simple, self-contained **challenge problems** that can be arranged into illustrative pedagogical flows. From there, we'll try to spur the development of **tutorials** showing how to tackle these problems with different tools. Our intention is for tutorials to help educate practitioners in formal methods and cryptography, and provide a basis for tool comparison.

Of course, HACS will continue to focus on its core theme of correctness and security of crypto code, including formal generation and verification of code; as well as informal techniques. We'll also cover other areas of cryptography (including PQC migration and signatures, anonymous credentials, MPC, FHE, PIR, threshold crypto, protocol design, web PKI, etc.) wherever we think our format and attendee mix can provide value.

The Plan for HACS 2025

HACS 2025 will be a three-day physical event in Sofia, Bulgaria, with the main workshop days on March 23 and 24, and an optional hack day on March 25. This will be the Sunday through Tuesday prior to the Real World Crypto 2025 conference, which is scheduled for March 26-28 in Sofia. The event will be co-organized and facilitated by Allen Gunn of Aspiration.

As always, HACS will be a highly interactive event, where crypto implementers, researchers, and experts in high-assurance and formal methods have lots of time to meet, learn from each other, and launch collaborations.

To that end, we will avoid lectures delivered to the entire group. Instead, we hope to spend most time in small-group "working sessions", focused on interactive discussion and collaboration. Some of these working sessions will be planned in advance, but others will emerge based on attendee interest, during the event.

The organizers will spend significant time before the event discussing goals with attendees and arranging workshop sessions to advance concrete objectives.